# Washington DC Security Management

**Zuletzt aktualisiert: 17.12.2025**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Inhaltsverzeichnis


**Security Operations** ..... **6**

Security Operations verstehen ..... 12

Die Anwendungssuite Security Operations ..... 14

Security Operations Szenarien und Beispiele ..... 21
[store-future: BEGIN review]

Reduzieren Sie die Zeit für Bedrohungsanalysen mithilfe von Automatisierung ..... 22
[store-future: BEGIN review]
[End]

Priorisieren Sie wichtige Schwachstellen ..... 28
[store-future: BEGIN review]
[End]

[End]

Security Operations und ServiceNow Store ..... 31

Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store herunter ..... 31

Installieren Sie eine Security Operations -Integration ..... 37

Aktualisieren Sie eine Anwendung, die zuvor aus dem heruntergeladen wurde ServiceNow Store ..... 41

Aktualisieren Sie Ihre Instanz auf den nächsten Familien-Release ..... 42

Cybersicherheits-Dashboard für Führungskräfte ..... 42

Wählen Sie Benchmark-Punktzahlen aus ..... 57

Legen Sie Ziele fest ..... 58

Security Simulation and Training Integration for Security Operations ..... 59

Security Incident Response ..... 61

Security Incident Response verstehen ..... 62

Setup von Security Incident Response ..... 71

Arbeitsbereich für Security Incident Response ..... 155

Security Incident-Erstellung ..... 267

Verwalten Sie Predictive Intelligence für von Benutzern gemeldetes Phishing ..... 308

Konfigurieren Sie Predictive Intelligence für von Benutzern gemeldetes Phishing ..... 313

Zuweisen von Sicherheitsanalysten ..... 315

Verwaltung von Security Incidents und eingehenden Anforderungen ..... 320

Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace ..... 388

Playbook-Ressourcen ..... 416

Security Incident Response-Berichterstellung ..... 549

Management schwerwiegender Sicherheits-Incidents ..... 559

Security Incident Response-Integrationen ..... 692

Mobile Experience für Security Incident Response ..... 1389

Security Incident Response Orchestration ..... 1427

Flow-Vorlagen für Security Incident Response ..... 1463
[store-future: BEGIN review]
[End]

Sicherheitsstatus-Überwachung ..... 1481


Automatische Übersetzung


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsstatus-Überwachung erkunden ... 1482
Vulnerability Response ... 1533
Die Anwendung Vulnerability Response erkunden ... 1534
Vulnerability Response – Implementierung ... 1608
Vulnerability Response-Integrationen ... 1761
Vulnerability Response Arbeitsbereiche ... 2035
Vulnerability Response Übersicht über die -Korrektur ... 2173
Analytics- und Reporting-Lösungen für Vulnerability Response ... 2283
Vulnerability Response Referenzinformationen ... 2332
Mobile Experience für Vulnerability Response ... 2376
Orchestration für Vulnerability Response ... 2398
Application Vulnerability Response ... 2404
Application Vulnerability Response erkunden ... 2406
Application Vulnerability Response konfigurieren ... 2410
Integration von Application Vulnerability Response mit anderen Anwendungen ... 2446
Application Vulnerability Response Schwachstellen werden korrigiert ... 2488
Platform Analytics-Lösungen für Application Vulnerability Response ... 2534
Application Vulnerability Response Referenzen ... 2547
Application Vulnerability Response -Produktansicht ... 2572
Container Vulnerability Response ... 2574
Container Vulnerability Response erkunden ... 2584
Container Vulnerability Response konfigurieren ... 2586
Integration von Container Vulnerability Response mit anderen Anwendungen ... 2593
Container-Schwachstellen werden korrigiert ... 2599
Analytics and Reporting-Lösungen für Container Vulnerability Response ... 2620
Container Vulnerability Response – Referenz ... 2629
Configuration Compliance ... 2637
Configuration Compliance erkunden ... 2639
Anwendung Configuration Compliance einrichten, installieren und konfigurieren ... 2668
Configuration Compliance-Integrationen ... 2722
Configuration Compliance Fehlerkorrektur ... 2818
Berichterstellung und Analytics für Configuration Compliance ... 2851
Configuration Compliance Referenzinformationen ... 2864
Vulnerability Response – Allgemein ... 2893
Framework für zusammengefasste Berichte ... 2893
Threat Intelligence ... 2900
Threat Intelligence verstehen ... 2901
Threat Intelligence einrichten ... 2906
IoC-Repository ... 2922
MITRE-ATT&CK™ -Framework – Übersicht ... 2967
Threat Intelligence – Administration ... 3036
Threat Intelligence-Integrationen ... 3038



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Orchestration für Threat Intelligence ... 3107
Security Case Management ... 3112
Security Operations allgemeine Funktionalität ... 3143
Erstellen und definieren Sie Filtergruppen in Security Operations ... 3146
Transformation freigegebener Daten ... 3148
Security Operations E-Mail-Verarbeitung ... 3151
Security Operations Feldzuordnung ... 3162
Security Operations Feldwerttransformationen ... 3167
Security Operations -Ergänzungsdatenzuordnung ... 3168
Security Operations benutzerdefinierte Eskalation ... 3171
Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen ... 3172
Erstellen Sie eine Betriebssystemgruppe ... 3174
Sicherheits-Tag-Gruppen und -Tags einrichten ... 3175
Sicherheitsanmerkungen ... 3179
Mit Security Support Common installierte Komponenten ... 3182
Modulzugriff nach Rolle für Security Operations-Anwendungen ... 3183
[store-future: BEGIN review]
[End]
Suche Security Operations ... 3875
Referenzen zur Integration mit Security Operations ... 3875
Security Operations Workflow-Auslöser ... 4016
Orchestration für Security Operations ... 4018
Data Loss Prevention Incident Response ... 4031
Data Loss Prevention Incident Response erkunden ... 4032
DLP IR Incident Response installieren und konfigurieren ... 4034
DLP-Administration für Incident Response ... 4036
Data Loss Prevention Incident Response Incident-Management ... 4090
Eingehende Integration für Data Loss Prevention Incident Response ... 4108
DLP-Integrationen ... 4111
Software-Stückliste ... 4153
Software Bill of Materials erkunden ... 4154

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Security Operations

ServiceNow® Security Operations bringt Incident-Daten aus Ihren Sicherheitstools in eine strukturierte Antwort-Engine, die intelligente Workflows, Automatisierung und eine enge Verbindung zur IT verwendet, um Bedrohungen basierend auf den Auswirkungen, die sie auf Ihr Unternehmen darstellen, zu priorisieren und zu beheben.

## Automatisieren Sie alle Ihre Sicherheitstools und arbeiten Sie nahtlos mit der IT zusammen

Mit Security Operationskönnen Sie den Wert Ihrer Now Platform® -Lösung voll ausschöpfen. Viele Unternehmen haben Probleme damit, Sicherheitsbedrohungen und -schwachstellen zu erkennen, sie zu priorisieren und sich mit der IT abzustimmen, um sie zu beheben. Mit Security Operationskönnen Sicherheitsanalysten und Schwachstellenmanager ihre Sicherheitstools nahtlos automatisieren und mit der IT kommunizieren, indem sie in einer einheitlichen Plattform arbeiten.

Hier können Sie die vollständige Infokarte mit den wichtigsten Funktionen von Security Operations anzeigen und herunterladen.

| | |
|---|---|
| | **Identifizieren, priorisieren und beheben Sie Schwachstellen in Software, Betriebssystemen und Assets**<br><br>Die Anwendung ServiceNow® Vulnerability Response hilft Unternehmen, Schwachstellen schnell und effizient zu erkennen und darauf zu reagieren. Scannen Sie Daten von führenden Anbietern, um Ihren Teams eine einzige Plattform für die Reaktion zu bieten, die von Sicherheit und IT gemeinsam genutzt werden kann, um Schwachstellen zu beheben. |
| | **Identifizieren, priorisieren und beheben Sie kritische Security Incidents**<br><br>Die Anwendung ServiceNow® Security Incident Response vereinfacht den Prozess der Identifizierung kritischer Incidents durch Anwendung leistungsstarker Workflow- und Automatisierungstools, die die Behebung beschleunigen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Identifizieren, priorisieren und korrigieren Sie falsch konfigurierte Assets**

Die Anwendung ServiceNow® Configuration Compliance priorisiert und korrigiert falsch konfigurierte Assets anhand von Daten, die aus Sicherheitskonfigurationsbewertungs-Scans von Drittanbietern gesammelt wurden.

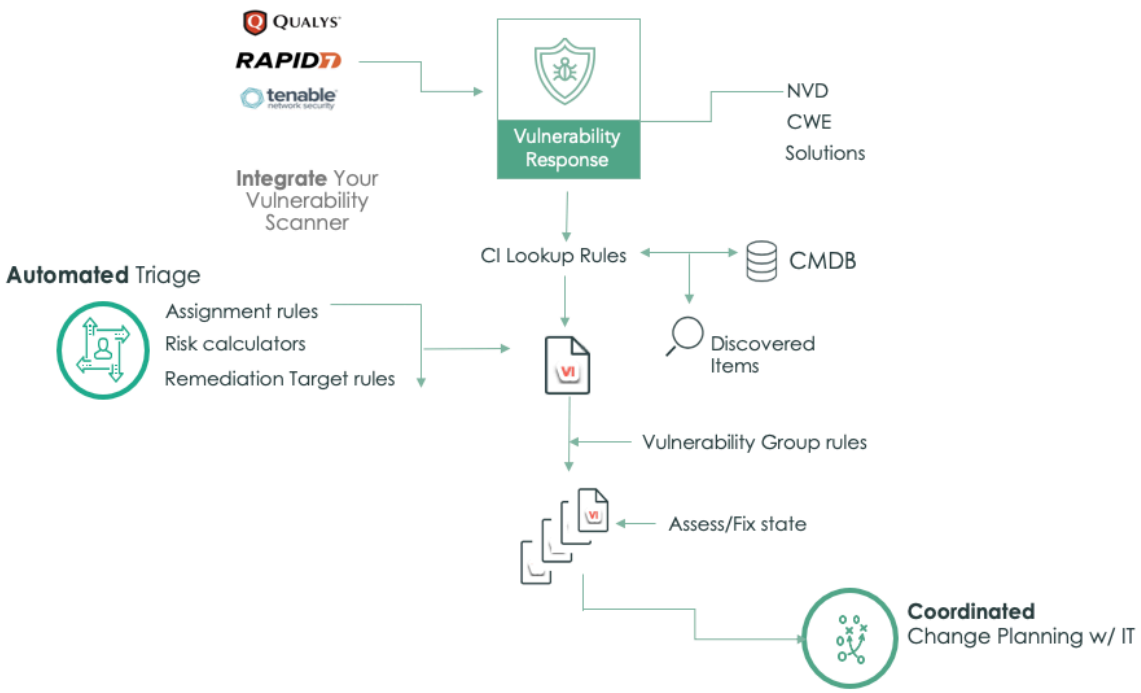
**Greifen Sie auf die STIX-Daten Ihres Unternehmens zu**

Die Anwendung ServiceNow® Threat Intelligence hilft Incident-Beantwortern, Kompromittierungsindikatoren (Indicators of Compromise, IoC) zu finden und nach tief liegenden Angriffen und Bedrohungen zu suchen. Die Ergebnisse werden direkt an Security Incidents gemeldet.

**Greifen Sie mit Ihrem Mobilgerät auf Security Operations zu**

Greifen Sie mit Ihrem Android- oder iOS-Mobilgerät auf die Anwendungen Vulnerability Response und Security Incident Response in Ihrer Instanz von Now Platform zu. Als Korrekturverantwortlicher oder Sicherheitsanalyst verwalten Sie Security Incidents und Schwachstellengruppen, damit Sie mit der Korrektur beginnen können, ohne an Ihren Desktop gebunden zu sein.

## Identifizieren, priorisieren und beheben Sie Schwachstellen in Software, Betriebssystemen und Assets




Die Anwendung Vulnerability Response importiert und gruppiert angreifbare Elemente automatisch gemäß Gruppenregeln, sodass Sie Schwachstellen schnell beheben können. Schwachstellendaten werden aus internen und externen Quellen abgerufen, z. B. aus der National Vulnerability Database (NVD) oder aus Integrationen von Drittanbietern. Vergleichen Sie Schwachstellendaten aus internen und externen Quellen. Erstellen Sie für alle angreifbaren Elemente Change-Anforderungen und Security Incidents mithilfe von Schwachstellengruppen, um Probleme zu beheben und Risiken zu minimieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

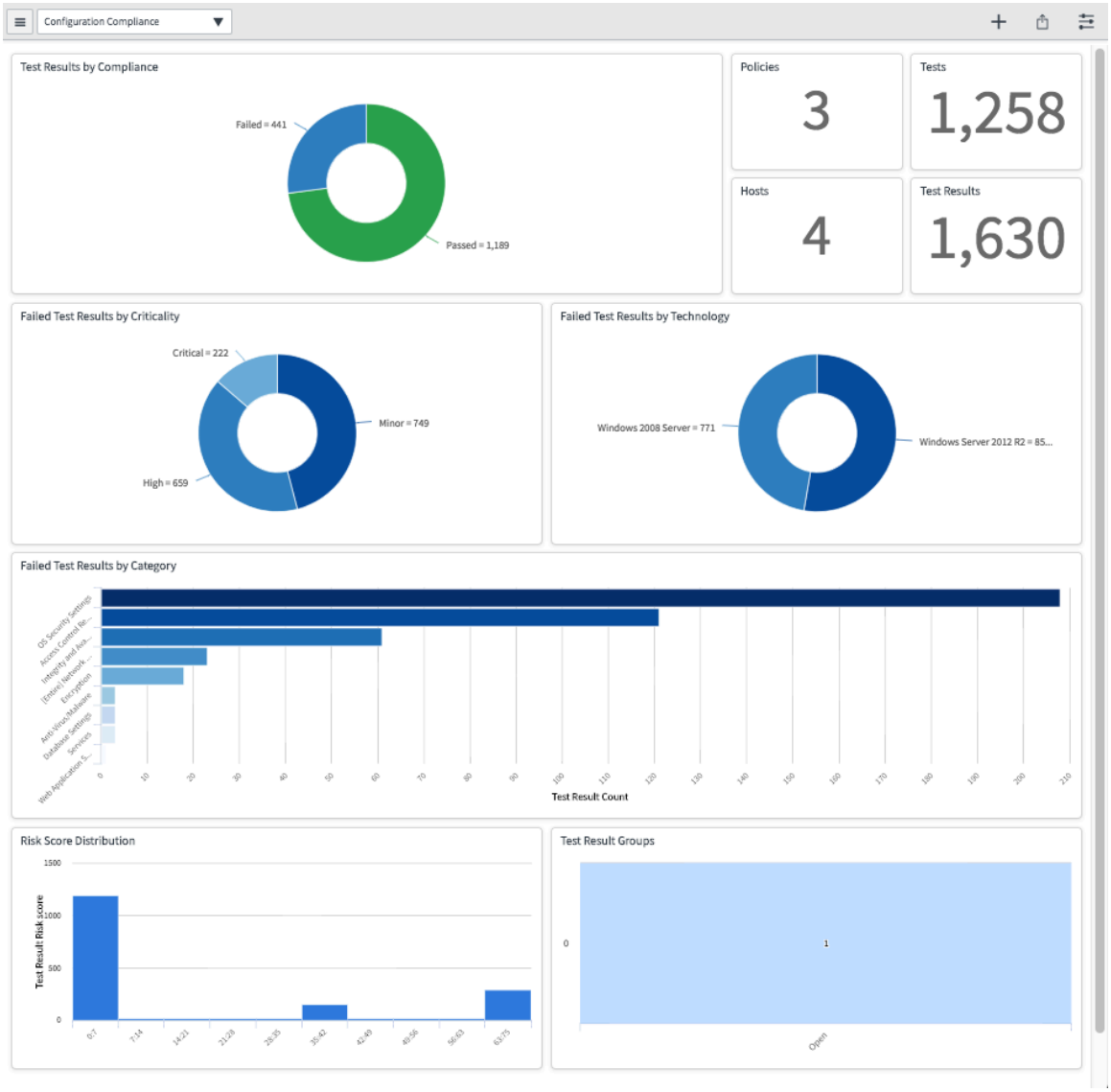
## Identifizieren, priorisieren und beheben Sie kritische Security Incidents

Mit der Anwendung Security Incident Response (SIR) integrieren Sie Ihre vorhandenen SIEM-Tools (Security Information and Event Manager) in die Anwendungen von Security Operations, um Bedrohungsdaten (über APIs oder E-Mail-Warnungen) zu importieren und automatisch priorisierte Security Incidents zu erstellen. Verwalten Sie den Lebenszyklus Ihrer Security Incidents von der ersten Analyse bis hin zu Eindämmung, Beseitigung und Wiederherstellung. Mit der Anwendung Security Incident Response erhalten Sie ein umfassendes Verständnis der von Ihren Analysten durchgeführten Incident-Reaktionsverfahren und verstehen Trends und Engpässe in diesen Verfahren mit analysebasierten Dashboards und Berichten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Identifizieren, priorisieren und korrigieren Sie falsch konfigurierte Assets

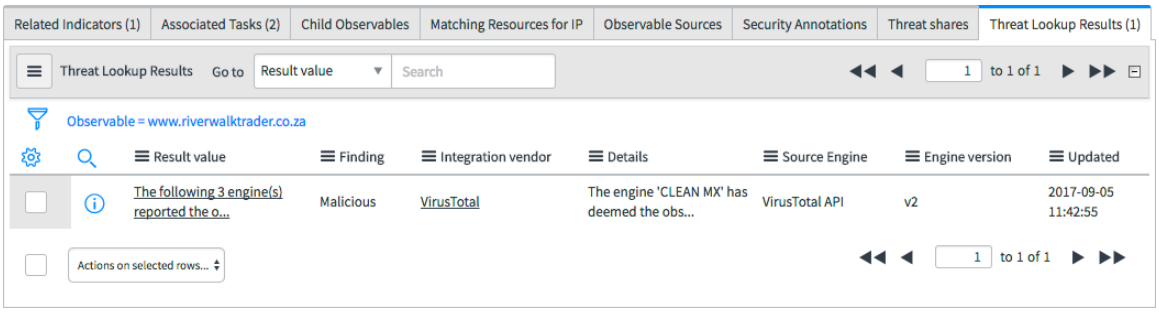



Verwenden Sie mit der Anwendung Configuration Compliance Testergebnisse aus SCA-Integrationen (Security Configuration Assessment) von Drittanbietern, um die Compliance mit Sicherheits- oder Unternehmensrichtlinien zu überprüfen. Diese Anwendung verwendet die im ServiceNow® Configuration Management Database (CMDB) aufgeführten Assets, um zu bestimmen, welche Elemente am kritischsten sind. Workflows und Automatisierung ermöglichen schnelle Aktionen für einzelne Assets oder Gruppen für Massenänderungen. Identifizieren und korrigieren Sie nicht konforme Konfigurationselemente. Importieren Sie automatisch Richtlinien, Tests, autoritative Quellen und Technologien, und weisen Sie Gruppen oder Einzelpersonen Testergebnisse zur Korrektur zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Greifen Sie auf die STIX-Daten Ihres Unternehmens zu

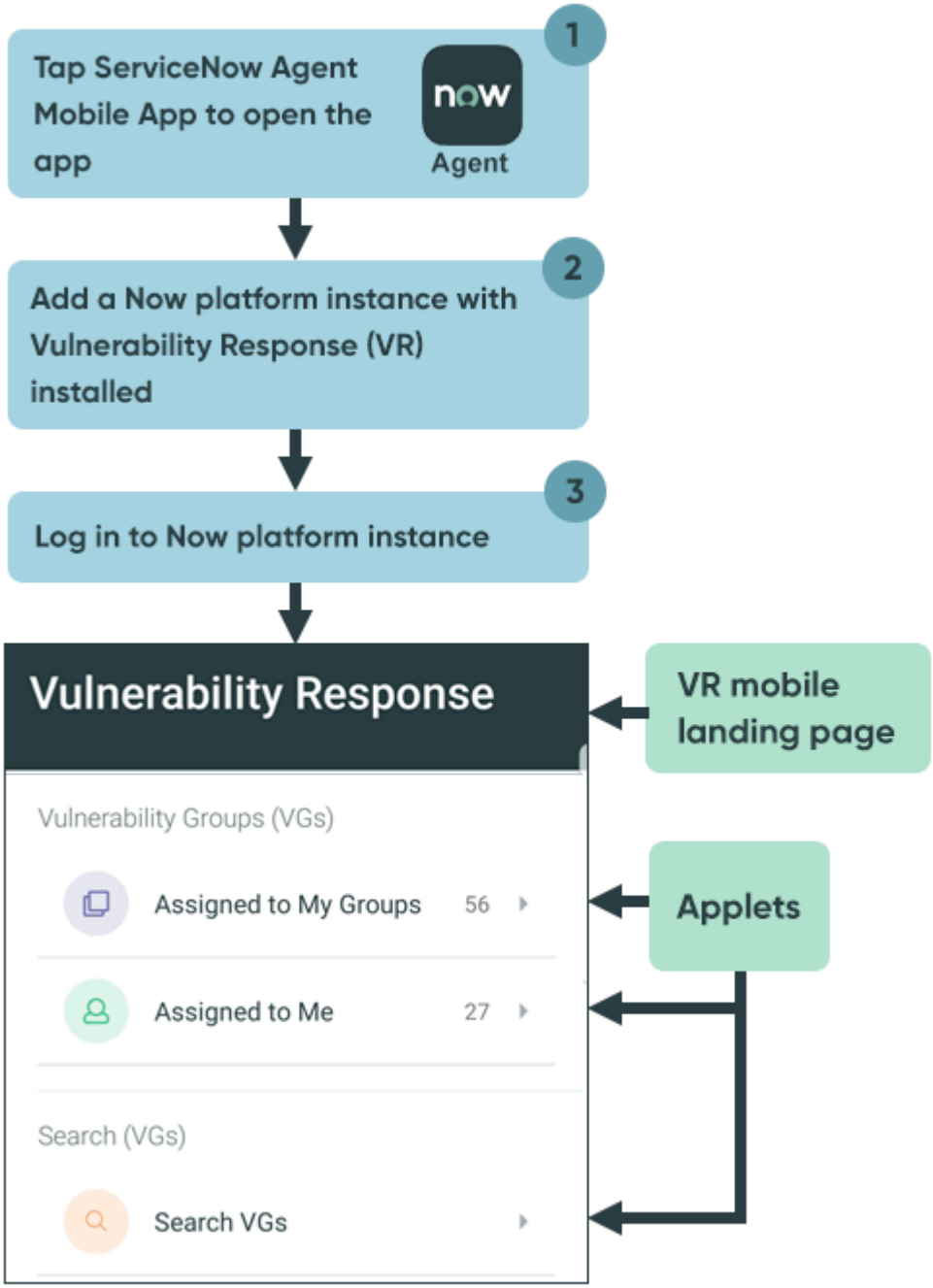



Verwenden Sie die Anwendung Threat Intelligence, um Bedrohungsfeeds automatisch nach relevanten Informationen zu durchsuchen, wenn ein IoC mit einem Security Incident verbunden ist und IoCs zur zusätzlichen Analyse an Drittanbieterquellen senden kann. Die Anwendung Threat Intelligence verwendet STIX (Strukturierter Bedrohungsinformationsausdruck) als Sprache, um Cyberbedrohungsinformationen auf standardisierte und strukturierte Weise zu beschreiben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Mobile Experience für Security Operations






Greifen Sie mit Ihrem Android- oder iOS-Mobilgerät auf die Anwendungen Vulnerability Response und Security Incident Response in Ihrer Instanz von Now Platform zu.

### Erste Schritte

- Eine Übersicht über Security Operations in Ihrer Instanz Now Platform finden Sie unter Sicherheitsvorgänge verstehen.
- Informationen zu allen Security Operations -Anwendungen, die im ServiceNow Store] zum Download verfügbar sind, finden Sie unter Sicherheitsvorgänge und im ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Mehr erfahren

- Was ist KI für Sicherheit?
- Was ist Patch-Management?
- Was ist SOAR?
- Was ist der CAIQ?
- Was ist das Mitre Att&ck Framework?
- Was ist Schwachstellenmanagement?
- Was ist Cloud-Sicherheit?
- Was ist DevSecOps?
- Was sind Sicherheitsvorgänge (SecOps)?
- Was ist ein Security Operations Center (SOC)?

### Anwendungen und Funktionen

- Vulnerability Response
- Security Incident Response
- Sicherheitsstatus-Überwachung
- Major Security Incident Management
- Configuration Compliance
- Threat Intelligence
- Data Loss Prevention
- Operational Technology Vulnerability Response
- Software-Stückliste

## Security Operations verstehen

Security Operations bringt Incident-Daten aus Ihren Sicherheitstools in eine strukturierte Antwort-Engine, die intelligente Workflows, Automatisierung und eine enge Verbindung zur IT verwendet, um Bedrohungen basierend auf den Auswirkungen, die sie auf Ihr Unternehmen darstellen, zu priorisieren und zu beheben.

### Security Operations in Kürze

Das Security Operations -Ökosystem kann je nach den Anforderungen Ihres Unternehmens und den von Ihnen lizenzierten Security Operations -Produkten auf verschiedene Arten konfiguriert werden. Das folgende Diagramm zeigt den Flow eines Basis Security Operations - -Systems.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Der erste Schritt besteht darin, die ServiceNow Discovery -Anwendung zu verwenden, um Anwendungen und Geräte in Ihrem Netzwerk zu finden, und dann die ServiceNow Configuration Management Database (CMDB) zu aktualisieren.
2. Integrieren Sie Ihre vorhandenen SIEM-Tools (Security Information and Event Manager) mit den Anwendungen Security Operations, um Bedrohungsdaten (über APIs oder E-Mail-Warnungen) zu importieren und automatisch priorisierte Security Incidents zu erstellen.
3. Verwenden Sie Workflows und die Anwendung Vulnerability Response, um Events, Security Incidents und Schwachstellen sofort zu priorisieren.
4. Ergänzen Sie Daten mit der Anwendung Threat Intelligence sowie anderen Funktionen für maschinelles Lernen oder künstliche Intelligenz.
5. Verwenden Sie Risikomanagement und andere Governance, Risk und Compliance -Anwendungen, um Unternehmens- und IT-Risiken, die sich negativ auf den Geschäftsbetrieb auswirken können, zu identifizieren, zu bewerten, darauf zu reagieren und sie kontinuierlich zu überwachen.
6. Workflows, die in alle Security Operations -Anwendungen integriert sind, reduzieren die Fehlersuche und den Arbeitsaufwand bei der Fehlerkorrektur.
7. Zeigen Sie mithilfe von Dashboards sofort detaillierte Informationen zu Ihrer Sicherheitslage an.

## Sicherheit mit IT verbinden

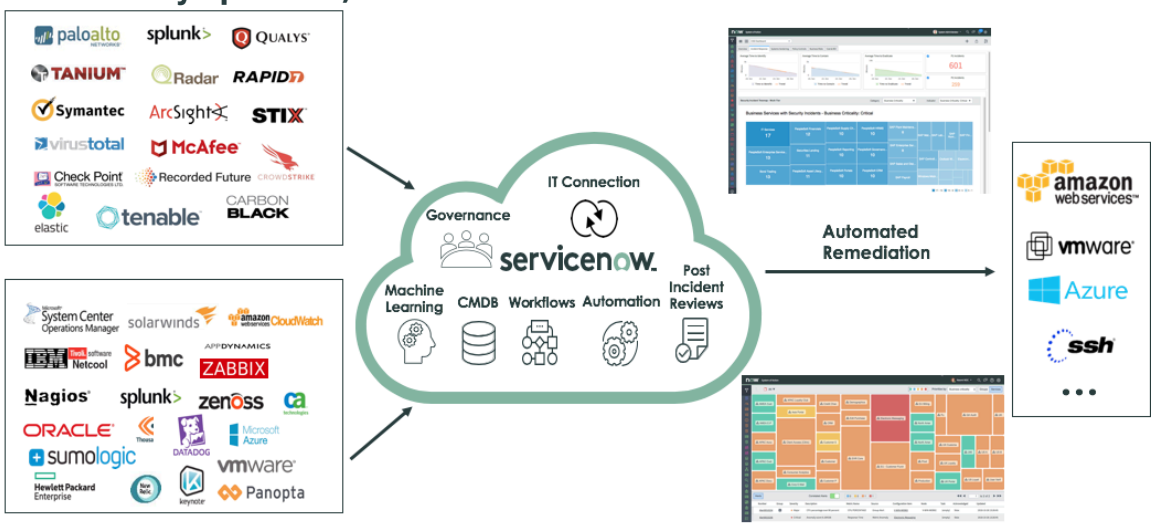
Mit Security Operationskönnen Sicherheitsanalysten und Schwachstellenmanager nahtlos mit der IT kommunizieren, indem sie in einer einheitlichen Plattform arbeiten. Sie können Patches und andere Aufgaben an die IT übergeben und gleichzeitig die Transparenz der Aufgaben beibehalten. Durch die kompetenzbasierte Weiterleitung werden Aufgaben den richtigen Beantwortern zugewiesen, und Servicelevel-Vereinbarungen stellen sicher, dass die Arbeit rechtzeitig ausgeführt wird.

Now Platform erleichtert die schnellere Zusammenarbeit zwischen Sicherheits- und IT-Personal. Vertrauliche Sicherheitsdaten werden jedoch weiterhin durch Benutzerrollen geschützt. Dies bedeutet, dass der Zugriff auf Sicherheitsdaten für Benutzer mit der Administratorrolle eingeschränkt werden kann, es sei denn, sie haben auch eine Sicherheitsrolle.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

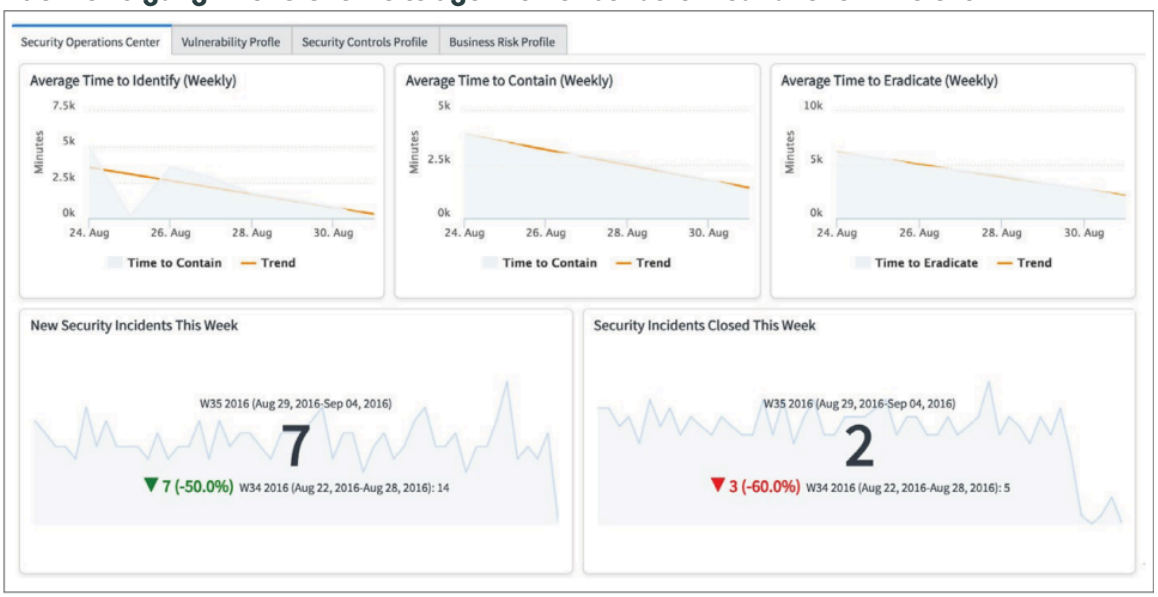
### IT and Security Operations, die auf der Now Platform arbeiten




## Visuelle Nachverfolgung Ihrer Sicherheit

Security Operations bietet rollenbasierte Dashboards und Berichte, die Sie anpassen können, um den Status Ihrer Sicherheit anzuzeigen. Alle Security Incidents und Schwachstellen mit angereichertem Kontext zeigen visuell, wie Ihre kritischen Business Services von Bedrohungen betroffen sind. Mit dem Produkt ServiceNow Performance Analytics erweiterte Dashboards zeigen den Status Ihrer Sicherheitsleistung im Laufe der Zeit an, sodass Sie nachverfolgen können, wie sich Ihre Sicherheitslage verbessert.

### Nachverfolgung Ihrer Sicherheitslage in einer benutzerfreundlichen Ansicht




## Die Anwendungssuite Security Operations .

Mit der Leistungsfähigkeit von Now PlatformSecurity Operations können Sie mit den Anwendungen von [] Ihre Sicherheitslösung an die Anforderungen Ihres Unternehmens und die Arten von Cyberbedrohungen anpassen, denen Sie ausgesetzt sind.

### Wie die Teile Security Operations zusammenpassen

Wie gezeigt scheint Security Operations ein Rätsel zu sein. Wenn jedoch die Teile zusammengefügt werden und Sie das Bild preisgeben, wird die Leistungsfähigkeit und

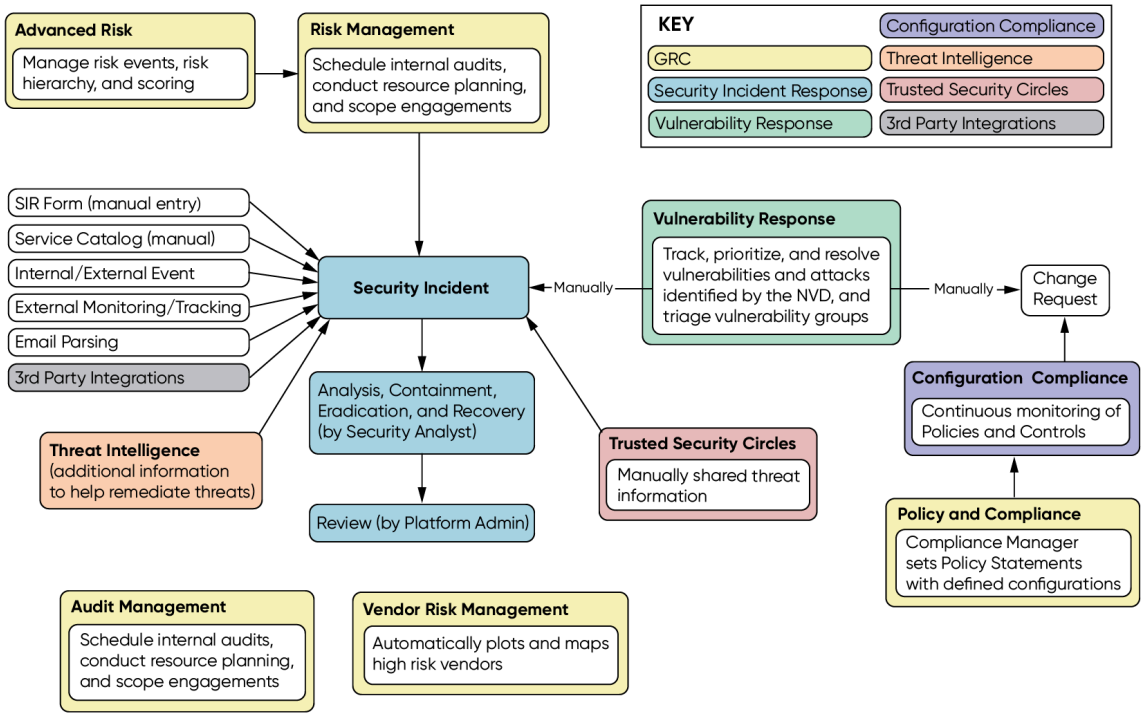
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flexibilität von Now Platform deutlich. Jede Anwendung und die andere Anwendung, die sie berührt, werden in den folgenden Abschnitten beschrieben.

**Hinweis:**
Die GRC-Anwendungen (Governance, Risk, and Compliance) sind nicht in der Anwendungssuite Security Operations enthalten. Sie integrieren jedoch Daten mit Security Operationsund teilen sie mit, sodass sie in den folgenden Beschreibungen und Diagrammen enthalten sind.

**Die Suite Security Operations (zum Vergrößern auf das Bild klicken)**




## Die Anwendung Security Incident Response .

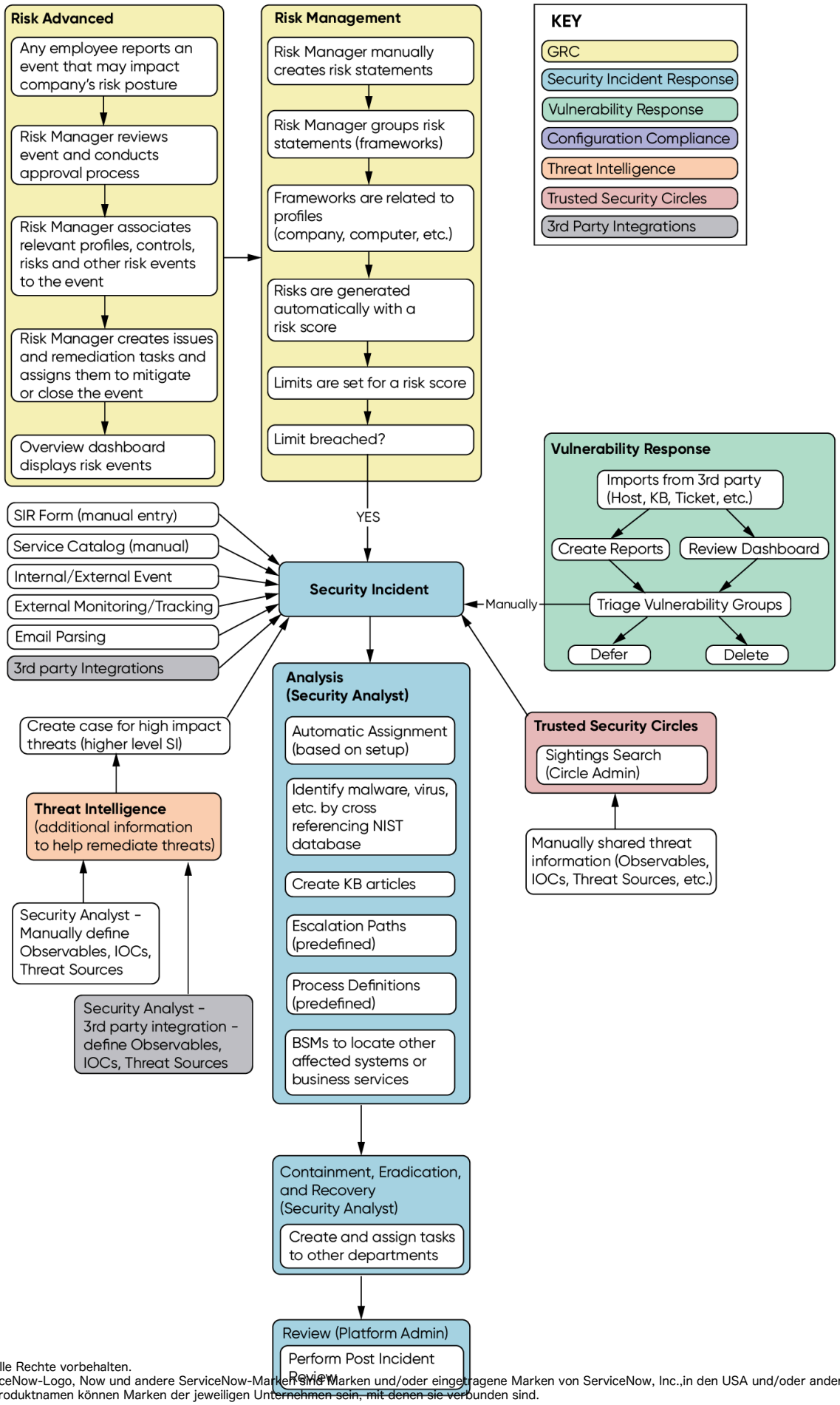
Das Herzstück des Security Operations -Ökosystems ist die Anwendung Security Incident Response (SIR). Security Incident Response vereinfacht den Prozess der Identifizierung kritischer Incidents durch die Anwendung leistungsstarker Workflow- und Automatisierungstools, die die Behebung beschleunigen. Integrieren Sie Ihre vorhandenen SIEM-Tools (Security Information and Event Manager) mit den Anwendungen Security Operations, um Bedrohungsdaten (über APIs oder E-Mail-Warnungen) zu importieren und automatisch priorisierte Security Incidents zu erstellen.

Wie dargestellt gibt es innerhalb des Security Operations -Ökosystems viele Möglichkeiten, Security Incidents automatisch und manuell zu erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Funktionsweise von Security Incident Response mit anderen Security Operations -Anwendungen (zum Vergrößern auf das Bild klicken)




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Antwortaufgaben einfach anzeigen und nachverfolgen. Mithilfe von SLA-Schwellenwerten benachrichtigt Security Incident Response Analysten, die Aufgaben zugewiesen sind, wenn sie nicht rechtzeitig abgeschlossen werden, oder die Aufgaben werden automatisch eskaliert, je nachdem, wie das System konfiguriert ist. Es werden also keine Aufgaben übersprungen und keine Entscheidungen ignoriert. Darüber hinaus können Analysten Stakeholder proaktiv über Telefonkonferenzen oder mithilfe der Connect-Chat-Funktion Stakeholder innerhalb von Now Platform auf dem Laufenden halten.

Security Incident Response automatisiert grundlegende Aufgaben wie Genehmigungsanforderungen, Malware-Scans oder Ergänzung von Bedrohungsdaten, wenn SIR in die Anwendung ServiceNow Threat Intelligence integriert ist. Diese Art der Automatisierung beschleunigt die Reaktion auf Incidents und ermöglicht dem Sicherheitsteam mehr Zeit für die Suche nach komplexen und kritischen Bedrohungen. Orchestration-Pakete für integrierte Sicherheitsprodukte automatisieren häufig wiederholte Aktionen, z. B. Firewall-Blockierungsanforderungen, in Security Operations. Mit Playbooks können Sie bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt lösen. Sie können beispielsweise Phishing-Angriffe und -Bedrohungen, die durch böswillige Codeaktivitäten verursacht werden, mithilfe von Playbooks beheben.

Alle Incident-Aktivitäten, von der Analyse und Untersuchung bis hin zu Eindämmung und Korrektur, werden in der -Plattform nachverfolgt. Wenn ein Incident geschlossen wird, wird eine Überprüfung nach dem Incident an alle Teammitglieder verteilt, um einen historischen Audit-Datensatz zur späteren Referenz zu erstellen.

**Hinweis:**
Weitere Informationen finden Sie unter Security Incident Response verstehen.

## Die Anwendung Vulnerability Response .

Die Anwendung Vulnerability Response hilft bei der Priorisierung Ihrer angreifbaren Assets und fügt Kontext hinzu, mit dem Sie feststellen können, wann geschäftskritische Systeme gefährdet sind. Mit der CMDB kann Vulnerability Response auch systemübergreifende Abhängigkeiten identifizieren und die geschäftlichen Auswirkungen von Änderungen oder Ausfallzeiten schnell bewerten. Sie können alle Schwachstellen anzeigen, die sich auf einen bestimmten Service auswirken, sowie den aktuellen Status aller Schwachstellen, die sich auf Ihre Organisation auswirken.

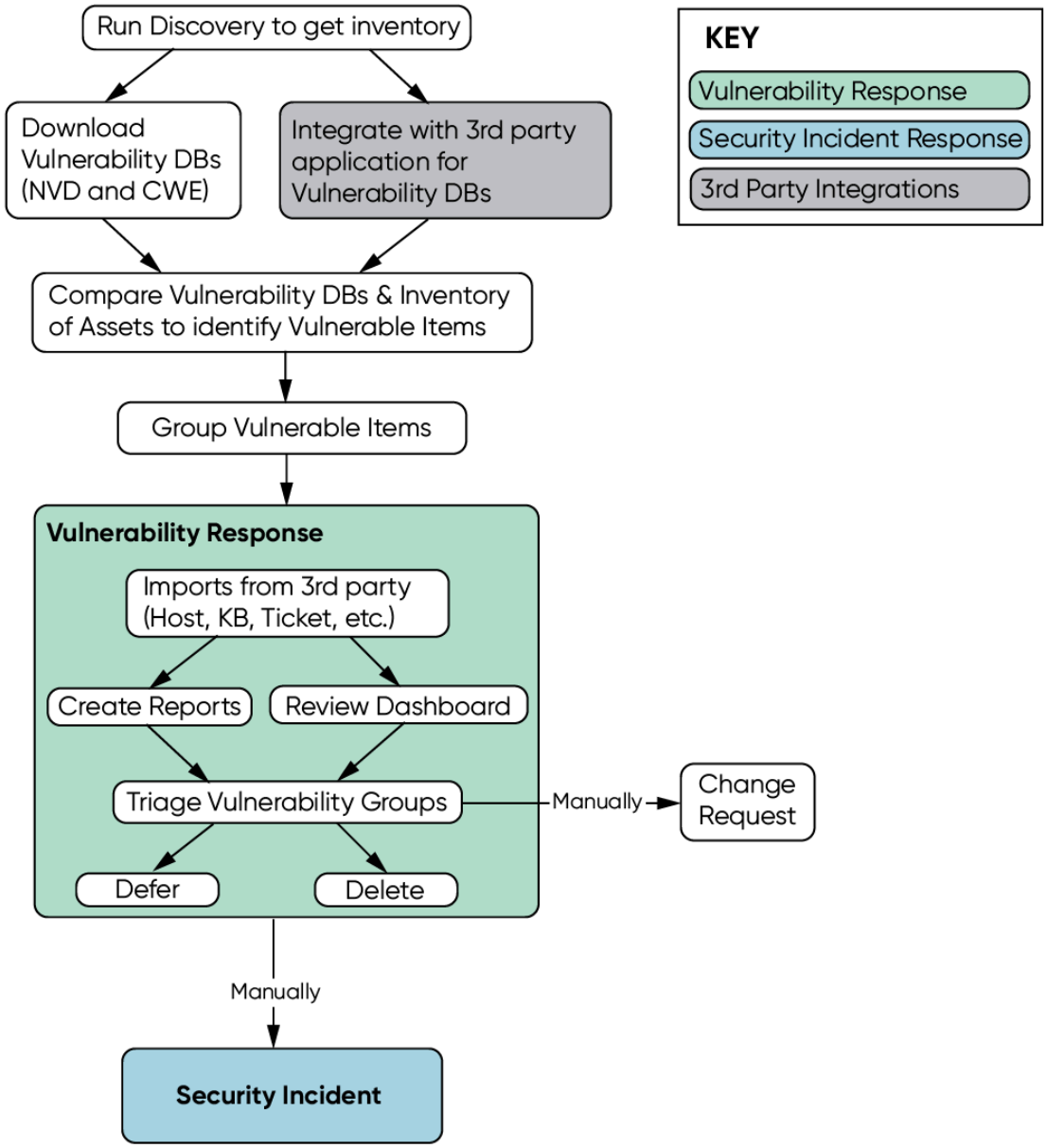
Reaktionsteams können auch die Workflow- und Automatisierungstools in Now Platform nutzen, um Schwachstellen schneller zu beheben. Wenn kritische Schwachstellen gefunden werden, kann ein Workflow automatisch eine Notfall-Patch-Genehmigungsanforderung initiieren. Nach der Genehmigung können Orchestration-Tools den Patch anwenden und einen zusätzlichen Schwachstellenscan auslösen, um sicherzustellen, dass das Problem behoben wurde.

Klicken Sie bei nicht dringenden Patches einfach auf eine Schaltfläche, um eine Change-Anforderung zu erstellen und die relevanten Informationen an die IT zu senden. Dies führt zu einer koordinierten Korrekturstrategie für Schwachstellen in Services und Assets, die die kritischsten Elemente schnell beheben kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wie Vulnerability Response mit anderen Security Operations -Anwendungen funktioniert





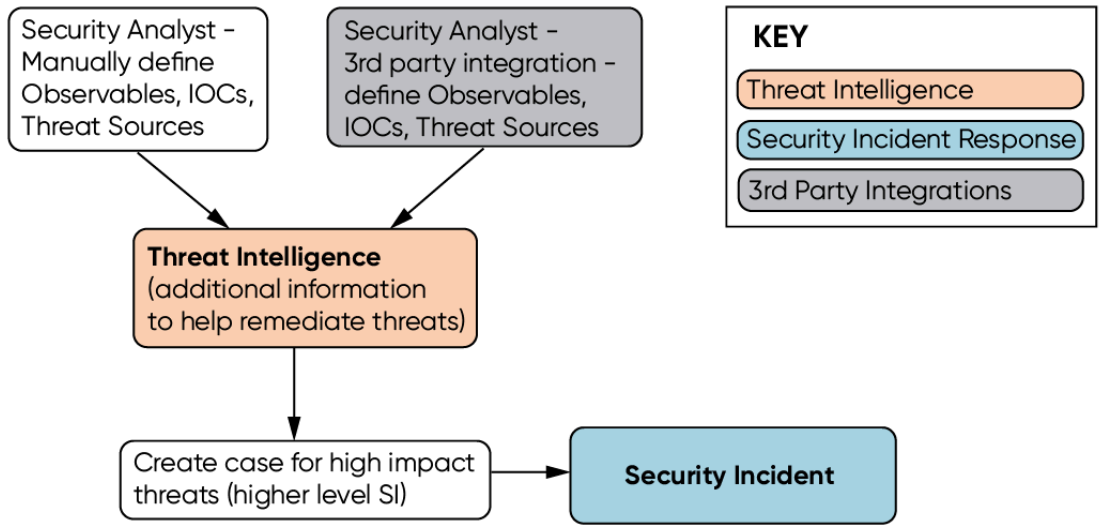

**Hinweis:**
Weitere Informationen finden Sie unter Die Anwendung Vulnerability Response erkunden.

## Die Anwendung Threat Intelligence .

Security Operations umfasst eine Threat Intelligence-Anwendung, die Incident-Beantworter dabei unterstützt, Kompromittierungsindikatoren (Indicators of Compromise, IoC) zu finden und nach tief liegenden Angriffen und Bedrohungen zu suchen. Sie durchsucht Bedrohungs-Feeds automatisch nach relevanten Informationen, wenn ein IoC mit einem Security Incident verbunden ist, und kann IoCs zur zusätzlichen Analyse an Drittanbieterquellen senden. Die Ergebnisse werden direkt im Security Incident-Datensatz zur Überprüfung durch Analysten gemeldet, wodurch wertvolle Zeit gespart wird. ServiceNow unterstützt mehrere Bedrohungsfeeds sowie STIX und TAXII, um Threat Intelligence-Daten aus verschiedenen Quellen zu integrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wie Threat Intelligence mit anderen Security Operations -Anwendungen funktioniert




**Hinweis:**
Weitere Informationen finden Sie unter.Threat Intelligence verstehen

## Die Anwendung Configuration Compliance .

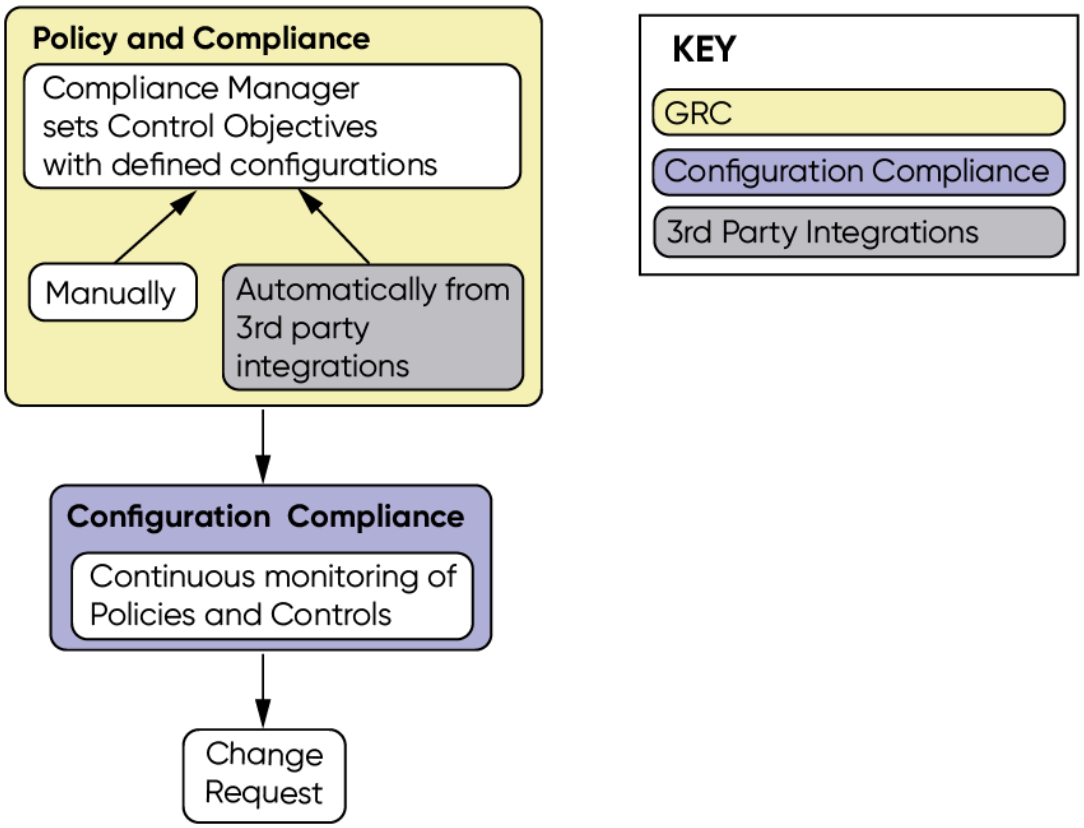
Falsch konfigurierte Software gefährdet Unternehmen. Configuration Compliance priorisiert und korrigiert falsch konfigurierte Assets anhand von Daten, die aus Scans von Sicherheitskonfigurationsbewertungen von Drittanbietern gesammelt wurden. Sie nutzt die CMDB, um zu bestimmen, welche Elemente am kritischsten sind. Workflows und Automatisierung ermöglichen schnelle Aktionen für einzelne Assets oder Gruppen für Massenänderungen.

Einfache Abstimmung mit der IT in einer einzigen Plattform, um Änderungen und Aktualisierungen vorzunehmen. Darüber hinaus können Configuration Compliance -Daten in die kontinuierliche Überwachungsfunktion von ServiceNow Governance, Risk und Compliance eingespeist werden, um das Risiko weiter zu mindern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wie Configuration Compliance mit anderen Security Operations -Anwendungen funktioniert




**Hinweis:**
Weitere Informationen finden Sie unter Configuration Compliance erkunden.

### Die Anwendungen Governance, Risk und Compliance .

Die Anwendungen ServiceNow Governance, Risk und Compliance (GRC) helfen Ihnen, ineffiziente Prozesse in Ihrem erweiterten Unternehmen in ein integriertes Risikoprogramm umzuwandeln. Durch kontinuierliche Überwachung und Automatisierung bietet ServiceNow eine Echtzeitansicht von Compliance und Risiken, verbessert die Entscheidungsfindung und erhöht die Leistung im gesamten Unternehmen und bei Lieferanten. Nur ServiceNow kann Geschäft, Sicherheit und IT mit einem integrierten Risiko-Framework verbinden, das manuelle, isolierte und ineffiziente Prozesse in ein einheitliches Programm umwandelt, das auf einer einzigen Plattform basiert.

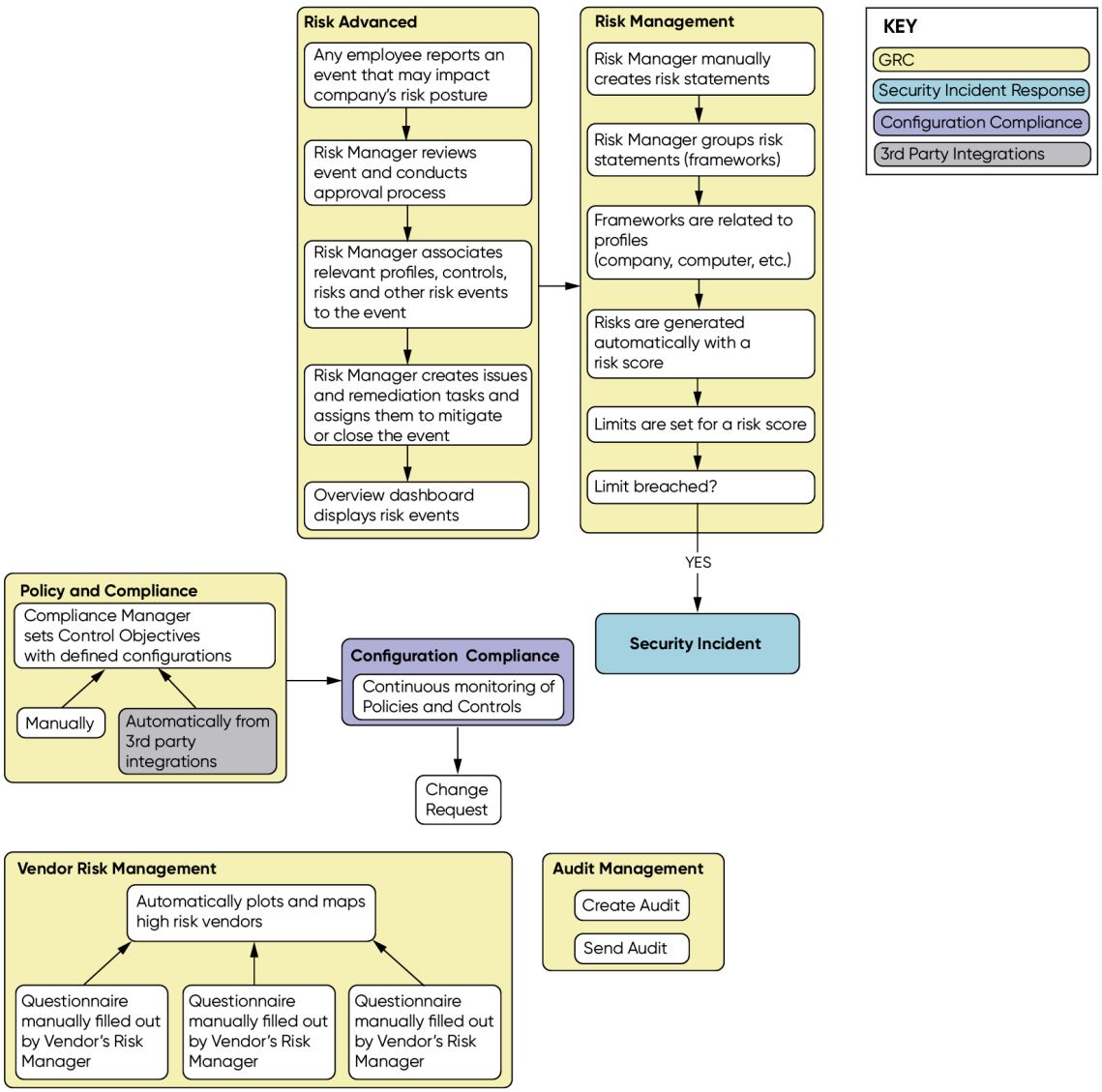
- Risikomanagement – Erkennen und bewerten Sie die Wahrscheinlichkeit sowie die geschäftlichen Auswirkungen eines Ereignisses basierend auf Daten, die in Ihrem erweiterten Unternehmen zusammengefasst werden, und reagieren Sie auf kritische Änderungen der Risikosituation.
- Policy and Compliance Management – Automatisieren Sie Best Practice-Lebenszyklen, vereinheitlichen Sie Compliance-Prozesse, und geben Sie Zusicherungen für ihre Effektivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Audit Management – Umfang und Priorität von Audit-Interaktionen anhand von Risikodaten und Profilinformationen festlegen, um wiederkehrende Audit-Ergebnisse zu beseitigen, die Audit-Gewährleistung zu verbessern und Ressourcen für interne Audits zu optimieren.
- Risikomanagement für Lieferanten –Einführung eines standardisierten und transparenten Prozesses zur Verwaltung des Lebenszyklus für Risikobewertungen, Sorgfaltspflicht und Risikobewältigung mit Geschäftspartnern und Lieferanten.

**Funktionsweise der Anwendungen [ Governance, Risk und Compliance mit Anwendungen Security Operations (zum Vergrößern auf das Bild klicken)**




**Hinweis:**
Weitere Informationen finden Sie unter Governance, Risk, and Compliance .

[store-future: BEGIN review]

## Security Operations Szenarien und Beispiele

Die Produkte ServiceNow® Security Operations können durch Untersuchung einiger Szenarien leicht verstanden werden. Diese Szenarien stellen Funktionen dar, die Sie bei der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

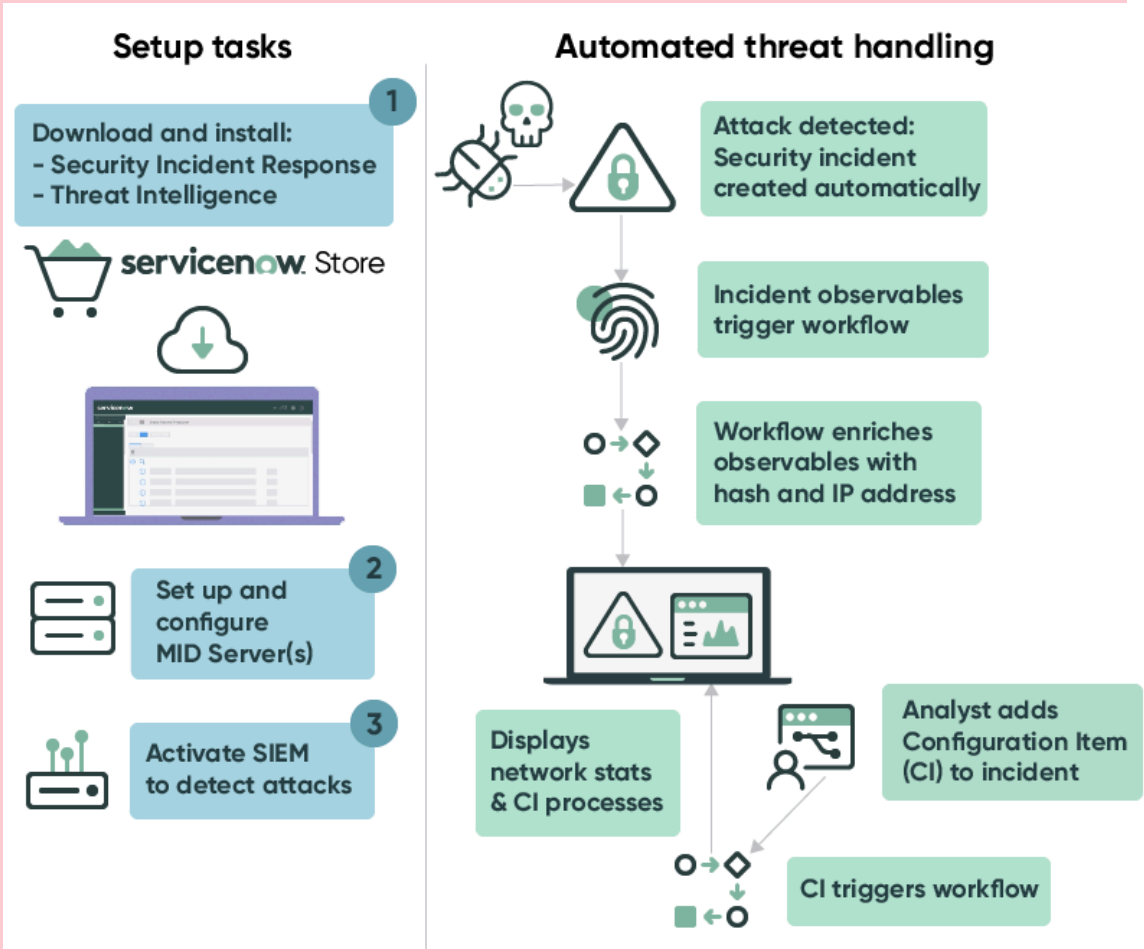
Verwendung der -Produkte verwenden können. Sie sollen Sie über die Leistungsfähigkeit und Flexibilität dieser Produkte informieren.

[End]
[store-future: BEGIN review]

## Reduzieren Sie die Zeit für Bedrohungsanalysen mithilfe von Automatisierung

Die Selektierung und Analyse von Security Incidents sind erforderliche Schritte, um während des Prozesses der Reaktion auf Bedrohungen falsch positive Meldungen auszusortieren und zu bestimmen, wie Sie Sicherheitsbedrohungen am besten identifizieren, eindämmen und beseitigen können.

Die Selektierung kann manuelle Schritte umfassen, um die Ursachen und Auswirkungen von Bedrohungen zu ermitteln. Durch die Automatisierung vieler Schritte können Sie den Zeit- und Arbeitsaufwand für die Analyse und Eindämmung von Bedrohungen erheblich reduzieren. Nachdem Sie die Automatisierung in Ihrer ServiceNow® Security Operations -Software eingerichtet haben, können Sie verschiedene Arten der Automatisierung ausführen. Beispielsweise können Sie Daten zu erkennbaren Elementen automatisch anreichern, wenn einem Security Incident ein erkennbares Element hinzugefügt wird. Oder Sie können laufende Prozesse anzeigen oder Netzwerkstatistiken abrufen, wenn ein CI in Ihrer CMDB zu einem Security Incident hinzugefügt wird. Mit diesen unten dargestellten Prozessen können Sie während der Bedrohungsanalyse wertvolle Zeit sparen.




In diesem Szenario wurde eine schädliche Datei vom SIEM-Tool (Security Information and Event Management) erkannt, das Ihr Unternehmen zur Bedrohungserkennung verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integration von Security Operations mit dem SIEM führt dazu, dass basierend auf der Art der erkannten Bedrohung automatisch ein Security Incident erstellt wird. Wenn die schädliche Datei bereits erkennbare Elemente enthielt oder der Sicherheitsanalyst nachträglich neue, nicht abgelaufene erkennbare Elemente hinzugefügt hat, wird automatisch ein Workflow ausgelöst, der die Datensätze der erkennbaren Elemente anreichert. Der Workflow bewirkt, dass die erkennbaren Elemente gescannt werden und der Hash und die IP-Adresse der Partei, die die Datei gesendet hat, dem Security Incident hinzugefügt werden.

Während der Selektierung kann der Analyst feststellen, dass Konfigurationselemente (CI), die in der CMDB des Unternehmens enthalten sind, durch den Angriff möglicherweise betroffen waren. Der Analyst fügt dem Security Incident daher die CIs hinzu. Wenn der Security Incident gespeichert wird, werden zwei weitere Workflows ausgeführt und Netzwerkstatistiken und laufende Prozesse im Zusammenhang mit den CIs werden dem Security Incident sofort hinzugefügt.

[End]

## Bereitet sich auf die Automatisierung von Threat Intelligence vor

Bevor die Automatisierung von Threat Intelligence im Bedrohungsreaktionsprozess verwendet werden kann, müssen Sie einige vorbereitende Setup-Schritte ausführen. Nach Abschluss des Setups werden die Workflows automatisch mit wenig oder gar keiner Benutzerunterstützung ausgeführt.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

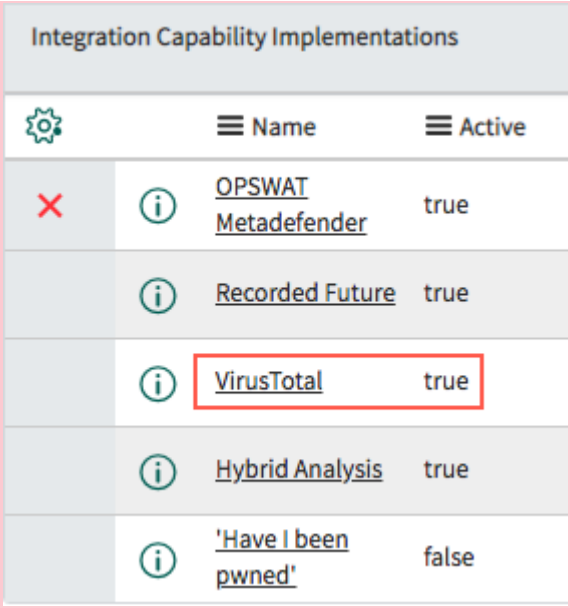
1. Laden Sie die herunter Security Incident Response und Threat Intelligence -Anwendungen aus dem ServiceNow Store.
2. Installieren Sie einen oder mehrere MID Server , und konfigurieren Sie Serviceanmeldeinformationen für jeden von ihnen .
3. Wenn die MID Server ausgeführt werden, stellen Sie sicher, dass die von Ihnen verwendete Implementierung der Integrationsfähigkeit (z. B. VirusTotal) für die Fähigkeit „Bedrohungssuche“ aktiv ist.
   Die Fähigkeit „Bedrohungssuche“ führt Suchvorgänge durch, um zu bestimmen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsbedrohungen zugeordnet sind.

   a. Navigieren zu **Security Operations** > **Integrationen** > **Integrationsfunktionen**.

   b. Klicken Sie auf **Bedrohungssuche**, und scrollen Sie nach unten zur zugehörigen Liste „Implementierung der Integrationsfähigkeit“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**c.** Suchen Sie die Implementierung, die Sie verwenden möchten, und vergewissern Sie sich, dass in der Spalte **Aktivtrue angezeigt**wird.

**d.** Wenn die Implementierung nicht aktiv ist, klicken Sie auf den **Namen**der Implementierung, aktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **Aktualisieren**.

## Daten erkennbarer Elemente automatisch ergänzen

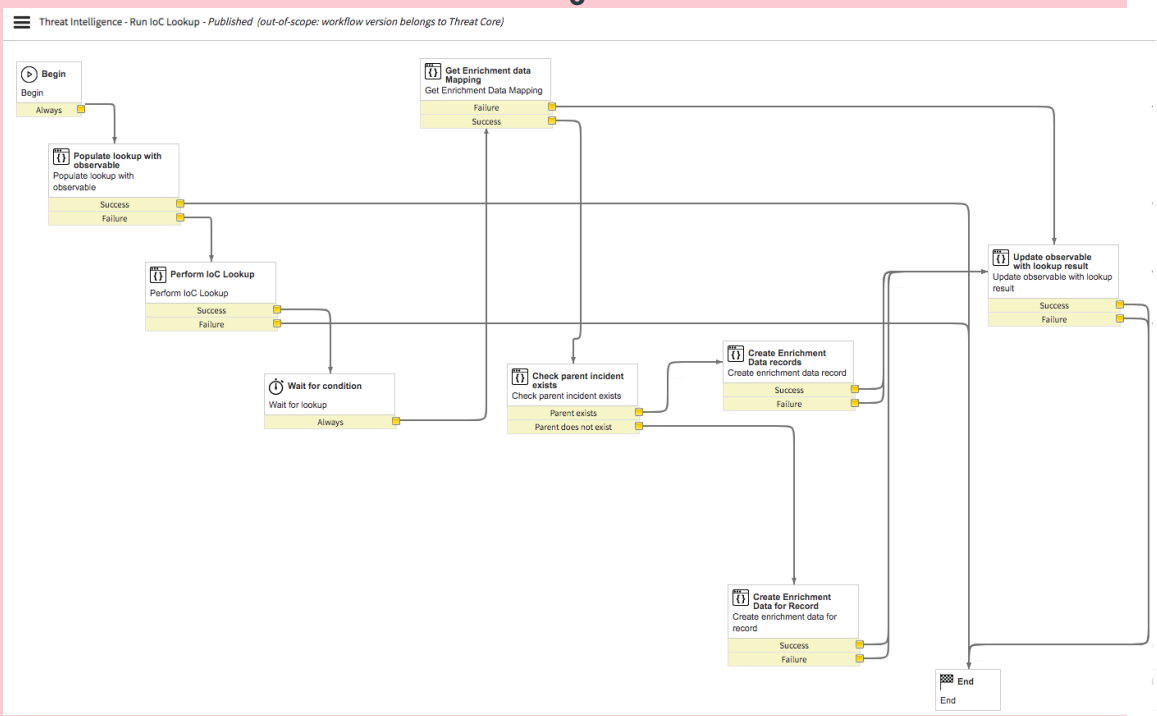
Nachdem Sie die Automatisierung von Threat Intelligence vorbereitet und einem Security Incident neue oder nicht abgelaufene Indicators of Compromise (IoC) hinzugefügt haben, wird der Workflow „Threat Intelligence – IoC-Suche ausführen“ automatisch ausgeführt.

Die Workflow-Aktivitäten extrahieren Informationen aus den IoCs, einschließlich des Hashs der verdächtigen Datei und der Ursprungs-IP-Adresse, ohne dass der Benutzer eingreifen muss.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Daten erkennbarer Elemente automatisch ergänzen




**Hinweis:**

Sie können die Suche auch manuell ausführen, indem Sie mindestens ein erkennbares Element auswählen, das bereits an den Security Incident angehängt ist, und in der Auswahlliste **Aktionen für ausgewählte Zeilen** die Option **Bedrohungssuche ausführen** auswählen.

Der Workflow führt die folgenden Aktivitäten aus:

1. Die Aktivität „ **Suche mit erkennbarem Element ausfüllen** “ versucht, ein vorhandenes erkennbares Element für eine Suche zu finden, die dem Wert und Typ der Suche entspricht, die der Aktivität als Eingabe bereitgestellt wurde.
   a. Wenn ein erkennbares Element gefunden wird, das den Eingaben entspricht, führt die Aktivität „ **IoC** -Suche durchführen“ dazu, dass eine Suche für die ScanID des Datensatzes durchgeführt wird.
   b. Wenn ein erkennbares Element gefunden wird, das nicht abgelaufen ist, wird die Suche nicht durchgeführt, und die Suchergebnisse im Security Incident werden mit Informationen aus dem erkennbaren Element aktualisiert. Weitere Informationen finden Sie unter Füllen Sie die Suche mit der Aktivität „Erkennbares Element“ aus.
2. Wenn eine IoC-Suche ausgeführt wird, werden mit den folgenden vier Aktivitäten zuerst Informationen aus der Ergänzungsdatenzuordnung abgerufen. Die Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaftendateien in ServiceNow-Datensätze um. Als Nächstes überprüfen sie, ob ein übergeordneter Security Incident vorhanden ist. Wenn dies der Fall ist, wird ein erkennbares Element erstellt und angereichert. Wenn nicht, wird das vorhandene erkennbare Element angereichert. Weitere Informationen finden Sie unter Erkennbares Element mit Suchergebnisaktivität aktualisieren.
   - **Ruft die Ergänzungsdatenzuordnung ab**
   - **Überprüfen Sie, ob der übergeordnete Incident vorhanden ist**

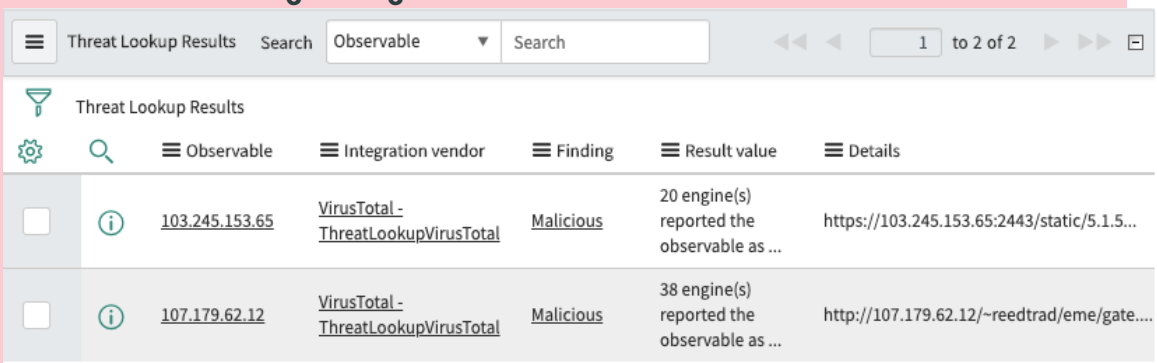


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ergänzungsdatensätze erstellen**
- **Erstellen Sie Ergänzungsdaten für Datensatz**

3. Nach Abschluss der Datenanreicherung aktualisiert die Aktivität **Erkennbares Element mit Suchergebnissen** aktualisieren die erkennbaren Elemente im Security Incident und schreibt die Ergebnisse in die zugehörige Liste „Ergebnisse der **Bedrohungssuche“**.

**Suche nach Bedrohungen – Ergebnisse**




## Ruft automatisch Netzwerkstatistiken und laufende Prozesse ab

Wenn Sie ein Configuration Item (CI) mit einem vollständig qualifizierten Windows-Domänennamen (FQDM) hinzufügen, der in der CMDB zu einem Security Incident gefunden wird, werden zusätzliche Workflows ausgeführt, um Netzwerkstatistiken und laufende Prozesse bereitzustellen.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

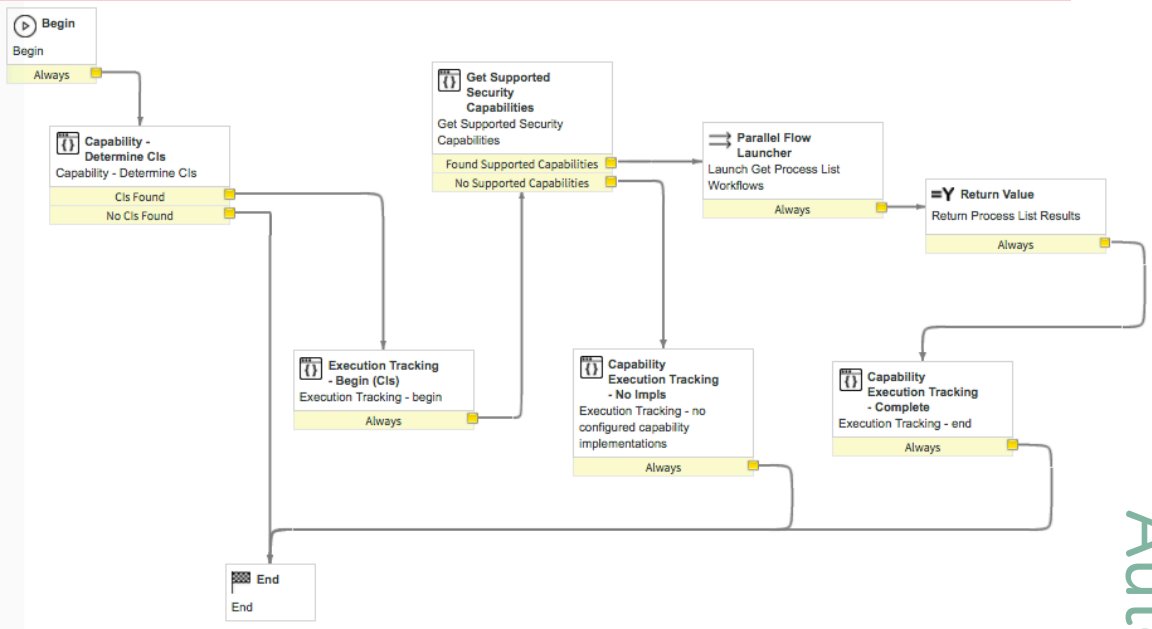
1. Füllen Sie die CMDB mit dem Discovery -Modul mit Windows-Domänennamen aus.

> **Hinweis:**
> Wenn Sie das ServiceNow Discovery -Modul nicht abonnieren, müssen Sie Ihre CMDB manuell ausfüllen oder ein Discovery-Produkt einer Drittpartei verwenden.

2. Fügen Sie dem Security Incident ein CI hinzu.
   Die folgenden beiden Workflows werden parallel ausgeführt.
   - Workflow „Security Operations – Laufende Prozesse abrufen“.: Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (CI) von einem Host ab. Verwenden Sie es, um eine Integration (z. B. Carbon Black) oder einen Windows-basierten Security Incident zu erfüllen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn der Workflow abgeschlossen ist, werden laufende Prozesse in der zugehörigen Liste **Laufende Prozesse** im Security Incident angezeigt.

**Laufende Prozesse**

Running Processes

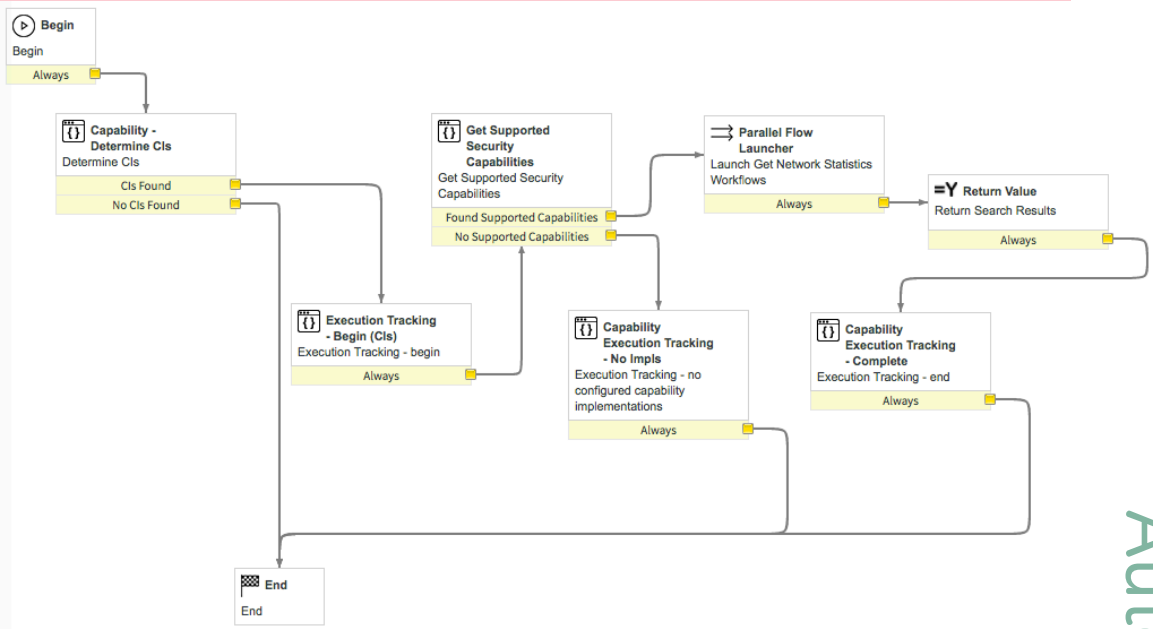
| Path | Command ... | Owner | PID | Parent PID | Security Tags |
|---|---|---|---|---|---|
| C:\Windows\syste... | C:\Windows\syste... | SYSTEM | 456 | 368 | UNKNOWN |
| C:\Windows\syste... | C:\Windows\syste... | LOCAL SERVICE | 856 | 456 | UNKNOWN |
| C:\Windows\syste... | \??\C:\Windows\sy... | SYSTEM | 1748 | 320 | UNKNOWN |
| C:\Windows\Syste... | C:\Windows\Syste... | NETWORK SERVICE | 3676 | 456 | UNKNOWN |
| C:\Windows\syste... | \ | Administrator | 2400 | 1056 | UNKNOWN |
| C:\demo\agent\jre\... | \ | SYSTEM | 6932 | 2540 | UNKNOWN |
| C:\Windows\syste... | \ | SYSTEM | 6720 | 2968 | UNKNOWN |
| | | SYSTEM | 4 | 0 | UNKNOWN |
| C:\Windows\syste... | C:\Windows\syste... | SYSTEM | 472 | 368 | UNKNOWN |
| C:\Windows\syste... | C:\Windows\syste... | NETWORK SERVICE | 964 | 456 | UNKNOWN |

1 to 10 of 50



- Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“.: Dieser Workflow ruft eine Liste der aktiven Netzwerkverbindungen von einem Host oder Endpunkt ab. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nach Abschluss des Workflows werden Netzwerkstatistiken in der zugehörigen Liste „**Netzwerkstatistiken“** im Security Incident angezeigt.

**Netzwerkstatistiken**

Workflow Activity History Search Started Search 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

| Started | Activity | State | Ended | Result | Fault Description |
|---|---|---|---|---|---|
| 2019-05-13 13:28:38 | Execution Tracking - begin | Finished | 2019-05-13 13:28:38 | | |
| 2019-05-13 13:28:38 | Get Supported Security Capabilities | Finished | 2019-05-13 13:28:38 | | |
| 2019-05-13 13:28:39 | Execution Tracking - end | Finished | 2019-05-13 13:28:39 | | |
| 2019-05-13 13:28:39 | End | Finished | 2019-05-13 13:28:39 | | |
| 2019-05-13 13:28:39 | Return Search Results | Finished | 2019-05-13 13:28:39 | | |
| 2019-05-13 13:28:38 | Determine CIs | Finished | 2019-05-13 13:28:38 | | |
| 2019-05-13 13:28:38 | Launch Get Network Statistics Workflows | Finished | 2019-05-13 13:28:39 | success | |
| 2019-05-13 13:28:38 | Begin | Finished | 2019-05-13 13:28:38 | | |

## Priorisieren Sie wichtige Schwachstellen

Wenn Ihr Netzwerk angegriffen wird, werden folgende typische Fragen gestellt: „Wie bestimmen wir unser Risiko?“ und noch wichtiger: „Wie bestimmen wir, welche Systeme zuerst angegangen werden sollen?“

Anfang 2018 wurden zwei kritische Schwachstellen offengelegt: **„Meltdown“** und **„Spectre“**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Priorisieren Sie wichtige Schwachstellen

Meltdown exposes cached data in personal computers, mobile devices, and cloud servers to attack.

Spectre allows an attacker to trick error-free apps, which follow best practices, into leaking their secrets. The safety checks inherent in those best practices actually make the apps more susceptible to Spectre.

Böswillige Programme können „Meltdown“ und „Spectre“ ausnutzen, um sich Zugriff auf geheime Schlüssel zu verschaffen, die im Speicher anderer ausgeführter Programme gespeichert sind. Fast drei Milliarden Systeme weltweit waren potenziell von den Schwachstellen betroffen, da sowohl Hardware- als auch Softwareanbieter sich bemühten, Patches in die Hand ihrer Kunden zu bekommen.

## Rangfolge der Bedrohungen anhand gescannter Daten in Vulnerability Response

Mit der Anwendung Security Operations Vulnerability Response stehen zahlreiche Methoden zum Ausführen von Schwachstellenprüfungenzur Verfügung. Wenn die Anwendung Security Incident Response aktiviert ist, können Sie Scans auch aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Sicherheitsscan-Anforderung initiieren.

Abhängig von der von Ihnen verwendeten Drittanbieterintegration werden Schwachstellendaten gescannt und mithilfe von APIs in die Anwendung Vulnerability Response importiert. Sie wird dann mit Ihren Assets in ServiceNow Configuration Management Database (CMDB)abgeglichen. Den resultierenden angreifbaren Elementen wird eine Risikopunktzahl zugewiesen, die auf mehreren Faktoren basiert, einschließlich des Schweregrads der Schwachstelle und der Bedeutung des betroffenen Assets.

### Risikopunktzahl

All Open Incidents

Search all incident columns

Create Incident

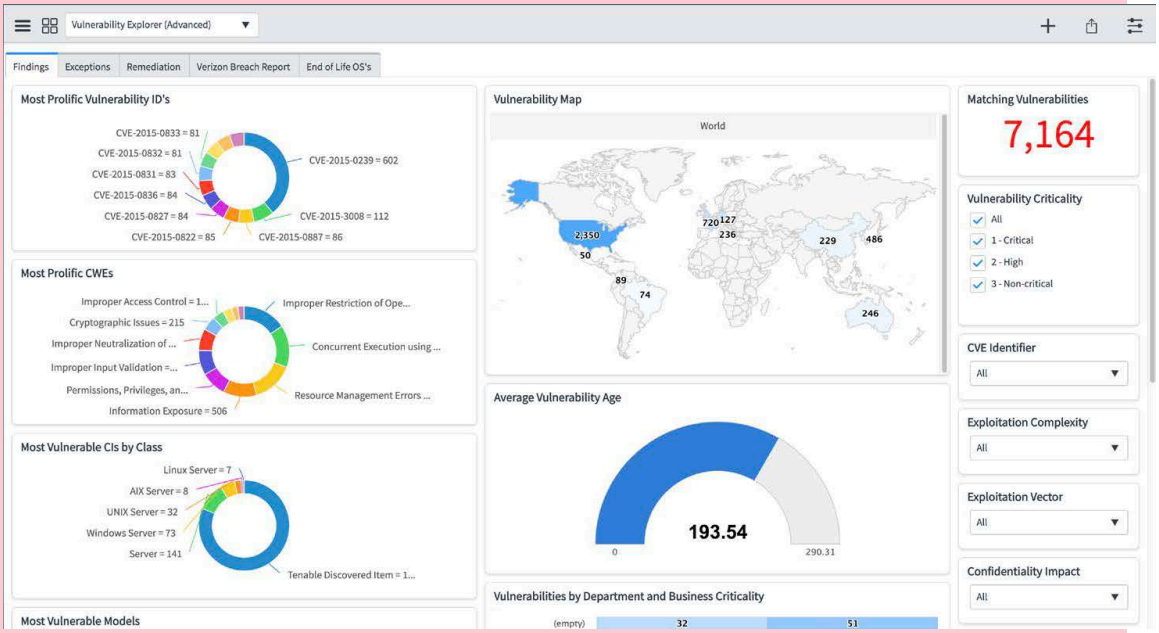
| Number | Risk Score | Short Description | Category | Source |
|---|---|---|---|---|
| SIR0001774 | 89 | DNS attack: zone transfer | Unauthorized access | Phone |
| SIR0001756 | 89 | online gambling (policy breach) | Policy violation | Phone |
| SIR0001736 | 89 | Email Malware in HQ | Malicious code act… | Alert |
| SIR0001742 | 82 | USB drive found in server port | Criminal activity/i… | Email |
| SIR0001784 | 82 | DNS redirect | Unauthorized access | Phone |
| SIR0001770 | 72 | Database moved | Unauthorized access | Phone |
| SIR0001776 | 69 | Sensitive data exposure (breach) | Unauthorized access | Phone |
| SIR0001761 | 65 | email open relay | Unauthorized access | Phone |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Risikopunktzahl ist konfigurierbar und ermöglicht eine schnelle Priorisierung. Alle Informationen über die Schwachstelle (z. B. was es ist, wie sie ausgenutzt wurde und wie die Bedrohung behoben werden kann) werden automatisch aus der National Vulnerability Database (NVD) in Vulnerability Response abgerufen, sodass keine manuelle Recherche erforderlich ist. Die konfigurierbaren Dashboards der Lösung zeigen sofort das allgemeine Schwachstellenrisiko Ihrer Organisation an.

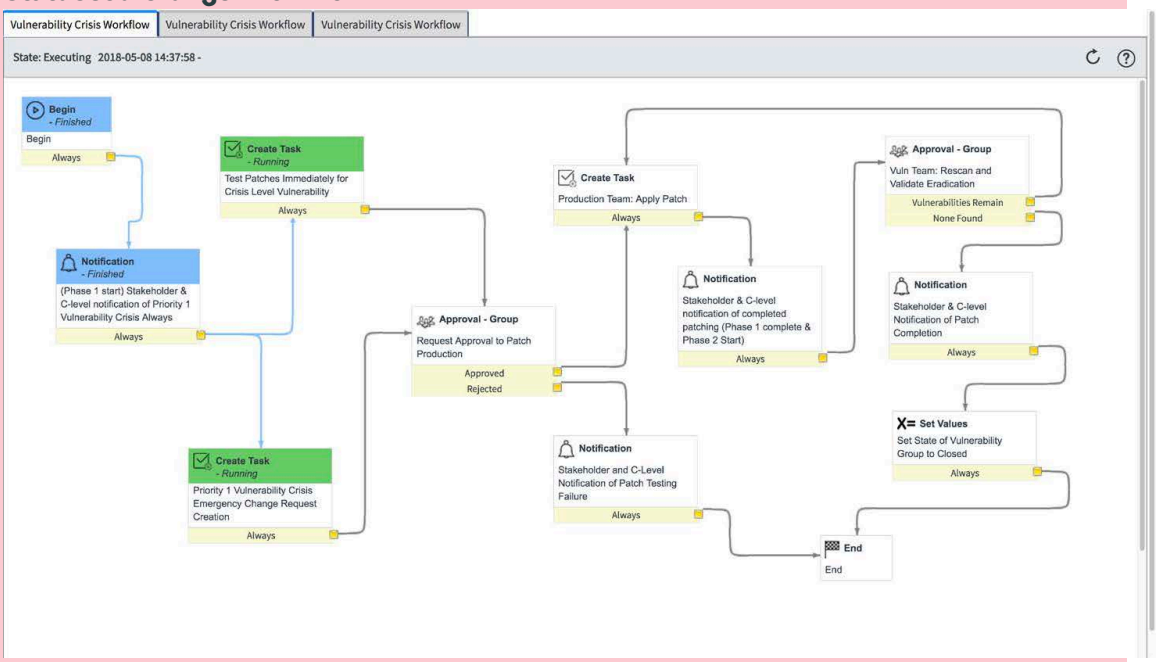
### VR-Dashboard




## Automatisierung der nächsten Schritte

Nachdem Sie die kritischsten angreifbaren Elemente identifiziert und priorisiert haben, automatisieren Security Operations -Workflows mehrere der nächsten Schritte.

### Statuscodierungs-Workflow




Für geschäftskritische angreifbare Elemente werden Anforderungen zur Genehmigung des automatischen Patching gesendet und die entsprechenden Besitzer benachrichtigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch entfällt die Notwendigkeit, nach dem Rufbereitschaftsanalysten zu suchen oder manuell zu entscheiden, welche Elemente als „kritisch“ gelten.

Nach Genehmigung und Abschluss des Patch wird automatisch ein zweiter Scan ausgeführt, um die Korrektur zu überprüfen. Mithilfe von Priorisierung, Workflows und Automatisierung werden die kritischsten Elemente zuerst behandelt.

## Security Operations und ServiceNow Store

Ab Madrid sind alle Security Operations Anwendungen und unterstützten Integrationen zum Download von ServiceNow Storeverfügbar. Auf diese Weise können Sie neue und aktualisierte Funktionen schneller erhalten. Bevor Sie Security Operations -Anwendungen verwenden können, müssen Sie überprüfen, ob Sie berechtigt sind (d. h., Sie haben gültige Lizenzen, um sie zu verwenden), sie aus dem ServiceNow Storeherunterladen und aktivieren.

Die ständig größer werdende Liste der Security Operations Anwendungen, die zum Download verfügbar sind, umfasst:

- Security Incident Response (und unterstützte Integrationen)
- Vulnerability Response (und unterstützte Integrationen)
- Threat Intelligence (und unterstützte Integrationen)
- Configuration Compliance
- Trusted Security Circle
- Data Loss Prevention Incident Response

Sehen Sie sich dieses fünfminütige Video an, um mehr über das Herunterladen von Security Operations- und GRC-Anwendungen aus dem ServiceNow Storezu erfahren. In diesem 5-minütigen Video wird beschrieben, wie Security Operations- und GRC-Anwendungen aus dem ServiceNow Store heruntergeladen werden

Der Prozess, den Sie verwenden, um Security Operations -Anwendungen und -Integrationen zu erhalten, hängt davon ab, ob Sie eine Anwendung zum ersten Mal herunterladen, eine Anwendung aktualisieren, die Sie zuvor aus dem ServiceNow Storeheruntergeladen haben, oder ein Upgrade von einem Familien-Release auf den nächsten durchführen.

### Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store herunter

Das erstmalige Herunterladen einer Anwendung aus dem ServiceNow Store umfasst eine Reihe einfacher Schritte. Einige der Schritte werden in ServiceNow Store ausgeführt, andere in Ihrer Instanz.

Mit ServiceNow Store können Sie Kernprodukte und -anwendungen herunterladen. Ein Produkt enthält eine oder mehrere Anwendungen, die als Gruppe lizenziert sind. Zum Beispiel ist Security Incident Response ein Produkt. Der Prozess umfasst die folgenden Schritte:

Erforderliche Rolle: admin.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In ServiceNow Storemüssen Sie sicherstellen, dass Sie über Berechtigungen (oder Lizenzen) für die Anwendung und ihre abhängigen Anwendungen verfügen.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

- Schließlich können Sie die Anwendung aktivieren und in Ihrer Instanz ausführen.

**Hinweis:**
Ab früheren Versionen von Rome und späteren Releases werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Wenn Sie beispielsweise die Anwendung [ Vulnerability Response aktivieren, wird auch das Plugin Vulnerability Response „ Dependencies“ aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie eine Anwendung ServiceNow Store ..

## Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab

Der erste Schritt bei der Installation einer Security Operations -Anwendung besteht darin, zu überprüfen, ob die Anwendung oder das Produkt und die zugehörigen Anwendungen über gültige ServiceNow -Berechtigungen verfügen.

### Vorbereitungen

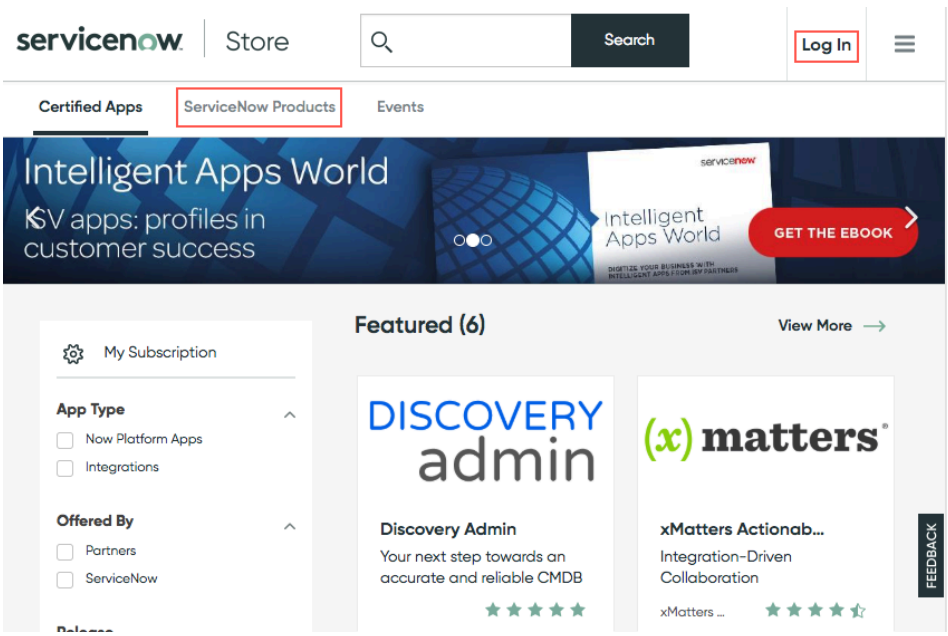
Erforderliche Rolle: admin

Personen, die Berechtigungen erwerben, müssen über ein Konto Now Support und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen verfügen.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen wurden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

### Prozedur

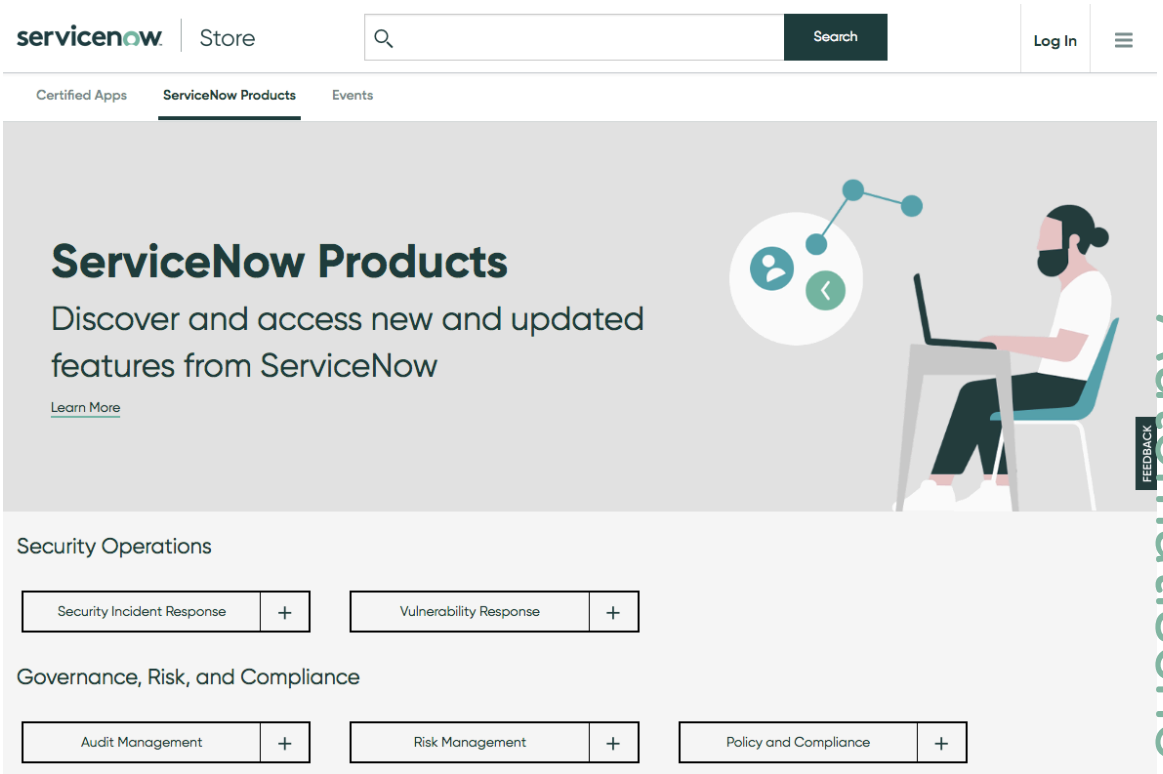
1. Navigieren Sie zu ServiceNow Store .




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Klicken Sie auf Anmelden, und melden Sie sich mit Ihren HI-**Anmeldeinformationen** an.
3. Klicken Sie auf die Registerkarte **ServiceNow-Produkte**, um alle verfügbaren ServiceNow Produkte anzuzeigen.
   Integrationen und andere Arten von Inhalten werden auf der Registerkarte **Zertifizierte Apps** angezeigt.



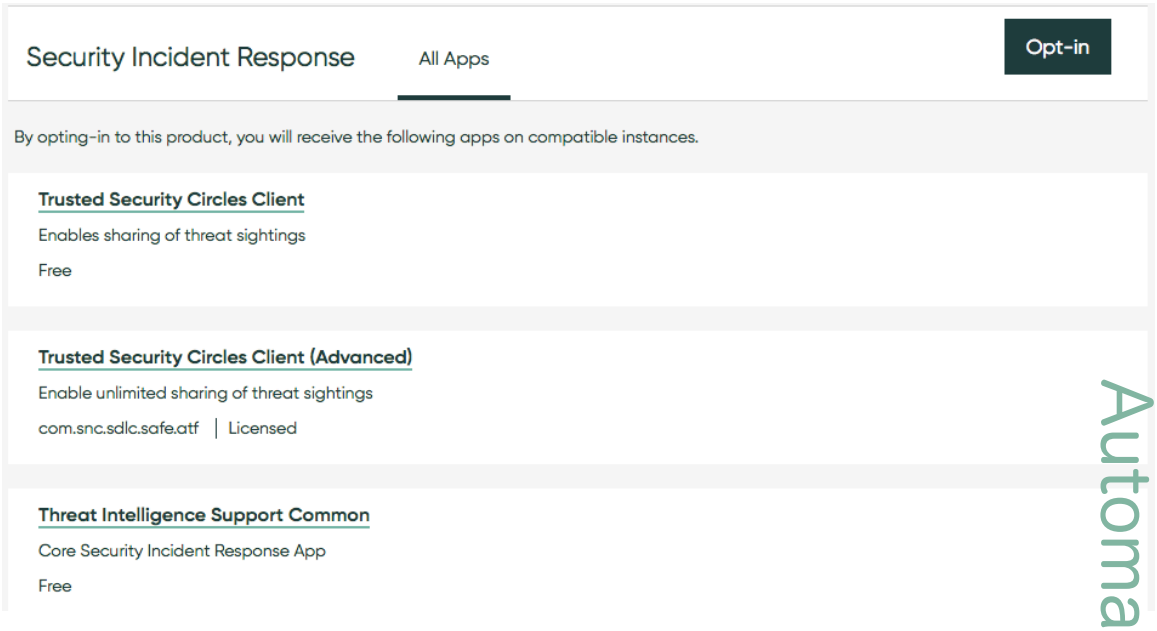

**Hinweis:**
Nehmen wir für dieses Beispiel an, dass Sie eine Berechtigung für das Produkt Security Incident Response erwerben.

4. Klicken Sie auf das Pluszeichen (+) neben dem Produktnamen, für den Sie eine Berechtigung erhalten.
   Alle Anwendungen, die dem Produkt zugeordnet sind, für das Sie eine Berechtigung erwerben, werden aufgelistet. Wenn Sie die Berechtigung für das Kernprodukt erworben haben, sind die darunter aufgeführten Anwendungen ebenfalls berechtigt.

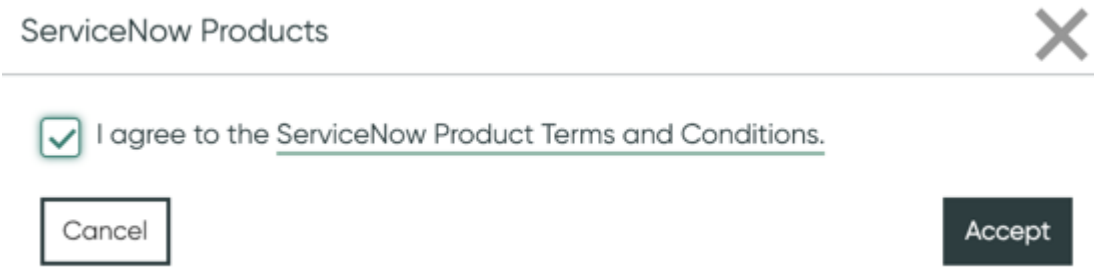
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können auch auf den Produktnamen klicken, um weitere Informationen zum Produkt und den zugehörigen Anwendungen anzuzeigen.




5. Klicken Sie auf **Opt-in**, um sicherzustellen, dass Sie über eine Berechtigung für das Produkt und die aufgeführten Anwendungen verfügen.
Sie werden aufgefordert, die allgemeinen Bedingungen von ServiceNow zu lesen und zu




akzeptieren.

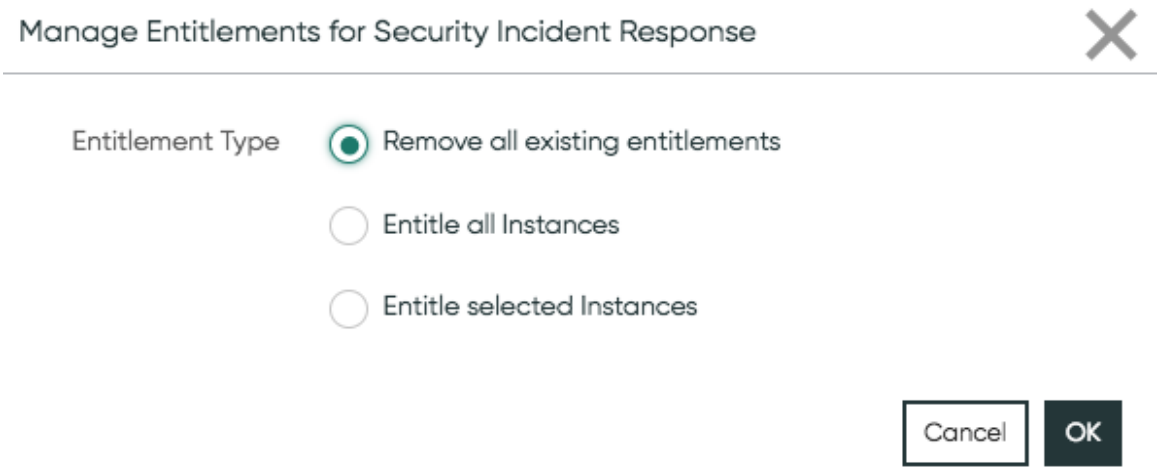
6. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
7. Beachten Sie, dass neben dem Produktnamen ein Häkchen und die Schaltfläche Berechtigungen verwalten angezeigt werden.

Das Häkchen zeigt an, dass Sie das Produkt und die zugehörigen Anwendungen abonniert haben. Es ist Zeit, Ihre Berechtigungen zu verwalten. Dies ist ein einmaliger Vorgang für dieses Produkt und alle anderen Produkte, die Sie in Zukunft installieren möchten.

8. **Wahlweise:** Sie können auf **Berechtigungen verwalten** klicken, um die Instanzen zu ändern, die von den Anwendungen betroffen sind, für die Sie berechtigt sind.

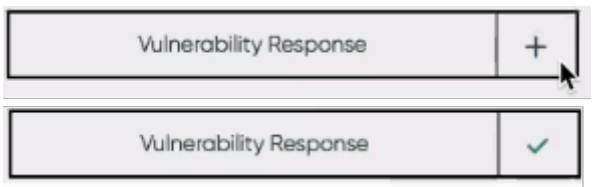
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






9. Nachdem Sie den allgemeinen Bedingungen von ServiceNow zugestimmt und Berechtigungen verwaltet haben, können Sie andere Produkte mit einem einzigen Klick berechtigen.




**Hinweis:**
Sie sind bereit, das Produkt zu aktivieren.

## Aktivieren Sie eine Anwendung ServiceNow Store .

Nachdem einer Anwendung die Berechtigung erteilt wurde, müssen Sie das Plugin für Abhängigkeiten aktivieren und die Anwendung aktivieren. Dieser Prozess gilt auch für Anwendungen, die in Test- und Entwicklungsumgebungsinstanzen heruntergeladen wurden.

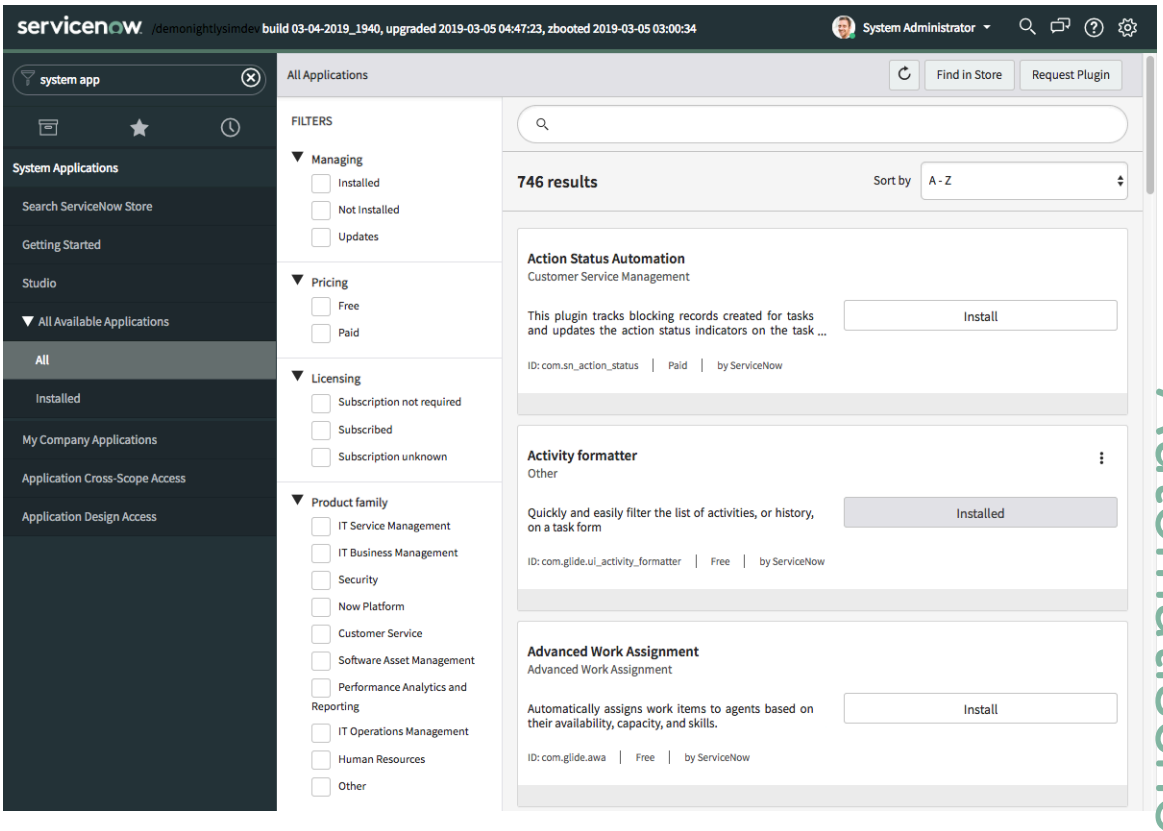
### Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

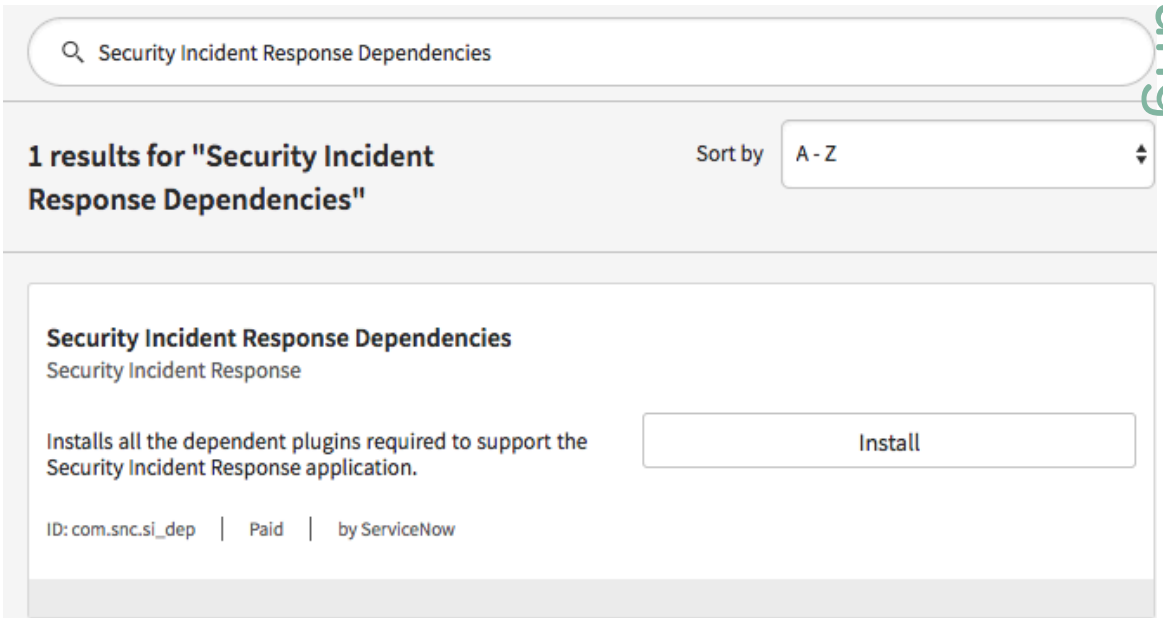
**1.** Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.




### Hinweis:

Ab Orlando werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Wenn Sie beispielsweise die Anwendung [ Vulnerability Response aktivieren, wird auch das Plugin Vulnerability Response „ Dependencies“ aktiviert. Daher sind die Schritte 2 bis 5 optional.

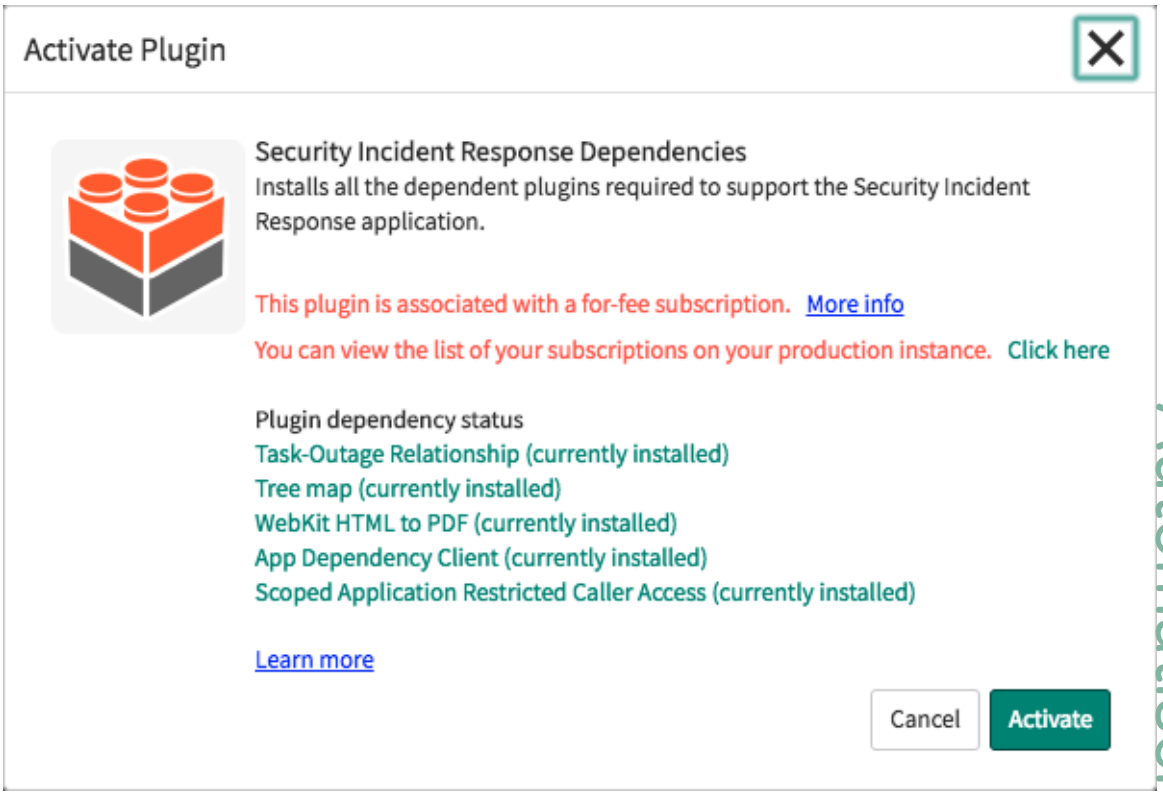
**2.** Suchen Sie nach dem Abhängigkeits-Plugin für die Anwendung, die Sie aktivieren möchten.
Wenn Sie beispielsweise Security Incident Responseaktivieren, suchen Sie das Plugin Security Incident Response „ Dependencies“.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Installieren**.
   Das Dialogfeld „Plugin aktivieren“ wird angezeigt.




4. Klicken Sie im Dialogfeld „ **Plugin aktivieren** “ auf **Aktivieren**.
5. Wenn die Aktivierung abgeschlossen ist, klicken Sie auf **Formular schließen und neu laden**.
6. Suchen Sie nun das Kernprodukt, das Sie aktivieren, klicken Sie auf das Kontrollkästchen **Mit Demodaten installieren**, wenn Sie Demodaten laden möchten, und klicken Sie auf **Installieren**.
   Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

> **Hinweis:**
> Wenn Sie das Kontrollkästchen **Mit Demodaten** installieren nicht aktivieren, können die Demodaten nachträglich nicht über den **Anwendungsmanager** installiert werden. Weitere Informationen dazu, wie Sie Demodaten nach der Erstinstallation installieren oder erneut installieren, finden Sie im Artikel Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] in der Knowledge Base von HI.

## Installieren Sie eine Security Operations -Integration

Alle ServiceNow -Integrationen sind auf der ServiceNow Storeverfügbar. Kernanwendungen wie Security Incident Response werden auf der Registerkarte **ServiceNow-Produkte** im Store angezeigt. Integrations-Add-ons werden auf der Registerkarte **Zertifizierte Apps** angezeigt.

### Vorbereitungen

Erforderliche Rolle: admin

Store-Installationen erfordern ein Now Support -Konto und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen.

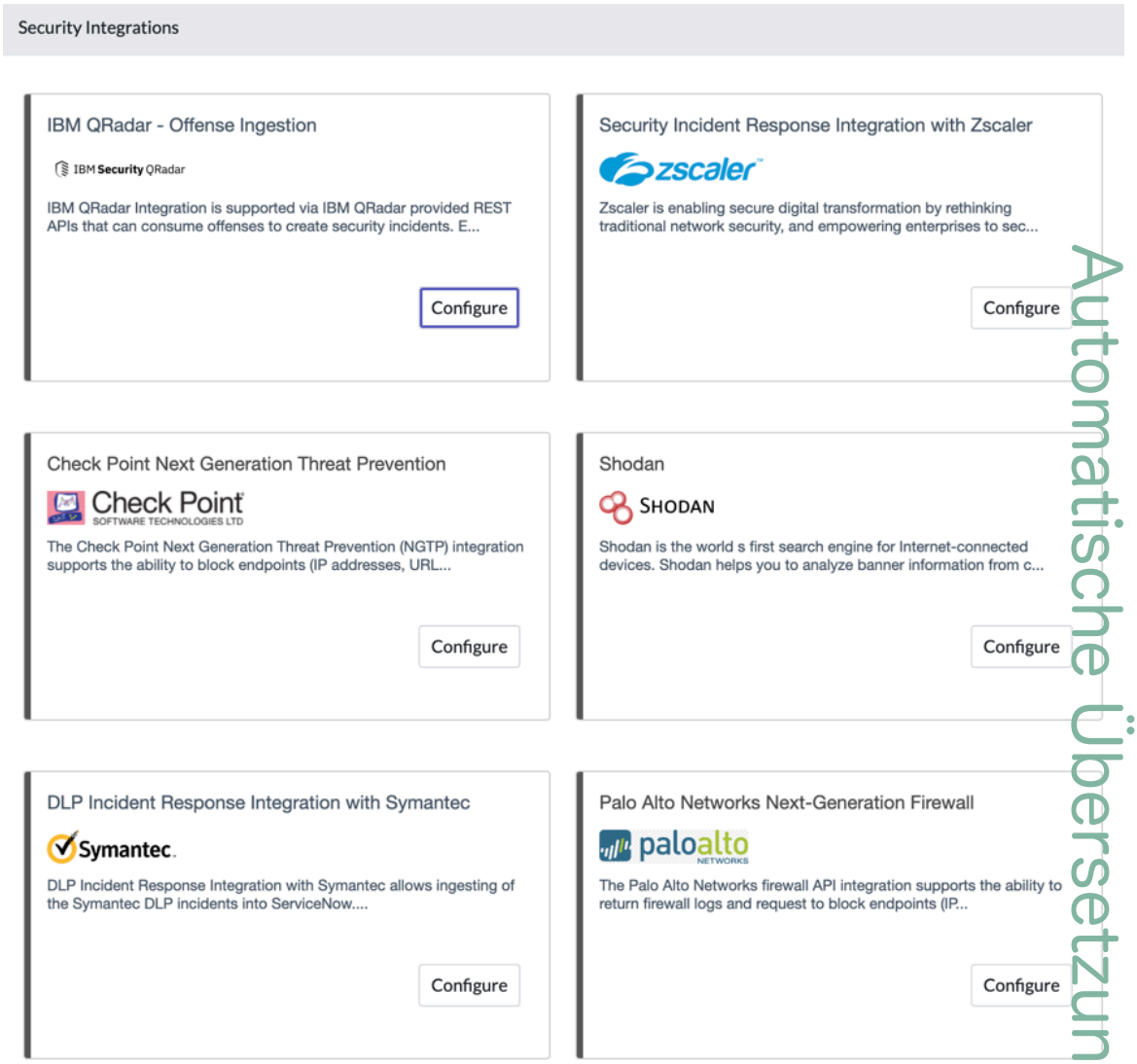
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** , nachdem Sie die Anwendung aus dem ServiceNow Store installiert haben.
   Konfigurationskacheln für die Integrationen werden angezeigt

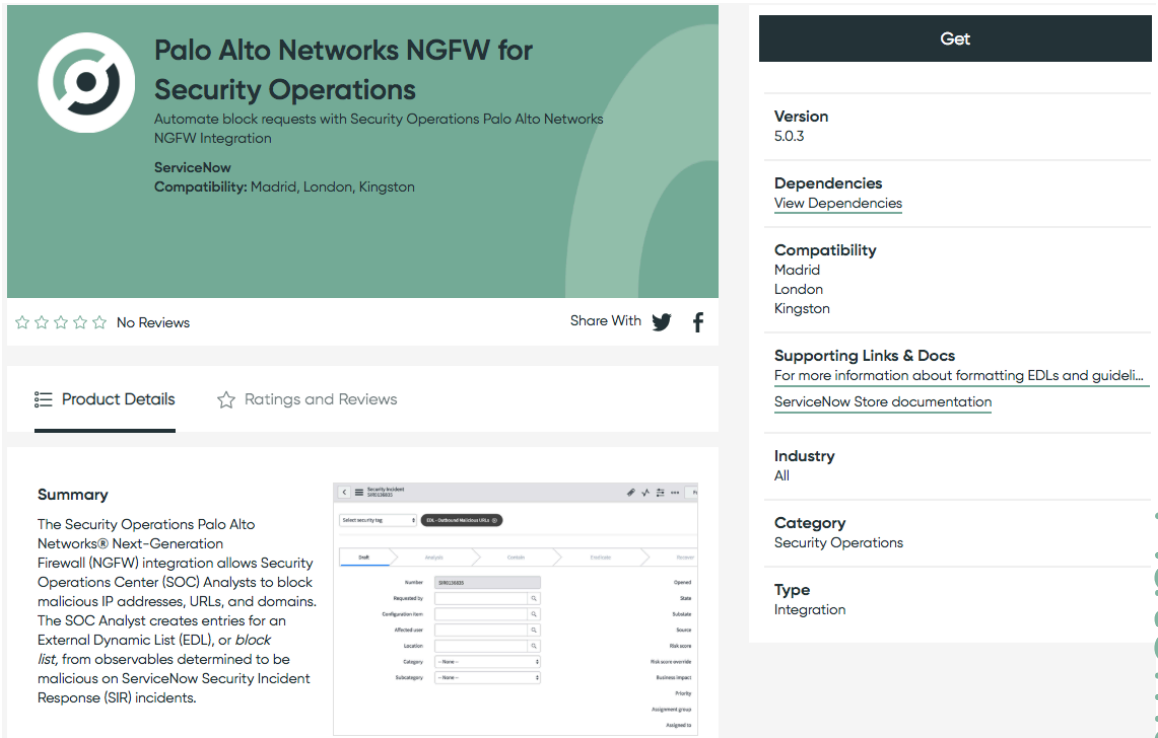
   **Hinweis:**




2. Suchen Sie die Integration, die Sie installieren möchten, und klicken Sie auf **Konfigurieren**.
   Die ausgewählte Integration wird im angezeigt ServiceNow Store

Automatische Übersetzung

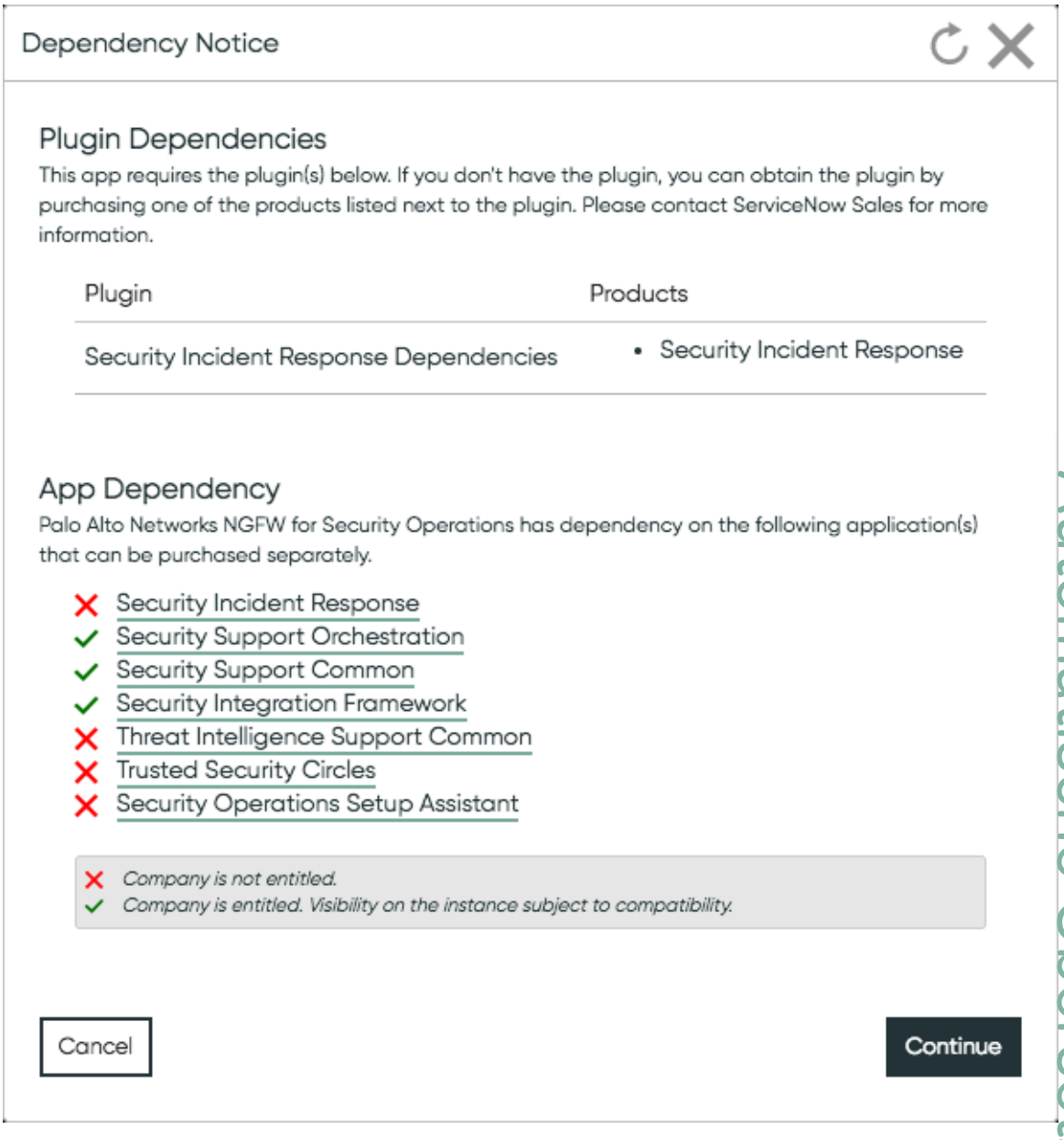
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Klicken Sie **auf Abhängigkeiten anzeigen**, und überprüfen Sie die aufgelisteten App-Abhängigkeiten.



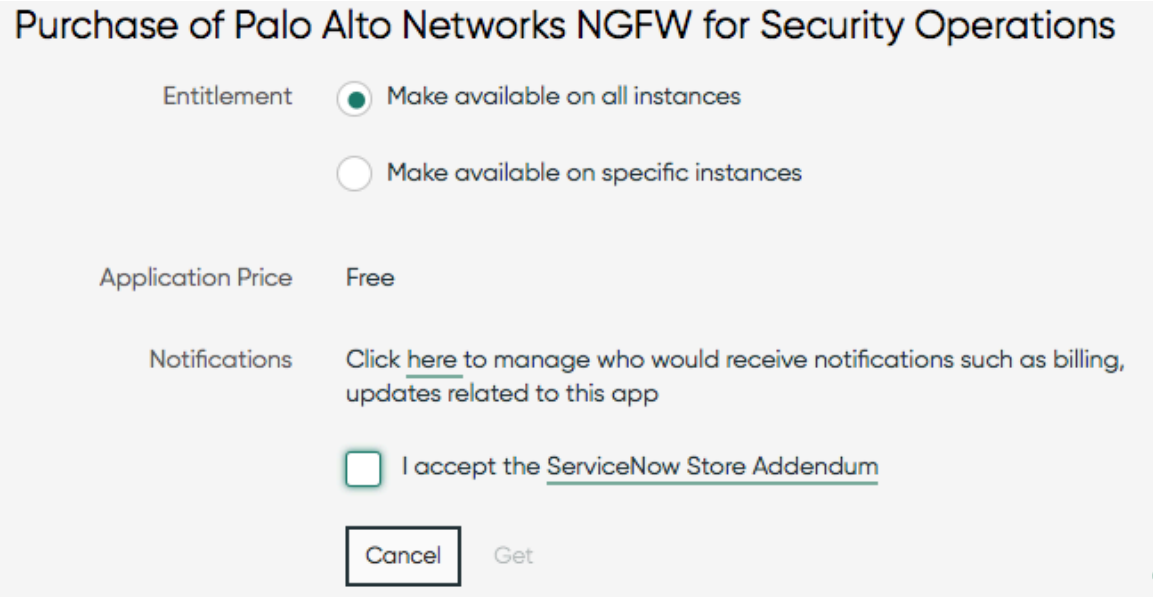
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wenn die Integration über Kernanwendungsabhängigkeiten verfügt, z. B. Security Incident Response, auf die Ihr Unternehmen noch keinen Anspruch hat:
   a. Befolgen Sie diese Anweisungen, um Berechtigungen zu erhalten, Abhängigkeits-Plugins herunterzuladen und die -Anwendungen zu aktivieren.
   b. Kehren Sie zu diesem Verfahren zurück.
   c. Klicken Sie auf **Fortsetzen**.
5. Klicken Sie auf **Abrufen**.
   Die allgemeinen ServiceNow-Bedingungen werden angezeigt.
6. Klicken Sie auf **Fortsetzen**.
   Ein Kaufbildschirm ähnlich dem folgenden wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Identifizieren Sie, für welche Instanzen die Integration verfügbar sein soll, verwalten Sie Ihre Benachrichtigungen, und aktivieren Sie das Kontrollkästchen **ServiceNow Store-Nachtrag**.
8. Klicken Sie auf **Abrufen**.

> **Hinweis:**
> Wenn Sie eine Anwendung zum Kauf herunterladen, klicken Sie auf **Kaufen**. Wenn Sie eine Anwendung herunterladen, für die Sie eine vorherige Genehmigung des Lieferanten einholen müssen, klicken Sie auf **App anfordern**.

9. Geben Sie den Instanznamen und einen Grund für die Anforderung ein, und klicken Sie dann auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
10. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
    Eine Liste der für die Installation verfügbaren Anwendungen wird angezeigt.
11. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Integration wird automatisch in Ihrer Instanz installiert.

## Aktualisieren Sie eine Anwendung, die zuvor aus dem heruntergeladen wurde ServiceNow Store

Wenn Sie zuvor eine Anwendung aus dem ServiceNow Store heruntergeladen haben und eine neue Version verfügbar ist, können Sie sie in Ihrer Instanz aktualisieren.

### Vorbereitungen

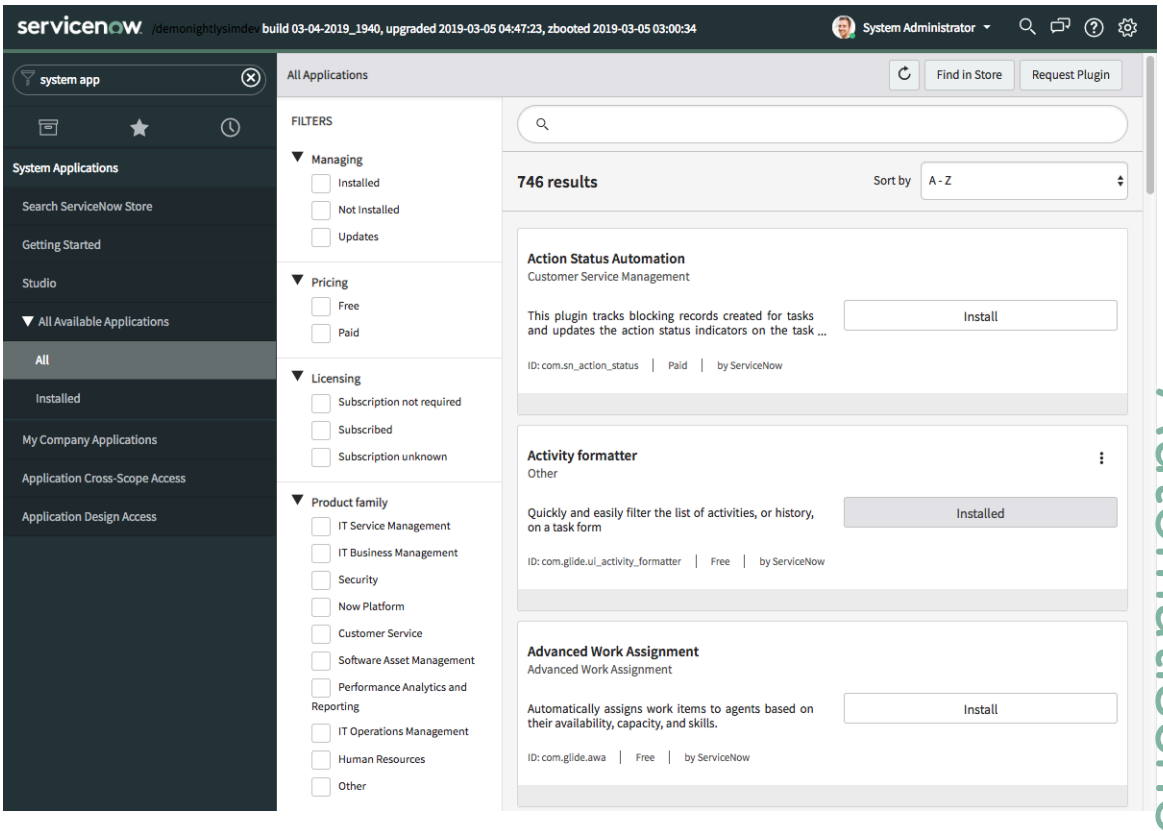
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.




2. Suchen Sie nach der Anwendung, die Sie aktualisieren möchten.
3. Wählen Sie die Version aus, auf die Sie upgraden möchten, und klicken Sie auf **Aktualisieren**.
   Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

## Aktualisieren Sie Ihre Instanz auf den nächsten Familien-Release

Wenn Sie derzeit einen Familien-Release (z. B. London) ausführen und auf den nächsten Release upgraden möchten, ist es nicht erforderlich, die Anwendungen von ServiceNow Storezu erwerben. Die Anwendung wird automatisch aktualisiert, wenn die Plattform auf die mindestens erforderliche Version aktualisiert wird.

### Vorbereitungen

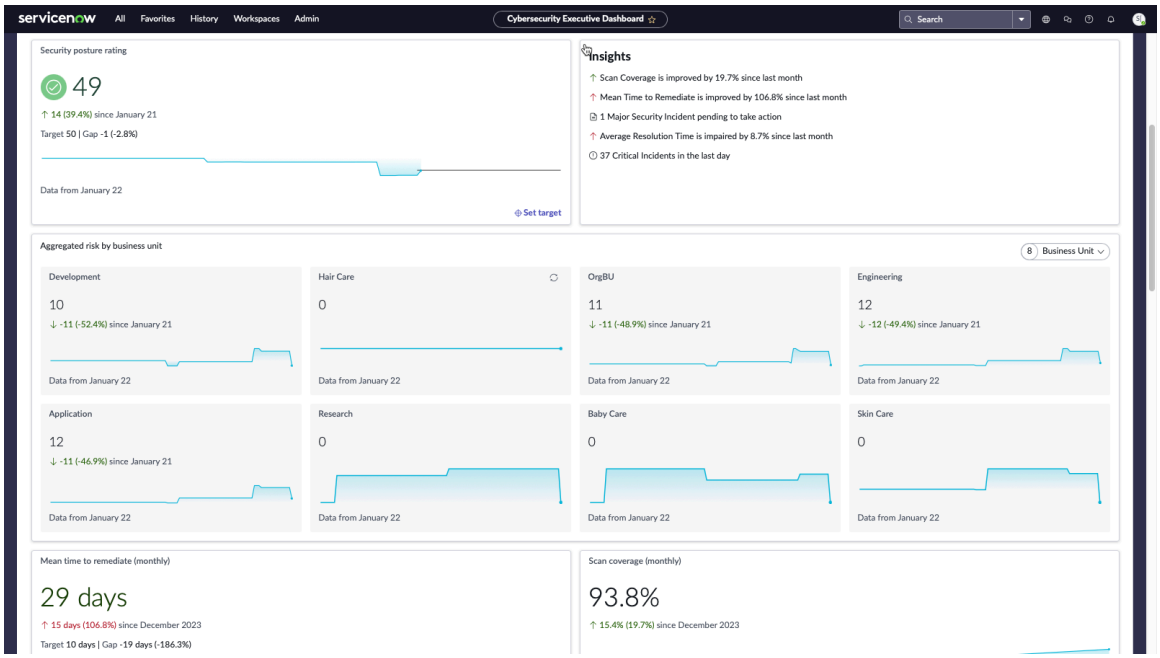
Erforderliche Rolle: admin

# Cybersicherheits-Dashboard für Führungskräfte

Das Cybersecurity Executive Dashboard ist eine umfassende Lösung, die Chief Information Security Officers (CISOs) und Führungskräften im Bereich Cybersicherheit Einblick in die Sicherheitslage und -initiativen der Organisation gibt. Das Dashboard konsolidiert Daten aus verschiedenen Produkten innerhalb der ServiceNow Security Operations-Suite.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Dashboard bietet die folgenden Funktionen:

- Organisationsweite Bewertung der Sicherheitslage
- Risikobewertungen nach Geschäftsbereich
- Anpassbare Überwachung
- Einheitliche Ansicht der Sicherheitslandschaft einer Organisation
- Benchmarking
- Benutzerfreundliche Schnittstelle
- Einblick in Phishing-Simulationsmetriken von KnowBe4 und Microsoft Defender für Office 365

Diese Funktionen ermöglichen eine proaktive Entscheidungsfindung durch schnellen Zugriff auf kritische Sicherheitsmetriken. Dies macht sie zu einem unentbehrlichen Tool für die Verbesserung der allgemeinen Sicherheitsresilienz und -bereitschaft.

## Erforderliche Now Platform-Rollen

- sn_bod.ciso, um das Dashboard anzuzeigen und freizugeben.
- sn_bod.ciso_admin, um das Dashboard anzuzeigen, freizugeben und Gewichtungen für die Bewertung der Sicherheitslage zu konfigurieren.

## Greifen Sie auf das Cybersicherheits-Dashboard für Führungskräfte zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cybersicherheits-Dashboard für Führungskräfte** > **Cybersicherheits-Dashboard für Führungskräfte**.

## Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwender | Dashboard-Verwendung |
| --- | --- |
| Chief Information Security Officers (CISOs) | CISOs erhalten Einblicke in Schwachstellenmanagement, Incident-Management, Sicherheitslage der Organisation, Phishing-Simulationsmetriken usw. für ihre Organisationen. |

## Indikatoren

**Host-SLA – Geschlossen**

Dieser Indikator wird täglich berechnet. Dabei werden alle Host-Schwachstellen berücksichtigt, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Container-SLA – Geschlossen**

Dieser Indikator wird täglich berechnet. Dabei werden alle Container-Schwachstellen berücksichtigt, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Anwendungs-SLA – Geschlossen**

Dieser Indikator wird täglich berechnet. Dabei werden alle Anwendungsschwachstellen berücksichtigt, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Testergebnis-SLA – Bestanden**

Dieser Indikator wird täglich berechnet. Es berücksichtigt alle Testergebnis-Schwachstellen, die zum Zeitpunkt der Berechnung übergeben werden.

**Host-SLA – Anzahl geschlossener**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Host-Schwachstellen, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Container-SLA – Anzahl geschlossener**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Container-Schwachstellen, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Anwendungs-SLA – Anzahl geschlossener**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Anwendungsschwachstellen, die zum Zeitpunkt der Berechnung geschlossen wurden.

**Testergebnis-SLA – Anzahl bestandener**

Dieser Indikator wird täglich gemessen. Berücksichtigt die Anzahl aller Testergebnis-Schwachstellen, die zum Zeitpunkt der Berechnung übergeben wurden.

**Gescannte Assets**

Dieser Indikator wird täglich berechnet. Dabei wird die Summe der Datenquellen-Assets (Scan-Abdeckung) zum Zeitpunkt der Berechnung berücksichtigt.

**Scannbare Assets**

Dieser Indikator wird täglich berechnet. Berücksichtigt wird die Summe der Datenquellen-Assets (Scan-Abdeckung), bei denen das scannbare Element zum Zeitpunkt der Berechnung keines ist.

**Angreifbare Elemente**

Dieser Indikator wird täglich berechnet. Berücksichtigt die aktiven angreifbaren Elemente zum Zeitpunkt der Berechnung.

**Angreifbares Anwendungselement**

Dieser Indikator wird täglich berechnet. Dabei werden die aktiven angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung berücksichtigt.

**Angreifbares Container-Element**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Indikator wird täglich berechnet. Dabei werden die aktiven angreifbaren Containerelemente zum Zeitpunkt der Berechnung berücksichtigt.

**Summiertes Alter der angreifbaren Elemente**

Dieser Indikator wird täglich berechnet. Berücksichtigt das aktive Gesamtalter angreifbarer Elemente zum Zeitpunkt der Berechnung.

**Summiertes Alter der angreifbaren Anwendungselemente**

Dieser Indikator wird täglich berechnet. Dabei wird das aktive Gesamtalter der angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung berücksichtigt.

**Offene angreifbare Elemente**

Dieser Indikator wird täglich berechnet. Sie berücksichtigt die offenen angreifbaren Elemente zum Zeitpunkt der Berechnung.

**Offene angreifbare Container-Elemente**

Dieser Indikator wird täglich berechnet. Sie berücksichtigt die offenen angreifbaren Containerelemente zum Zeitpunkt der Berechnung.

**Offene angreifbare Anwendungselemente**

Dieser Indikator wird täglich berechnet. Dabei werden die offenen angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung berücksichtigt.

**Zurückgestellte VITs**

Dieser Indikator wird täglich berechnet. Es verfügt über eine Indikatorquelle als angreifbares Host-Element.

**Zurückgestellte AVITs**

Dieser Indikator wird täglich berechnet. Sie verfügt über eine Indikatorquelle als angreifbares Anwendungselement.

**Zurückgestellte CVITs**

Dieser Indikator wird täglich berechnet. Es verfügt über eine Indikatorquelle als angreifbares Containerelement.

**Warten auf Implementierung – aktive AEs**

Dieser Indikator wird täglich berechnet. Dabei werden die angreifbaren Elemente mit dem Status „Warten auf Implementierung“ zum Zeitpunkt der Berechnung berücksichtigt.

**Offene Konfigurationsprobleme – Testergebnisse**

Dieser Indikator wird täglich berechnet. Sie verfügt über eine Indikatorquelle als Testergebnis für das Unified Vulnerability Response Dashboard.

**SI – Durchschnittliche Zeit für Identifizierung**

Dieser Indikator wird täglich berechnet. Es berücksichtigt den Security Incident, bei dem die Definition Zeit für die Identifizierung zum Zeitpunkt der Berechnung ist.

**SI – Durchschnittliche Dauer**

Dieser Indikator wird täglich berechnet. Es berücksichtigt den Security Incident, bei dem die Definition eine Incident-Statusdauer zum Zeitpunkt der Berechnung ist.

**Anzahl der offenen schwerwiegenden Security Incidents**

Dieser Indikator wird täglich berechnet. Er berücksichtigt offene schwerwiegende Security Incidents zum Zeitpunkt der Berechnung.

**Anzahl der geschlossenen Security Incidents**

Dieser Indikator wird täglich berechnet. Dabei werden geschlossene Security Incidents zum Zeitpunkt der Berechnung berücksichtigt.

**Geschlossene angreifbare Anwendungselemente**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Indikator wird täglich berechnet. Dabei werden zum Zeitpunkt der Berechnung geschlossene angreifbare Anwendungselemente berücksichtigt.

**Geschlossene angreifbare Container-Elemente**

Dieser Indikator wird täglich berechnet. Dabei werden geschlossene angreifbare Containerelemente zum Zeitpunkt der Berechnung berücksichtigt.

**Geschlossene angreifbare Elemente**

Dieser Indikator wird täglich berechnet. Dabei werden geschlossene angreifbare Elemente zum Zeitpunkt der Berechnung berücksichtigt.

**Maximale Risikopunktzahl für angreifbares Elemente abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Elemente zum Zeitpunkt der Berechnung.

**Maximale Risikopunktzahl für angreifbares Container-Element abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Containerelemente zum Zeitpunkt der Berechnung.

**Maximale Risikopunktzahl für angreifbare Anwendungselemente abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Anwendungselemente zum Zeitpunkt der Berechnung.

**Summierte Risikopunktzahl von VITs**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen angreifbarer Elemente zum Zeitpunkt der Berechnung.

**Summierte Risikopunktzahl von AVIs**

Dieser Indikator wird täglich berechnet. Dabei wird die Summe der Risikopunktzahlen von angreifbaren Anwendungselementen zum Zeitpunkt der Berechnung berücksichtigt.

**Summierte Risikopunktzahl von CVIs**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von angreifbaren Containerelementen zum Zeitpunkt der Berechnung.

**Maximale Risikopunktzahl für SI-Incidents abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikowerte von Security Incidents zum Zeitpunkt der Berechnung.

**Max. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikowerte für eine Fehlkonfiguration der Testergebnisse zum Zeitpunkt der Berechnung.

**Durchschn. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen**

Dieser Indikator wird täglich berechnet. Berücksichtigt die durchschnittlichen Risikopunktzahlen für eine Fehlkonfiguration der Testergebnisse zum Zeitpunkt der Berechnung.

**Anzahl der offenen Security Incidents**

Dieser Indikator wird täglich berechnet. Dabei werden offene Security Incidents zum Zeitpunkt der Berechnung berücksichtigt.

**Phishing-Übersicht**

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der Sicherheitssimulationsmetriken zum Zeitpunkt der Berechnung.

**Aggregierte MTTR**

Berechnet die durchschnittliche Zeit, die zum Schließen von Schwachstellen (Hosts, Container und Anwendungen) benötigt wurde, und die Zeit zum Schließen der Testergebnisse in Tagen. [[Host-SLA – Geschlossen]] + [[Anwendungs-SLA – Geschlossen]] + [[Container-SLA –



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geschlossen]] + [[Testergebnis-SLA – Bestanden]]) / ([[Host-SLA – Anzahl geschlossener]] + [ [Anwendungs-SLA – Anzahl geschlossener Elemente]] + [[Testergebnis-SLA – Anzahl bestandener Elemente]] + [[Container-SLA – Anzahl geschlossener Elemente]])

**Aktuelle Scan-Abdeckung**

Berechnet die Scan-Abdeckung in Prozent anhand des Verhältnisses zwischen der Anzahl der monatlich gescannten Elemente und der Gesamtzahl der Elemente, die im selben Zeitraum gescannt werden können. var monatlichScannedItems = [[Gescannte Assets / Pro Monat - Durchschnitt +]]; var monatlichScannableItems = [[Scannbare Assets / Pro Monat - Durchschnitt +]]; var res; if (monthlyScannedItems == 0) res = 0; Else res = monthScannedItems / monthScannableItems * 100; if (res > 100) res = 100; res;

**Durchschnittliches Alter aktiver angreifbarer Elemente**

Berechnet das Durchschnittsalter aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen) in Tagen. ([[Summiertes Alter der angreifbaren Elemente]] + [[Summiertes Alter der angreifbaren Anwendungselemente]] + [[Summiertes Alter der angreifbaren Container-Elemente]]) / ([[Angreifbare Elemente]] + [[Angreifbare Anwendungselemente]] + [[Angreifbare Container-Elemente]])

**Aktive VITs nach Alter und Risikobewertung**

Berechnet die Gesamtanzahl aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen), kategorisiert nach Alter und Ebene der Risikobewertung. [[Offene angreifbare Elemente]] + [[Offene angreifbare Container-Elemente]] + [[Offene angreifbare Anwendungselemente]]

**Zurückgestellte angreifbare Elemente**

Berechnet die Gesamtanzahl aller angreifbaren Elemente (Hosts, Container und Anwendungen) mit dem Status „Zurückgestellt“. [[Zurückgestellte VITs]] + [[Zurückgestellte AVITs]] + [[Zurückgestellte CVITs]]

**Durchschnittliche Lösungszeit der geschlossenen Security Incidents**

Berechnet die durchschnittliche Zeit in Tagen, die zum Schließen der Security Incidents benötigt wurde. ([[Summierte Dauer der geschlossenen Security Incidents]] / [[Anzahl der geschlossenen Security Incidents]]) /24

**Sicherheitslagenbewertung**

Berechnet täglich die Gesamtsicherheitsbewertungen. Die Berechnung erfolgt basierend auf der zusammengefassten Risikopunktzahl. varsecPostureRating = 100 – [[Rollup-Risikopunktzahl]]; sekPostureRating;

**Rollup-Risikopunktzahl.**

Berechnet die endgültige Rollup-Risikopunktzahl, bei der die Rollup-Risikopunktzahl von angreifbaren Elementen, Fehlkonfigurationen, Security Incidents und schwerwiegenden Security Incidents mit den jeweiligen Gewichtungen multipliziert wird, die aus der Rollup-Tabelle für die Sicherheitslage abgerufen werden. var numMajorIncidents = [[Anzahl offener schwerwiegender Security Incidents]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; sonst majorSIRiskScore = 0; rollUpRiskScore = ([[Rollup-Risikopunktzahl für Schwachstelle]] * 20 + [[Rollup-Risikopunktzahl für Fehlkonfiguration]] * 20 + [[Max. Risikopunktzahl für SI-Incidents abrufen]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

**Schwachstellen-Rollup-Risikopunktzahl**

Berechnet die zusammengefasste Risikopunktzahl der Schwachstelle, wobei die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl angreifbarer Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. var maxRiskScore = 100; var count = [[Aktive VITs nach Alter und Risikobewertung]]; var countRiskScore; if (0 == count) countRiskScore = 0; Else if (Anzahl > 10.000) countRiskScore = maxRiskScore; Else if (count > 1000) countRiskScore = (maxRiskScore



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

* 0,80); Else if (count > 100) countRiskScore = (maxRiskScore * 0.60); Else if (count > 10) countRiskScore = (maxRiskScore * 0,40); sonst countRiskScore = (maxRiskScore * 0,20); var vulRiskScore = ([[Max. Punktzahl aus allen angreifbaren Elementen abrufen]] * 0 + [[Durchschnittliche Risikopunktzahl aller angreifbaren Elemente]] * 100 + countRiskScore * 0)/100; angreiferRiskScore;

**Maximale Punktzahl aus allen angreifbaren Elementen abrufen**

Berechnet die zusammengefasste Risikopunktzahl der Schwachstelle, wobei die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl angreifbarer Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. var maxScoreForVI = [[Max. Risikopunktzahl für angreifbare Elemente abrufen]], maxScoreForCVI = [[Max. Risikopunktzahl für angreifbares Container-Element abrufen]], maxScoreForAVI = [[Max. Risikopunktzahl für angreifbare Anwendungselemente abrufen]], maxScore; if (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; Else if (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI ) maxScore = maxScoreForCVI; sonst maxScore = maxScoreForAVI; maxScore;

**Durchschnittliche Risikopunktzahlen aller angreifbaren Elemente**

Berechnet die durchschnittliche Risikopunktzahl aller angreifbaren Elemente (Hosts, Container und Anwendungen). var summedRiskScore = [[Summierte Risikopunktzahl von VITs]] + [[Summierte Risikopunktzahl von AVIs]] + [[Summierte Risikopunktzahl von CVIs]], avgRiskScore; var totalVulCount = [[Offene angreifbare Elemente]] + [[Offene angreifbare Anwendungselemente]] + [[Offene angreifbare Container-Elemente]]; if(summedRiskScore == 0) avgRiskScore = 0; Else if(totalVulCount .=0 ) avgRiskScore = summedRiskScore / totalVulCount; avgRiskScore;

**Fehlkonfiguration – Rollup-Risikopunktzahl**

Berechnet die zusammengefasste Risikopunktzahl der Fehlkonfiguration anhand der Testergebnisse, die als Fehlgeschlagen, Fehler oder Unbekannt kategorisiert sind. var maxRiskScore = 100; var count = [[Offene Konfigurationsprobleme – Testergebnisse]]; var countRiskScore; if (0 == count) countRiskScore = 0; Else if (Anzahl > 10.000) countRiskScore = maxRiskScore; Else if (count > 1000) countRiskScore = (maxRiskScore * 0,80); Else if (count > 100) countRiskScore = (maxRiskScore * 0.60); Else if (count > 10) countRiskScore = (maxRiskScore * 0,40); sonst countRiskScore = (maxRiskScore * 0,20); var missRiskScore = ([[Max. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen]] * 0 + [[Durchschnittliche Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen]] * 100 + countRiskScore * 0)/100; falschRiskScore;

**Durchschnittliche Zeit bis Beseitigung**

Berechnet die durchschnittliche Zeit bis zur Beseitigung von Security Incidents in Tagen [[SI – Durchschnittliche Dauer > Security Incident-Status = Beseitigen]] / 1440

**Durchschnittliche Zeit für Identifizierung**

Berechnet die durchschnittliche Zeit in Tagen, die für die Identifizierung von Security Incidents benötigt wurde. [[SI – Durchschnittliche Zeit für Identifizierung]] / 1440

**Durchschnittliche Zeit bis zur Eindämmung**

Berechnet die durchschnittliche Zeit in Tagen, die für die Eindämmung von Security Incidents benötigt wurde. [[SI – Durchschnittliche Dauer > Security Incident-Status = Eindämmen]] / 1440

**Einhaltung des Korrekturziels**

Berechnet den monatlichen Prozentsatz der Einhaltung des Korrekturziels aus Testergebnissen, angreifbaren Elementen, angreifbaren Containerelementen und angreifbaren Anwendungselementen. Die Zieleinhaltung wird durch die Anzahl der Elemente bestimmt, die das festgelegte Ziel erfüllt haben. ([[Geschlossene Testergebnisse > Status des Korrekturziels (geschlossen) = Ziel erfüllt]] + [[Geschlossene angreifbare Container-Elemente > Status des Korrekturziels (geschlossen) = Ziel erfüllt]] + [[Geschlossene angreifbare Anwendungselemente



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> Status des Korrekturziels (geschlossen). ) = Ziel erfüllt]] + [[Geschlossenes angreifbares Element > Status des Korrekturziels (Geschlossen) = Ziel erfüllt]]) / ([[Geschlossene Testergebnisse]] + [[Geschlossene angreifbare Container-Elemente]] + [[Geschlossene angreifbare Anwendungselemente ]] + [[Geschlossenes angreifbares Element]]) * 100;

**Effizienz der monatlichen Fehlerbehebung (alle angreifbaren Elemente)**

Berechnet den monatlichen Prozentsatz geschlossener angreifbarer Elemente, angreifbarer Container-Elemente und angreifbarer Anwendungselemente im Gegensatz zu neu identifizierten Elementen. var monatlichClosedItems = [[Geschlossene angreifbare Elemente / Pro Monat SUM +]] + [[Geschlossene angreifbare Container-Elemente / Pro Monat SUM +]] + [[Geschlossene angreifbare Anwendungselemente / Pro Monat SUM +]]; var monthsNewItems = [[Angreifbare Elemente / Pro Monat SUM +]] + [[Angreifbare Container-Elemente / Pro Monat SUM +]] + [[Angreifbare Anwendungselemente / Pro Monat SUM +]], res; if (monthlyClosedItems == 0) res = 0; Else if (monthlyNewItems .=0) res = monthClosedItems / monthsNewItems * 100; if (res > 1000) res = 1000; res;

## BreakdownsAufgliederungen

- Geschäftsbereich
- Risikobewertung
- Altersbereich
- Zuweisungsgruppe (einheitlich)
- Nachbesserungszielstatus (geschlossen)
- Asset-Klasse
- Asset-Kategorie
- Risikobewertung (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Status des Security Incidents
- Priorität von Security Incident
- Kategorie von Security Incident
- Phishing-Event

## Datenvisualisierung

| Metriken | Typ | Beschreibung |
|---|---|---|
| Ziele | Anzeige | Zeigt das festgelegte Ziel an, das für eine Metrik abgedeckt werden soll.<br><br>Weitere Informationen finden Sie unter Legen Sie Ziele fest. |
| Bewertung der Sicherheitslage | Einzelne Punktzahl | Gesamtpunktzahl der Sicherheitslage der Organisation unter Berücksichtigung von angreifbaren Elementen, Security Incidents, schwerwiegenden |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| | | Security Incidents und Fehlkonfigurationen. |
| Einblicke | Hervorhebungen | Highlights des gesamten Dashboards. |
| Zusammengefasstes Risiko nach Geschäftsbereich | Einzelne Punktzahl | Konsolidiertes Risiko für jeden Geschäftsbereich unter Berücksichtigung von angreifbaren Elementen, Security Incidents, schwerwiegenden Security Incidents und Fehlkonfigurationen im Zusammenhang mit dem Geschäftsbereich.<br><br>Sie können die Informationen für maximal 10 Geschäftsbereiche anzeigen.<br><br>Die Punktzahlen werden basierend auf dem Sicherheitslage-Rollup berechnet. Navigieren zu **Alle** > **Cybersicherheits-Dashboard für Führungskräfte** > **Sicherheitslage-Rollups** , um die Gewichtung für jede Kategorie anzuzeigen.<br><br>Die Berechnung der Bewertung der Sicherheitslage erfolgt wie folgt:<br><br>Bewertung der Sicherheitslage = 100 – Aggregierte Risikopunktzahl.<br><br>Die Punktzahl des aggregierten Risikos wird anhand des gewichteten Durchschnitts der folgenden Komponenten bestimmt:<br>• Die zusammengefasste Risikopunktzahl aller aktiven angreifbaren Elemente (RVIT).<br>• Die zusammengefasste Risikopunktzahl aller aktiven Konfigurationstestergebnisse (RCTR). |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| | | • Die maximale Risikopunktzahl unter allen aktiven Security Incidents (RSI).<br>• Wenn mindestens ein schwerwiegender Security Incident aktiv ist, wird RMSI auf 100 festgelegt. Wenn kein schwerwiegender Security Incident aktiv ist, wird der RMSI auf 0 (RMSI) festgelegt.<br><br>Weitere Informationen zur Rollup-Berechnung für angreifbare Elemente und Fehlkonfigurationen finden Sie unter Vulnerability Response Rollup-Rechner. |
| Schwachstellen | Einzelne Punktzahl | Zusammengefasstes Risiko für einen bestimmten Geschäftsbereich, wobei nur die angreifbaren Elemente berücksichtigt werden. |
| Falsche Konfigurationen | Einzelne Punktzahl | Zusammengefasstes Risiko für einen bestimmten Geschäftsbereich, wobei nur Fehlkonfigurationen berücksichtigt werden. |
| Security Incidents | Einzelne Punktzahl | Zusammengefasstes Risiko für einen bestimmten Geschäftsbereich, wobei nur Security Incidents berücksichtigt werden. |
| Schwerwiegende Security Incidents | Einzelne Punktzahl | Zusammengefasstes Risiko für einen bestimmten Geschäftsbereich, wobei nur schwerwiegende Security Incidents berücksichtigt werden. |
| Durchschnittliche Zeit bis zur Fehlerkorrektur (monatlich) | Einzelne Punktzahl | Durchschnittliche Zeit bis zur Schließung von Schwachstellen und fehlgeschlagenen Testergebnissen für alle |

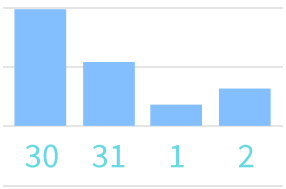
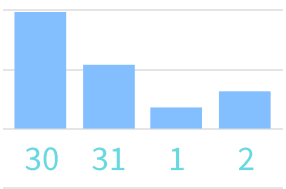
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
| --- | --- | --- |
| | | Assets (Hosts, Container und Anwendungen) in einem Monat.<br><br>Außerdem werden die folgenden Metriken bereitgestellt:<br>• Prozentuale Änderung gegenüber dem Vormonat.<br>• Ziel: Ziel in Tagen, um die Schwachstellen zu beheben.<br>• Abstand: Differenz in Tagen zwischen dem Ziel und der tatsächlichen Zeit, die für die Korrektur der Schwachstellen benötigt wurde.<br>• Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche.<br>• Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt<br><br>Informationen zum Anzeigen der Benchmark-Punktzahlen finden Sie unter Wählen Sie Benchmark-Punktzahlen aus. |
| Durchschnittliches Alter aktiver Schwachstellen (monatlich) | Einzelne Punktzahl | Monatliches Durchschnittsalter aller drei Arten von angreifbaren Elementen. Sie bietet auch einen Vergleich des aktuellen Monatsalters mit dem vorherigen Monat.<br><br>Außerdem werden die folgenden Metriken bereitgestellt:<br>• Prozentuale Änderung gegenüber dem Vormonat.<br>• Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. |

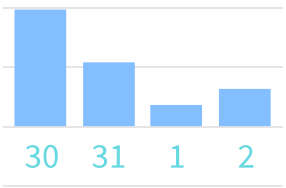


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| | | • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt |
| Schwachstellen nach Risikobewertung und Alter | Heatmap | Aufgliederung der aktiven Schwachstellen für Hosts, Container und Anwendungen nach Risikobewertung und Alter. |
| Einhaltung des Korrekturziels nach Zuweisungsgruppe | Vertikaler   | Verhältnis der Summe der geschlossenen VITs, AVITs, CVITs und Testergebnisse, bei denen der Zielstatus „Ziel erfüllt“ ist, zur Summe der geschlossenen VITs, AVITs, CVITs und Testergebnisse. |
| Scan-Abdeckung (monatlich) | Einzelne Punktzahl | Prozentsatz der monatlich gescannten Assets von allen Assets. Sie bietet auch einen Vergleich des aktuellen Monatsprozentsatzes mit dem vorherigen Monat.<br>Außerdem werden die folgenden Metriken bereitgestellt:<br>• Prozentuale Änderung gegenüber dem Vormonat.<br>• Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche.<br>• Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt |
| Gescannte im Vgl. zu CMDB Assets | Vertikaler   | Monatliche Anzahl der gescannten und Configuration Management Database (CMDB) Assets nach CI-Klassen. |

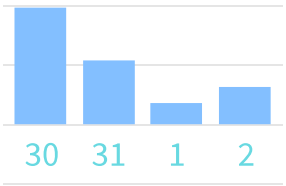


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| Schwachstellen nach Risikobewertung und Alter | Heatmap | Anzahl der offenen angreifbaren Elemente, angreifbaren Containerelemente und angreifbaren Anwendungselemente, kategorisiert nach Risikobewertung und Alter. |
| Schwachstellen nach Asset-Kategorie und Risikobewertung | Vertikaler   | Anzahl der offenen angreifbaren Elemente, angreifbaren Containerelemente und angreifbaren Anwendungselemente, kategorisiert nach Asset-Kategorie und Risikobewertung (kritisch, hoch und mittel). |
| Durchschnittliches Alter aktiver Schwachstellen (monatlich) | Einzelne Punktzahl | Monatliches Durchschnittsalter aller drei Arten von angreifbaren Elementen. Sie bietet auch einen Vergleich des aktuellen Monatsalters mit dem vorherigen Monat. |
| Trend für aktive kritische und Schwachstellen mit hoher Anfälligkeit | | Täglicher Trend der Anzahl der angreifbaren Elemente, angreifbaren Container-Elemente und angreifbaren Anwendungselemente mit kritischer und hoher Risikobewertung. |
| Trend aktiver kritischer und hoher Fehlkonfigurationen | | Täglicher Trend der Fehlkonfigurationen mit den Risikobewertungen „Kritisch“ und „Hoch“. |
| Effizienz der Fehlerbehebung (monatlich) | Einzelne Punktzahl | Prozentsatz der monatlich geschlossenen angreifbaren Elemente im Vergleich zu monatlich aktiven angreifbaren Elementen.<br><br>Außerdem werden die folgenden Metriken bereitgestellt:<br>• Prozentuale Änderung gegenüber dem Vormonat.<br>• Ziel: Ziel in Prozent für die Behebung der Schwachstellen. |

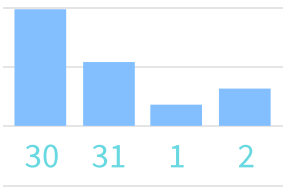
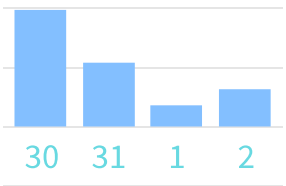


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| | | • Abstand: Abstand zwischen Ziel und aktueller Punktzahl.<br>• Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche.<br>• Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt |
| Nach Grund und Zuweisungsgruppe zurückgestellt | Vertikaler   | Anzahl der angreifbaren Elemente, angreifbaren Container-Elemente und angreifbaren Anwendungselemente, die sich im Status „Zurückgestellt“ befinden. Sie werden nach Grund und Zuweisungsgruppe kategorisiert. |
| Schwerwiegende Security Incidents | Einzelne Punktzahl | Anzahl der offenen schwerwiegenden Security Incidents |
| Durchschnittliche Lösungszeit für Security Incidents (monatlich) | Einzelne Punktzahl | Monatliche durchschnittliche Lösungszeit geschlossener Security Incidents in Tagen<br>Außerdem werden die folgenden Metriken bereitgestellt:<br>• Prozentuale Änderung gegenüber dem Vormonat.<br>• Ziel: Ziel in Tagen, um die Schwachstellen zu beheben.<br>• Abstand: Der Abstand zwischen den tatsächlichen Tagen, die für die Lösung benötigt wurden, und dem für die Korrektur festgelegten Ziel.<br>• Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Metriken | Typ | Beschreibung |
|---|---|---|
| | | • Globale Benchmark: Durchschnitt der Metriken der Peers im globalen Markt |
| Durchschnittliche Zeit bis Beseitigung (monatlich) | Einzelne Punktzahl | Monatliche durchschnittliche Lösung in Tagen zur Beseitigung von Security Incidents. |
| Durchschnittliche Zeit für Identifizierung (monatlich) | Einzelne Punktzahl | Monatliche durchschnittliche Lösung in Tagen zur Identifizierung von Security Incidents. |
| Durchschnittliche Zeit bis zur Eindämmung (monatlich) | Einzelne Punktzahl | Monatliche durchschnittliche Lösung in Tagen zur Eindämmung von Security Incidents. |
| Aktive Incidents nach Priorität und Kategorie | Heatmap | Anzahl der aktiven Security Incidents, kategorisiert nach Priorität und Kategorie |
| Trend geschlossener und offener Incidents | | Monatlicher Trend der Anzahl der geschlossenen und geöffneten Security Incidents. |
| Aktive Incidents nach Status | Vertikaler   | Anzahl der aktiven Security Incidents für jeden Status. |
| Übersicht über die monatliche Phishing-Simulation (KnowBe4) | Vertikaler   | Summe der Benutzer, die Aktionen wie Öffnen, Auswählen und Melden in der Phishing-Simulation ausgeführt haben, zusammen mit der Summe der Gesamtbenutzer jeder Simulation für den vorherigen Monat. |

## Zu installierende Anwendungen

Sie müssen die folgenden Anwendungen installieren, um die Punktzahl in die Widgets auszufüllen. Je nachdem, welche Anwendung Sie verwenden, müssen Sie möglicherweise die abhängigen Anwendungen installieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wenn Sie verwenden | Installieren |
|---|---|
| Vulnerability Response | • Performance Analytics for Vulnerability Response<br>• Vulnerability Response – Allgemein<br>• Vulnerability Response<br>• Vulnerability Response und Configuration Compliance für Container<br>• Configuration Compliance |
| Phishing-Integrationen | • Security Simulation and Training Integration for SecOps<br>• KnowBe4-Integration für SecOps<br>• Microsoft Defender für Office365-Integration für SecOps |
| Security Incident Response | • Performance Analytics for Security Incident Response<br>• Security Incident Response<br>• Management schwerwiegender Sicherheits-Incidents |

### Geplante Aufgaben für die Datenerfassung

Die folgenden geplanten Aufgaben werden ausgeführt, um automatisch Punktzahlen für neue Daten zu sammeln.

| Regelmäßige Aufgabe | Häufigkeit | Beschreibung |
|---|---|---|
| Benchmark-Punktzahlen hochladen | Bei Bedarf | Sammelt Punktzahlen von der Instanz und veröffentlicht sie in der zentralen Instanz. Die Benchmark-Algorithmen berechnen die besten Punktzahlen der Branche. |
| Benchmark-Punktzahlen herunterladen | Bei Bedarf | Lädt die Benchmark-Punktzahlen herunter. Sie ist in der Tabelle „Benchmark-Punktzahlen“ [sn_bm_client_score_list] verfügbar. |

## Wählen Sie Benchmark-Punktzahlen aus

Rufen Sie Benchmark-Punktzahlen ab, indem Sie Ihre Instanz bei der zentralen Instanz von ServiceNow registrieren. Letztere verwaltet Informationen aus mehreren Branchen, um die Benchmark-Punktzahl bereitzustellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: admin

### Prozedur

1. Führen Sie die folgenden Schritte aus, um Ihre Instanz bei der Zentralinstanz zu registrieren:

   a. Navigieren zu **Alle** > **Systemeigenschaften**

   b. Wählen Sie die Systemeigenschaft *sn_bm_client.central_instance_url*.

   c. Geben Sie im Feld **Wert** die URL der zentralen Benchmark-Instanz ein.

   **Hinweis:**
   Wenn die Instanz bereitgestellt wird, werden Ihre Details automatisch an die zentrale Instanz übertragen.

   d. Wählen Sie im Widget die Option **Opt-in** aus, um zu validieren und eine Verbindung mit der zentralen Instanz herzustellen.

2. Führen Sie die folgenden Schritte aus, um Ihre Punktzahl in die zentrale Instanz hochzuladen:

   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**

   b. Wählen Sie die geplante Aufgabe *Upload the benchmark scores* aus.

   c. Wählen Sie **Aktualisieren**.
   Die Punktzahlen werden in die zentrale Instanz hochgeladen. Die geplanten Aufgaben der Zentralinstanz werden jedoch einmal im Monat ausgeführt, um die Punktzahlen in den Dashboard-Widgets zu aktualisieren.

3. Führen Sie die folgenden Schritte aus, um die Punktzahl aus der Zentralinstanz herunterzuladen:

   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**

   b. Wählen Sie die geplante Aufgabe *Download the benchmark scores* aus.

   c. Wählen Sie **Jetzt ausführen**.
   Die Punktzahlen sind in der Tabelle „Benchmark-Punktzahlen“ [sn_bm_client_score_list] verfügbar, die sich in den Dashboard-Widgets widerspiegelt.

## Legen Sie Ziele fest

Legen Sie Ziele in Tagen fest, um die Schwachstellen, Security Incidents und Fehlkonfigurationen zu beheben.

### Vorbereitungen
Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wählen Sie im Widget **Set target** (Ziel festlegen) aus.
2. Klicken Sie auf der Seite „KPI-Details“ auf das Symbol **Ziele**.
3. Aktivieren Sie das Kontrollkästchen **Für alle**.
4. Geben Sie im Feld **Ziel** die Anzahl der Tage ein, in denen Sie das Ziel erreichen möchten.
5. Wählen Sie das Zielstartdatum aus.
6. Wählen Sie das Zielreviewdatum aus.
7. Wählen Sie **Aktualisieren**.

## Security Simulation and Training Integration for Security Operations

Stärken Sie die Abwehr Ihres Unternehmens gegen wichtige Cybersicherheitsbedrohungen, indem Sie Phishing-Integrationen in das Cybersicherheits-Dashboard für Führungskräfte integrieren. Die Phishing-Integrationen verbessern das Cybersicherheits-Dashboard für Führungskräfte durch die nahtlose Einbindung von Daten aus Phishing-Simulationstools von Drittanbietern wie KnowBe4 und Microsoft Defender für Office 365.

Die folgenden Integrationen erweitern die Fähigkeiten des Cybersicherheits-Dashboards für Führungskräfte und bieten eine einheitliche Perspektive auf die Sicherheitslage Ihres Unternehmens, die Bereitschaft der Mitarbeiter und die Anfälligkeit für Phishing-Angriffe:

- KnowBe4-Integration
- Microsoft Defender für Office 365-Integration

### Konfigurieren Sie die Knowbe4-Integration

Erhalten Sie durch die Integration mit KnowBe4, einer führenden Schulungsplattform für Cybersicherheitsbewusstsein, sofortige Einblicke in die Anfälligkeit Ihrer Mitarbeiter für Phishing-Angriffe. Identifizieren Sie durch die KnowBe4-Integration Trends und Verbesserungsbereiche in Ihren Schulungsprogrammen für Cybersicherheit, überwachen Sie die allgemeine Phishing-Resilienz und stärken Sie proaktiv die Sicherheitsmaßnahmen Ihres Unternehmens.

#### Vorbereitungen

Erforderliche Rolle: sn_sec_phish.admin und sn_sec_phish_kb4.kb4_admin

#### Prozedur

1. Navigieren zu **Alle** > **KnowBe4-Integration** > **KnowBe4-Konfigurationen**.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Details aus:

**Formular „KnowBe4-Konfiguration“.**

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz mithilfe des Suchsymbols aus. |
| Basis-URL | URL für die Integration mit KnowBe4. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| API-Schlüssel | API-Schlüssel, der vom KnowBe4-Konto abgerufen wurde. |
| Seite | Seitenzahl, von der Simulationen abgerufen werden sollen. |
| Seitengröße | Anzahl der Simulationen, die enthalten sein sollen. |

**a.** Wählen Sie **Neu** aus, wenn keine Integrationsinstanz verfügbar ist.

**b.** Füllen Sie im Formular die folgenden Details aus:

**Formular „Integrationsinstanz".**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Integrationsinstanz. |
| Anwendung | Name der Anwendung (KnowBe4 Integration for SecOps). |
| Integration | KnowBe4 ist die Standardeinstellung. |
| Aktiv | Der Standardwert ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv. |
| Beschreibung | Kurzbeschreibung der Integrationsinstanz. |

4. Wählen Sie **Absenden**.
5. Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**.
6. Wählen Sie Knowbe4-Integration aus.
7. Wählen Sie **Jetzt** ausführen aus, um KnowBe4 auszuführen und Daten zu erfassen.

## Konfigurieren Sie Microsoft Defender für die Office 365-Integration

Erhalten Sie durch die nahtlose Integration mit Microsoft Defender für Office 365 wertvolle Einblicke in Phishing-Simulationsmetriken direkt im Cybersicherheits-Dashboard für Führungskräfte.

### Vorbereitungen

Erforderliche Rolle: sn_sec_phish_msatk.ms_admin

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Attack-Integration** > **Microsoft Attack-Konfigurationen**.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Details aus:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Microsoft Attack-Konfiguration“**

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz mithilfe des Suchsymbols aus. |
| Mandanten-ID | Mandanten-ID der im Microsoft Azure-Portal erstellten Anwendung. |
| Client-ID | Client-ID der im Microsoft Azure-Portal erstellten Anwendung. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel der im Microsoft Azure-Portal erstellten Anwendung. |
| Lesezeichen | Datum, ab dem die Simulationen abgerufen werden müssen. |
| Token-URL | Basis-URL, von der aus das Token für den Zugriff auf die Microsoft Simulations-API erstellt wird. |
| Gesamte Simulations-URL | Basis-URL der Microsoft Simulations-API. |

**a.** Wählen Sie **Neu** aus, wenn keine Integrationsinstanz verfügbar ist.

**b.** Füllen Sie im Formular die folgenden Details aus:

**Formular „Integrationsinstanz“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Integrationsinstanz. |
| Anwendung | Name der Anwendung (Microsoft Defender für Office 365). |
| Integration | Drittpartei-Integrationsreferenz (Microsoft Attack-Integration). |
| Aktiv | Der Standardwert ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv. |
| Beschreibung | Kurzbeschreibung der Integrationsinstanz. |

**4.** Wählen Sie **Absenden**.

**5.** Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**.

**6.** Wählen Sie Microsoft Attack-Integration aus.

**7.** Wählen Sie **Jetzt** ausführen aus, um auszuführen und Daten von Microsoft zu erfassen.

## Security Incident Response

Die Anwendung ServiceNow® Security Incident Response verfolgt den Fortschritt von Security Incidents von der Erkennung und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur letzten Überprüfung nach dem Incident, der Erstellung von Knowledge Base-Artikeln und dem Abschluss.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

| | | |
|---|---|---|
| Erkunden<br>• Washington DC<br>• Security Incident Response verstehen<br>• Domain Separation und Security Incident Response<br>• Sicherheits-UI (Video) | Einrichten<br>• Security Incident Response installieren und konfigurieren<br>• Security Incident Response-Prozessdefinition verstehen | Verwalten<br>• Andere zusätzliche Security Incident Response Setup-Aufgaben<br>• Security Incident Response-Berichterstellung |
| Verwenden<br>• Verwaltung von Security Incidents und eingehenden Anforderungen<br>• Verwalten Sie Suchen und Scans<br>• Verwalten von Aktivitäten nach Incidents<br>• Mobile Experience für Security Incident Response | Entwickeln<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden<br>• Security Incident Response Orchestration | Integrieren<br>• Security Incident Response-Integrationen<br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen |
| Problembehandlung und Hilfe<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | | |

Automatische Übersetzung

## Security Operations-Apps im Store anfordern

Wenn Sie ein neuer Security Operations -Kunde mit London Patch 6 oder höher sind, besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten.

# Security Incident Response verstehen

Verwalten Sie mit Security Incident Response (SIR) den Lebenszyklus Ihrer Security Incidents von der ersten Analyse bis hin zu Eindämmung, Beseitigung und Wiederherstellung. Mit Security Incident Response erhalten Sie ein umfassendes Verständnis der von Ihren Analysten durchgeführten Incident-Reaktionsverfahren und verstehen Trends und Engpässe in diesen Verfahren mit analysebasierten Dashboards und Berichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Einführung in Security Incident Response und die ersten Schritte mit der Anwendung.

Sehen Sie sich dieses neunminütige Video an, um mehr über den SIR-Prozess, die Verwendung von Security Incident Response zur Abwehr von Angriffen und die Anzeige von Sicherheitsaktivitäten im Security Incident Response Explorer zu erfahren.

Integrierte Integrationen mit Cybersicherheitslösungen von Drittanbietern und von Partnern entwickelte Integrationen aus dem ServiceNow Store ermöglichen die Sicherheitsautomatisierung und -orchestrierung für eine effiziente und genaue Reaktion auf Incidents.

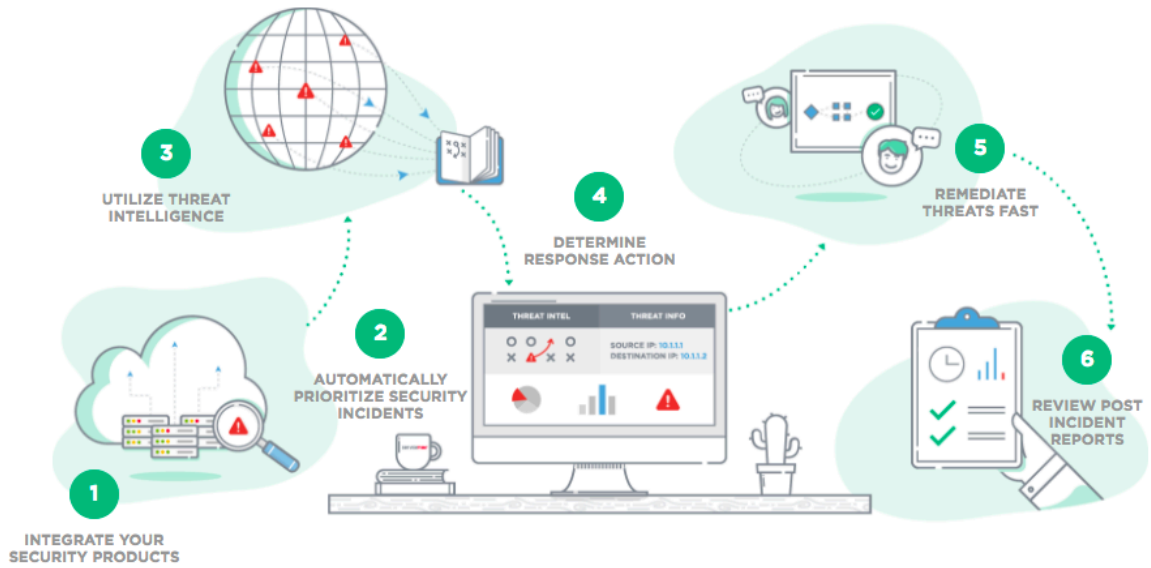
Um Ihre Untersuchungen zu schützen und Security Incidents vertraulich zu behandeln, bietet Security Incident Response die Möglichkeit, den Zugriff auf das System auf bestimmte sicherheitsbezogene Rollen und ACLs zu beschränken. Nicht-Sicherheitsadministratoren können vom Zugriff ausgeschlossen werden, es sei denn, Sie gewähren ihnen ausdrücklich Zutritt.

**Hinweis:**
IT-Systemadministratoren [admin] können die Identität von ServiceNow-Benutzern annehmen. Wenn ein Administrator jedoch die Identität eines Benutzers mit einer Anwendungsadministratorrolle für Security Incident Response annimmt, kann er nicht auf die von dieser Rolle gewährten Funktionen zugreifen, einschließlich Security Incidents und Profilinformationen. Der Zugriff auf Module und Anwendungen in der Navigationsleiste ist ebenfalls eingeschränkt. Außerdem kann der Administrator das Passwort eines Benutzers mit einer Anwendungsadministratorrolle für Security Incident Response nicht ändern.

## SIR-Informationsfluss

Security Incident Response verwendet den folgenden Informationsfluss, von der Integration über die Untersuchung bis hin zur Lösung und Überprüfung.

**Informationsfluss in Security Incident Response**




## Discovery

Security Incidents können auf folgende Arten protokolliert oder erstellt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aus dem Security Incident-Formular
- Aus Events, die intern erzeugt oder von externen Überwachungs- oder Schwachstellennachverfolgungssystemen über Warnungsregeln oder manuell erstellt werden
- Aus externen Überwachungs- oder Nachverfolgungssystemen
- Aus dem Servicekatalog

### Analyse

Abhängig von der ausgewählten Ansicht, die Sie verwenden (Standard, Nicht-IT-Sicherheit, Sicherheits-ITIL usw.) kann das Security Incident-Formular eine beliebige Kombination von Schwachstellen, Incidents, Changes, Problemen, Aufgaben für das betroffene CI und das betroffene CI anzeigen Gruppen. Das System kann Malware, Viren und andere Schwachstellenbereiche identifizieren, indem es auf die Datenbank des National Institute of Standards and Technology (NIST) oder andere Erkennungssoftware von Drittanbietern verweist. Nach der Lösung von Security Incidents können Sie jeden Incident verwenden, um einen Sicherheits-Knowledge Base-Artikel zur späteren Referenz zu erstellen.

Führen Sie weitere Analysen mithilfe einer Business Service-Übersicht durch, um andere betroffene Systeme oder Business Services zu finden, die infiziert werden können.

### Eindämmung, Beseitigung und Wiederherstellung

Während Sie Schwachstellen überwachen und analysieren, können Sie Aufgaben erstellen und anderen Abteilungen zuweisen. Sie können eine Business Service-Übersicht verwenden, um Aufgaben, Probleme oder Änderungen für alle betroffenen Systeme, Dokumente, Aktivitäten, SMS-Nachrichten, Brückenanrufe usw. zu erstellen.

### Prüfung

Nachdem der Incident gelöst wurde, können vor dem Abschluss weitere Schritte ausgeführt werden. Sie können eine Überprüfung nach Incidents durchführen. Das Erstellen von Knowledge Base-Artikeln kann bei zukünftigen ähnlichen Incidents hilfreich sein. Signifikante Incidents erfordern möglicherweise eine Überprüfung der Lösung nach dem Incident. Diese Überprüfung kann verschiedene Formen annehmen. Beispiel:

- Führen Sie eine Besprechung durch, um den Incident zu besprechen und Antworten zu sammeln.
- Schreiben und verteilen Sie an die Teams, die an einem Incident gearbeitet haben, eine Liste mit Fragen zur Lösungsüberprüfung, die für jede Kategorie oder Priorität des Incident entwickelt wurden.
- Incident-Manager können den Bericht schreiben und Informationen selbst sammeln.

Ein Bericht zur Überprüfung der Incident-Lösung kann automatisch generiert werden, der Folgendes enthält:

1. eine Zusammenfassung dessen, was getan wurde
2. die Zeitleiste
3. Typ des aufgetretenen Security Incidents
4. alle zugehörigen Incidents, Changes, Probleme, Aufgaben, CI-Gruppen
5. die Details der Lösung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darüber hinaus ist ein automatisiertes Umfragesystem zur Überprüfung der Lösung von Security Incidents verfügbar. Sie erfasst die Namen aller Benutzer, die einem Security Incident zugewiesen sind, und sendet eine benutzerdefinierte Umfrage, um Daten über die Behandlung des Incident zu sammeln. Diese Daten können dann in einem generierten Security Incident-Überprüfungsbericht zur Verfügung gestellt werden, den Sie in einen endgültigen Entwurf bearbeiten können. Ähnliche Daten können einem Knowledge Base-Artikel hinzugefügt werden, um gelernte Lektionen und Schritte zur Lösung ähnlicher Probleme in der Zukunft zu enthalten.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Security Incident Response – Terminologie

Die folgenden Begriffe werden in Security Incident Responseverwendet.

| Begriff | Definition |
|---|---|
| Aktiv | Alle Security Incidents, die sich nicht im Status „Geschlossen“ oder „Abgebrochen“ befinden |
| Administratorsperre | Die Möglichkeit, den Zugriff von Security Incident Response auf Mitarbeiter mit sicherheitsbezogenen Rollen und ACLs zu beschränken. |
| Eingehende Sicherheitsanforderungen | Anforderungen, die für Sicherheitsanforderungen mit geringen Auswirkungen übermittelt werden, z. B. die Anforderung eines neuen elektronischen Abzeichens. |
| Verwalten von Aktivitäten nach Incidents | Eine Überprüfung der Herkunft und Behandlung eines Security Incident. Das Endprodukt ist ein Bericht nach dem Incident, der alle durchgeführten Aktionen und die Gründe dafür dokumentiert. |
| Antwortaufgaben | Aufgaben, die einem Security Incident zugewiesen sind, um Aktionen als Reaktion auf die Bedrohung nachzuverfolgen. |
| Security Incident-Rechner verstehen | Rechner, die zum Aktualisieren von Datensatzwerten verwendet werden, wenn vorkonfigurierte Bedingungen erfüllt sind. |
| Security Incident-Verzeichnisübersichten | Diagrammtyp, der Security Incident-Daten hierarchisch in Form von geschachtelten Rechtecken anzeigt. |
| Bedrohungssuche | Eine vom Security Incident-Katalog übermittelte Anforderung zum Scannen von Dateien, URLs und IP-Adressen auf Malware. |
| Schwachstellenscan | Eine über das Security Incident-Formular initiierte Anforderung zum Scannen betroffener Ressourcen (Server, Computer und andere Konfigurationselemente) auf Schwachstellen. |

## Domain Separation und Security Incident Response

Die Domänentrennung wird in Security Incident Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

## Übersicht

In der Anwendung Security Incident Response ermöglicht die Domänentrennung Service Providern (SPs), SOC- (Security Operations Center) und Security Incident Response-Verfahren (SIR) für den Kundenstamm zu standardisieren, den sie bedienen, mit geringeren Betriebskosten und einer höheren Servicequalität. Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt und niemals für andere Clients verfügbar sind.

**Unterstützung der Domänentrennung in Security Incident Response nach Versionsveröffentlichungen**

| Release | Support-Stufe | Notizen |
|---|---|---|
| Genf, Helsinki | Kein Support | Initiierung der Domänentrennung auf Datenebene |
| Istanbul | Nur Daten | |
| Jakarta | Ebene 2 (Daten, Anforderer, Erfüller) | **Neue Funktionen**: Unterstützung für Integrationen von Drittanbietern mit Domänentrennung der Ebene 2 unter einer einzigen Integrationsinstanz, einschließlich Threat Intelligence-Integrationen |
| Kingston | Ebene 2 (Daten, Anforderer, Erfüller) | **Neue Funktionen**: Die Integration der Sichtungssuche für SIR ist mit mehreren Instanzen aktiviert, aber alle Instanzen befinden sich weiterhin unter einer einzigen Domäne. Beispiel: Wenn zwei Instanzen einer Splunk-Integration konfiguriert sind (SplunkCLOUD und SplunkCORP), werden beide weiterhin für Aktivitäten zur Reaktion auf Incidents in einer |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Unterstützung der Domänentrennung in Security Incident Response nach Versionsveröffentlichungen (Fortsetzung)**

| Release | Support-Stufe | Notizen |
|---|---|---|
| | | einzigen Domäne genutzt, in der die Implementierung ursprünglich konfiguriert wurde. |
| London | Ebene 2 (Daten, Anforderer, Erfüller) | **Neue Funktionen**: Alle Integrationen befinden sich in mehreren Domänen |
| Madrid | Ebene 2 (Daten, Anforderer, Erfüller) | Alle Integrationen können sich jetzt über mehrere Domänen erstrecken. Im obigen Beispiel kann SplunkCloud Domäne1 und SplunkCORP Domäne2 sein. |
| New York | Ebene 2 (Daten, Anforderer, Erfüller) | Alle Integrationen befinden sich in mehreren Domänen. |
| Orlando | Standard | Alle Integrationen befinden sich in mehreren Domänen. |
| Paris | Standard | Alle Integrationen befinden sich in mehreren Domänen. |

Die Domänentrennung für die Anwendung Security Incident Response umfasst die folgenden Produktfunktionen:

- Sicherheitswarnungen werden an die entsprechende Domäne des Benutzers weitergeleitet, dessen ID/Anmeldeinformationen/Bereich den Incident generiert und als Security Incident registriert ist.
- Warnungen generieren „erkennbare Elemente“, die statusbehaftete Eigenschaften oder messbare Events darstellen: Sicherheits-Workflows in der Domäne des Security Incident werden verwendet, um die Reaktion zu orchestrieren.
- Integrationen werden in der Domäne des Security Incident für die Antwortautomatisierung konfiguriert.
- Fähigkeiten werden in der Domäne des Security Incident für die Automatisierung der Reaktion konfiguriert. Zu diesen Funktionen (ab Kingston-Release) gehören:
  - Bedrohungssuche
  - Erkennbares Element ergänzen
  - Konfigurationselement anreichern
  - Laufenden Prozess abrufen
  - Netzwerkstatistiken abrufen
  - Anforderung blockieren
  - Host isolieren
  - Sichtungssuche
  - E-Mails suchen und löschen
  - In Beobachtungsliste veröffentlichen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ergebnisse aus der Antwortautomatisierung (z. B. Bedrohungssuche oder Sichtungssuche) werden in der Domäne des Security Incident gespeichert.
- Andere Security Incidents werden in derselben Domäne des Security Incident basierend auf einem gemeinsam genutzten Satz von erkennbaren Elementen mit Querverweisen versehen.
- Andere Benutzer werden in der Domäne des Security Incident referenziert.
- Konfigurationselemente werden in derselben Domäne wie der Security Incident referenziert.
- Manuelle Antwortaufgaben werden der Domäne des Security Incident hinzugefügt.
- Knowledge Base-Artikel und Ausführungsbücher werden in der Domäne des Security Incident referenziert.
- Security Incident Response-Metriken, die für Incidents in der Domäne relevant sind, werden in Dashboards sowie in der Berichterstellung angezeigt.

**Hinweis:**
In den vorherigen Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänen in der NOW Platform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

## Funktionsweise der Domänentrennung in Security Incident Response

Die Anwendung Security Incident Response verwaltet den Lebenszyklus eines Security Incident End-to-End. Die folgenden Anwendungsfälle sind für die Domänentrennung geeignet:

- **Erfassung von Events und Warnungen**, um Security Incidents zu erstellen, auf die der Analyst im Kunden-SOC oder MSP reagieren kann:
  - E-Mail-Parser (plattformbasiert, von Benutzern gemeldetes Phishing, benutzerdefiniert)
  - Deduplizierungs-Events/-Warnungen vor der Incident-Erstellung
  - Automatische Extraktion von erkennbaren Elementen
  - Anwendungen im SIEM-Store einer Drittpartei
- **Ergänzung** der an den Incidents beteiligten Artefakte (IP, URLs, Domänen, Datei-Hashes):
  - Asset-Ergänzung (CMDB)
  - Benutzer (Plattform)
  - Automatisierung: Ergänzung erkennbarer Elemente (z. B. WhoIs)
- **Untersuchen Sie** die Incidents mithilfe der Artefakte und ihrer Reputation oder Zuordnung zu bekannten Bedrohungen
  - Orchestrate: Playbooks und Knowledge Base-Artikel
  - Automatisierung: Bedrohungssuche (z. B. VirusTotal), Sichtungssuche (z. B. Splunk), laufende Prozesse abrufen (z. B. Carbon Black)
- **Beseitigen Sie** die am Incident beteiligten bedrohungsbezogenen Artefakte basierend auf der durchgeführten Untersuchung
  - Orchestrate: Playbooks und Knowledge Base-Artikel
  - Automatisierung: E-Mails suchen und löschen (z. B. Microsoft Exchange), IP blockieren (z. B. Palo Alto Firewall)
- Effizienz von Vorgängen zur Reaktion auf Incidents**messen**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Performance Analytics Dashboards: Produktivitäts- und Incident-Trends
- Rekonstruktion von Incident-Untersuchungsschritten aus Arbeitsnotizen
- Überprüfung nach Incident

### Domänentrennung – Einrichtung

Das Einrichten der Domänentrennung für Security Incident Response erfordert keine zusätzlichen Schritte. Alle Security Incident Response -Tabellen erfassen die Domänenspalte, nachdem die Instanz domänengetrennt wurde.

### Domänengetrennte Daten

Daten können domänengetrennt sein, was Folgendes bedeutet:

- Security Incidents in einer Domäne können nicht aus anderen Domänen angezeigt werden.
- Aus dem Security Incident extrahierte erkennbare Elemente werden in derselben Domäne platziert und können nicht aus anderen Domänen angezeigt werden.
- Bis zum Kingston-Release sind konfigurierte Drittanbieterintegrationen in der globalen Domäne vorhanden und für alle anderen Domänen in der Instanz zugänglich.
- Im Madrid-Release können Drittanbieterintegrationen pro Domäne konfiguriert und aktiviert werden. Dies bedeutet, dass die in einer Domäne aktivierte und konfigurierte Integration nicht in einer anderen Domäne genutzt werden kann.
- Automatisierungen, die für die erkennbaren Elemente mithilfe von Drittanbieterintegrationen ausgeführt werden (für Bedrohungsuntersuchung, Eindämmung oder Beseitigung), platzieren ihre Ergebnisse in der Domäne des Security Incidents und die Ergebnisse können nicht von einer anderen Domäne aus angezeigt werden.
- In einer Domäne erstellte Orchestration-Workflows sind in einer anderen Domäne nicht sichtbar.
- Fähigkeiten (wie in der Funktionsliste der vorherigen Fähigkeiten beschrieben), die aufgerufen werden, bleiben domänenübergreifend generisch, wobei die aufgerufene Fähigkeit domänenspezifisch implementiert wird. Beispielsweise kann eine Sichtungssuche für eine IP eine Splunk-Implementierung in einer Domäne und eine QRadar-Implementierung in einer anderen Domäne aufrufen.

### Konfiguration

Alle Aspekte der Produktkonfiguration sind in einer domänengetrennten Umgebung in sich abgeschlossen. Das Setup kann für einzelne Domänen angepasst werden.

**Hinweis:**
Geschäftslogik und die Prozesse in Nr. 2 bis 5 unten können innerhalb der Mandantendomäne verwaltet werden.

Die folgenden Aufgaben müssen konfiguriert werden:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Systemverwaltung
   - Weisen Sie Benutzern und Benutzergruppen Rollen zu: Mit Security Incident Response installierte Benutzerrollen
   - Installieren Sie mindestens ein Integrations-Plugin einer Drittpartei, um mit Security Incident Responsezu arbeiten: Security Incident Response-Integrationen
2. Security Incident Response -Administration
   - Rollen hinzufügen oder überprüfen: Mit Security Incident Response installierte Komponenten
   - Konfigurieren Sie Gruppen und Benutzer: Erstellen Sie eine Security Incident-Gruppe
   - Incident-Eskalationen einrichten: Eskalieren Sie einen Security Incident
   - Richten Sie Risikopunktzahl-Rechner für Security Incidents ein: Security Incident-Rechner verstehen
   - Servicelevel-Vereinbarungen einrichten: Erstellen Sie eine Security Incident Response SLA
   - Richten Sie Prozessdefinitionen für Security Incidents ein: Security Incident Response-Prozessdefinition verstehen
   - Richten Sie Prozesse für die Überprüfung nach Incidents ein: Verwalten von Aktivitäten nach Incidents
3. E-Mail-Einstellungen für Security Incidents
   - Legen Sie den Posteingang für die E-Mail-Analyse fest: Security Operations E-Mail-Analyse
   - Richten Sie E-Mail-Parser für die Warnungserfassung ein: Erstellen Sie E-Mail-Parser in Security Operations
   - Richten Sie E-Mail-Abgleichregeln für von Benutzern gemeldetes Phishing ein: Erstellen Sie Regeln, um von Benutzern gemeldete Phishing-Angriffe zu validieren
   - Richten Sie Aktionen bei eingehender E-Mail ein: Aktionenbei eingehender E-Mail
4. Einstellungen für das Security Incident-Playbook
   - Überprüfen und richten Sie die Runbook-Dokumente ein: Erstellen Sie ein Security Incident Response-Runbook
   - Security Incident-Workflows einrichten: Security Operations allgemeine Funktionalität
5. Fähigkeitskonfigurationen
   - Blockanforderung: Security Operations Integration - Block Request-Fähigkeit
   - E-Mail suchen und löschen: Security Operations-Integration – E-Mail-Such- und Löschfunktion
   - Konfigurationselement anreichern: Integration von Security Operations – CI-Fähigkeit ergänzen
   - Erkennbares Element anreichern: Integration von Sicherheitsvorgängen – Fähigkeit „Erkennbares Element anreichern“.
   - Netzwerkstatistiken abrufen: Integration mit Security Operations – Fähigkeit „Netzwerkstatistiken abrufen“.
   - Laufende Prozesse abrufen: Integration mit Security Operations – Fähigkeit „Laufende Prozesse abrufen“.
   - Host isolieren: Security Operations Integration - Host-Fähigkeit isolieren
   - In Beobachtungsliste veröffentlichen: Integration von Sicherheitsvorgängen – Fähigkeit „In Beobachtungsliste veröffentlichen“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sichtungssuche: Integration von Sicherheitsvorgängen – Sichtungssuchfunktion
- Bedrohungssuche: Security Operations-Integration – Funktion „Bedrohungssuche“.

### Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Mandantendomänenbesitzer erstellen ihre eigenen E-Mail-Analyseregeln für die Erfassung von Security Incidents.
- Mandantendomänenbesitzer können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Mandantendomänenbesitzer können ihre eigenen Workflows für die Reaktion auf Incidents erstellen.
- Mandantendomänenbesitzer können eigene Incident-Kategorien, Knowledge Base-Artikel zur Reaktion auf Incidents und Runbooks erstellen, die mit Workflows zur Reaktion auf Incidents verknüpft werden sollen.
- Benutzer der Mandantendomäne erstellen und schließen ihre eigenen Security Incidents.

### Geschäftslogik und Prozesse, die nach Instanzbesitzer domänengetrennt sein können

- Security Incident Response -Benutzer und -Gruppen
- Security Incident Response -Integrationen (ab Madrid-Release)
- E-Mail-Analyseregeln für die Incident-Erstellung
- Geschäftsregeln zum Konsolidieren mehrerer Events oder Warnungen in einem Security Incident
- Workflows für die Orchestration der Reaktion auf Incidents
- Risikopunktzahl-Rechner für Security Incidents
- Eskalationspfad für Security Incidents
- Security Incident-SLAs
- Prozessdefinitionen für Security Incidents
- Prozesse zur Überprüfung nach einem Incident für Security Incidents

**Zugehörige Informationen**

Domänentrennung für Service Provider

## Setup von Security Incident Response

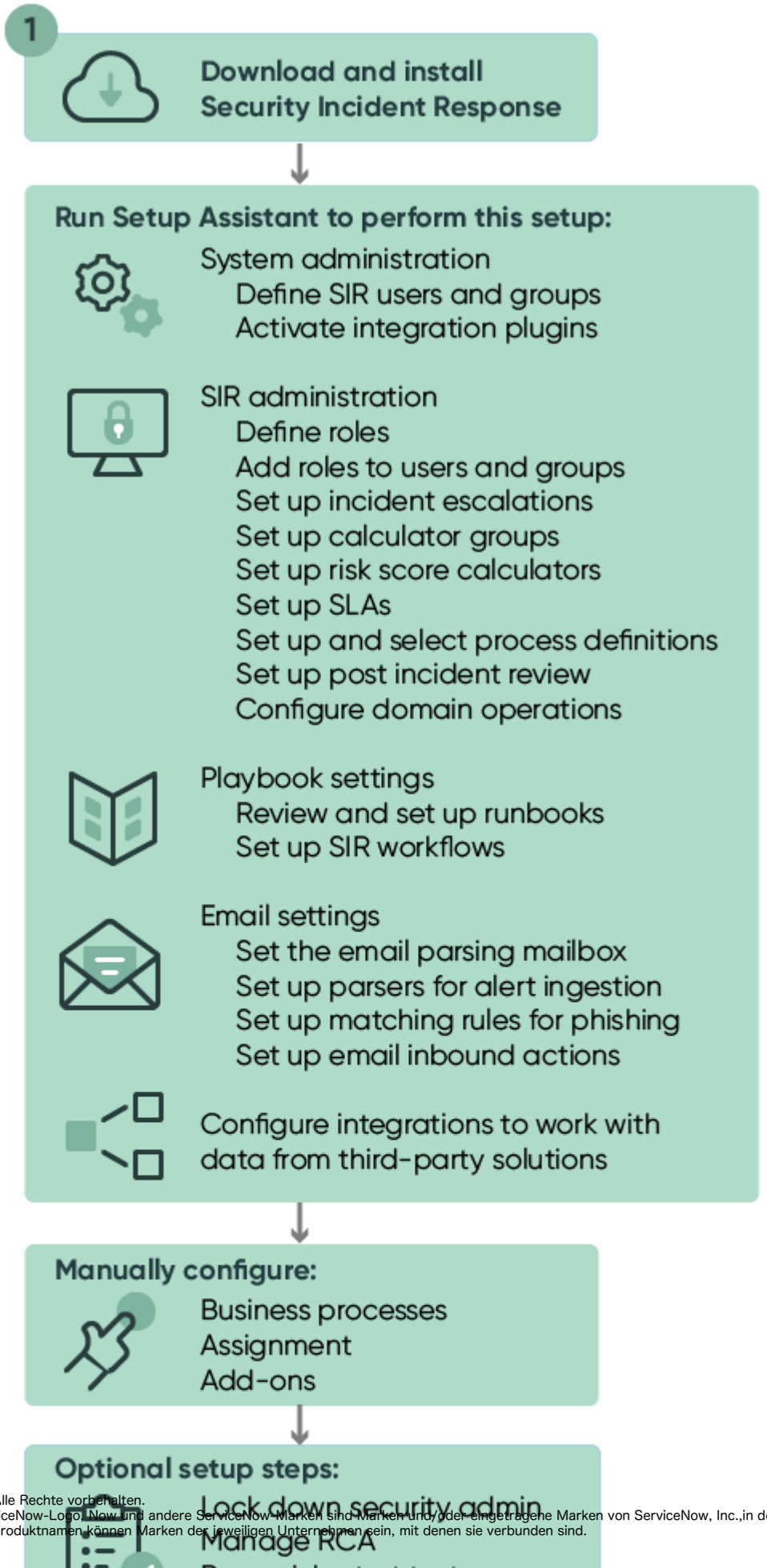
Das Setup für Security Incident Response umfasst einige obligatorische Schritte und mehrere optionale Schritte, die von Ihren spezifischen Anforderungen abhängen. Nachdem Sie Security Incident Response aus dem ServiceNow Store heruntergeladen und installiert haben, können Sie den Setup-Assistenten ausführen, um die grundlegende Konfiguration für Security Incident Response und Integrationen von Drittanbietern durchzuführen.

### Der Setup-Prozess Security Incident Response .

Das folgende Diagramm veranschaulicht den Setup-Prozess. Sie ist in zwei Teilprozesse unterteilt: Herunterladen und Konfigurieren der Anwendung Security Incident Response und Herunterladen und Konfigurieren von Security Analyst Workspace.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der erste Setup-Schritt besteht aus herunterladen Security Incident Response Anwendung aus dem ServiceNow Store. Nach Abschluss des Downloads werden mehrere abhängige Anwendungen, einschließlich des Setup-Assistenten, geladen und können zur Konfiguration von Security Incident Responseverwendet werden.

## Setup-Assistent

Der Setup-Assistent von Security Incident Response ist eine assistentenähnliche Anwendung, die Sie Schritt für Schritt durch die Einrichtung Ihrer Basisinstanz Security Incident Response führt.

Die Setup-Schritte sind einigermaßen selbsterklärend. Wenn Sie jedoch zusätzliche Erklärungen benötigen, finden Sie zusätzliche Unterstützung in der Referenz des Setup-Assistenten. Nachdem Sie das Setup mit dem Setup-Assistenten abgeschlossen haben, können Sie nach Bedarf weitere optionale Setup-Verfahrenausführen. Diese Verfahren umfassen Optionen für:

- Anforderungslebenszyklus einrichten
- Erstellen von Katalogen und Anforderungen
- Benachrichtigungen konfigurieren
- Manuelle und automatische Zuweisung einrichten
- Knowledge Base, verwaltete Dokumente und Aufgabenaktivitäten aktivieren

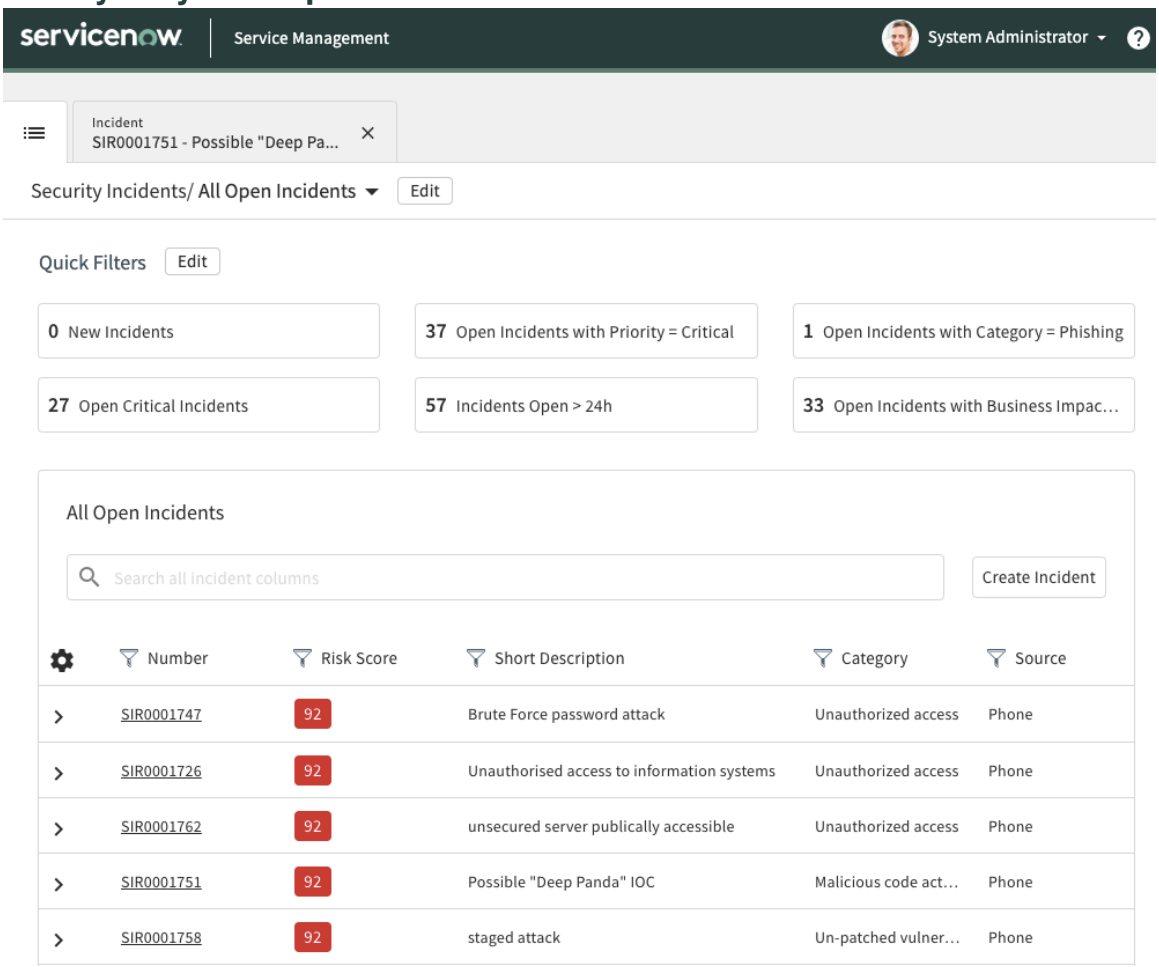
## Security Analyst Workspace

Wenn Sie die Konfiguration von [] abgeschlossen haben, können Sie Security Analyst WorkspaceSecurity Incident Response installieren und konfigurieren, was die Analyse von Security Incidents vereinfacht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Analyst Workspace**




Zuerst müssen Sie die Anwendung aus dem ServiceNow Store herunterladen und dann konfigurieren. Der Konfigurationsprozess umfasst das Einrichten primärer und sekundärer Filter zum Eingrenzen der Liste der zu analysierenden Security Incidents.

Nachdem Sie die Anwendung installiert und konfiguriert haben, können Sie den Security Analyst Workspace öffnen, indem Sie zu navigieren **Security Incident** > **Incidents (neue UI)**.

## Security Incident Response installieren und konfigurieren

Bevor Sie Security Incident Response in Ihrer Instanz ausführen, müssen Sie es aus dem ServiceNow Store herunterladen und die Konfigurationsschritte ausführen.

### Vorbereitungen

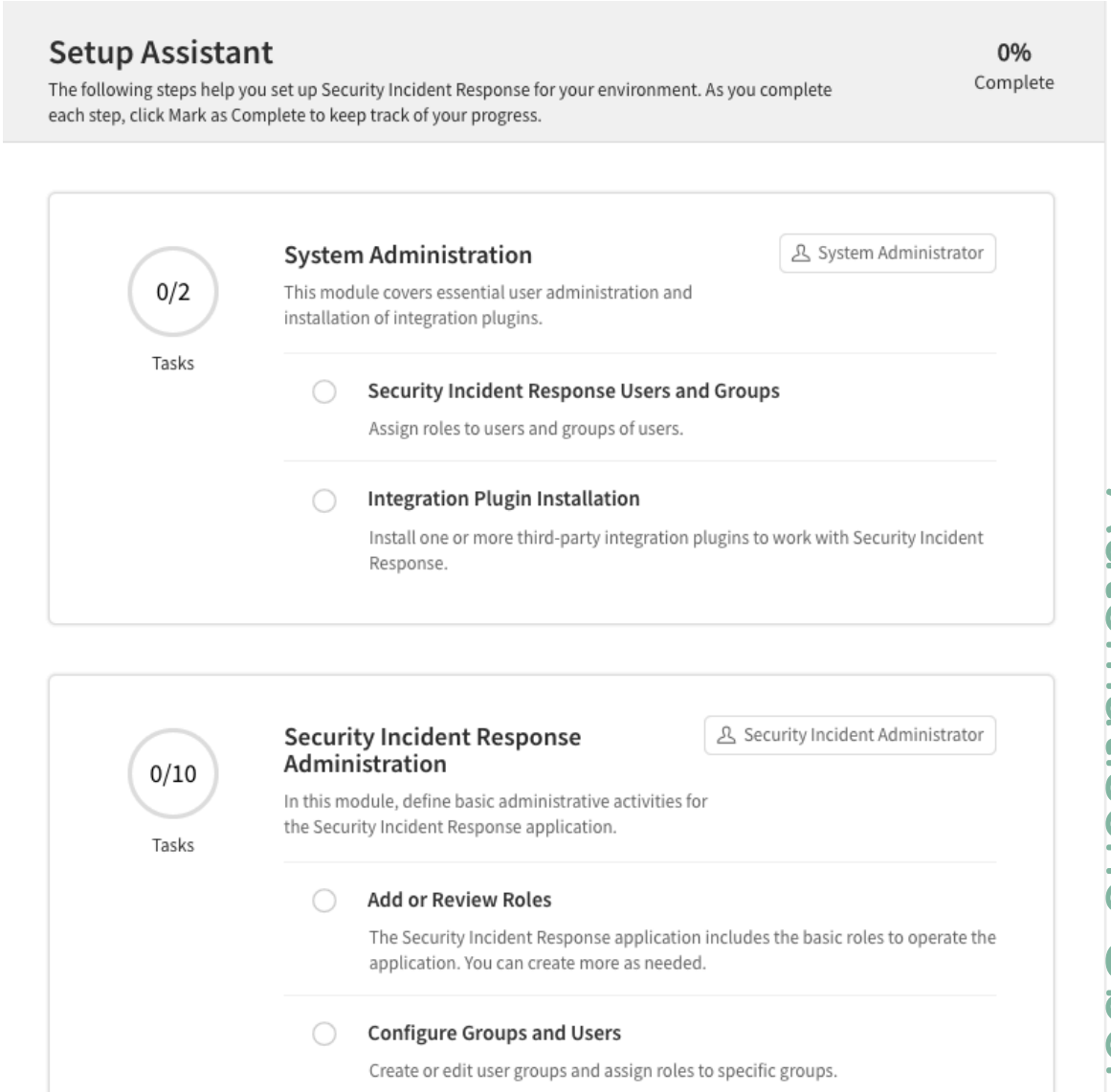
Erforderliche Rolle: admin

### Prozedur

1. Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store.
2. Nachdem Sie die Anwendung Security Incident Response und alle zugehörigen Anwendungen heruntergeladen haben, navigieren Sie zu **Security Incident** > **Setup des Analyst Workspace** > **Setup-Assistent**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Befolgen Sie die Anweisungen in den Formularen, um das Basissystem Security Incident Response zu konfigurieren.
   Weitere Informationen zu einigen der komplizierteren Setup-Aufgaben finden Sie bei Bedarf unter Referenz zum Setup-Assistenten.

### Laden Sie den Security Analyst Workspace herunter, und installieren Sie ihn

Bevor Sie die neue Benutzeroberfläche von Security Incident Response in Ihrer Instanz ausführen, müssen Sie sie aus dem ServiceNow® Store herunterladen und installieren.

#### Vorbereitungen

Um eine reibungslose Installation zu gewährleisten, stellen Sie sicher, dass Sie über die erforderlichen ServiceNow Rollen für Ihre Instanz verfügen. Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:

- Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Security Incident Response-Administrator“ [sn_si.admin] zu.
- Der Security Incident Response-Administrator [sn_si.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

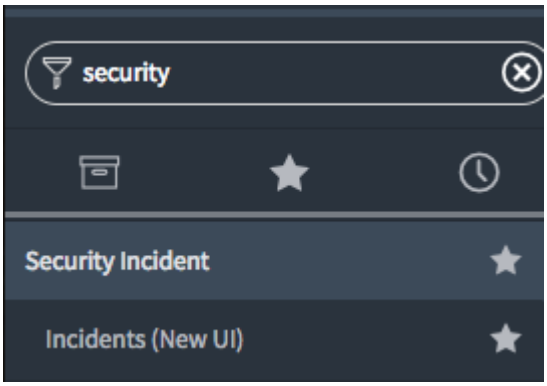
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin

### Prozedur

1. Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store und installieren die Anwendung **Security Incident Response UI**.
2. Nach Abschluss der Installation können Sie den Security Analyst Workspace öffnen, indem Sie zu navigieren **Security Incident** > **Incidents (neue UI)**




### Mit Security Incident Response installierte Komponenten

Beim Herunterladen und Aktivieren der Anwendung Security Incident Response werden verschiedene Arten von Komponenten installiert, z. B. Benutzerrollen, Tabellen, Eigenschaften und geplante Aufgaben.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

## Installierte Eigenschaften

Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.

| Eigenschaft | Verwendung |
|---|---|
| Standardmäßige Startzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, formatiert als 08:00<br><br>sn_si.default.start.time | • **Typ**: Zeichenfolge<br>• **Standardwert**: 08:00<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Standardmäßige Endzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, im Format 17:00<br><br>sn_si.default.end.time | • **Typ**: Zeichenfolge<br>• **Standardwert**: 17:00<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Verwendung |
|---|---|
| Schließen Sie erkennbare Elemente des Zieltyps zusammen mit anderen erkennbaren Elementen des Kontexttyps in die Security Incident-Benutzer- und CI-Beziehungen ein<br><br>sn_si.link_dest_ip | Bestimmt, ob ein erkennbares Security Incident-Element mit dem Kontexttyp „Ziel“ auf den Registerkarten „ **Konfigurationselemente“** oder „ **Betroffene Benutzer** “ angezeigt wird. Standardmäßig werden erkennbare Elemente mit einem Zielkontexttyp ausgeschlossen. Um die erkennbaren Elemente einzubeziehen, wählen Sie Ja. |
| Lassen Sie Anpassungen zu, wenn Sie ein Problem oder eine Change-Anforderung aus einem Security Incident erstellen<br><br>sn_si.popup | Wenn ein Problem oder ein Change erstellt wird, öffnet diese Eigenschaft ein Popup-Fenster, um die Anforderung zu ändern.<br><br>Wenn diese Eigenschaften auf **false**festgelegt sind, hat das Problem oder die Change-Anforderung dieselbe Priorität, Kurzbeschreibung und Beschreibung wie der Security Incident, ohne dass diese Felder hinzugefügt oder bearbeitet werden können.<br><br>• **Typ**: true \| false<br>• **Standardwert**: true<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Ordnen Sie die Ergebnisse der Sichtungssuche den CIs in der CMDB zu.<br><br>sn_si.associate_ci_with_sighting_search | Bei „true“ enthalten Sichtungssuchergebnisse zugeordnete Konfigurationselemente, die sich in Ihrer CMDB befinden.<br><br>• **Typ**: true \| false<br>• **Standardwert**: true<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Risikopunktzahlen im Bereich werden grün hervorgehoben und im Format 0–49 angegeben<br><br>sn_si.risk.punktzahl.grün | In der Liste „Security Incidents“ werden Security Incidents mit einer Risikopunktzahl zwischen 0 und 49 mit einem grünen Punkt markiert. |
| Die Risikopunktzahl im Bereich wird orange hervorgehoben und im Format 50–79 angegeben<br><br>sn_si.risk.score.orange | In der Liste „Security Incidents“ werden Security Incidents mit einer Risikopunktzahl zwischen 50 und 79 mit einem orangefarbenen Punkt markiert. |
| Die Risikopunktzahl im Bereich wird rot hervorgehoben und im Format 80–100 angegeben<br><br>sn_si.risk.score.red | In der Liste „Security Incidents“ werden Security Incidents mit einer Risikopunktzahl zwischen 80 und 100 mit einem roten Punkt markiert. |
| Dieser Parameter aktiviert oder deaktiviert Sichtungssuchkonfigurationen, die diese Funktion implementiert haben. | Bei „true“ können Sichtungssuchen für aktivierte Integrationen durchgeführt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Verwendung |
|---|---|
| sn_si.enable_sighting_search | • **Typ**: true \| false<br>• **Standardwert**: true<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Die Anzahl der Zeilen mit Rohdaten, die gespeichert werden, wenn eine Sichtungssuche ausgeführt wird. Bereich 0 bis 100<br><br>sn_si.sighting_search_raw_data_rows | Diese Eigenschaft ist standardmäßig auf 50 Zeilen mit Rohdaten festgelegt. Die Hälfte der Ergebniszeilen wird ab Beginn des Suchzeitrahmens und die andere Hälfte ab Ende des Suchzeitrahmens gemeldet. Wenn Sie also 50 Zeilen auswählen, stammen 25 vom Beginn des Suchzeitrahmens und 25 vom Ende des Suchzeitrahmens. |
| Incident-Status automatisch auf „Eindämmen“ erhöhen, wenn eine Antwortaufgabe auf „In Bearbeitung“ gesetzt wird<br><br>sn_si.rollup_task_state | Erwägen Sie bei der Verwendung von Flows oder Workflows, diese Eigenschaft auf **false**zu setzen. Auf diese Weise können Sie den Incident-Status in Flows oder Workflows steuern. Sie hilft auch, potenzielle Konflikte beim Übergang von einem Incident-Status in einen anderen zu vermeiden.<br>• **Typ**: true \| false<br>• **Standardwert**: true<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| **Zuweisungseigenschaften für Security Incident Response** | |
| Standortgewichtung<br><br>sn_si.location.weight | Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Zuweisung eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise der Standort für eine Aufgabe berücksichtigt wird, wird der Standortgewichtungswert der Sicherheitsanalystenbewertung hinzugefügt.<br>• **Typ**: Ganzzahl<br>• **Standardwert**: 10<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Gewichtung der Kompetenzen<br><br>sn_si.skills.weight | Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Zuweisung eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise Kompetenzen für eine Aufgabe berücksichtigt werden, wird der Kompetenzgewichtungswert der Sicherheitsanalystenbewertung hinzugefügt.<br>• **Typ**: Ganzzahl<br>• **Standardwert**: 10<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Verwendung |
| --- | --- |
| Legen Sie die maximale Anzahl von Sicherheitsanalysten fest, die durch die automatische Zuweisung verarbeitet werden sollen<br><br>sn_si.max.agents.verarbeitet | Das System hat ein absolutes Limit von 300 Sicherheitsanalysten. Wenn Sie mehr als 300 angeben, wird der Wert auf diese Ebene festgelegt. Das System kann eine Aufgabe nicht automatisch für eine Einsatzgruppe versenden, die mehr Sicherheitsanalysten als den konfigurierten Wert enthält.<br>• **Typ**: Ganzzahl<br>• **Standardwert**: 100<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Gewichtung Zeitzone<br><br>sn_si.timezone.weight | Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Zuweisung eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise die Zeitzone des Sicherheitsanalysten für eine Aufgabe berücksichtigt wird, wird der Gewichtungswert der Zeitzone der Bewertung des Sicherheitsanalysten hinzugefügt.<br>• **Typ**: Ganzzahl<br>• **Standardwert**: 10<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Zwischen Ende einer Aufgabe und dem Reistestart der nächsten hinzuzufügende Dauer (in Minuten).<br><br>sn_si.work.spacing | Ein Beispiel für einen gültigen Zeitwert ist 10.<br>• **Typ**: Ganzzahl<br>• **Standardwert**: 0<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Angegebene Journalfelder, die `Code-` Tags enthalten, die den Inhalt als HTML rendern.<br><br>sn_si.journal_field.html_enabled | • **Typ**: Zeichenfolge<br>• **Standardwert**: work_notes, Comments<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Berechnet die betroffenen Services im Hintergrund.<br><br>sn_si.refresh_impacted.event | Die zugehörige Liste „Betroffene Services/Betroffene CIs“ wird durch Events generiert. Wenn diese Option aktiviert ist, wird die Aktualisierung im Hintergrund ausgeführt, und dem Incident werden Sicherheits-Tags hinzugefügt.<br><br>Legen Sie den Wert auf **„true“ fest**, um den Vorgang im Hintergrund auszuführen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Verwendung |
|---|---|
| | • **Typ**: true \| false<br>• **Standardwert**: false<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |
| Rufen Sie den kritischen Service aus vorab berechneten Daten ab.<br><br>sn_si.critical_service.calculator.use_cache | Aktiviert den Rechner für kritische Services, um vorberechnete Daten von Konfigurationselementen zu verwenden.<br><br>Legen Sie den Wert auf „ **true** “ fest, um in vorab berechneten Daten zu suchen<br><br>• **Typ**: true \| false<br>• **Standardwert**: false<br>• **Standort**: **Security Incident** > **Administration** > **Eigenschaften** |

## Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| Sicherheitsvorfall-Administrator<br><br>[sn_si.admin] | Vollständige Kontrolle über alle Security Incident Response Daten. Verwaltet bei Bedarf auch Gebiete und Kompetenzen.<br><br>**Hinweis:**<br>Im Basissystem hat der Administrator auch Zugriff auf sn_si.admin. Security Incident Response kann vom Administrator eingeschränkt werden, solange mindestens einem anderen Benutzer die Sicherheitsadministratorrolle zugewiesen ist. | • assessment_admin<br>• catalog_admin<br>• decision_table_admin<br>• decision_table_reader<br>• filter_admin<br>• flow_designer<br>• pd_author<br>• pd_content_author<br>• pd_operator<br>• skill_admin<br>• skill_model_admin<br>• sn_si.analyst<br>• sn_si.knowledge_admin<br>• sn_si.manager<br>• sn_sec_cmn.admin<br>• sn_si.restriction_access_manager<br>• sn_si.special_access_read_manager<br>• sn_si.special_access_write_manager<br>• sn_ti.malicious_attachment_access |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | | • sn_ti.observable.admin<br>• tags_admin<br>• template_admin<br>• territory_admin<br>• treemap_admin<br>• user_admin |
| Security Incident-Analyst<br><br>[sn_si.analyst] | Verwalten Sie Security Incidents. Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Änderungen und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren. | • pd_operator<br>• snc_platform_rest_api_access<br>• sn_msi.promoter<br>• sn_msi.proposer<br>• sn_si.basic<br>• sn_ti.malicious_attachment_access |
| Security Incident – Standard<br><br>[sn_si.basic] | Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Änderungen und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren. | • canvas_user<br>• document_management_user<br>• email_composer<br>• flow_operator<br>• inventory_user<br>• pa_viewer<br>• service_fullfiller<br>• skill_user<br>• sn_sec_cmn.write<br>• sn_si.read<br>• sn_ti.observable.read<br>• sn_ti.observable.write<br>• sn_ti.read<br>• task_activity_writer<br>• task_editor<br>• treemap_user |
| Chief Information Security Officer (CISO)<br><br>[sn_si.ciso] | CISO-Dashboard anzeigen und bearbeiten. Wenn das Plugin Vulnerability Response aktiviert ist, können Benutzer mit dieser Rolle dem Dashboard auch Schwachstellen-Bedeutungsdefinition-Treemaps | • pa_viewer<br>• sn_si.basic<br>• sn_si.read |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | hinzufügen. Dasselbe können Sie auch mit dem Plugin Security Incident Response tun. | |
| Security Incident Extern<br><br>[sn_si.external] | Zeigen Sie alle Security Incidents an, die zu ihrer jeweiligen Gruppe gehören.<br><br>**Hinweis:**<br>Die folgenden beiden Regeln gelten im gesamten ServiceNow, unabhängig vom bereichsbezogenen Administrator oder der bereichsbezogenen App.<br>• Wenn Sie einen Benutzer zu einer Gruppe hinzufügen, weisen Sie dieser Gruppe auch Rollen zu. Wenn Sie einen Benutzer aus einer Gruppe entfernen, werden auch die geerbten Rollen entfernt.<br>• Jede Rolle kann von einer Rolle mit höherer Priorität zugewiesen werden. | service_fulfiller |
| Security Incident-Integrationsbenutzer<br><br>[sn_si.integration_user] | Externe Tools können neue Security Incident-Datensätze bereitstellen und Security Incident-Datensätze aktualisieren. | import_transformer |
| Security Incident – Wissensadministrator<br><br>[sn_si.knowledge_admin] | Verwalten, aktualisieren und löschen Sie die Informationen in der Knowledge Base für Security Incidents. | • knowledge_admin<br>• sn_si.read |
| Sicherheitsvorfallmanager<br><br>[sn_si.manager] | Gleicher Zugriff wie Sicherheitsanalysten. | • pd_author<br>• pd_operator<br>• sn_si.basic |
| Lesen Sie den Security Incident<br><br>[sn_si.read] | Lesen Sie Security Incidents. | • canvas_user<br>• sn_sec_cmn.read<br>• sn_templated_snip.template_snippet_read |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | | • sn_ti.observable.read<br>• workspace_user |
| Zugriffsmanager für Sicherheitsbeschränkungen [sn_si.restriction_access_manager] | Ermöglicht Benutzern oder Gruppen, Einschränkungen für Security Incidents durchzusetzen. Dies gilt nur für Feldänderungen. | N/V |
| Security Incident – Spezieller Zugriff<br><br>sn_si.special_access | Bietet Zugriff auf bestimmte Security Incidents für Benutzer außerhalb der Security Operations-Organisation. | N/V |
| Security Special Access Enabler [sn_si.special_access_enabler] | Bietet einem Benutzer außerhalb der Security Operations-Organisation eine spezielle Zugriffsrolle für bestimmte Security Incidents. | N/V |
| Security Incident – Sonderzugriff – Lesemanager [sn_si.special_access_read_manager] | Verwalten Sie die Rolle „Security Incident – Spezialzugriff“ [sn_si.special_access]. Verwenden Sie diese Rolle, um das Feld **Lesezugriff** im Security Incident-Formular zu ändern. Diese Rolle kann von sn_si.admin zugewiesen werden. | sn_si.special_access_enabler |
| Security Incident – Manager für Sonderzugriffsautoren [sn_si.special_access_write_manager] | Verwalten Sie die Rolle „Security Incident – Spezialzugriff“ [sn_si.special_access]. Verwenden Sie diese Rolle, um das Feld **Privilegierter Zugriff** im Security Incident-Formular zu ändern. Diese Rolle kann von sn_si.admin zugewiesen werden. | sn_si.special_access_enabler |

## Installierte Scheduled Jobs

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Suchen Sie nach erkennbaren Security Incident-Elementen | Führt eine Suche nach erkennbaren Elementen in einem benutzerdefinierten Zeitplan durch. |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Nachrichtenfeed-Konfiguration<br><br>[sn_si_feed_configuration] | Konfigurationsdatensätze, die zum Definieren des im Security Incident-Newsfeed angezeigten Inhalts verwendet werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| Zuweisungsregel für die Überprüfung nach Incidents<br>[sn_si_pir_condition] | Automatisiert die Auswahl von Teilnehmern einer Umfrage zur Überprüfung nach Incidents, wenn ein Security Incident geschlossen wird. |
| Security Incident<br>[sn_si_incident] | Speichert einen Security Incident, die Antworten auf den Incident, alle verknüpften Aufgaben, Changes, Probleme und Incidents im Zusammenhang mit diesem Security Incident |
| Security Incident-Angriffsvektoren<br>[sn_si_attack_vector] | Optionen für Angriffsvektoren |
| Security Incident Audit-Protokoll<br>[sn_si_audit_log] | Speichert Audit-Protokolle zur Ergänzung von Security Incidents. |
| Security Incident-Rechner<br>[sn_si_calculator] | Ein Rechner zum Festlegen bestimmter Security Incident-Felder, wenn bestimmte Bedingungen erfüllt sind. |
| Security Incident-Rechnergruppe<br>[sn_si_calculator_group] | Eine Gruppierung von Security Incident-Rechnern. Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet. |
| Security Incident Enrichment-Firewall<br>[sn_si_enrichment_firewall] | Erweitert aus der Basistabelle (sn_sec_cmn_enrichment_data_base) und enthält alle für die Palo Alto Networks-Firewall spezifischen Ergänzungsdatensätze. |
| Security Incident-Ergänzung – Malware-Ergebnisse<br>[sn_si_enrichment_malware] | Erweitert aus der Basistabelle (sn_sec_cmn_enrichment_data_base) und enthält alle für Malware spezifischen Ergänzungsdatensätze. |
| Netzwerkstatistiken zur Ergänzung von Security Incidents<br>[sn_si_enrichment_network_statistics] | Erweitert aus der Basistabelle (sn_sec_cmn_enrichment_data_base) und enthält alle Ergänzungsdatensätze, die für Netzwerkstatistiken spezifisch sind. |
| Ausgeführte Prozesse der Ergänzung von Security Incidents<br>[sn_si_enrichment_running_processes] | Erweitert aus der Basistabelle (sn_sec_cmn_enrichment_data_base) und enthält alle Ergänzungsdatensätze, die für laufende Prozesse spezifisch sind. |
| Security Incident-Ergänzung – Laufende Services<br>[sn_si_enrichment_running_service] | Erweitert aus der Basistabelle (sn_sec_cmn_enrichment_data_base) und enthält alle Ergänzungsdatensätze, die für ausgeführte Services spezifisch sind. |
| Security Incident-E-Mail-Suche<br>[sn_si_m2m_incident_email_search] | Ordnet E-Mail-Suchdatensätze Security Incidents zu. |
| Security Incident-Import<br>[sn_si_incident_import] | Importtabelle für Security Incidents. Wird verwendet, um Security Incidents aus externen Systemen zu erstellen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| Definition des Security Incident-Prozesses<br>[sn_si_process_definition] | Speichert die Konfiguration für Security Incident-Prozess-Flows. |
| Auswahl der Prozessdefinition für Security Incidents<br>[sn_si_process_definition_selector] | Speichert die Definition des Security Incident-Prozesses, die für Security Incidents verwendet werden soll. |
| Security Incident-bezogener Kundenservicefall<br>[sn_si_m2m_incident_customerservice_case] | Ordnet Kundenservicefälle und Security Incidents zu |
| Zugehörige Ergänzungsdaten für Security Incidents<br>[sn_si_m2m_incident_enrichment] | Ordnet Security Incidents und zugehörige Ergänzungsdatensätze zu. |
| Security Incident Response Aufgabe<br>[sn_si_task] | Verwaltet Teilaufgaben im Zusammenhang mit der Behandlung eines Security Incident. Diese Aufgaben können Sicherheitspersonal oder Personen in anderen Abteilungen zugewiesen werden, um die Kommunikation zwischen Abteilungen und die Aufgabennachverfolgung zu verwalten. |
| Security Incident Response Aufgabenvorlage<br>[sn_si_task_template] | Wird verwendet, um eine Security Incident Response -Aufgabe zu erstellen. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um automatisch einen Satz geeigneter Teilaufgaben für eine bestimmte Art von Security Incident zu erstellen. |
| Security Incident-Runbook-Dokument<br>[sn_si_runbook_document] | Ordnet Bedingungen oder Filter für Security Incidents einem Wissensartikel zu. Wird verwendet, um Runbook-Verfahren für die Korrektur von Security Incidents anzugeben. |
| Security Incident-Vorlage<br>[sn_si_incident_template] | Wird verwendet, um einen Security Incident zu erstellen. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um einen vordefinierten Security Incident zu erstellen. |
| Sicherheitsanforderung<br>[sn_si_request] | Eine sicherheitsbezogene Anforderung an das Sicherheitsteam. |
| Anforderung eines Sicherheitsscans<br>[sn_si_scan_request] | Eine Anforderung für eine Bedrohungssuche. |
| Schweregradrechner<br>sn_si_severity_calculator | Definiert die Werte für Schweregrad, Auswirkung, Risiko und Relevanz für einen Security Incident. |
| Von Aufgabe betroffener Benutzer<br>[sn_si_m2m_task_affected_user] | Eine m:n-Tabelle, die Security Incidents betroffenen Benutzern zuordnet. |
| Vorlagen-Workflow – Aktivitätsergebnisauswertung<br>[sn_si_wf_activity_outcome_evaluator] | Ordnet eine Fähigkeit einem Bewertungsskript zu. Ein neuer Subflow kann einem Vorlagen-Workflow hinzugefügt werden, um das Ergebnis einer |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| | Antwortaufgabe festzulegen, anstatt es von einem Analysten manuell festlegen zu lassen. |

### Andere zusätzliche Security Incident Response Setup-Aufgaben

Wenn Sie Administrator in der globalen Domäne sind, konfigurieren Sie, wie Security Incident Response mit täglichen Vorgängen umgeht.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Hinweis:**

Diese Optionen sind in vielen Service Management-Anwendungen Standard und verwenden daher die Service Management-Terminologie. Zum Beispiel wird „Anforderung“ für die Hauptaufgabe (d. h. den Security Incident) verwendet, und „Aufgabe“ wird für Teilaufgaben oder Antwortaufgaben verwendet.

Wenn Sie Administrator in einer Domäne unter der globalen Domäne sind, können Sie den Bildschirm „Konfigurationen“ anzeigen, die Einstellungen jedoch nicht ändern.

**Prozedur**

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Konfiguration**.
   Die Optionen zum Konfigurieren der Anwendungen sind auf den folgenden Registerkarten organisiert:
   - Die Registerkarte **Geschäftsprozess** enthält Optionen für das Einrichten des Anforderungslebenszyklus, das Erstellen von Katalogen und Anforderungen und das Konfigurieren von Benachrichtigungen.
   - Die Registerkarte **Zuweisung** enthält Optionen für die Einrichtung der manuellen und automatischen Zuweisung.
   - Die Registerkarte **Add-Ons** enthält Optionen zum Aktivieren der Wissensdatenbank, verwalteter Dokumente und von Aufgabenaktivitäten.
2. Füllen Sie die Felder auf der Registerkarte **Geschäftsprozess aus**.

**Konfigurationsbildschirm – Registerkarte „Geschäftsprozess“.**

| Feld | Beschreibung |
|---|---|
| **Lebenszyklus** | |
| Zum Schließen oder Abbrechen einer Anforderung oder Aufgabe sind Arbeitsnotizen erforderlich. | Aktivieren Sie diese Option, damit der Benutzer Arbeitsnotizen eingeben muss, bevor ein Security Incident oder eine Antwortaufgabe geschlossen oder abgebrochen werden kann. |
| Arbeitsnotizen zur Aufgabe in die Anforderung kopieren | Aktivieren Sie diese Option, um Arbeitsnotizen zur Antwortaufgabe mit den Arbeitsnotizen zum Security Incident zu synchronisieren. Wenn also Arbeitsnotizen in der Aufgabe hinzugefügt werden, werden dieselben Arbeitsnotizen im übergeordneten Security Incident angezeigt. |
| **Katalog- und Anforderungserstellung** | |
| Anforderungen per eingehender E-Mail erstellen und aktualisieren | Aktivieren Sie diese Option, um Security Incidents aus eingehenden E-Mails zu erstellen oder zu aktualisieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Anforderungen werden erstellt mit | Wählen Sie **Katalog oder ein reguläres Formular** aus, um den Katalog zu aktivieren und die automatische Veröffentlichung von Security Incident-Vorlagen im Katalog zu ermöglichen.<br><br>Wählen Sie **nur das reguläre Formular** aus, um den Katalog zu deaktivieren und die automatische Veröffentlichung von Security Incident-Vorlagen im Katalog zu deaktivieren. |
| Mit Vorlagen wird ein eigenes Katalogelement erstellt. | Aktivieren Sie diese Option, um die automatische Veröffentlichung von Katalogelementen für die Anwendung zu aktivieren. |
| **Benachrichtigungen** | |
| Wenn sich bei einer Anforderung oder Aufgabe das ausgewählte Feld ändert, wird eine Benachrichtigung an die Empfänger gesendet | Sie können Benachrichtigungen so konfigurieren, dass sie an bestimmte Empfänger gesendet werden, wenn sich ausgewählte Felder in Security Incidents und Antwortaufgaben ändern.<br>**a.** Wählen Sie unter **Tabelle**die Option **Anforderung (Security Incident** ) oder **Aufgabe (Antwortaufgabe)**aus.<br>**b.** Wählen Sie unter **Feld** das Feld zum Generieren von Benachrichtigungen aus. Wenn eine Änderung am ausgewählten Feld vorgenommen wird, wird eine Benachrichtigung an die identifizierten Empfänger gesendet.<br>**c.** Wählen Sie unter **Empfänger**einen oder mehrere Empfänger aus.<br>**d.** Wenn **ein bestimmter Benutzer** oder **eine bestimmte Gruppe** ausgewählt ist, werden Sie aufgefordert, einen Benutzer oder eine Gruppe auszuwählen.<br>**e.** Um weitere Benachrichtigungen mit anderen Feldern oder Empfängern zu definieren, wiederholen Sie die vorherigen Schritte für den nächsten Satz von Benachrichtigungseinstellungen.<br>**f.** Um eine Benachrichtigung zu entfernen, klicken Sie auf das ⊖ rechts neben der Benachrichtigung. |

**3.** Klicken Sie auf die Registerkarte **Zuweisung**, und füllen Sie die Felder aus.

**Konfigurationsbildschirm – Registerkarte „Zuweisung“.**

| Feld | Beschreibung |
|---|---|
| Zuweisungsmethode für Anforderungen | Wählen Sie die Methode für die Zuweisung von Security Incidents aus:<br>○ **automatische Zuweisung verwenden**: Security Incidents werden automatisch zugewiesen.<br>○ **Verwenden eines Workflows**: Security Incidents werden durch den ausgewählten Workflow zugewiesen.<br>○ **Manuell**: Security Incidents werden manuell zugewiesen. |
| Diesen Workflow zur Zuweisung von Anforderungen verwenden | Wählen Sie den Workflow für die Weiterleitung von Security Incidents aus. Dieses Feld wird angezeigt, wenn in der Liste |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Zuweisungsmethode für Anforderungen** die Option **Workflow verwenden** ausgewählt wird. |
| Zuweisungsmethode für Aufgaben | Wählen Sie die Methode für die Zuweisung von Antwortaufgaben aus:<br>○ **automatische Zuweisung verwenden**: Antwortaufgaben werden automatisch zugewiesen.<br>○ **Verwenden eines Workflows**: Antwortaufgaben werden durch den ausgewählten Workflow zugewiesen.<br>○ **manuell**: Antwortaufgaben werden manuell zugewiesen. |
| Verwenden Sie diesen Workflow, um Aufgaben zuzuweisen | Wählen Sie den Workflow für die Zuweisung von Antwortaufgaben aus. Dieses Feld wird angezeigt, wenn in der Liste **Zuweisungsmethode für Aufgaben** die Option **Workflow verwenden** ausgewählt wird. |
| Anforderungen oder Aufgaben basierend auf Abdeckungsgebieten von Zuweisungsgruppen zuweisen | Aktivieren Sie diese Option, um die Zuweisung von Security Incidents und Reaktionsaufgaben auf Gruppen zu beschränken, die den Standort der Aufgabe abdecken. |
| **Zeitplanung** | |
| Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird die Zeitzone für Aufgaben berücksichtigt | Aktivieren Sie diese Option, um die Zeitzone des Mitarbeiters zu berücksichtigen, wenn Sie eine Aufgabe zuweisen. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Reaktionsaufgaben ausgewählt ist. |
| **Zusätzliche Faktoren** | |
| Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird deren Standort berücksichtigt | Aktivieren Sie diese Option, um bei der Zuweisung von Aufgaben Mitarbeitern den Vorzug zu geben, die sich näher am Aufgabenstandort befinden. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Reaktionsaufgaben ausgewählt ist. |
| Bei der automatischen Auswahl von Mitarbeitern für Aufgaben werden bestimmte Kompetenzen vorausgesetzt. | Wählen Sie aus, inwieweit die Fähigkeiten von Service Desk-Mitarbeitern mit einer Aufgabe abgeglichen werden müssen, wenn die automatische Zuweisung bestimmt wird.<br>○ Wählen Sie **alle** aus, um festzulegen, dass ein zugewiesener Service Desk-Mitarbeiter über alle Kompetenzen verfügen muss, um die Aufgabe auszuführen. Ein Service Desk-Mitarbeiter, dem auch nur eine Kompetenz fehlt, wird eliminiert.<br>○ Wählen Sie **einige** aus, wenn Sie Service Desk-Mitarbeiter benötigen, die über die meisten der für die Ausführung der Aufgabe erforderlichen Kompetenzen verfügen.<br>○ Wählen Sie **Keine** aus, wenn Sie Agenten automatisch zuweisen möchten, ohne Kompetenzen zu berücksichtigen. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Reaktionsaufgaben ausgewählt ist. |
| Bei automatischer Auswahl wird versucht, allen Aufgaben in einer Anforderung denselben Service Desk-Mitarbeiter zuzuweisen | Aktivieren Sie diese Option, um alle Antwortaufgaben für einen Security Incident automatisch demselben Service Desk-Mitarbeiter zuzuweisen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **Add-ons**, und füllen Sie die Felder aus.

**Konfigurationsbildschirm – Registerkarte „Add-ons“.**

| Feld | Beschreibung |
|---|---|
| **Dokumentation** | |
| Eigene Knowledge Base aktivieren | Aktivieren Sie diese Option, um die Knowledge Base für Security Incident Responsezu aktivieren. |
| Verwaltete Dokumente aktivieren | Aktivieren Sie diese Option, um eine zugehörige Liste zu den verwalteten Dokumenten hinzuzufügen. |
| Aufgabenaktivitäten aktivieren | Aktivieren Sie diese Option, um Aufgabeninteraktionen und Kommunikationen wie Telefonanrufe und E-Mail-Nachrichten zu protokollieren. |

5. Klicken Sie auf **Speichern**.

### Sperren Sie die Sicherheitsverwaltung

Um Untersuchungen zu schützen und Security Incidents vertraulich zu behandeln, können Sie den Zugriff Security Incident Response auf sicherheitsspezifische Rollen und ACLs beschränken. Nicht-Sicherheitsadministratoren können vom Zugriff ausgeschlossen werden, es sei denn, Sie gewähren ihnen ausdrücklich Zutritt.

#### Vorbereitungen

Wenn die Anwendung Security Incident Response aktiviert ist, wird dem Systemadministratorbenutzer standardmäßig die Rolle sn_si.admin gewährt. Der Systemadministrator ist der einzige Administrator, der Sicherheitsgruppen und Benutzer einrichten kann.

Eine Sicherheitsrolle ist erforderlich, um Zugriff auf die Funktionen und Datensätze von Security Incident Response zu haben.

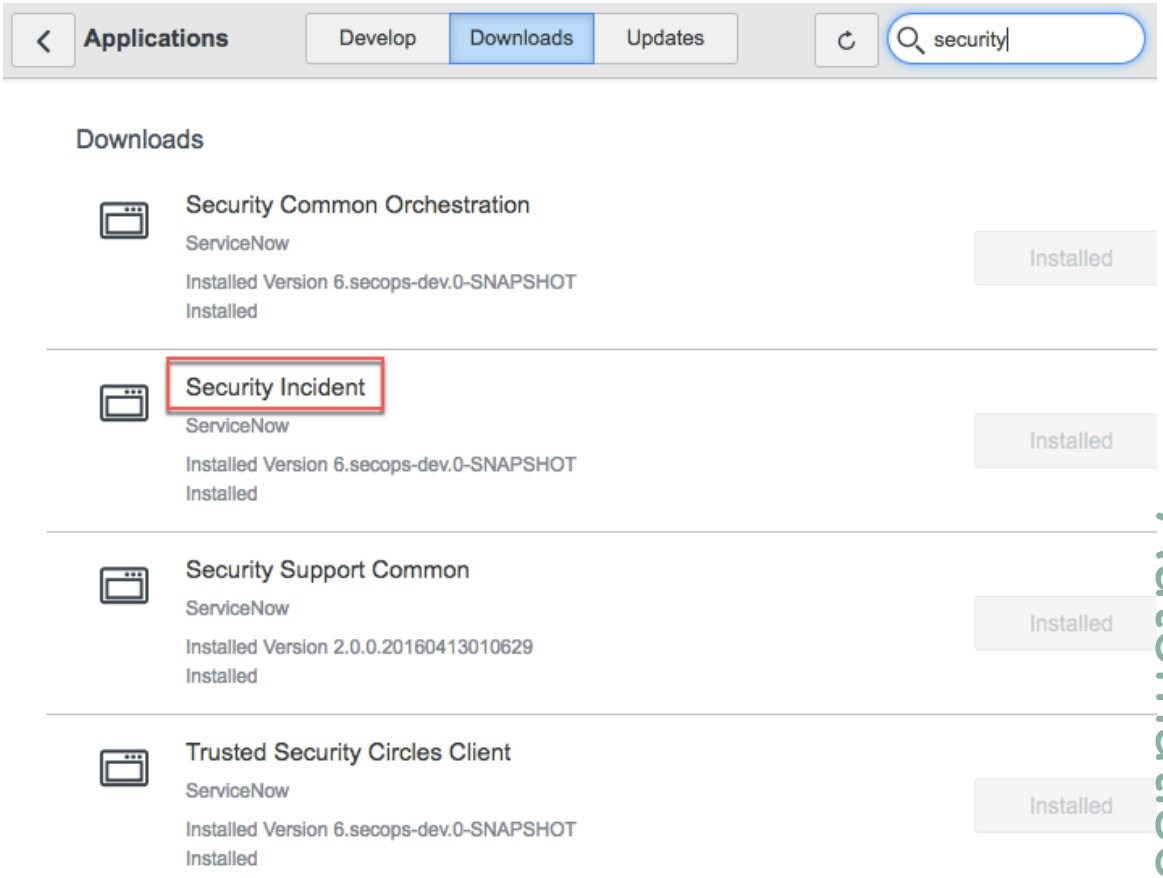
Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Nachdem das Plugin Security Incident Response aktiviert wurde, weist ein Benutzer mit der Administratorrolle mindestens einem Benutzer die Rolle des bereichsbezogenen Administrators (sn_si.admin) zu.
2. Der Benutzer mit der Administratorrolle wechselt in den Bereich Security Incident.
3. Navigieren zu **Systemanwendungen** > **Anwendungen**.
4. Klicken Sie auf **Downloads**.
5. Geben Sie **Sicherheit** in das Feld **Anwendungen** durchsuchen ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Security Incident**.
7. Scrollen Sie nach unten zu **Zugehörige Links**, und klicken Sie auf **Entfernen aus der Rolle des Administrators**.
8. Melden Sie sich ab und wieder an.
   Der Administratorbenutzer kann nicht auf die Anwendung Security Incident Response zugreifen.

**Zugehörige Informationen**

Anwendungsverwaltung

### Verwalten Sie den eingeschränkten Aufruferzugriff

Mit der RCA-Funktion (Restricted Caller Access) kann ein Administrator den bereichsübergreifenden Zugriff auf eine Anwendung oder Anwendungsressource definieren und Zugriffsanforderungen zulassen oder verweigern. Diese Funktion ist in Security Incident Response standardmäßig aktiviert, damit Sicherheitsanalysten vertrauliche sicherheitsbezogene Informationen schützen können.

Ein Feld mit der Bezeichnung **Aufruferzugriff** wurde allen Tabellen und Skripteinbindungen in Security Incident Responsehinzugefügt, und das Feld ist standardmäßig auf **Anruferverfolgung festgelegt**. Diese Einstellung bedeutet, dass Anwendungsbereiche Zugriff auf Security Incident Response Tabellen und Skripteinbindungen haben. Es wird jedoch für jeden Datensatz ein Nachverfolgungsdatensatz erstellt und in der Tabelle „Eingeschränkte Aufruferzugriffsberechtigung“ [sys_restricted_caller_access] gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Seien Sie vorsichtig, wenn Sie Datensätze von **„Anruferverfolgung“** zu „ **Anrufer eingeschränkt“**ändern. Auf Datensätze mit diesem Status kann erst zugegriffen werden, wenn ein Administrator den Zugriff manuell erlaubt. Der Administrator muss zu navigieren **Systemanwendungen** > **Anwendung – Eingeschränkter Aufruferzugriff**, suchen Sie die Tabelle oder Skripteinbindung, für die Zugriff angefordert wurde, und ändern Sie das Feld **Status** von **Angefordert** in **Zulässig**.

**Zugehörige Informationen**

Einstellungen für eingeschränkte Anruferzugriffsberechtigungen

Legen Sie den Anwendungsbereich, die Anwendungsressource und den Event-Zugriff fest

## Schnellstarttests für Security Incident Response ausführen

Überprüfen Sie, ob Security Incident Response weiterhin funktioniert, nachdem Sie Konfigurationsänderungen vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwicklung einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Security Incident Response-Schnellstarttests erfordern die Aktivierung des Plugins „Security Incident Response“ (com.snc.security_incident) und das Laden der Demodaten.

### Security Incident Response-Tests

| Test | Beschreibung | Release-Version |
|---|---|---|
| SIR: Sicherheitsincident erstellen | Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Sicherheitsincident-Formular erstellen kann. | Washington DC |
| SIR: Sicherheitsincident über den Sicherheitsincident-Katalog erstellen | Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Katalog erstellen kann. | Washington DC |
| SIR: Lebenszyklus des Sicherheitsincident | Validiert die Antwortaufgaben des Richtlinienverletzungs-Workflows. | Washington DC |
| SIR: Bedrohungssuche | Validiert die Funktion der Bedrohungssuche. | Washington DC |
| SIR: PIR Assessments OOTB configuration (SIR: PIR-Bewertungen – OOTB-Konfiguration) | Mit diesem Test können Sie PIR-Bewertungen und Basissystemkonfigurationen validieren. | Washington DC |
| SIR: PIR Assessments conditional configuration (SIR: PIR-Bewertungen – Bedingte Konfiguration) | Verifiziert, dass Security Incidents, die der obligatorischen bedingten Regel entsprechen, erst geschlossen werden, wenn die Bewertung nach dem Incident abgeschlossen ist.<br><br>Verifiziert, dass Security Incidents, die der optionalen bedingten Regel entsprechen, geschlossen | Washington DC |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident Response-Tests (Fortsetzung)

| Test | Beschreibung | Release-Version |
|---|---|---|
| | werden können, wenn die Bewertung nach dem Incident abgeschlossen ist.<br><br>Verifiziert, dass für Security Incidents, die keiner Regel entsprechen, keine Bewertungen generiert werden. | |
| SIR: PIR-Laufzeitverifizierung | Überprüft, ob PIR-Berichte gemäß dem neuen Design konfiguriert und an Sicherheits-Incidents angehängt werden. | Washington DC |
| SIR: Setupverifizierung der PIR-Designzeit | Überprüft, ob der Sicherheit-Incident je nach Administratorkonfiguration der Berichtsvorlage zugeordnet wird. | Washington DC |
| SIR: Security Incident mit einem vorhandenen schwerwiegenden Security Incident verknüpfen | Verknüpfen Sie einen Security Incident mit einem vorhandenen schwerwiegenden Security Incident, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden. | Washington DC |
| SIR: Security Incident als schwerwiegenden Security Incident hochstufen | Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident hoch, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden. | Washington DC |
| SIR: Security Incident als schwerwiegenden Security Incident vorschlagen | Schlagen Sie einen Security Incident als einen schwerwiegenden Security Incident vor, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden. | Washington DC |
| Verifiziert, dass nur zulässige Mitglieder auf den Security Incident zugreifen können, sobald „Beschränkung erzwingen“ aktiviert ist | Verifiziert, dass nur die zulässigen Mitglieder auf den Security Incident zugreifen können, sobald „Beschränkung erzwingen“ aktiviert ist. | Washington DC |
| Verifiziert, dass nur zulässige Gruppen auf den Security Incident zugreifen können, sobald | Verifiziert, dass nur die zulässigen Gruppen auf den Security Incident zugreifen können, sobald | Washington DC |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident Response-Tests (Fortsetzung)**

| Test | Beschreibung | Release-Version |
|---|---|---|
| „Beschränkung erzwingen“ aktiviert ist | „Beschränkung erzwingen“ aktiviert ist. | |
| Lesezugriff validieren | Validieren Sie den Anzeigezugriff. | Washington DC |
| Schreibzugriff validieren | Validieren Sie den Bearbeitungszugriff. | Washington DC |

**Zugehörige Informationen**

Schnellstarttests

### Referenz zum Setup-Assistenten

Der Setup-Assistent führt Sie durch die Schritte, die Sie zum Einrichten des Security Incident Response Basissystems ausführen müssen. Dieser Abschnitt enthält zusätzliche Informationen zu den komplizierten Schritten, für die Sie möglicherweise weitere Erklärungen benötigen.

### Erstellen Sie eine Security Incident Response -Prozessdefinition

Sie können eine Prozessdefinition erstellen, um zu definieren, wie Security Incidents von einem Status in den nächsten übergehen. Prozessdefinitionen geben Service Desks und Endbenutzern Hilfe bei der Nachverfolgung des Problems während des gesamten Lebenszyklus.

#### Vorbereitungen

Erforderliche Rolle: sn.si_admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Prozessdefinition**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

**Erstellen von Prozessdefinitionen**

| Feld | Beschreibung |
|---|---|
| Name | Name des Datensatzes, der den in der Skripteinbindungsdatei codierten Prozess beschreibt. Der Name wird als Auswahl in der Liste **Prozessdefinitionsauswahl** angezeigt. |
| Skripteinbindung | Der Name (einschließlich des Präfix `sn_si.` ) der Skripteinbindung, die die Definition des Prozesses enthält. Das Skript muss sich im Anwendungsbereich Security Incident (`sn_si`) befinden. Weitere Informationen finden Sie unter Erstellen Sie eine benutzerdefinierte Security Incident Response Skripteinbindung für Prozessdefinitionen. Wenn dieses Feld keinen gültigen Skripteinbindungsnamen enthält, wird die Standarddefinition ProcessDefinition_NIST_Stateful verwendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beschreibung | Hilfreiche Informationen zur Skripteinbindung. |
| Bestellen | Bestimmt die Position in der Prozessdefinitionsliste. |
| Aktiv | Wenn diese Option aktiviert ist, kann diese Prozessdefinition auf der Seite „ **Prozessdefinitionsauswahl** “ ausgewählt werden. |

4. Klicken Sie auf **Absenden**.

**Zugehörige Informationen**

Prozessauswahl für Security Incident Response

Security Incident Response-Prozessdefinition verstehen

### Security Incident Response-Prozessdefinition verstehen

Security Incident Response Prozessdefinition ersetzt Statusabläufe und stellt Endbenutzern und Service Desks den Status eines Problems bereit. Eine Prozessdefinition hilft, das Problem während seines Lebenszyklus nachzuverfolgen. Security Incident Response ist eine Service Management (SM)-Anwendung, die über eigene Status verfügt. Ungültige Status werden als Teil von Prozessauswahlgemeldet.

## Security Incident Response – Prozessdefinition

Die Standardprozessdefinition (NIST Stateful) definiert die folgenden Incident-Status:

**Hinweis:**
Die verfügbaren Status variieren je nach aktuellem Status des Incident.

### Status der Security Incident-Prozessdefinition

| Status | Beschreibung |
|---|---|
| Entwurf | Der Initiator der Anforderung fügt Informationen zum Security Incident hinzu, der jedoch noch nicht zur Bearbeitung bereit ist. |
| Analyse | Der Incident wurde zugewiesen, und das Problem wird analysiert. |
| Eindämmen | Das Problem wurde identifiziert, und das Sicherheitspersonal arbeitet daran, es einzudämmen und Schadensbegrenzung durchzuführen. Zu diesen Aktionen gehören das Offlineschalten von Servern, das Trennen von Geräten vom Internet und das Überprüfen, ob Sicherungen vorhanden sind. |
| Beseitigen | Das Problem wurde eingedämmt, und das Sicherheitspersonal unternimmt Schritte, um das Problem zu beheben. |
| Wiederherstellen | Das Problem wurde gelöst, und die Betriebsbereitschaft der betroffenen Systeme wird überprüft. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Status der Security Incident-Prozessdefinition (Fortsetzung)**

| Status | Beschreibung |
|---|---|
| Prüfung | Der Security Incident ist abgeschlossen, und alle Systeme funktionieren wieder normal. Eine Überprüfung nach dem Incident ist jedoch noch erforderlich. |
| Geschlossen | Der Incident ist abgeschlossen, aber bevor ein Security Incident geschlossen werden kann, müssen Sie die Informationen auf der Registerkarte **Abschlussinformationen** ausfüllen. |

## Prozessdefinitionen für Security Incident-Aufgaben

Die folgenden Prozessdefinitionen werden für Security Incident-Aufgaben verwendet.

**Status der Aufgabenprozessdefinition**

| Status | Beschreibung |
|---|---|
| Bereit | Die Aufgabe kann bearbeitet werden, nachdem sie einem Service Desk-Mitarbeiter zugewiesen wurde. |
| Zugewiesen | Die Aufgabe wird einem Service Desk-Mitarbeiter zugewiesen. |
| In Bearbeitung | Der zugewiesene Service Desk-Mitarbeiter arbeitet an der Aufgabe. |
| Abgeschlossen | Die Aufgabe ist abgeschlossen. |
| Abgebrochen | Die Aufgabe wurde abgebrochen. |

NIST unterstützt die folgenden zwei Modelle:

- **NIST Stateful**

  Mit dieser Prozessdefinition können Analysten in sequenzieller Reihenfolge von einem Status in einen anderen wechseln, ohne einen Schritt zu überspringen. Wenn der Analyst beispielsweise mit dem Status „ **Entwurf** “ beginnt, lautet die sequenzielle Reihenfolge dieser Prozessdefinition „ **Entwurf**“ >**„Analyse“**> „**Eindämmen**“ > „**Beseitigen**“ > „**Wiederherstellen**“. Daher ist die Stateful-Prozessdefinition des NIST unidirektional und ermöglicht es Analysten, nur zu den Vorwärtsstatus zu gelangen.

  Hier ein weiteres Beispiel: Wenn der Analyst mit dem Status „Analyse“ beginnt, lautet die sequenzielle Reihenfolge dieser Prozessdefinition **„Analyse“**> „**Eindämmen**“ > „**Beseitigen**“ > „**Wiederherstellen**“.

- **NIST Open**

  Diese Prozessdefinition ermöglicht es Analysten, von einem Status in einen anderen zu wechseln, entweder vorwärts oder rückwärts. Wenn der Analyst beispielsweise mit dem Status **„Analyse“** beginnt, kann die Reihenfolge der Prozessdefinition entweder „ **Analyse“**> „**Eindämmen**“ > „**Beseitigen**“ > „**Wiederherstellen** “ oder **„Analyse**>**Entwurf**“ sein. Daher ist die NIST Open-Prozessdefinition bidirektional und ermöglicht es Analysten, je nach ihren Anforderungen in den Status „Vorwärts“ oder „Rückwärts“ zu wechseln.

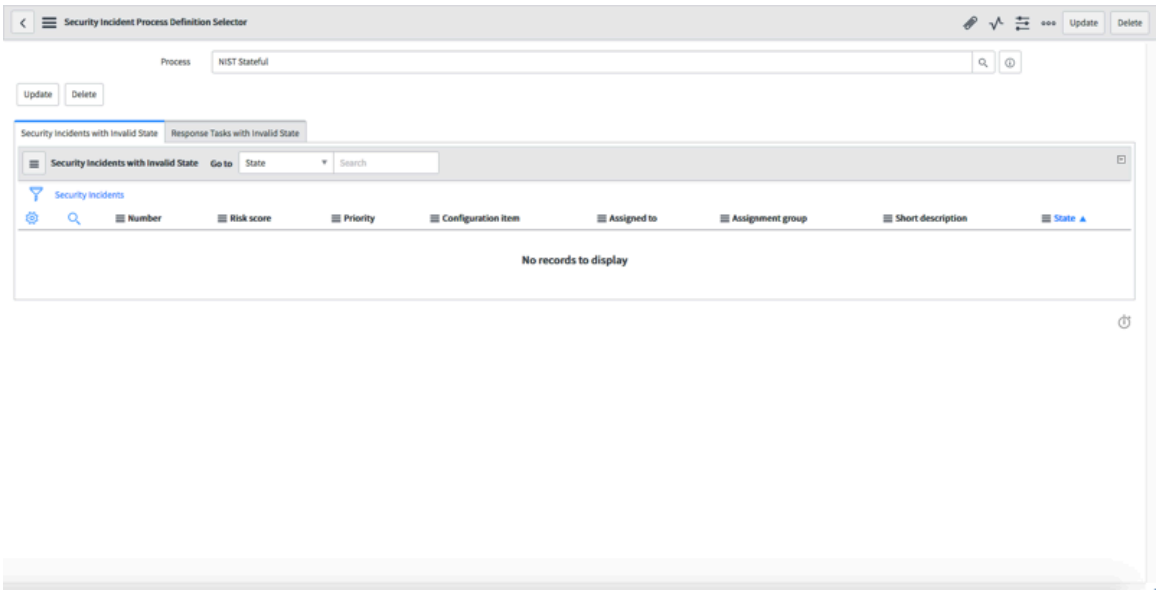


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozessauswahl für Security Incident Response

Prozessauswahl listet Prozesse mit ungültigen Status für Security Incidents und Antwortaufgaben auf.

Ein Administrator kann den Incident oder die Aufgabe entweder manuell oder mithilfe eines Skripts in einen gültigen Status versetzen. Eine leere zugehörige Liste (keine Incidents; keine Aufgaben) gibt an, dass sich jede aktive Aufgabe in einem gültigen Status befindet. Die verfügbaren Status variieren je nach aktuellem Status des Incident. Weitere Informationen finden Sie unter Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen.




### Wählen Sie eine Security Incident Response Prozessdefinition aus

Sie können die Prozessdefinition auswählen, die für die entsprechenden Status für Security Incidents und Reaktionsaufgaben Ihres Unternehmens verwendet werden soll.

## Vorbereitungen

Erforderliche Rolle: admin und sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

## Prozedur

1. Navigieren zu **Alle** > **Security Incident Response** > **Administration** > **Prozessauswahl**.
2. Klicken Sie auf das Suchsymbol, um die verfügbaren Prozessdefinitionen aufzulisten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie eine Prozessdefinition aus.
4. Klicken Sie auf **Aktualisieren**.

### Erstellen Sie eine benutzerdefinierte Security Incident Response Skripteinbindung für Prozessdefinitionen

Erstellen Sie ein benutzerdefiniertes Prozessdefinitionsskript für die entsprechenden Status für Security Incidents und Reaktionsaufgaben Ihres Unternehmens.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

Die Hauptskripteinbindung sn_si.ProcessDefinition steuert Prozessdefinitionen. **Prozessdefinition** bestimmt, welche Definition verwendet wird (mithilfe der **Prozessauswahl**). Sie ruft die entsprechende Skripteinbindungsdatei auf, um die Anfangsstatus und Übergänge für Security Incidents und Antwortaufgaben zu bestimmen.

## Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

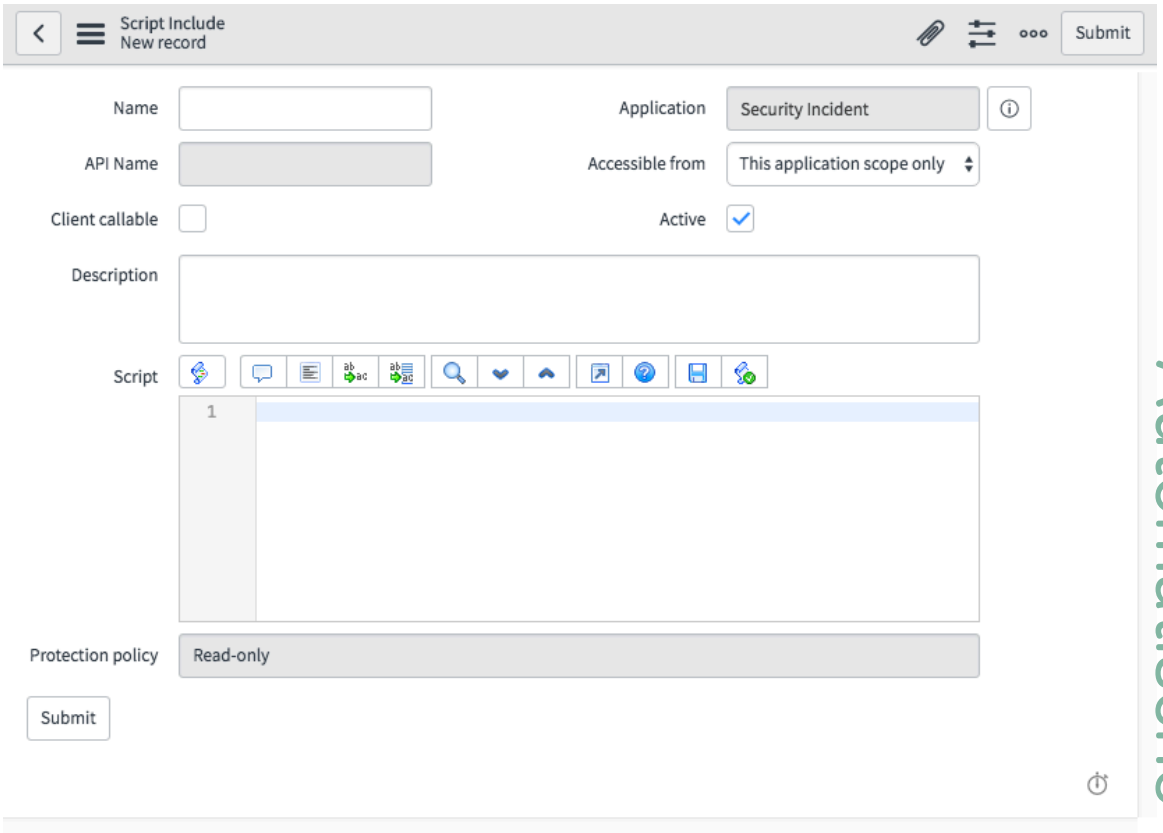
### Erstellen von Prozessdefinitionen

| Feld | Beschreibung |
|---|---|
| Name | Name dieser Skripteinbindung. |
| API-Name | Erstellt basierend auf dem Namen der Skripteinbindung. |
| Vom Client aufrufbar | Macht die Skripteinbindung für Client-Skripts, Listen- und Berichtsfilter, Referenzqualifizierer oder, verfügbar, falls, als Teil der URL angegeben ist. |
| Anwendung | Security Incident |
| Zugänglich von | Wählen Sie **Nur Dieser Anwendungsbereich aus** . |
| Aktiv | Wenn diese Option aktiviert ist, kann diese Skripteinbindung auf der Seite „ **Prozessdefinition** “ ausgewählt werden. |
| Beschreibung | Hilfreiche Informationen zur Skripteinbindung. |
| Skript | Definiert das serverseitige Skript, das ausgeführt werden soll, wenn es von anderen Skripts aufgerufen wird.<br><br>Das Skript muss eine einzelne JavaScript-Klasse oder eine globale Funktion definieren. Der Klassen- oder Funktionsname muss mit dem Wert im Feld Name übereinstimmen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Weitere Informationen zu Skriptinhalten finden Sie unter Prozessdefinition Skripteinbindung. |




4. Klicken Sie auf **Absenden**.

### Zugehörige Informationen

Prozessdefinition Skripteinbindung

## Prozessdefinition Skripteinbindung

Die Skripteinbindung „Prozessdefinition“ stellt Methoden zum Definieren einer Prozessdefinition bereit.

Implementieren Sie die hier beschriebenen Konstanten, Attribute, Arrays und Methodenaufrufe, um eine Skripteinbindung für Prozessdefinitionen anzupassen.

## Verwendungszweck

Verwenden Sie diese Skripteinbindung, um eine Prozessdefinition zu erstellen.

## Text der Skripteinbindung

Der Skripteinbindungstext besteht aus drei Abschnitten:

- Konstanten: Definitionen des Anfangsstatus
- Security Incident and Response Task: Prozessdefinitions-Arrays
- Methodenaufrufe: Abrufen von Informationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Konstanten

Konstanten werden verwendet, um die Anfangsstatus von Security Incidents und Reaktionsaufgaben zu definieren.

Die Verwendung von Konstanten ist optional, wird jedoch aus Gründen der Lesbarkeit empfohlen. Beispiel:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Die später von den folgenden Methoden verwendet werden:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

Der nächste Satz von Konstanten definiert die Status für Security Incidents und Antwortaufgaben.

Jedes Array enthält auch die Definition, welche Status verfügbar sind, wenn sich der Incident oder die Aufgabe in einem bestimmten Status befindet.

Beispiel:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

Das Beispiel ist ein Array von Objekten. Jedes Objekt definiert einen Status und mögliche Übergangsstatus.

Die Reihenfolge des Statusobjekts bestimmt die gewünschte Reihenfolge für den Flow.

Wenn sich die Aufgabe im Status „Entwurf“ befindet (Wert 1), sind folgende Status möglich: 1 (Entwurf, d. h. keine Änderung) und 10 (Bereit, nächster Schritt im Prozess).

Es gibt keine Begrenzung für die Anzahl der Übergänge aus einem Status. Die Status „Abschließen – vollständig“ und „Abgebrochen“ sind Endstatus und weisen daher keine möglichen Statusübergänge auf.

Die Reihenfolge der Attribute im Objekt ist nicht wichtig. Wenn es die Definition klarer macht, setzen Sie die Bezeichnung zuerst.

## Attribute

Erforderliche Attribute in einem Statusdefinitionsobjekt sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- state: numerischer Wert des Status
- label: Visuell lesbarer Text, der dem Status zugeordnet ist
- Auswahl: ein Array von Statuswerten, in die der Status übergehen kann (bestimmt den Inhalt der Status-Dropdown-Liste)

Optionale Attribute:

- obligatorisch: Liste der Feld-IDs, die in diesem Status obligatorisch werden
- schreibgeschützt: Liste der Feld-IDs, die in diesem Status schreibgeschützt werden
- Sichtbar: Liste der Feld-IDs, die in diesem Status sichtbar werden
- notmandatory: Liste der Feld-IDs, die in diesem Status nicht obligatorisch werden
- notvisible: Liste der Feld-IDs, die in diesem Status nicht mehr sichtbar wären

**Hinweis:**

Wenn optionale Attribute verwendet werden, liegt es in der Verantwortung des Autors, sicherzustellen, dass Felder zwischen den Status sichtbar/unsichtbar, obligatorisch/nicht obligatorisch, sichtbar/ausgeblendet oder schreibgeschützt gemacht werden.

Wenn Sie beispielsweise ein Feld in einem Status ausblenden, wird es später in einem anderen Status nicht sichtbar, es sei denn, das Attribut „Sichtbar“ wird verwendet.

### Arrays der Prozess-Flow-Definition

Um die im Prozess-Flow-Formatierer angezeigten Informationen zu definieren (die Leiste oben in den Formularen „Security Incident“ und „Antwortaufgabe“) benötigt das System Informationen darüber, was für jeden Status angezeigt werden soll.

Beispiel:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

Das TASK_PF-Array ist eine Sammlung von Bezeichnungen, Bedingungen und Beschreibungen, die zur Bestimmung des in der Prozessformatierer-Leiste angezeigten Texts verwendet werden (einschließlich Reihenfolge und Aktivität).

In diesem Beispiel wird der Text „Bereit“ als zweites Element angezeigt. Er wird hervorgehoben, wenn die Aufgabe die Bedingung „state=10^EQ“ erfüllt.

Wenn der Mauszeiger über den Text bewegt wird, wird die Beschreibung „Security Incident Response-Aufgabe ist bereit zur Zuweisung“ angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Status können zu einem einzelnen Formatiererstatus kombiniert werden.

Im Beispiel werden die Status „Abschließen – vollständig“ und „Abgebrochen“ in der oberen Leiste als „Geschlossen“ angezeigt.

### Methodenaufrufe

Die folgenden Methoden müssen in der Skripteinbindung vorhanden sein, da sie von sn_si.ProcessDefinition verwendet werden:

| Rückgabetyp | Methodenübersicht | Beschreibung |
|---|---|---|
| Zeichenfolge | getInitialIncidentState: Funktion() | Gibt den anfänglichen numerischen Wert des Incident-Status zurück |
| Zeichenfolge | getInitialTaskState: Funktion(): | Gibt den numerischen Wert des anfänglichen Aufgabenstatus zurück |
| Array von Zeichenfolgen | getIncidentStates: Funktion(): | Array des Incident-Status zurückgeben |
| Array von Zeichenfolgen | getTaskStates: Funktion(): | gibt das Array des Aufgabenstatus zurück |
| Array von Objekten | getIncidentProcessFlows: Funktion(): | Gibt das Definitions-Array des Incident-Prozess-Flows zurück |
| Array von Objekten | getTaskProcessFlows: Funktion (): | Gibt das Definitions-Array des Aufgabenprozess-Flows zurück |

Die nächsten Methoden werden immer dann aufgerufen, wenn ein Incident oder eine Aufgabe aktualisiert wird, und ermöglichen Aktionen für bestimmte Change-Übergänge.

| Rückgabetyp | Methodenübersicht | Beschreibung |
|---|---|---|
| void | performIncidentStateChange: function(current, previous) | In den Beispielen wird diese Methode verwendet, um SM-bezogene Werte festzulegen und sicherzustellen, dass ein Incident aus „Entwurf“ entfernt wird, sobald ihm jemand zugewiesen wurde. |
| void | PerformTaskStateChange: function(current, previous) | Im Beispiel wird diese Methode verwendet, um Zeitstempel zu aktualisieren (bei Zuweisung und Abschluss) und die Aufgabe von „Bereit“ auf „Zugewiesen“ zu verschieben, sobald das Feld „assigned_to“ ausgefüllt ist. |

Dieselben Aktionen, die von diesen beiden Methoden ausgeführt werden, können mithilfe einer Geschäftsregel ausgeführt werden. Durch die Definition in der Skripteinbindung wird das Wechseln von Prozessdefinitionen erleichtert.

#### Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen

Ein Administrator kann den Security Incident oder die Aufgabe entweder manuell oder mithilfe eines Skripts auf gültige Status zurücksetzen. Die verfügbaren Status variieren je nach aktuellem Status des Incident.

### Vorbereitungen

Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

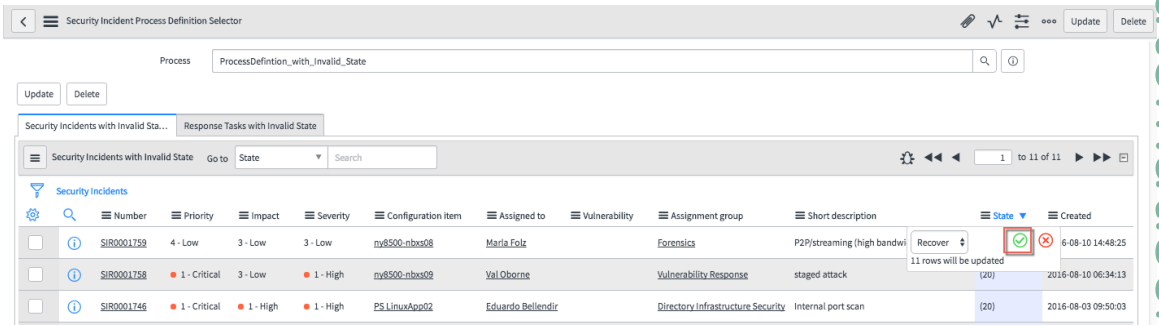
### Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie die Prozessdefinitionen gewechselt haben, unterstützt die neue Definition möglicherweise einige der alten Status nicht. Um die verwaisten Incident- oder Aufgabenstatus zu korrigieren, können Sie Ihre Prozessdefinition ändern, Ihre Skripteinbindung bearbeitenoder jeden Incident oder jede Aufgabe manuell öffnen, um den Status zu aktualisieren. Im Allgemeinen ist das Aktualisieren des Status (was in großen Mengen möglich ist) die einfachste Lösung.

Um Status in Massen zu ändern, gehen Sie wie folgt vor:

### Prozedur

1. Navigieren zu **Alle** > **Prozessauswahl**.
2. **Markieren** Sie das Feld Status für die Incidents oder Aufgaben, die Sie ändern möchten.
3. Doppelklicken Sieauf das Feld Status im ersten Datensatz, wählen Sie den neuen **Status aus,** und **klicken** Sie auf das grüne Häkchen ( ), um die Änderung abzuschließen.




4. Klicken Sie auf **Aktualisieren**.

## Erstellen Sie eine Security Incident-Gruppe

Richten Sie eine Security Incident-Gruppe ein, und weisen Sie ihr die entsprechenden Rollen und Benutzer zu.

### Vorbereitungen

Erforderliche Rollen:

- Wenn Sie die Rolle user_admin haben, können Sie Security Incident-Zuweisungsgruppen erstellen.
- Wenn Sie die Rolle sn_si.admin haben, können Sie Security Incident-Zuweisungsgruppen erstellen und bearbeiten.

### Warum und wann dieser Vorgang ausgeführt wird

Benutzer in einer Gruppe erben die Rollen der Gruppe, sodass Sie nicht jedem Benutzer separat Rollen zuweisen müssen.

Es wird empfohlen, in Ihrer Organisation so viele Gruppen wie erforderlich zu erstellen. Es wird auch empfohlen, eine Gruppe für Administratoren zu erstellen und die Administratorrolle nur dieser Gruppe zuzuweisen.

### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen** oder **Security Incident** > **Setup** > **Gruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Weitere Informationen finden Sie unter Benutzergruppen erstellen .

4. Stellen Sie sicher, dass Sie den **Security Incident** -Typ für diese Gruppe auswählen.
   a. Wenn das Feld **Typ** nicht sichtbar ist, konfigurieren Sie das Formular, um es hinzuzufügen.
   b. Klicken Sie auf das Schlosssymbol neben dem Feld **Typ**.
   c. Klicken Sie auf das Referenz-Suchsymbol ( ).
   d. Suchen Sie nach dem **Security Incident** -Typ, und wählen Sie ihn aus.
5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. **Fügen** Sie in der zugehörigen Liste Rollen die Rollen hinzu, die jedes Mitglied dieser Gruppe erhält. Wenn Sie beispielsweise eine Gruppe für Security Incident Response Teammitglieder erstellen, fügen Sie sn_si.analyst hinzu. Wenn Sie eine Gruppe für Security Incident Response Administratoren erstellen, fügen Sie sn_si.admin hinzu.
7. **Fügen** Sie in der zugehörigen Liste „Gruppenmitglieder“ Benutzer zu dieser Gruppe hinzu.
8. Klicken Sie auf **Aktualisieren**.

### Erstellen Sie eine Rechnergruppe für Security Incidents

Security Incident-Rechnergruppen werden zum Gruppieren von Rechnern verwendet.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Security Incident-Rechners. |
| Anwendung | Die Anwendung, die diesen Datensatz enthält. |
| Bestellung | Die Reihenfolge, in der der Security Incident Calculator ausgeführt wird. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Beschreibung | Eine Beschreibung dieser Rechnergruppe. |
| Erstellt von | Geben Sie den Namen des Benutzers ein, der erstellt hat |

4. Klicken Sie auf **Absenden**.

### Erstellen Sie einen Security Incident-Rechner

Mit Security Incident-Rechnern können Sie den Schweregrad eines Security Incident anhand vordefinierter Formeln berechnen. Sie können nach Bedarf eigene Security Incident-Rechner definieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**.
2. Klicken Sie auf den Namen der Gruppe, für die Sie einen Rechner erstellen möchten, oder erstellenSie eine Rechnergruppe.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Security Incident-Rechners. |
| Rechnergruppe | Name der Gruppe, zu der dieser Rechner gehört.<br>**Hinweis:**<br>Die Rechnergruppe kann erstellt oder geändert werden, nachdem Sie **Name** und **Tabelle**eingegeben haben. |
| Tabelle | Wählen Sie die Tabelle aus, die für diesen Rechner verwendet werden soll.<br>Wenn Sie Rechner zu anderen Tabellen als „Schwachstelle“ [sn_vul_vulnerability] und „Angreifbares Element“ [sn_vul_vulnerable_item] hinzufügen, müssen Sie diesen Tabellen Geschäftsregeln und UI-Aktionen hinzufügen. So sehen Sie sich Beispiele an:<br>○ Navigieren zu **Systemdefinition** > **Business-Regeln**, und suchen Sie die Geschäftsregel **Schweregrad berechnen** in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item].<br>○ Navigieren zu **System-UI** > **UI-Aktionen**, und suchen Sie die UI-Aktion „ **Schweregrad** berechnen“ in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item].<br>Außerdem müssen der Schwachstellenadministratorrolle vollständige Lese- und Schreibfunktionen (oder save_as_template) für jede von einem Rechner verwendete Tabelle gewährt werden, damit die auf die Vorlage anzuwendenden Werte ordnungsgemäß angezeigt werden. |
| Anwendung | Die bereichsbezogene Anwendung, zu der der Rechner gehört. |
| Bestellung | Die Reihenfolge, in der der Security Incident Calculator ausgeführt wird. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Aktiv | Schalten Sie den Rechner ein oder aus. |
| Beschreibung | Eine Beschreibung dieses Rechners. |

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarten Anzuwendende **Bedingungen** und **Werte werden angezeigt**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Füllen Sie die Felder auf der Registerkarte **Bedingungen** entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Filtergruppe verwenden | Aktivieren Sie diese Checkbox, um eine vordefinierte Filtergruppe zu verwenden, oder erstellen Sie eine neue Filtergruppe, um die Rechnerkriterien zu definieren. |
| Filtergruppe | Wählen Sie die Filtergruppe aus, die zum Definieren eines Rechners verwendet werden soll.<br><br>Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppen verwenden** aktiviert haben. |
| Erweiterte Bedingungen verwenden | Aktivieren Sie diese Checkbox, um anzugeben, dass eine Skriptbedingung verwendet wird, um zu bestimmen, wann dieser Rechner angewendet wird. Wenn Sie das Kontrollkästchen aktivieren, wird das Feld **Erweiterte Bedingungsskripts** angezeigt.<br><br>Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert haben, wird dieses Feld ausgeblendet.<br><br>**Hinweis:**<br>Bevor Sie erweiterte Bedingungen definieren und Skripts schreiben, um zu bestimmen, wann die Security Incident-Rechner angewendet werden, kehren Sie zur Liste der Security Incident-Rechner zurück. Erkunden Sie die Rechnerdatensätze, die im Lieferumfang des Basissystems enthalten sind. |
| Bedingung | Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet wird.<br><br>Wenn Sie eines der Kontrollkästchen **Filtergruppeverwenden oder Erweiterte Bedingungen** verwenden aktiviert haben, wird dieses Feld ausgeblendet. |

7. Klicken **Sie auf die Registerkarte Anzuwendende Werte** und füllen Sie die Felder im Formular entsprechend aus.
Sie haben die Möglichkeit, ein Skript zum Definieren der auf die Berechnung anzuwendenden Werte zu erstellen oder eine Vorlage basierend auf Feldern in der ausgewählten Tabelle zu definieren.

| Feld | Beschreibung |
|---|---|
| Skriptwerte verwenden | Aktivieren Sie diese Checkbox, um Feldwerte mit einem Skript zu definieren. |
| Skriptwerte | Definiert, auf welche Werte die Berechnungen angewendet werden sollen.<br><br>Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Skriptwerte verwenden** aktiviert haben. |
| Vorlage | Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**. Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten. |

8. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident-Rechner verstehen

Security Incident-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.

Das Security Incident Response Basissystem enthält die folgenden Security Incident-Rechnergruppen und -Rechner. In jeder Gruppe wird der erste Rechner ausgeführt, der die Bedingungen erfüllt.

#### Security Incident-Rechner im Basissystem

| Name der Security Incident-Rechnergruppe | In der Gruppe enthaltene Rechner | Beschreibung |
|---|---|---|
| Geschäftsauswirkung | Aus Schweregradrechnern zusammenfassen | Dieser Rechner wird an den Sicherheitskritikalitätsrechner delegiert, der die Relevanz durch Gewichtung der Werte anderer Felder bestimmt. |
| Schweregrad | Betroffenes Geschäft | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators. |
| | Wichtiger Service betroffen | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung.<br><br>Wenn das Konfigurationselement im Security Incident einem äußerst wichtigen Business Service zugeordnet ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition des Rechners erhöht. |
| | Kritische Serviceänderungen | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung.<br><br>Wenn der Security Incident die Bedingungen erfüllt, wird ein Skript ausgeführt, um zu definieren, auf welche Ebenen die Felder angehoben werden. Wenn das Konfigurationselement im Security Incident einem sehr kritischen oder einigermaßen kritischen Business Service zugeordnet ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition des Rechners erhöht. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident-Rechner im Basissystem (Fortsetzung)

| Name der Security Incident-Rechnergruppe | In der Gruppe enthaltene Rechner | Beschreibung |
|---|---|---|
| | Multi-Attack-Vektoren | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators.<br><br>Wenn das Konfigurationselement im Security Incident mit Angriffsvektoren aus dem Internet, E-Mail und Identitätswechsel verknüpft ist, werden die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** entsprechend der Definition des Rechners erhöht. |
| | Legen Sie die Priorität mit Kategorie und Services fest | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators.<br><br>Die Security Incident-Priorität wird auf **1 – Kritisch** festgelegt, wenn die folgenden Bedingungen erfüllt sind:<br>• Dem Security Incident sind betroffene Services zugeordnet, von denen einer kritisch ist.<br>• Die Security Incident-Kategorie ist eine der folgenden:<br>◦ Denial of Service<br>◦ Spear-Phishing<br>◦ Böswillige Code-Aktivität<br><br>**Hinweis:**<br>Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe „Starter Security Operation“ haben. |
| | Legen Sie die Priorität für erkennbare Elemente fest | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators.<br><br>Die Security Incident-Priorität wird auf **1 – Kritisch** festgelegt, wenn die folgenden Bedingungen erfüllt sind: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident-Rechner im Basissystem (Fortsetzung)**

| Name der Security Incident-Rechnergruppe | In der Gruppe enthaltene Rechner | Beschreibung |
|---|---|---|
| | | • Dem Security Incident sind betroffene Services zugeordnet, von denen einer kritisch ist.<br>• Die Security Incident-Kategorie ist eine der folgenden:<br>◦ Denial of Service<br>◦ Spear-Phishing<br>◦ Böswillige Code-Aktivität<br>• Eines der zugeordneten erkennbaren Elemente oder Indikatoren weist eine Sichtungsanzahl auf, die zwei Sichtungen mit aktiven Indikatoren überschreitet (d. h. die erkennbaren Elemente oder Indikatoren werden aus mehreren Quellen als schlecht bestätigt).<br>**Hinweis:** Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe „Advanced Security Operation“ haben und das Plugin „Threat Feeds“ aktivieren. |
| Anwenderrelevanz | Anwenderrelevanz abrufen | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators.<br>Dieser Schweregradrechner bewirkt, dass sich die Geschäftskritikalität des Benutzers in **1 - Kritisch** ändert, wenn das Feld **Abteilung** in **Finanzen**geändert wird. |
| | Ruft die Benutzergruppenrelevanz ab | Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators.<br>Dieser Schweregradrechner enthält ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Schweregradrechner

Wenn Sie einen Security Incident erstellen, enthalten die Felder **Risikopunktzahl**, **Geschäftsauswirkung**und **Priorität** Standardwerte. Wenn Sie den Incident speichern, validiert eine Geschäftsregel die Informationen im Security Incident automatisch anhand von Bedingungen, die in jedem Ihrer aktiven Schweregradrechner definiert sind. Sie werden jeweils für einen Sicherheitsrechner in der Reihenfolge validiert, die durch das Feld **Reihenfolge** in jedem Rechner festgelegt ist. Wenn die Informationen im Security Incident mit den in einem der Rechner definierten Bedingungen übereinstimmen, werden die Feldwerte für den Schweregrad entsprechend den im Rechner eingerichteten Regeln aktualisiert.

Angenommen, Sie erstellen einen Security Incident für ein betroffenes CI, und das CI ist äußerst kritisch. Wenn der Security Incident gespeichert wird, werden die CI-Informationen mit den in den Schweregradrechnern definierten Bedingungen verglichen. Wenn der Security Incident anhand des Schweregradrechners „ **Kritisch vom Service betroffen** “ validiert wird, werden die Schweregradfelder automatisch aktualisiert, und oben im Security Incident wird eine Meldung ähnlich der folgenden angezeigt.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

Sie können diese Schweregradrechner unverändert verwenden oder sie bearbeiten, um sie den Anforderungen Ihres Unternehmens anzupassen. Wenn Sie beispielsweise Web- und E-Mail-Bedrohungen identifizieren möchten, die für den Geschäftsbereich Finance spezifisch sind, können Sie die Bedingungen des **Multi-Angriffsvektor-** Rechners ändern:

- [Angriffsvektor] [enthält] [Web]
- [Angriffsvektor] [enthält] [E-Mail]
- [Geschäftsbereich] [enthält] [Finanz]

Sie können die Schweregradwerte in einem vorhandenen Security Incident auch jederzeit aktualisieren, indem Sie den Datensatz öffnen und auf den zugehörigen Link **Schweregrad berechnen** klicken.

## Risikopunktzahl-Rechner für Security Incidents

Die Rechner **„Priorität mit Kategorie und Servicesfestlegen“ und „Priorität mit erkennbaren Elementen** festlegen“ werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen.

## Benutzerrelevanzrechner

Die beiden Rechner in der **Benutzerrelevanzgruppe** (**Benutzerrelevanz abrufen** und **Benutzergruppenrelevanz abrufen**) bieten Beispiele dafür, wie Sie die Relevanz basierend auf Kriterien, die in einem Benutzerdatensatz definiert sind, oder basierend auf der Gruppe, zu der ein Benutzer gehört, steuern können.

Sie können nach Bedarf bearbeitet werden, oder es können neue Benutzerrelevanzrechner erstellt werden.

Der Rechner für **Benutzerrelevanz** abrufen bewirkt, dass sich die Geschäftsrelevanz des Benutzers in **1 - Kritisch** ändert, wenn das Feld **Abteilung** in **Finanzen**geändert wird.

Der Rechner für Benutzergruppenrelevanz ändert die Geschäftskritikalität des Benutzers in **1 - Kritisch,** wenn der Benutzer der **Datenbankgruppe** hinzugefügt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
**„Benutzergruppenrelevanz abrufen“** ist ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird. Wenn Sie weitere Gruppen hinzufügen möchten, um eine Relevanzänderung zu initiieren, fügen Sie in der ersten Zeile des Skripts eine durch Kommas getrennte Liste mit Gruppen-sys_ids hinzu. Beispiel: `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id]`.

### Berechnungen der Security Incident-Risikopunktzahl

Die Risikopunktzahl wird als arithmetisches Mittel berechnet, das das Risiko basierend auf der Priorität eines Security Incident, der Art des Security Incident (Denial of Service, Spear Phishing oder böswillige Codeaktivität) und der Anzahl der Quellen darstellt, die einen fehlgeschlagenen ausgelöst haben Reputationspunktzahl für einen Indikator.

Die Risikopunktzahl hilft bei der Priorisierung der Security Incident-Arbeit für die Analysten.

Die Security Incident-Rechner**„Priorität mit Kategorie und Servicesfestlegen“ und „Priorität mit erkennbaren** Elementen festlegen“ werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen. Darüber hinaus lösen die folgenden Geschäftsregeln die automatische Berechnung von Risikopunktzahlen aus:

- Schweregrad berechnen
- Aktualisieren Sie die Risikopunktzahl
- Aktualisieren Sie die SI-Risikopunktzahl

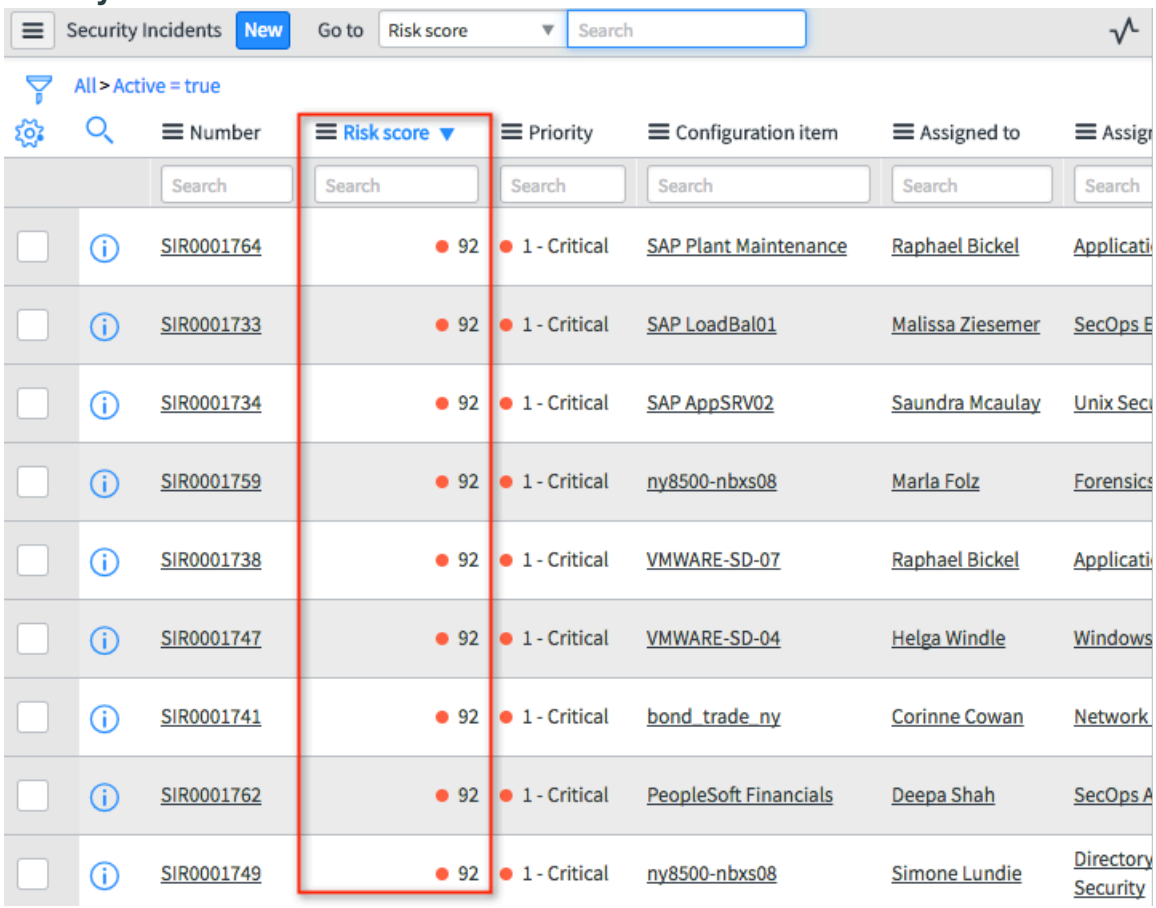
**Hinweis:**
Der im Basissystem verfügbare Risikorechner hängt von Ihrer Security Operations-Preisstufe ab.

Wenn Sie sich eine Liste von Security Incidents im Basissystem ansehen, beachten Sie die Spalte **Risikopunktzahl**.



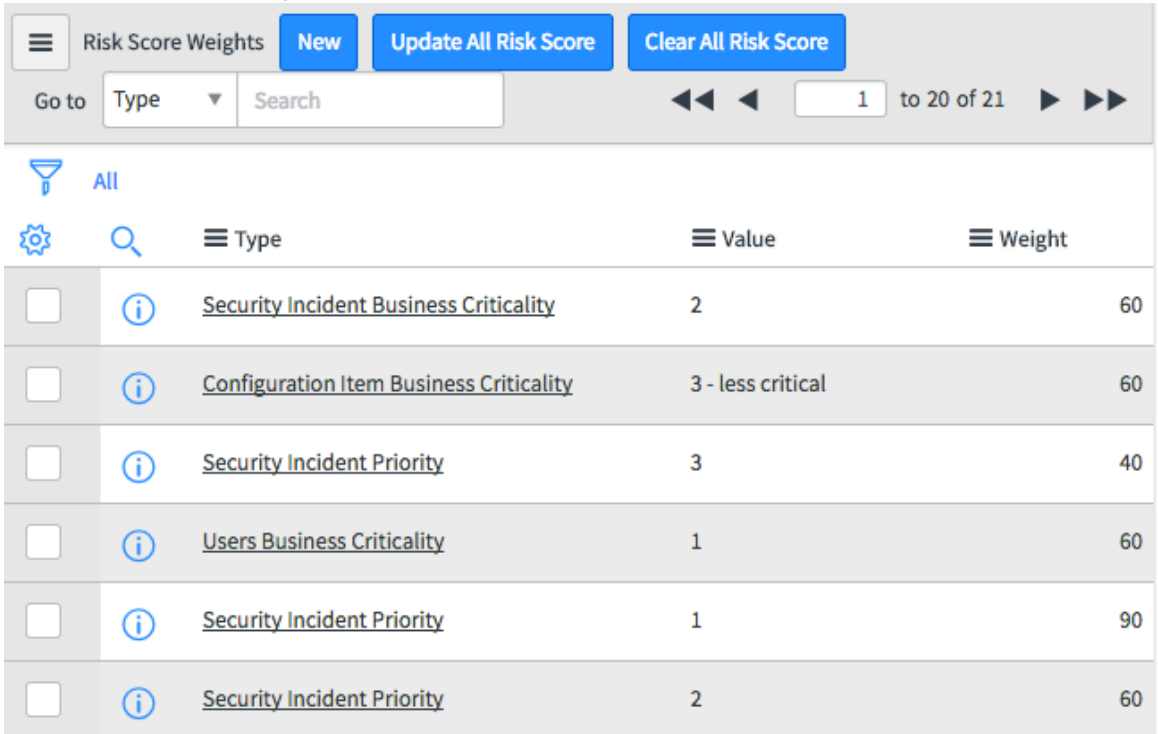
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incidents**




Die Risikopunktzahl wird anhand von Gewichtungen berechnet, die in **der Risikopunktzahlkonfiguration**definiert sind.

**Risikopunktzahlkonfiguration**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wenn für einen Security Incident die **Geschäftsauswirkung** auf **2-Hoch** und die **Priorität** auf **3-Mittel**festgelegt ist, werden die entsprechenden Gewichtungen in der Tabelle „Risikopunktzahl-Gewichtungen“ gesucht und wie folgt berechnet:

**Security Incident – Geschäftsauswirkung** mit einem Wert von 2 = einer Gewichtung von 60.

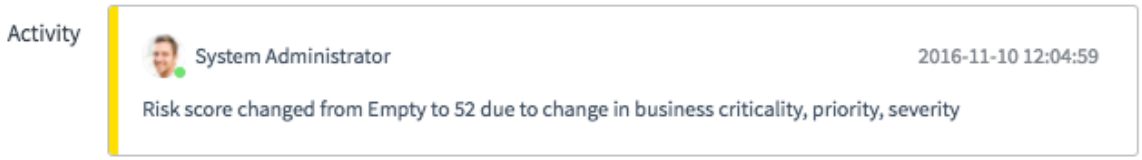
**Security Incident-Priorität** mit einem Wert von 3 = einer Gewichtung von 40.

(60 + 40)/2 = Risikopunktzahl 50.

Die Position des Security Incident in der Security Incident-Liste wird dann basierend auf der aktualisierten Risikopunktzahl neu angeordnet.

Wenn im obigen Beispiel die **Geschäftsauswirkung** oder die **Priorität** des Security Incidents geändert werden, wird die Risikopunktzahl neu berechnet, und die Änderungen werden in den Arbeitsnotizen angezeigt.

**Arbeitsnotizen**




Die Arbeitsnotizen werden aktualisiert, wenn die folgenden Felder geändert werden (wodurch die Risikopunktzahl aktualisiert wird):

- **Geschäftsauswirkung** auf das Security Incident-Formular
- **Priorität** im Formular „Security Incident“.
- **Schweregrad** im Security Incident-Formular (standardmäßig ausgeblendet)
- **Geschäftsauswirkung** auf die zugehörige Liste **„Betroffene Benutzer** “.
- **Geschäftsauswirkung** auf die zugehörige Liste **Betroffene Services**
- **Geschäftsauswirkung** auf Schwachstellen in der zugehörigen Liste „Angreifbare **Elemente** “.

Darüber hinaus werden die Arbeitsnotizen in den folgenden Situationen aktualisiert:

- Wenn eine Zuordnung zwischen betroffenen Benutzern und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen betroffenen Services und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen angreifbaren Elementen und einem Security Incident erstellt oder geändert wird

Arbeitsnotizen werden auch aktualisiert, wenn im Formular „Gewichtungen der Risikopunktzahl“ auf **Alle Risikopunktzahlen** aktualisieren und **Alle Risikopunktzahlen löschen**geklickt wird.

### Verwalten Sie die Gewichtungen der Risikopunktzahl

Die Risikopunktzahlgewichtungen, die zur Berechnung von Risikopunktzahlen in Security Incidents verwendet werden, können einzeln entfernt oder aktualisiert werden. Sie können auch für alle Security Incidents entfernt oder aktualisiert werden. Die Möglichkeit, sie aus Security Incidents zu entfernen, ist nützlich, wenn Gewichtungswerte geändert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

**Hinweis:**
Benutzer mit der Rolle „sn_si.read“ können die Konfiguration der Risikopunktzahl in Security Incident Responseanzeigen.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Konfiguration der Risikopunktzahl**.

   **Hinweis:**
   Benutzer mit der Rolle „sn_si.read“ können die Konfiguration der Risikopunktzahl anzeigen, indem sie zu navigieren **Security Incident** > **Warnungen und Ereignisse** > **Risikopunktzahlkonfiguration**.

2. Um eine neue Gewichtung der Risikopunktzahl hinzuzufügen, klicken Sie auf **Neu**, und geben Sie Informationen in die Felder ein.

| Feld | Beschreibung |
|---|---|
| Typ | Wählen Sie den Typ der Risikopunktzahl aus, die Sie definieren. |
| Wert | Geben Sie den Wert an, der dem ausgewählten Typ zugeordnet ist. Wenn für den Typ mehrere Werte verfügbar sind, sollten Sie mehrere Risikopunktzahl-Gewichtungsdatensätze definieren. Beispiel: Security Incident-Priorität mit einem Wert von 1, Security Incident-Priorität mit einem Wert von 2 usw. |
| Gewichtung | Gewichtung, die dem ausgewählten Typ/Wert-Paar zugeordnet ist. Gültige Einträge liegen zwischen 0 und 100, wobei 0 die niedrigste und 100 die höchste Gewichtung ist. |

3. Klicken Sie auf **Absenden**.
4. Führen Sie nach Bedarf einen dieser Schritte aus.
   - Um einen Risikopunktzahl-Gewichtungsdatensatz zu löschen, öffnen Sie ihn in der Liste und klicken Sie auf **Löschen**.
   - Um alle Risikopunktzahl-Gewichtungsdatensätze zu löschen, klicken Sie auf **Alle Risikopunktzahlen löschen**.
   - Um alle Risikopunktzahl-Gewichtungsdatensätze zu aktualisieren, klicken Sie auf **Alle Risikopunktzahlen**aktualisieren.

## Erstellen Sie eine Security Incident Response SLA

Sie können eine Servicelevel-Vereinbarung (Service Level Agreement, SLA) für Security Incident Responsedefinieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **SLAs**.
2. Klicken Sie auf **Neu**.
   Feldbeschreibungen und detaillierte Anweisungen finden Sie unter Create an SLA definition .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Reparieren Sie Security Incident-SLAs

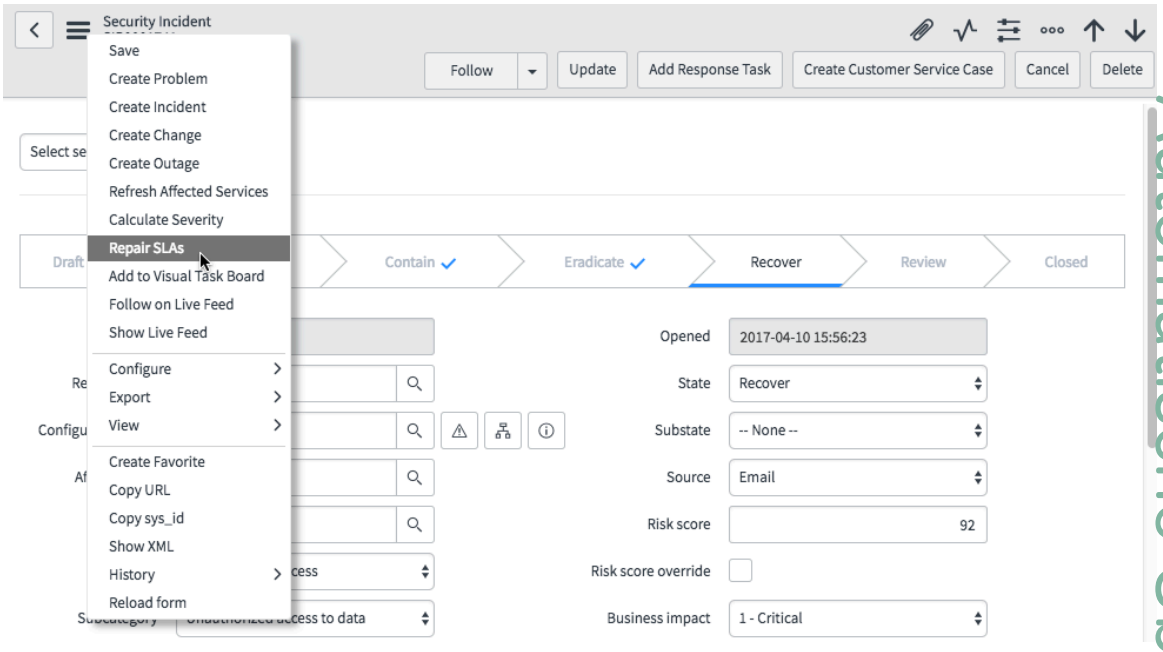
Sie können SLA-Datensätze reparieren, um sicherzustellen, dass die SLA-Zeit- und -Dauerinformationen korrekt sind.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn es noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie SLAs reparieren möchten.
2. Klicken Sie auf das Kontextmenü der Formularkopfzeile, und wählen Sie **SLAs reparieren aus**:




3. Klicken Sie im Bestätigungsfeld Warnung auf **OK**.
   Weitere Informationen finden Sie unter SLAs reparieren .

### Erstellen Sie ein Security Incident Response-Runbook

Ein Runbook ist eine Zuordnung zwischen einem veröffentlichten Wissensartikel und einer bestimmten Aufgabe. Während Sie die Aufgabe ausführen, wird automatisch ein Wissensartikel im Runbook geöffnet, der Informationen enthält, die für die Aufgabe relevant sind.

#### Vorbereitungen

In der Knowledge Base von Security Incident Response Runbook müssen Wissensartikel vorhanden sein. Wenn Sie einen Wissensartikelzu Security Incidents erstellen, stellen Sie sicher, dass Sie **Security Incident Response Runbook** im Feld **Knowledge Base** auswählen. Nachdem Sie den Artikel veröffentlicht haben, können Sie auf die Schaltfläche **Runbook erstellen klicken**.

Erforderliche Rolle: sn.si.knowledge_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können Runbooks während der Erstellung von Security Incidents oder Antwortaufgaben verwenden, oder Sie können die Knowledge Base-Artikel in einem Runbook mit Aufgaben im Playbook verknüpfen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**.
2. Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Wissensartikel | Wählen Sie einen Wissensartikel aus, der in das Runbook aufgenommen werden soll. |
| Aktiv | Aktivieren Sie das Kontrollkästchen, um das Runbook im **Filternavigator**verfügbar zu machen. |
| Filtergruppe verwenden | Aktivieren Sie diese Checkbox, um eine vordefinierte Filtergruppe zu verwenden, oder erstellen Sie eine neue Filtergruppe, um die Runbook-Kriterien zu definieren. |
| Filtergruppe | Wählen Sie die Filtergruppe aus, die zum Definieren eines Runbooks verwendet werden soll.<br>Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Filtergruppen verwenden** aktiviert ist. |
| Tabelle | Wählen Sie entweder Security Incident [sn_si_incident] oder Security Incident Response Aufgabe [sn_si_task] aus.<br>Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert und eine Filtergruppe ausgewählt haben, wird in diesem Feld standardmäßig die Tabelle verwendet, die der ausgewählten Filtergruppe zugeordnet ist. |
| Bedingung | Legen Sie die Bedingungen fest, die dieses Runbook mit dem Incident oder der Aufgabe verbinden.<br>Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert und eine Filtergruppe ausgewählt haben, werden die **Bedingungsfelder** nicht angezeigt. |

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarte Wissensartikeldetails und eine Reihe von Schaltflächen werden angezeigt.
4. Um die Details des Runbooks anzuzeigen, klicken Sie auf die Registerkarte **Knowledge Base-Details**.
5. Um den Wissensartikel so anzuzeigen, wie er dem Benutzer angezeigt wird, klicken Sie auf **Artikel anzeigen**.
6. Bis Um die Details des Wissensartikels zu bearbeiten , klicken Sie auf **Artikel bearbeiten**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie Regeln, um von Benutzern gemeldete Phishing-Angriffe zu validieren

Wenn Ihre Mitarbeiter E-Mails erhalten, die Phishing-Angriffe zu sein scheinen, können sie Ihnen diese über eine Phishing-E-Mail-Adresse melden. Die verdächtige E-Mail wird anhand der von Ihrer Organisation definierten Regeln validiert.

**Vorbereitungen**
Bevor E-Mail-Abgleichregeln zur Identifizierung potenzieller Phishing-Angriffe verwendet werden können, definieren Sie eine E-Mail-Adresse, an die von Ihren Mitarbeitern weitergeleitete E-Mails zur Verarbeitung gesendet werden. Sie haben die folgenden Optionen zum Definieren dieser E-Mail-Adresse (vorausgesetzt, die E-Mail-Domäne Ihres Unternehmens ist acme.com):

- Definieren Sie eine E-Mail-Adresse wie **acme+phishing@service-now.com**. Das Tag **+phishing** wird von SMTP unterstützt, um die Filterung zu ermöglichen, und Ihre Instanz kann an sie gesendete E-Mails empfangen.
- Definieren Sie eine E-Mail-Adresse, z. B. **phishing@acme.com** (Ihr Exchange-Postfach), die sie wiederum an **acme+phishing@service-now.com** (Ihr Instanzpostfach, das durch eine E-Mail-Weiterleitungsregel definiert ist) weiterleitet.

Erforderliche Rolle: sn_sec_cmn.write

**Warum und wann dieser Vorgang ausgeführt wird**
Wenn ein Mitarbeiter auf eine verdächtige E-Mail stößt, sollte er sie als Anhang an Ihre Phishing-E-Mail-Adresse weiterleiten. Wenn die angehängte E-Mail mit einer Regel übereinstimmt, die eine Bedrohung definiert, wird ein Security Incident erstellt.

**Prozedur**

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Anwender hat Phishing gemeldet**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

**Formular „E-Mail-Abgleichregeln“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für diese E-Mail-Abgleichregel. Beispiel: Vom Anwender gemeldetes Phishing. |
| Bedingungen | Verwenden Sie den -Bedingungsgenerator , um zu überprüfen, ob eine E-Mail an die Phishing-E-Mail-Adresse Ihres Unternehmens gesendet wurde, um einen Phishing-Angriff zu verhindern. Siehe folgendes Beispiel. |

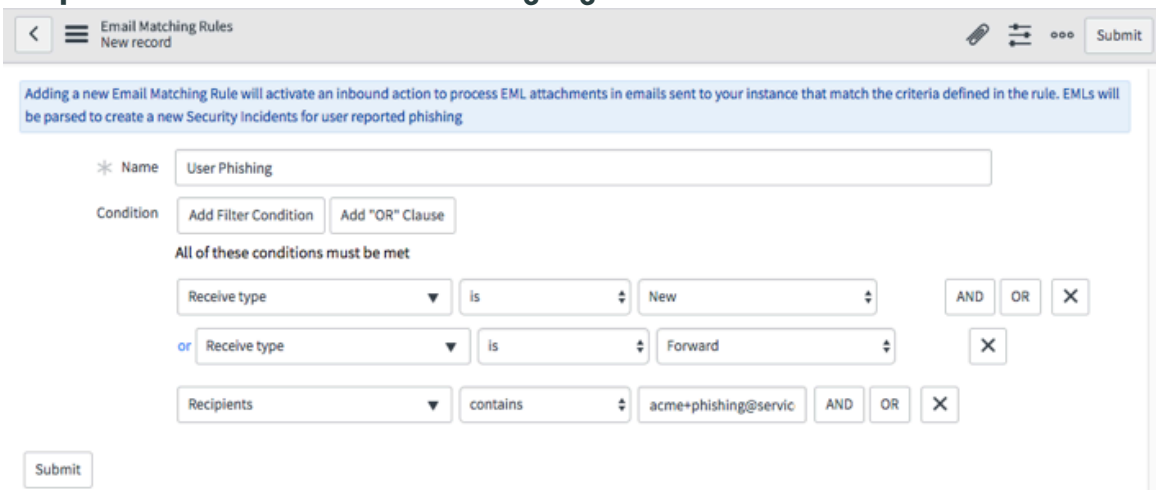
4. Klicken Sie auf **Absenden**.

**Example:**
Dieses Beispiel zeigt eine Übereinstimmungsregel für die Behandlung von von Benutzern gemeldetem Phishing.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Beispiel für eine E-Mail-Übereinstimmungsregel




## Konfigurieren Sie die Eigenschaften Security Analyst Workspace

Konfigurieren Sie die Benutzeroberfläche des Incident-Datensatzes in Security Analyst Workspace, um die Felder anzugeben, die Sie anzeigen möchten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Geben Sie die Felder an, die in Ihrem Incident-Datensatz angezeigt werden sollen, und die Reihenfolge, in der die Felder im Formular „Security Incident“ und im Formular „Antwortaufgabe“ angezeigt werden müssen. Sie können auch ein Limit für die Anzahl der Felder festlegen, die Sie anzeigen möchten.

**Hinweis:**

Sie können Regeln erstellen, um zu bestimmen, welche Ansicht für ein bestimmtes Formular verwendet werden soll. Im Basissystem sind mehrere Ansichten enthalten, einschließlich der Ansichten „Standard“ und „Neue SIR-UI“. Mehrere Ansichtsregeln werden auch mit dem Basissystem geliefert, einschließlich der Regel Alle anderen Antwortaufgaben. Diese Regel erzwingt die Standardansicht im Antwortaufgabenformular, wenn die in der Ansichtsregel angegebene Bedingung erfüllt ist. Security Analyst Workspace verwendet die Ansicht „SIR New UI“. Wenn die in Security Analyst Workspace angezeigten Formularfelder nicht mit den Formularfeldern in der klassischen Umgebung übereinstimmen, wird höchstwahrscheinlich eine Ansichtsregel erzwungen. Um die Ansicht „ **SIR New UI** “ für das Formular zu verwenden, müssen Sie die Ansichtsregel deaktivieren. Weitere Informationen finden Sie unter Steuern, wann das System eine Ansicht anzeigt .

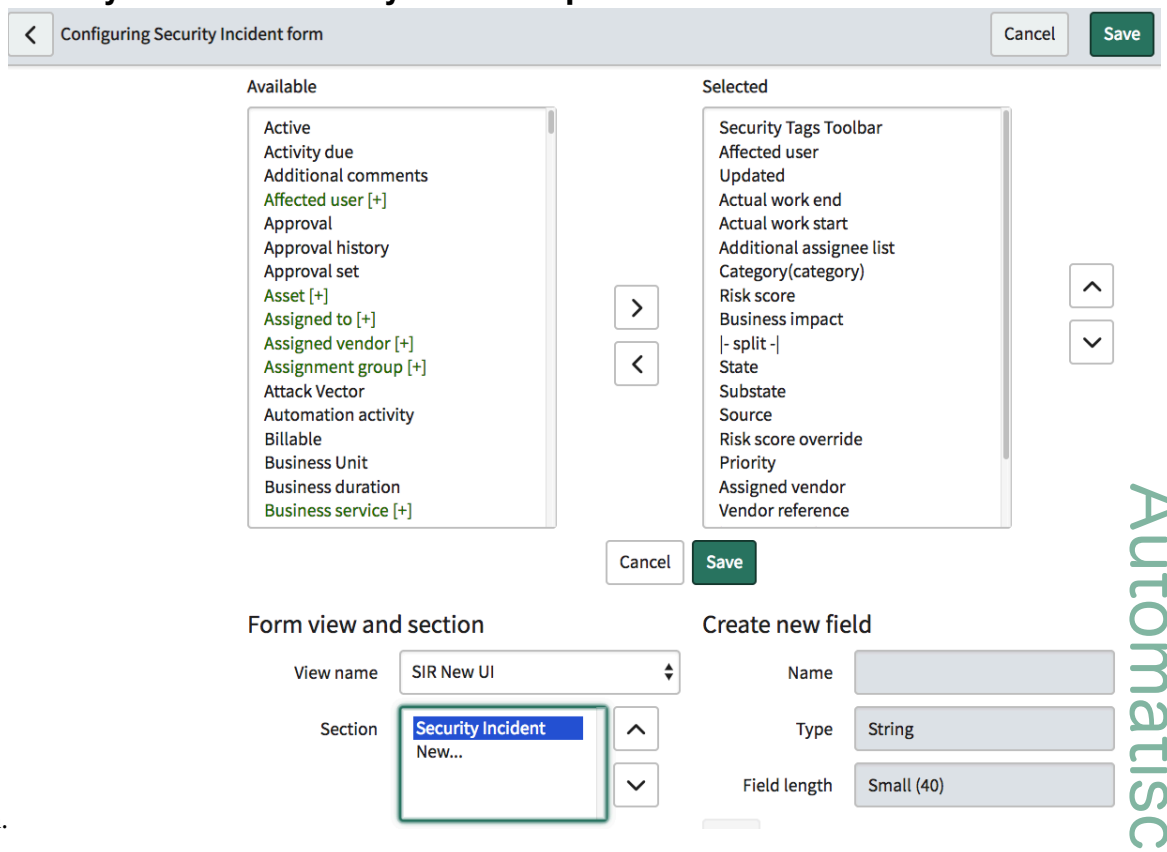
### Prozedur

1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.
2. Um den Security Incident-Datensatz zu öffnen, klicken Sie auf einen Security Incident-Link.
3. Um zur Formularseite „Security Incident konfigurieren“ zu navigieren, klicken Sie auf das ☰ -Menüsymbol, und wählen Sie **Konfigurieren** > **Formularlayout**.
4. **Wählen Sie in der Liste Name** anzeigen die Option **SIR Neue UI**aus.
5. Wählen Sie im Feld **Abschnitt** den entsprechenden Abschnitt aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies kann **Security Incident** oder **Security Incident Response**




**Task**sein.

6. Wählen Sie die Felder und die Reihenfolge aus, in der sie im Incident-Banner in der neuen Benutzeroberfläche angezeigt werden sollen.
7. Klicken Sie auf **Speichern**.

### Hinweis:

- Bestimmte Felder sind in den Bannern für Incidents und Antwortaufgaben standardmäßig ausgeblendet. Ändern Sie die ausgeblendeten oder angezeigten Felder, indem Sie die Eigenschaften `sn_app_secops_ui.form.excluded_fields.incident` und `sn_app_secops_ui.form.excluded_fields.response_task` ändern, wie in Eigenschaften des Security Analyst Workspacebeschrieben.
- Geben Sie die Anzahl der Felder an, die in den Incident- und Antwortaufgabenbannern und in der ersten Zeile des Incident-Banners angezeigt werden können, indem Sie die folgenden Eigenschaften festlegen:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

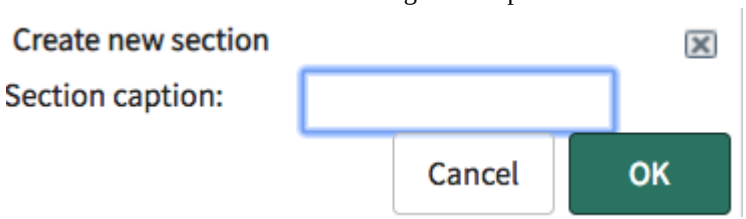
8. Navigieren Sie zu, um die Stile der gepunkteten Kreise zu konfigurieren, die neben einem Feldwert im Incident-Datensatz angezeigt werden, z. B. **System-UI** > **Feldstile** und ändern oder erstellen Sie einen neuen Stildatensatz für die spezifische Tabelle und den Feldnamen.
   Die Eigenschaft Hintergrundfarbe im Feld Stil des Stildatensatzes bestimmt die Farbe des gepunkteten Kreises.
9. Um das aktualisierte Incident-Banner anzuzeigen, klicken Sie auf **Security Incidents** > **Incidents (neue UI)** , um zum Incident-Datensatz in Security Analyst Workspace zu navigieren und die Seite zu aktualisieren, um das aktualisierte Incident-Banner anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Um das Banner für Antwortaufgaben im Incident-Datensatz zu konfigurieren, navigieren Sie zu **Security Incidents** > **Antwortaufgaben** > **Alle Aufgaben anzeigen** und wiederholen Sie die Schritte.
11. Wenn Sie eine neue Aufgabentabelle erstellen, die die Basistabelle „Security Incident Response-Aufgabe“ erweitert, müssen Sie der Tabelle auch die Ansicht „SIR – Neue UI“ hinzufügen.

    a. Wählen Sie in der Liste **Name** anzeigen die Option **Neu**aus.




    b. Geben Sie im Fenster „Neue Ansicht erstellen“ **SIR New UI** (Groß-/Kleinschreibung beachten) ein, und klicken Sie auf **OK**.

## Ergebnisse

Die Banner für Security Incidents und Antwortaufgaben werden in Security Analyst Workspace (Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace) aktualisiert.

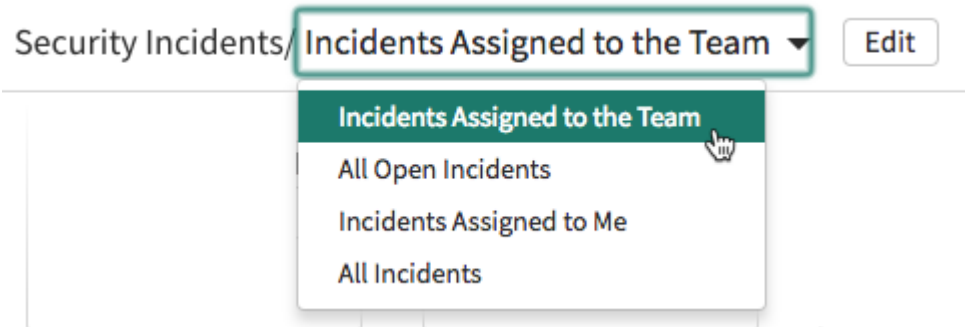
### Richten Sie primäre und sekundäre Filter für ein Security Analyst Workspace

Das Security Analyst Workspace Basissystem enthält eine Reihe von primären Filtern zum Eingrenzen der Liste der zu analysierenden Security Incidents (für Ihnen zugewiesene Security Incidents, alle offenen Incidents usw.) und eine Reihe von Schnellfiltern (oder sekundären Filtern) zum Eingrenzen die Liste noch weiter (nach neuen Incidents, offenen Incidents, nur kritischen Incidents usw.).

## Vorbereitungen

Sie können die klassische Umgebung verwenden, um zusätzliche primäre und sekundäre Filter zu definieren.

Wenn Sie Filter definieren, die in Security Analyst Workspaceverwendet werden sollen, können Sie Tags zuweisen, um anzugeben, ob sie als primäre oder sekundäre Filter verwendet werden können. Primäre Filter werden oben in der Security Incident-Liste angezeigt.




Klicken Sie neben der Option Schnellfilter auf **Bearbeiten**, um sekundäre (oder schnelle) Filter auszuwählen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin oder sn_sec_cmn.write

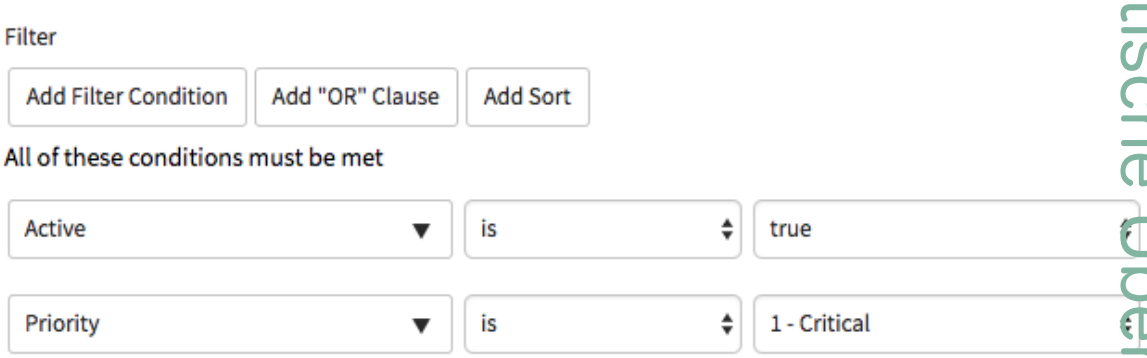
### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Filter**.
2. Klicken Sie auf **Neu**, und führen Sie die folgenden Schritte aus.

   a. Geben Sie einen **Titel**ein.

   b. Wählen Sie **Security Incident [sn_si_incident]** aus der Auswahlliste **Tabelle** aus.

   c. Fügen Sie Ihre Filterbedingungen hinzu.
   Zum Beispiel verwendet der Filter **Offene Incidents mit Priorität = Kritisch** die folgenden Bedingungen.




   d. Klicken Sie auf **Absenden**.

3. Wenn die Spalte **Tags** in der Filterliste nicht sichtbar ist, klicken Sie auf das Zahnradsymbol, und personalisieren Sie die Ansicht, um sie hinzuzufügen.
4. Suchen Sie den von Ihnen erstellten Filter, und fügen Sie eines der folgenden Tags hinzu, um anzugeben, wie der Filter in Security Analyst Workspaceangezeigt werden soll.
   - **SN_SI_Primary**: Wenn dieses Tag ausgewählt ist, kann der Filter aus dem Slushbucket des primären Filters in Security Analyst Workspaceausgewählt werden.
   - **SN_SI_Primary_OOB**: Wenn dieses Tag ausgewählt ist, wird der Filter standardmäßig auf der Seite **Ausgewählt** des primären Filter-Slushbuckets angezeigt.
   - **SN_SI_Secondary**: Wenn dieses Tag ausgewählt ist, kann der Filter aus dem sekundären (Schnell-)Filter-Slushbucket ausgewählt werden.
   - **SN_SI_Secondary_OOB**: Wenn dieses Tag ausgewählt ist, wird der Filter standardmäßig auf der Seite **Ausgewählt** des primären Filter-Slushbuckets angezeigt.

**Zugehörige Informationen**

Erstellen und bearbeiten Sie Filter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eigenschaften des Security Analyst Workspace

Diese Systemeigenschaften werden zum Konfigurieren des Sicherheitsanalysten-Arbeitsbereichs verwendet.

Es gibt zwei Arten von Eigenschaften:

- Eigenschaften, die normalerweise nicht geändert werden, wie sys_ids und Produktschlüssel.
- Eigenschaften, die nach Bedarf geändert werden können, z. B. lange Abfrageintervalle und Konfigurationen der Benutzeroberfläche.

**Hinweis:**
Die Eigenschaften des Security Analyst Workspace befinden sich an folgendem Speicherort: **Security Incident** > **Setup des Analyst Workspace** > **Eigenschaften des Analystenarbeitsbereichs**.

### Eigenschaften des Security Analyst Workspace

| Eigenschaftsname | Beschreibung |
|---|---|
| Felder, die im Antwortaufgabenbanner standardmäßig ausgeblendet sind.<br><br>sn_app_secops_ui.form.excluded_fields.response_task | • **Typ**: Zeichenfolge<br>• **Standardwert**:<br>◦ Nummer<br>◦ Kurzbeschreibung<br>◦ Kommentare<br>◦ work_notes<br>◦ Kommentare_und_Arbeitsnotizen<br>◦ work_notes_list<br>◦ Automation_activity |
| Felder, die im Incident-Banner standardmäßig ausgeblendet sind.<br><br>sn_app_secops_ui.form.excluded_fields.incident | • **Typ**: Zeichenfolge<br>• **Standardwert**:<br>◦ Nummer<br>◦ Kurzbeschreibung<br>◦ Kommentare<br>◦ work_notes<br>◦ Kommentare_und_Arbeitsnotizen<br>◦ work_notes_list<br>◦ Automation_activity<br>◦ security_tags |
| Der Hintergrundfarbstil wird auf die hier aufgeführten Felder angewendet. | • **Typ**: Zeichenfolge<br>• **Standardwert**: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eigenschaften des Security Analyst Workspace (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| sn_app_secops_ui.form.color_coded_fields | ○ Geschäftsrelevanz<br>○ impact<br>○ Priorität<br>○ risk_score<br>○ Schweregrad |
| Bei „true“ haben Tabellen, die aus der Basis-Antwortaufgabentabelle „sn_si_task“ erweitert wurden, auch Zugriff auf E-Mail-Vorlagen, die für die Basis-Antwortaufgabentabelle erstellt wurden.<br><br>sn_app_secops_ui.extend.base.response_task.email_templates | • **Typ**: true \| false<br>• **Standardwert**: true |
| Legt die Breite jedes Zusammenfassungsfelds in jedem Antwortaufgabenbanner fest.<br><br>sn_app_secops_ui.task_summary.single_summary.width.response_task | • **Typ**: Ganzzahl<br>• **Standardwert**: 10 |
| Legt die Breite jedes Zusammenfassungsfelds in jedem Incident-Banner fest.<br><br>sn_app_secops_ui.task_summary.single_summary.width.incident | • **Typ**: Ganzzahl<br>• **Standardwert**: 15 |
| Legt ein Limit für die Anzahl der im Incident-Banner zulässigen Zusammenfassungsfelder fest.<br><br>sn_app_secops_ui.task_summary.single_summary.limit.incident | • **Typ**: Ganzzahl<br>• **Standardwert**: 12 |
| Legt ein Limit für die Anzahl der im Antwortaufgabenbanner zulässigen Zusammenfassungsfelder fest.<br><br>sn_app_secops_ui.task_summary.single_summary.limit.response_task | • **Typ**: Ganzzahl<br>• **Standardwert**: 12 |
| Legt ein Limit für die Anzahl der in der ersten Zeile des Incident-Banners zulässigen Zusammenfassungsfelder fest.<br><br>sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line | • **Typ**: Ganzzahl<br>• **Standardwert**: 3 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eigenschaften des Security Analyst Workspace (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| Kommagetrennte Liste von Feldern, die Benutzerfotos enthalten können.<br><br>sn_app_secops_ui.form.user_fields | • **Typ**: Zeichenfolge<br>• **Standardwert**:<br>  ○ impacted_user<br>  ○ caller<br>  ○ sys_updated_by<br>  ○ sys_created_by<br>  ○ opened_by<br>  ○ closed_by<br>  ○ übermittelt_von |
| Legt die Breite jedes Zusammenfassungsfelds in jeder Incident-Vorschauansicht fest.<br><br>sn_app_secops_ui.task_summary.single_summary.width.incident_peek | • **Typ**: Ganzzahl<br>• **Standardwert**: 13,5 |
| Kommagetrennte Liste von Feldern, die die Zeit anzeigen.<br><br>sn_app_secops_ui.form.time_fields | • **Typ**: Zeichenfolge<br>• **Standardwert**:<br>  ○ opened_at<br>  ○ sys_created_on<br>  ○ sys_updated_on |
| Steuert die Häufigkeit (in Millisekunden), mit der die Ergebnisse der Sichtungssuche aktualisiert werden.<br><br>sn_app_secops_ui.poller_interval.search_action | • **Typ**: Ganzzahl<br>• **Standardwert**: 30000<br><br>**Minimum**: 15.000 |
| Steuert die Häufigkeit (in Millisekunden), mit der die Anzahl- oder Abfragedaten aktualisiert wird.<br><br>sn_app_secops_ui.poller_interval.related_list | • **Typ**: Ganzzahl<br>• **Standardwert**: 30000<br><br>**Minimum**: 15.000 |
| Steuert die Häufigkeit (in Millisekunden), mit der die Ergebnisdaten aktualisiert werden (für das Playbook).<br><br>sn_app_secops_ui.poller_interval.playbook_tasks | • **Typ**: Ganzzahl<br>• **Standardwert**: 30000<br><br>**Minimum**: 15.000 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eigenschaften des Security Analyst Workspace (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| ID für den Workflow „Security Operations Integration – Host isolieren“.<br><br>sn_app_secops_ui.workflow.id.isolierung_host | • **Typ**: Zeichenfolge<br>• **Standardwert**: d72041f1ff203200c68c84648e94fa5e |
| ID für den Workflow „Security Operations Integration – Beobachtungsliste“.<br><br>sn_app_secops_ui.workflow.id.publish_to_watchlist | • **Typ**: Zeichenfolge<br>• **Standardwert**: 35800c0eff343200c68c84648e94fa85 |
| ID für den Workflow „Security Operations Integration - Block Request“.<br><br>sn_app_secops_ui.workflow.id.block_request | • **Typ**: Zeichenfolge<br>• **Standardwert**: 11a6a5270b9032008f9108e3c5673a24 |
| ID für die Benutzerrolle sn_si_analyst<br><br>sn_app_secops_ui.roles.id.sn_si.write | • **Typ**: Zeichenfolge<br>• **Standardwert**: 66878663ff123100158bffffffffffffff8d |
| ID für die Benutzerrolle sn_si_read.<br><br>sn_app_secops_ui.roles.id.sn_si.read | • **Typ**: Zeichenfolge<br>• **Standardwert**: ae878663ff123100158bffffffffffffff8e |
| ID für die Benutzerrolle sn_si_admin<br><br>sn_app_secops_ui.roles.id.sn_si.admin | • **Typ**: Zeichenfolge<br>• **Standardwert**: 22878663ff123100158bffffffffffffff8d |
| ID für den Workflow „Microsoft Exchange – E-Mails suchen und löschen“.<br><br>sn_app_secops_ui.email.phishing.manual.workflow | • **Typ**: Zeichenfolge<br>• **Standardwert**: ed9f289cc310220031fbdccdf3d3aeb4 |
| ID für die benutzerdefinierte Aktion Zu Deny-Liste hinzufügen auf der Registerkarte „Durchsuchen“ in Security Analyst Workspace.<br><br>sn_app_secops_ui.explore.action.direct.id.deny_list | • **Typ**: Zeichenfolge<br>• **Standardwert**: DENY_e9bd0ac50b632200263a089b37673a0b |
| ID für die benutzerdefinierte Aktion Zu Allow-Liste hinzufügen auf der Registerkarte „Durchsuchen“ in Security Analyst Workspace | • **Typ**: Zeichenfolge<br>• **Standardwert**: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eigenschaften des Security Analyst Workspace (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| sn_app_secops_ui.explore.action.direct.id.allow_list | |
| ID für die UI-Aktion „Bedrohungssuche ausführen“.<br><br>sn_app_secops_ui.explore.action.id.run_threat_lookup | • **Typ**: Zeichenfolge<br>• **Standardwert**: da5ff4420b540300263a089b37673ae7 |
| ID für die Integrationsfähigkeit der Bedrohungssuche<br><br>sn_app_secops_ui.explore.capability.id.threat_lookup | • **Typ**: Zeichenfolge<br>• **Standardwert**: 39344d4f0b273200263a089b37673ab1 |
| ID für die benutzerdefinierte Aktion „Anreicherung erkennbarer Elemente“ auf der Registerkarte „Untersuchen“ in Security Analyst Workspace.<br><br>sn_app_secops_ui.explore.action.id.observable_enrichment | • **Typ**: Zeichenfolge<br>• **Standardwert**: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673 |
| ID für die Integrationsfunktion „Erkennbares Element anreichern“.<br><br>sn_app_secops_ui.explore.capability.id.observable_enrichment | • **Typ**: Zeichenfolge<br>• **Standardwert**: 9ad183640b1003009f66e94685673af4 |
| ID für die UI-Aktion „In Beobachtungsliste veröffentlichen“.<br><br>sn_app_secops_ui.explore.action.id.publish_to_watchlist | • **Typ**: Zeichenfolge<br>• **Standardwert**: 8ee94002ff743200c68c84648e94faf9 |
| ID für die Sperranforderungs-UI-Aktion.<br><br>sn_app_secops_ui.explore.action.id.block_request | • **Typ**: Zeichenfolge<br>• **Standardwert**: 7158f6e40b2032008f9108e3c5673adf |
| ID für die UI-Aktion „Sichtungssuche ausführen“.<br><br>sn_app_secops_ui.explore.action.id.sightings_search | • **Typ**: Zeichenfolge<br>• **Standardwert**: 43f91a6f0b032200b97c67d985673a2c |
| ID für die UI-Aktion „Untergeordneten Security Incident erstellen“.<br><br>sn_app_secops_ui.explore.action.id.create_child_incident | • **Typ**: Zeichenfolge<br>• **Standardwert**: 5a6882645363530099d5ddeeff7b1272 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eigenschaften des Security Analyst Workspace (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| ID für die UI-Aktion „Sicherheitsanmerkung hinzufügen“.<br><br>sn_app_secops_ui.explore.action.id.add_security_annotation | • **Typ**: Zeichenfolge<br>• **Standardwert**: 1e3a3e723b5332005a9149a4d2efc4eb |
| ID für die benutzerdefinierte CI-Ergänzungsaktion auf der Registerkarte „Durchsuchen“ in Security Analyst Workspace.<br><br>sn_app_secops_ui.explore.action.id.ci_enrichment | • **Typ**: Zeichenfolge<br>• **Standardwert**: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1 |
| ID für die UI-Aktion „Host isolieren“.<br><br>sn_app_secops_ui.explore.action.id.isolate_host | • **Typ**: Zeichenfolge<br>• **Standardwert**: d6244e0aff203200c68c84648e94fad3 |
| ID für die UI-Aktion „Mehrere erkennbare Elemente hinzufügen“.<br><br>sn_app_secops_ui.explore.action.id.multiple_observable | • **Typ**: Zeichenfolge<br>• **Standardwert**: 138de478d78322007a6de294de6103aa |
| Produktschlüssel für ag-Grid-Enterprise.<br><br>sn_app_secops_ui.ag-grid-license | • **Typ**: Zeichenfolge<br>• **Standardwert**: ServiceNow_ServiceNow_5Devs2_August_2018__MTUzM |

### Zusätzliche Konfiguration des Sicherheitsanalysten-Arbeitsbereichs

Konfigurieren Sie Security Analyst Workspace, und definieren Sie Filter, UI-Aktionen und zugehörige Listen.

- Konfiguration des Zielseitenfilters
- UI-Aktionen aktivieren
- Formular-UI-Aktionen
- Konfiguration der zugehörigen Liste
- UI-Aktionen für zugehörige Listen
- Systemeigenschaften der Formularkonfiguration
- Aktivieren Sie Playbooks für die Analystenauswahl

### Konfiguration des Zielseitenfilters

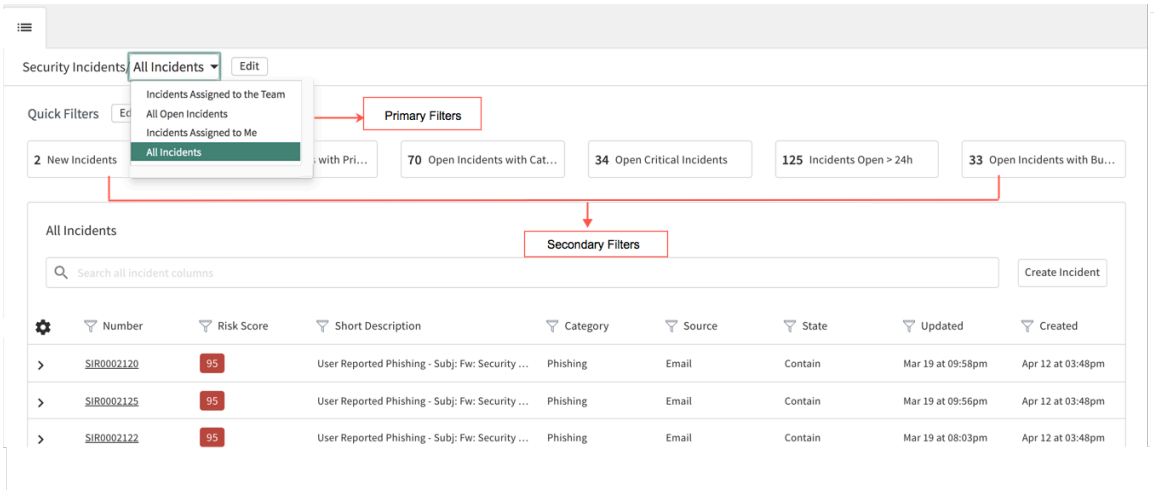
Sie können neue Filter hinzufügen oder vorhandene Filter ändern, die im Security Analyst Workspaceangezeigt werden.

Security Analyst Workspace verfügt über primäre und sekundäre Filter, mit denen Sie die Liste der Security Incidents filtern können, sodass Sie die Security Incidents, die Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

analysieren möchten, schnell finden. Weitere Informationen finden Sie unter Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace.




## Erstellen Sie einen neuen Filter

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfiguration der Zielseitenfilter**.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Titel für den Filter ein, geben Sie die Filterbedingung an, und klicken Sie auf **Absenden**, um zur vorherigen Seite zurückzukehren.

   Der neu hinzugefügte Filter wird auf der Seite aufgelistet.
4. Fügen Sie ein Tag für diesen Filter hinzu, um anzugeben, ob es sich um einen primären oder sekundären Filter handelt. Die folgenden Tags sind verfügbar:
   - SN_SI_Primär
   - SN_SI_Secondary

## Bearbeiten Sie vorhandene Filter

Sie können auch Folgendes tun:

- Vorhandene Filter ändern: Klicken Sie auf den Titel eines vorhandenen Filters. Ändern Sie den Titel und die Filterbedingung, und klicken Sie auf **Aktualisieren**.
- Tags ändern: Wählen Sie einen Filter aus, und klicken Sie in der Zielseiten-Filterkonfiguration auf die Spalte Tag. Sie können das vorhandene Tag löschen oder ein neues Tag für den Filter hinzufügen.

### UI-Aktionen aktivieren

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind.

**Hinweis:**
Um die UI-Aktionen zu ändern, melden Sie sich als Benutzer mit den folgenden Rollen an:

- ui_action_admin
- ui_page_admin
- web_service_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt zwei Arten von UI-Aktionen, die für Security Analyst Workspacekonfiguriert werden können:

- Dialogbasierte UI-Aktion
- Serverseitige UI-Aktion

**Dialogbasierte UI-Aktion**

Um Dialogfeld-basierte UI-Aktionen in Security Analyst Workspacezu aktivieren, nehmen Sie die folgenden Änderungen an den UI-Seiten vor, die den entsprechenden Standard-UI-Aktionen zugeordnet sind.

1. **HTML-Abschnitt**: Ändern Sie den HTML-Abschnitt, um das *`Reaktionseingabe`* -Tag einzubeziehen. Der Tag-Wert für die *`Reaktionseingabe`* wird im Client-Skriptabschnitt verwendet, um zu ermitteln, ob die UI-Seite über Security Analyst Workspacegestartet wurde. Ein Beispiel ist unten dargestellt:

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Client-Skript**: Zusätzliche Logik muss im Client-Skript geschrieben werden, wenn die *`Reaktionskennzeichnung`* „wahr“ ist. Dies ist erforderlich, um die Schaltflächenereignisse „ **Absenden** “ und „ **Abbrechen** “ zu verarbeiten, die im Dialogfeld angezeigt werden.
   a. Event-Handler onCancel () muss das Event „SIR_WORKBENCH_POPUP_CANCEL“ vom senden Security Analyst Workspace
   b. Event-Handler onSubmit () muss das Event „SIR_WORKBENCH_POPUP_SUBMIT“ vom senden Security Analyst Workspace
3. Die Ausführung des Verarbeitungsskripts wird im Kontext Security Analyst Workspace übersprungen, da die Aktion „onSubmit“ so geändert wurde, dass sie „falsch“ zurückgibt, wenn der Tag-Wert der *`Reaktionseingabe`* „wahr“ ist. Die Logik des Verarbeitungsskripts muss entweder über ein vom Client aufrufbares Skript (aufgerufen über die GlideAjax-API) oder einen REST-Ressourcenendpunkt behandelt werden.

Weitere Informationen finden Sie auf den folgenden Beispiel-UI-Seiten:

- Beispiel für UI-Aktion „Zugehörige Liste“: In Beobachtungsliste veröffentlichen (Name der UI-Seite: veröffentlichen_to_watchlist)
- Beispiel für Formular-UI-Aktion: Problem erstellen (Name der UI-Seite: create_prb_change_inc)

**Serverseitige UI-Aktion**

Gehen Sie wie folgt vor, um serverseitige UI-Aktionen zu aktivieren:

Die Logik des Standard-UI-Aktionsskripts muss als Teil einer geskripteten REST-Ressource behandelt werden.

Weitere Informationen finden Sie in den folgenden Beispielformular-UI-Aktionen:

- Ausfall erstellen
- Abbrechen

### Formular-UI-Aktionen

Sie können die UI-Aktionen konfigurieren, die im Security Analyst Workspaceangezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Voraussetzungen:**

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.

Führen Sie die folgenden Schritte aus, um eine Formular-UI-Aktion für Security Analyst Workspacezu konfigurieren:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **UI-Aktionen für Formulare**.
2. Geben Sie die folgenden Details ein:

| Feldname | Beschreibung |
|---|---|
| Aktion | Wählen Sie eine UI-Aktion aus der Auswahlliste aus. |
| Typ | Wählen Sie den Aktionstyp aus. Dies kann sein:<br>○ Dialogbasierte Aktion: Diese Art von Aktion wird verwendet, wenn Benutzerinteraktionen oder -eingaben erforderlich sind, um eine bestimmte Geschäftslogik auszuführen.<br>○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Benutzereingabe aus.<br>**Hinweis:**<br>Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren. |
| Anwendung | Der Name des Anwendungsbereichs (Security Incident Response UI), in dem die UI-Aktion hinzugefügt wird, wird hier angezeigt. |
| **Dialogbasierte Aktion**<br>Wenn Sie im Feld Typ die Option Dialogbasierte Aktion auswählen, geben Sie die folgenden Details ein: | |
| UI-Seite | Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist. |
| Dialogfeldtitel | Geben Sie einen Titel für die Dialogaktion ein. |
| Breite und Höhe des Dialogfelds | Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein. |
| Skript | Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt nur den Parameter `sysparm_sys_id` zurück. Sie können dies überschreiben, indem Sie hier andere Parameter angeben. |
| **Serverseitige Aktion**<br>Wenn Sie Serverseitige Aktion im Feld Typ auswählen, geben Sie die folgenden Details ein: | |
| Geskriptete Rest-Ressource | Wählen Sie die geskriptete REST-Ressource aus, die die Aktion definiert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

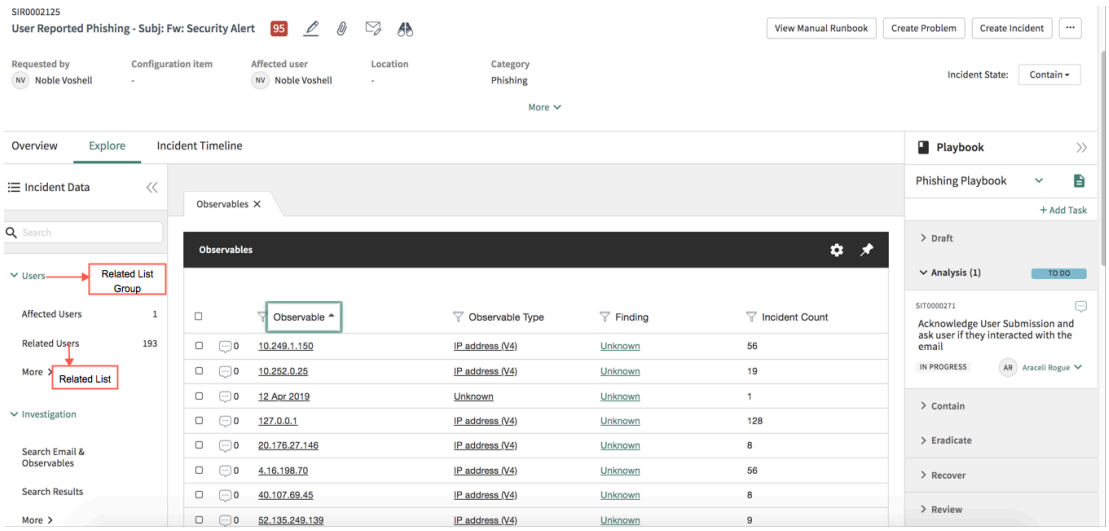
| Feldname | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Die **SIR-UI-ANALYSE-** ACL muss der REST-Ressource hinzugefügt werden. |

3. Klicken Sie auf **Absenden**.
4. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
5. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Die neue UI-Aktion wird oben auf der Seite angezeigt.

Um eine vorhandene Formular-UI-Aktion zu ändern, klicken Sie auf den Aktionsnamen, um zur Seite „Formular-UI-Aktionen“ zu navigieren. Sie können den Aktionsnamen, den Typ und die restlichen Felder basierend auf dem ausgewählten Typ ändern.

### Konfiguration der zugehörigen Liste

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die im Security Analyst Workspaceangezeigt werden.




### Fügen Sie eine zugehörige Listengruppe hinzu

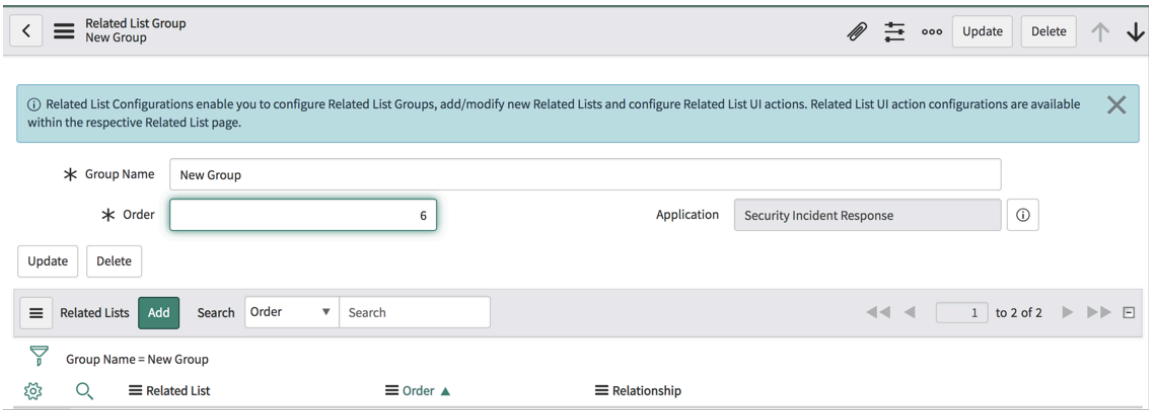
Führen Sie die folgenden Schritte aus, um eine zugehörige Listengruppe hinzuzufügen:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfiguration zugehöriger Listen**.
2. Klicken Sie auf **Neu**, um eine neue zugehörige Listengruppe hinzuzufügen. Geben Sie den Gruppennamen und die Reihenfolge ein, in der er auf der Seite „Incidents (Neue UI)“ angezeigt werden soll.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**. Die neu hinzugefügte Gruppe wird auf der Seite Zugehörige Listengruppen angezeigt.




### Fügen Sie eine zugehörige Liste hinzu

Führen Sie die folgenden Schritte aus, um eine neue zugehörige Liste hinzuzufügen:

1. Klicken Sie auf den Link Zugehörige Listengruppe.
2. Klicken Sie im Abschnitt „Zugehörige Listen“ auf **Hinzufügen**, um eine neue zugehörige Liste hinzuzufügen.

   Wenn die Schaltfläche **Hinzufügen** nicht angezeigt wird, überprüfen Sie, ob Sie sich im selben Anwendungsbereich wie die zugehörige Listengruppe befinden.
3. Wählen Sie die zugehörige Liste aus, die in die Gruppe aufgenommen werden soll.

   **Hinweis:**
   Wenn eine bestimmte zugehörige Liste nicht angezeigt wird, gehen Sie wie folgt vor:

   a. Navigieren zu **System-UI** > **Zugehörige Listen** und suchen Sie nach zugehörigen Listen in der Tabelle `sn_si_incident`.

   b. Klicken Sie auf die Tabelle `sn_si_incident`, die der Ansicht „ **Neue SIR-UI**“ zugeordnet ist.

   c. Klicken Sie im Abschnitt „Zugehörige Listeneinträge“ auf **Neu**, um die zugehörige Liste der Ansicht „ **Neue SIR-UI** “ hinzuzufügen.
4. Geben Sie die Reihenfolge an, in der sie angezeigt werden sollen, und klicken Sie auf **Absenden**.

   Die von Ihnen hinzugefügte zugehörige Liste wird in Security Analyst Workspaceangezeigt .

Um eine vorhandene zugehörige Listengruppe zu ändern, klicken Sie auf den Gruppennamen, um zur Seite „Zugehörige Listengruppe“ zu navigieren. Sie können den Gruppennamen und die Reihenfolge ändern und zugehörige Listen in der Gruppe hinzufügen oder löschen.

### UI-Aktionen für zugehörige Listen

Sie können den zugehörigen Listen, die im Security Analyst Workspaceangezeigt werden, neue UI-Aktionen hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Voraussetzungen:**

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren.

Führen Sie die folgenden Schritte aus, um eine neue UI-Aktion „Zugehörige Liste“ hinzuzufügen:

1. Navigieren zu **Security Incidents** > **Setup von Analyst Workspace (neue UI)** > **Konfiguration zugehöriger Listen**.
2. Klicken Sie auf den Gruppennamen. Die Konfigurationsseite „Zugehörige Listengruppe“ wird angezeigt.
3. Klicken Sie auf die zugehörige Liste, für die Sie eine UI-Aktion hinzufügen möchten.
4. Klicken Sie im Abschnitt „Zugehörige Liste“ UI-Aktionen auf **Hinzufügen**.
5. Geben Sie die folgenden Details ein:

| Feldname | Beschreibung |
|---|---|
| Aktion | Wählen Sie eine UI-Aktion aus der Auswahlliste aus. |
| Typ | Wählen Sie den Aktionstyp aus. Dies kann sein:<br>○ Dialogbasierte Aktion: Diese Art von Aktion wird verwendet, wenn Benutzerinteraktionen oder -eingaben erforderlich sind, um eine bestimmte Geschäftslogik auszuführen.<br>○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Benutzereingabe aus.<br>**Hinweis:** Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in Security Analyst Workspaceverfügbar sind. Details siehe UI-Aktionen aktivieren. |
| Anwendung | Der Name des Anwendungsbereichs (Security Incident Response UI), in dem die UI-Aktion hinzugefügt wird, wird hier angezeigt. |
| **Dialogbasierte Aktion**<br>Wenn Sie im Feld Typ die Option Dialogbasierte Aktion auswählen, geben Sie die folgenden Details ein: | |
| UI-Seite | Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist. |
| Dialogfeldtitel | Geben Sie einen Titel für die Dialogaktion ein. |
| Breite und Höhe des Dialogfelds | Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein. |
| Skript | Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt nur die Parameter `sysparm_incident_id`, `sysparm_record_table`und `sysparm_related_sys_ids` zurück. Sie können sie überschreiben, indem Sie hier andere Parameter angeben. |
| **Serverseitige Aktion** | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feldname | Beschreibung |
|---|---|
| Wenn Sie Serverseitige Aktion im Feld Typ auswählen, geben Sie Folgendes an: | |
| Geskriptete Rest-Ressource | Wählen Sie die geskriptete REST-Ressource aus, die die Aktion definiert.<br>**Hinweis:**<br>Die **SIR-UI-ANALYSE-** ACL muss der REST-Ressource hinzugefügt werden. |

6. Klicken Sie auf **Absenden**.
7. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
8. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Starten Sie die entsprechende Zugehörige Liste, um die neue UI-Aktion anzuzeigen.

### Systemeigenschaften der Formularkonfiguration

Diese Systemeigenschaften definieren die Formularaktualisierungsintervalle für die Playbook-Aufgaben.

Um diese Eigenschaften zu konfigurieren, navigieren Sie zu **Setup von Analyst Workspace (neue UI)** > **Eigenschaften des Analystenarbeitsbereichs**.

| Eigenschaft | Standardwert | Beschreibung |
|---|---|---|
| sn_app_secops_ui.poller_interval.playbook_tasks | 10000 ms | Die Intervallzeit, die von der Playbook-Komponente verwendet wird, um ihre Antwortaufgaben für jede konfigurierte Intervallzeit zu aktualisieren. |
| sn_app_secops_ui.poller_interval_count.playbook_tasks | 3 | Die Anzahl der Abfragen der Playbook-Komponente für Antwortaufgaben. |
| sn_app_secops_ui.poller_interval.related_lists | 30000 ms | Diese Intervallzeit wird von der Komponente „Durchsuchen“ verwendet, um die Anzahl der zugehörigen Listen für jede konfigurierte Intervallzeit zu aktualisieren. |

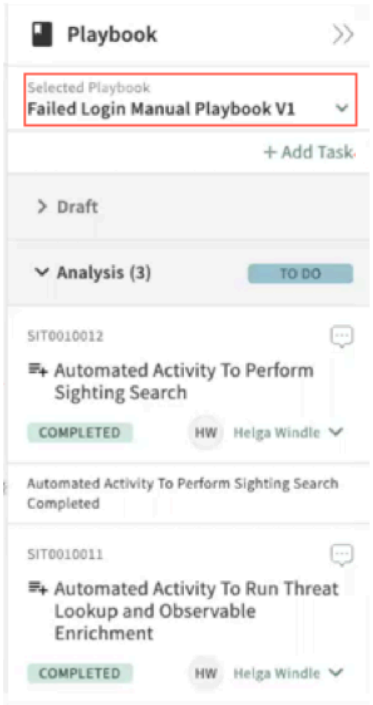
### Aktivieren Sie Playbooks für die Analystenauswahl

Fügen Sie der Playbook-Auswahlliste neue Playbooks hinzu.

Sie können ein geeignetes Playbook auswählen, um Security Incidents im Security Analyst Workspace (Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace) zu untersuchen. Die Playbook-Auswahloption unterstützt nur Playbooks, die mit Flow Designer erstellt wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nachdem Sie ein Playbook mit Flow Designer erstellt haben, führen Sie die folgenden Schritte aus, um es in die Auswahlliste Ausgewähltes Playbook aufzunehmen:

1. Navigieren Sie zur Tabelle *sys_hub_flow*.
2. Suchen Sie mit Flow Designer nach dem neuen Playbook, das Sie erstellt haben.
3. Fügen Sie das Tag **sir_playbook** den Playbooks hinzu, die Sie in die Auswahlliste Ausgewähltes Playbook aufnehmen möchten.

**Hinweis:**
Alte Playbooks, die nicht von Workflows zu Flow Designer migriert wurden, werden nicht in der Liste angezeigt. Wenn jedoch ein mit Workflows erstelltes Playbook einem Security Incident entweder durch eine Auslöserbedingung oder durch manuelle Auswahl zugewiesen wird (mithilfe der Option **Orchestration** ausführen in der klassischen Umgebung), wird dieses Playbook gestartet, wenn Sie den Security Incident in Security Analyst Workspaceöffnen.

### Problembehandlung bei Security Incident Response

In diesem Abschnitt werden wichtige Tipps zur Problembehandlung und häufig gestellte Fragen im Zusammenhang mit Security Incident Response behandelt.

## Probleme mit Zugriffskontrollregeln

Zugriffskontrollregeln ermöglichen den Zugriff auf die angegebene Ressource, wenn alle der folgenden drei Bedingungen erfüllt sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Benutzer hat eine der in der **Rollenliste** angegebenen Rollen, oder die Liste ist leer.
- Bedingungen im Feld **Bedingung** werden als „wahr“ ausgewertet, oder die Bedingungen sind leer.
- Das Skript im **Skriptfeld** (erweitert) wird als „wahr“ ausgewertet oder legt die Variablenantwort **auf** „wahr“ fest oder ist leer.

Weitere Informationen zu Zugriffskontrollregeln finden Sie unter Exploring Access Control Lists

**Wichtig:**
Wenn die Option Administratorüberschreibungen für eine Security Incident-Tabelle deaktiviert ist und der Administrator auf die Security Incident-Tabelle zugreifen kann, finden Sie weitere Informationen unter **KB1444673**

## Security Incident Response Platform Analytics-Lösungen

Platform Analytics-Lösungen enthalten vorkonfigurierte Dashboards. Die Dashboards enthalten wichtige Metriken für die Analyse Ihres Security Incident Response -Prozesses, z. B. neue Security Incidents oder das Durchschnittsalter offener Security Incidents.

Verwenden Sie die Platform Analytics-Widgets im Dashboard, um Daten im Zeitverlauf zu visualisieren, Ihre Geschäftsprozesse zu analysieren, und Verbesserungsbereiche zu identifizieren. Mit Platform Analytics-Lösungen können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

**Wichtig:**
Richten Sie Platform Analytics-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie die Lösung, bevor Sie sie in der Produktion aktivieren.

Die Lösung Security Incident Response Performance Analytics ist über den ServiceNow Storeverfügbar. Weitere Informationen zum Herunterladen und Installieren dieser Anwendung finden Sie unter Sicherheitsvorgänge und im ServiceNow Store.

**Hinweis:**
Um die Funktionalität zu bewerten, können Sie Performance Analytics-Lösungen und In-Form-Analysen für nicht lizenzierte Instanzen aktivieren Performance Analytics. Sie haben jedoch die folgenden Einschränkungen:

- Sie können keine neuen Indikatoren erstellen.
- Sie können keine Daten sammeln, die älter als 180 Tage sind.

Lizenzieren Sie Performance Analytics für vollständige Funktionalität. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

**Wichtig:**
Standardmäßig ist das Datenerfassungslimit für die Eigenschaft `(com.snc.pa.dc.max_records)` in Performance Analytics auf 5.000 Datensätze festgelegt. Sie können dieses Limit jedoch entsprechend Ihren Anforderungen erhöhen, z. B. 50.000 Datensätze. Eine Erhöhung dieses Grenzwerts kann sich jedoch auf die Leistung während der Datenerfassung oder bei der Ausführung von Vorgängen in der Snapshot-Tabelle auswirken. Weitere Informationen zu den Performance Analytics-Eigenschaften finden Sie unter Performance Analytics properties .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zugehörige Informationen

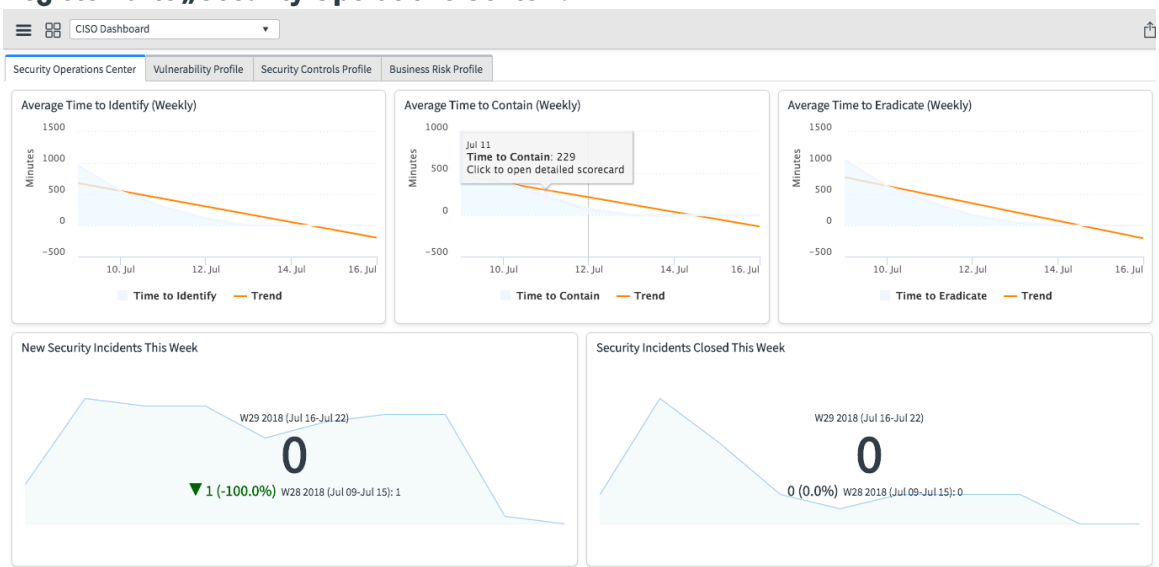
Platform Analytics-Lösungen

Performance Analytics-Abonnement aktivieren

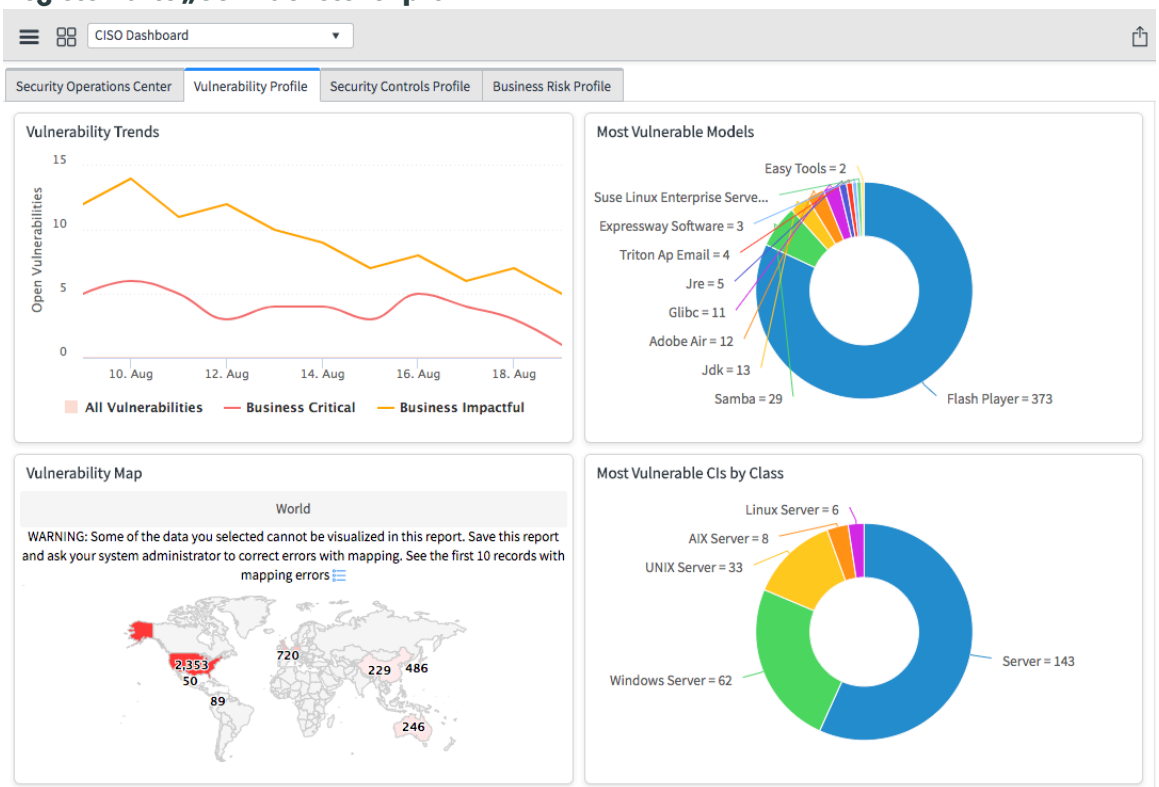
## CISO-Dashboard

Dieses Dashboard zeigt die allgemeine Sicherheitslage Ihrer Organisation, einschließlich Sicherheitsschwachstellen und Incidents.

### Registerkarte „Security Operations Center“.



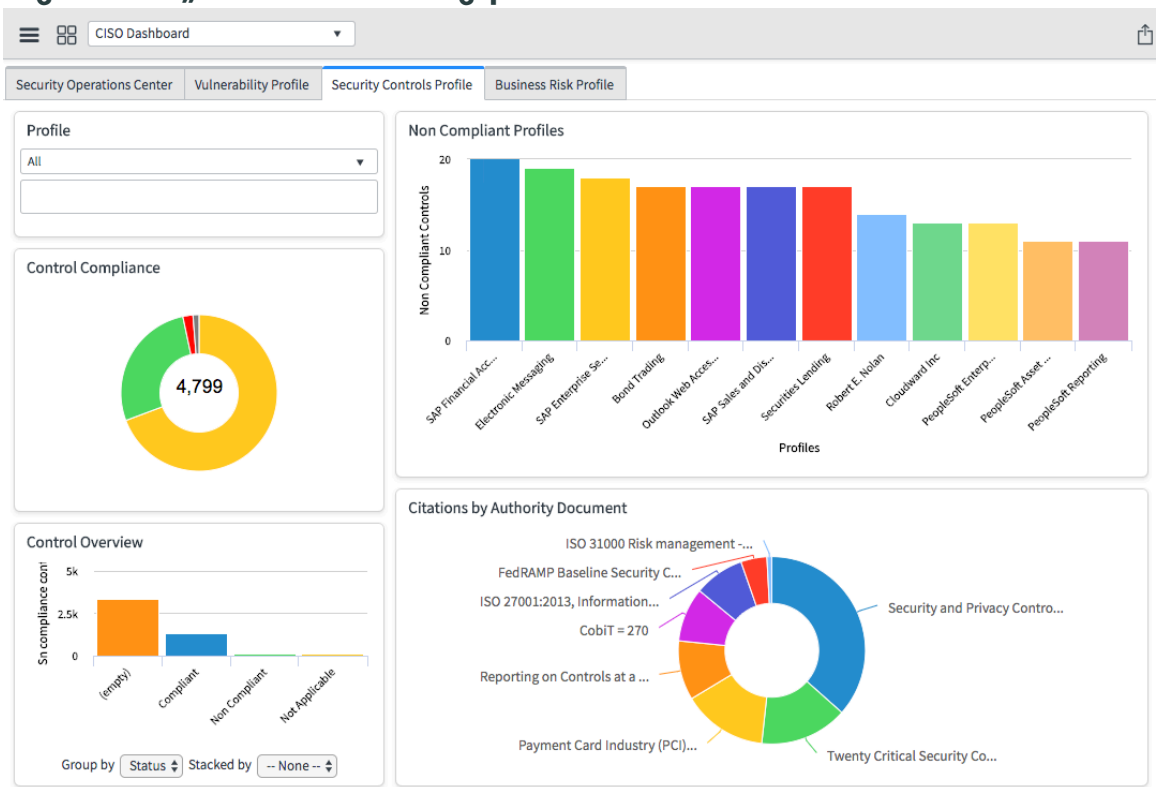

### Registerkarte „Schwachstellenprofil“



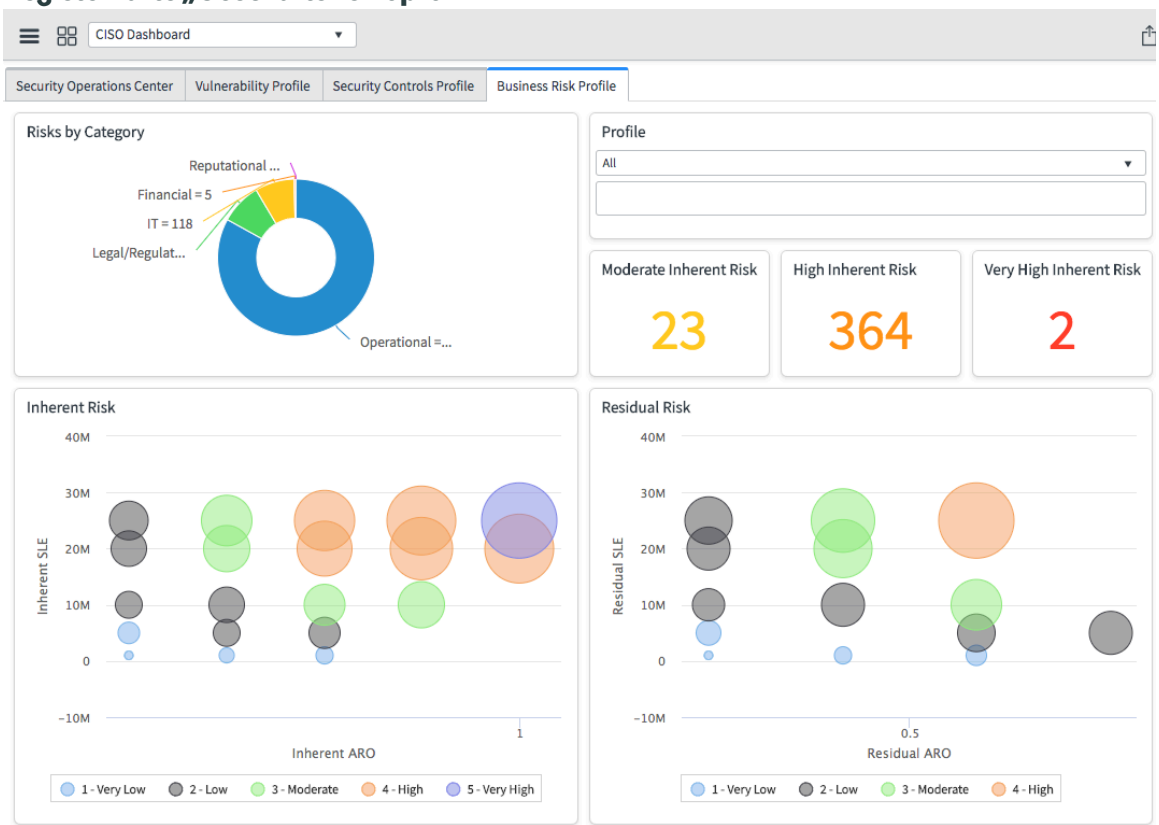

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Sicherheitssteuerungsprofil“




## Registerkarte „Geschäftsrisikoprofil“




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Endbenutzer und Rollen

| Endbenutzer und Ziel | Erforderliche Rolle |
|---|---|
| CISO: Benötigt klare Transparenz in Bezug auf die aktuelle Sicherheitslage der gesamten Organisation | sn_si.ciso |

## CISO-Dashboard-Indikatoren

Das CISO-Dashboard enthält die folgenden Leistungskennzahlen:

**SI: Durchschnittliche Zeit bis zur Identifizierung**

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Identifizierung eines Security Incident benötigt wird, täglich berechnet.

**Durchschnittliche Zeit bis zur Eindämmung**

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Eindämmung eines Security Incident benötigt wird, täglich berechnet.

**Durchschnittliche Zeit bis Beseitigung**

Täglich berechneter 7-Tage-Durchschnitt der Zeit in Minuten, die zur Beseitigung eines Security Incident benötigt wird. Sowohl die durchschnittliche Zeit bis zur Eindämmung als auch die durchschnittliche Zeit bis zur Beseitigung basieren auf dem Indikator „SI – Durchschnittliche Dauer“, aufgeschlüsselt nach Security Incident-Status.

**Neue Security Incidents diese Woche**

Wöchentliche Summe der Punktzahl des täglichen Indikators „Anzahl der neuen Security Incidents“.

**Geschlossene Security Incidents (wöchentlich)**

Die laufende Summe über sieben Tage des täglichen Indikators „Anzahl der geschlossenen Security Incidents“.

**Neue Security Incidents nach Priorität**

Tägliche Aufgliederung des Indikators „Anzahl der neuen Security Incidents“ nach Priorität.

**Neue vs. geschlossene Security Incidents (wöchentlich).**

Die laufende Summe über sieben Tage des Indikators „Anzahl der neuen Incidents“ wird im Diagramm mit der laufenden Summe über sieben Tage des Indikators „Anzahl der geschlossenen Incidents“ verglichen.

**Security Incident-Heatmap**

Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land zeigt.

**Security Incident-Verzeichniszuordnung**

Eine interaktive Verzeichnisübersicht, in der Sie Folgendes auswählen können:

- Security Incidents pro Business Service, aufgeschlüsselt nach Geschäftskritikalität
- Security Incidents aufgeschlüsselt nach Kategorie oder Unterkategorie des Incident
- Security Incidents pro Zuweisungsgruppe oder pro Beauftragten
- „Opferstatistiken“ von Security Incidents pro betroffener Ressource oder betroffenem Benutzer



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## BreakdownsAufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

- Business-Relevanz
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Lösungscode für Security Incident
- Priorität von Security Incident
- Status des Security Incidents
- SI – Business-Service
- Schwachstelle

## Datenvisualisierungen

Das Dashboard enthält die folgenden Visualisierungen:

| Titel | Typ | Beschreibung |
|---|---|---|
| Security Incidents offen für mehr als 30 Tage nach Zuweisungsgruppe und Status | Heatmap | Zeigt Modelle mit den angreifbarsten Elementen an. |
| Risiken nach Kategorie | Ring | Listet das Alter der erneut geöffneten angreifbaren Elemente auf. |
| Zitate nach Berechtigungsdokument | Ring | Anzahl der aktiven Schwachstellen |
| Security Incidents mit Beauftragtem, der nicht aktiv ist | Heatmap | Zeigt die Anzahl der offenen angreifbaren Elemente an, die mit Schwachstellen (Common Vulnerability Enumeration (CVE)-Datensätze) verknüpft sind, von den meisten bis zu den wenigsten. |
| Security Incidents, die seit mehr als 30 Tagen nicht aktualisiert wurden, nach Zuweisungsgruppe und Status | Heatmap | Zeigt Herausgeber mit den angreifbarsten Elementen an. |
| Schwachstellenübersicht | Karte | Eine Weltkarte, die Schwachstellen nach Standort zeigt |
| Modelle mit den meisten Schwachstellen | Ring | Die Anwendungen, die die meisten Schwachstellen enthalten |
| CIs mit den meisten Schwachstellen nach Klasse | Ring | CIs nach Servertyp |
| Services mit besonders wichtigen Schwachstellen | Liste | |
| Nicht konforme Profile | Balken | Nicht konforme Steuerungen nach Profil |
| Kontrollübersicht | Balken | Anzahl der konformen und nicht konformen Kontrollen |



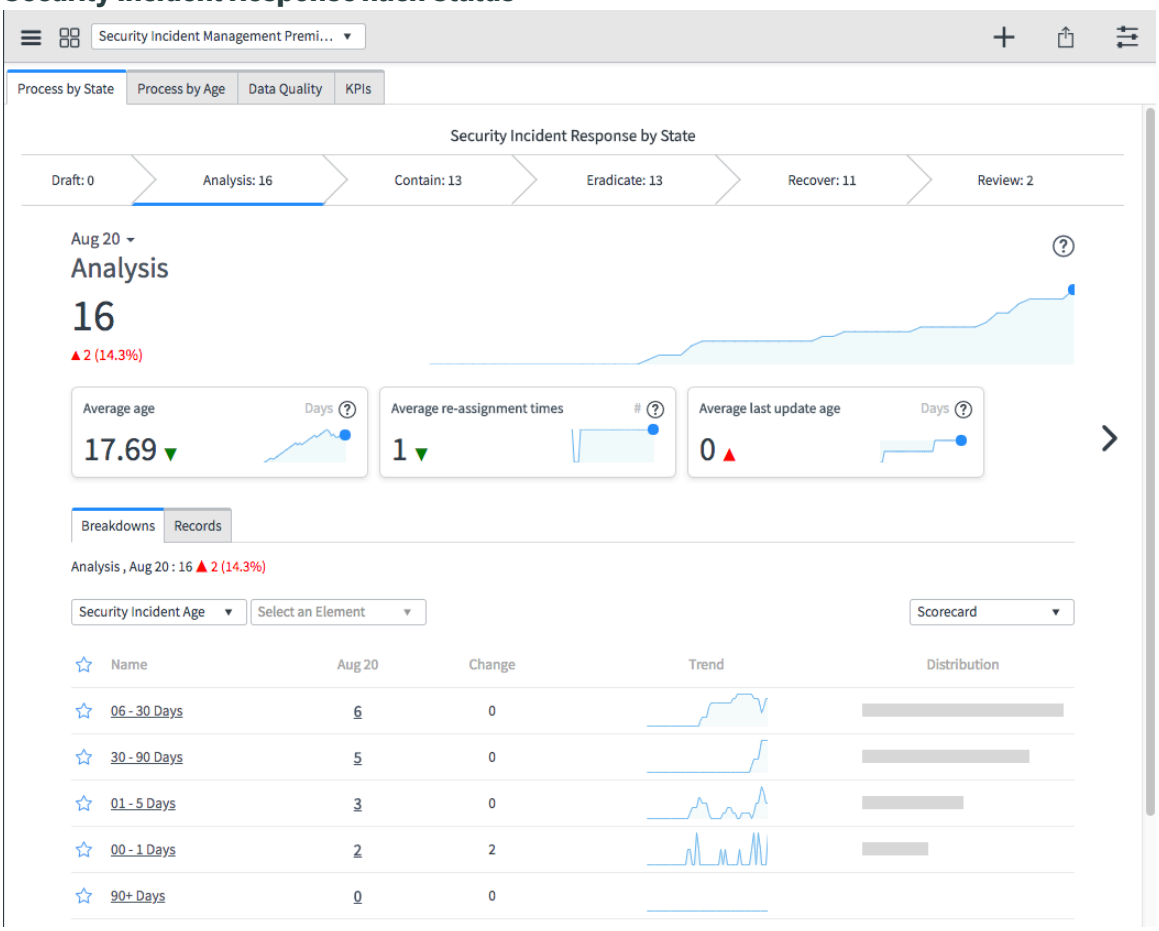
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Titel | Typ | Beschreibung |
|---|---|---|
| Richtlinienausnahmen | Liste | Richtlinienausnahmen mit Priorität, Besitzer und Kurzbeschreibung |
| Risiken nach Kategorie | Ring | Die Anzahl der Risiken in jeder Risikokategorie |
| Inhärentes Risiko | Blase | Inhärente SLE im Vergleich zu inhärenter ARO |
| Restrisiko | Blase | Rest-SLE im Vergleich zu Rest-ARO |
| Moderates, hohes und sehr hohes Risiko | | Die Anzahl der mittleren, hohen und sehr hohen Risiken |
| Risiko nach Profil | Gestapelte für gestapelte Leiste | Risikoanzahl, bei der Sie auswählen können, nach was gruppiert und gestapelt werden soll |

### Security Incident Management Premium-Dashboard

Dieses Dashboard verwendet erweiterte Platform Analytics Visualisierungen, um Sicherheitsmanager bei der Nachverfolgung des Umfangs, der Leistung und des Fortschritts von Security Incidents zu unterstützen, von der ersten Analyse/Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung. Die lizenzierte Version von Performance Analytics ist daher erforderlich.

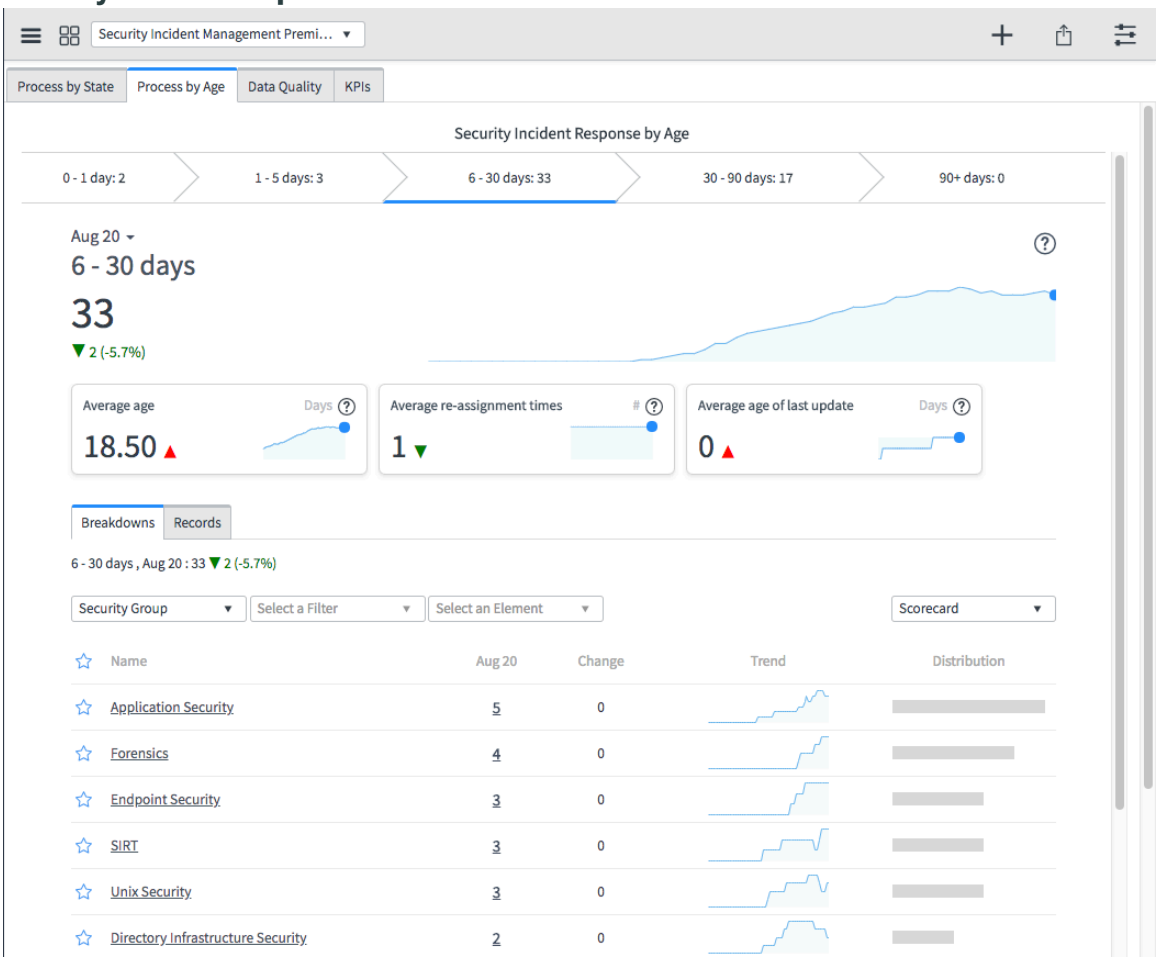
#### Security Incident Response nach Status




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident Response nach Alter




## Endbenutzer und Rollen

| Endbenutzer und Ziel | Erforderliche Rolle | Vorteile |
|---|---|---|
| Security Response Manager: Benötigt klare Transparenz in Bezug auf den Gesamtstatus und das Volumen von Security Incidents im Zusammenhang mit Anwendungen und Services. | sn_si.manager | Kann die allgemeine Sicherheitslage überprüfen und die Mitglieder von Zuweisungsgruppen anpassen. |
| Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben, während er nach Bedarf Gebiete und Kompetenzen verwaltet. | sn_si.admin | Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden. |
| Security Response-Analysten: Müssen schnell priorisieren, auf welche Schwachstellen der Schwerpunkt basierend auf der Relevanz für die Organisation gelegt werden soll. | sn_si.analyst | Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Änderungen und Ausfälle im |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Endbenutzer und Ziel | Erforderliche Rolle | Vorteile |
|---|---|---|
| | | Zusammenhang mit ihren Incidents erstellen und aktualisieren. |

## Security Incident Management Premium-Indikatoren

Die Registerkarten Nach Status verarbeiten und Nach Alter verarbeiten enthalten Workbench-Widgets mit den folgenden Indikatoren:

**Durchschnittliches Alter**

Der Indikator „Durchschnittliches Alter der offenen Security Incidents“ verwendet die Formel [[Summiertes Alter der offenen Security Incidents]]/[[Anzahl der offenen Security Incidents]]/24, um ein Ergebnis in Tagen anzugeben.

**Durchschnittliche Anzahl Neuzuweisungen**

Der Indikator Durchschnittliche Neuzuweisung offener Security Incidents verwendet die Formel Summierte Neuzuweisungen offener Security Incidents / Anzahl offener Security Incidents.

**Durchschnittliches Alter der letzten Aktualisierung**

Der Indikator Durchschnittliches Alter der letzten Aktualisierung offener Security Incidents verwendet die Formel Summiertes Alter der letzten Aktualisierung offener Security Incidents / Anzahl der offenen Security Incidents / 24, um ein Ergebnis in Tagen zu erhalten.

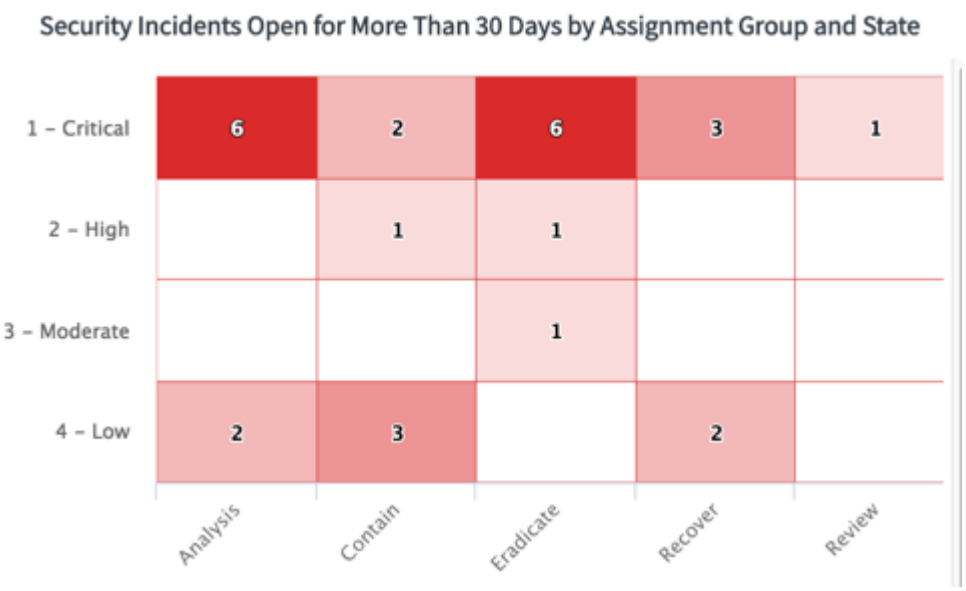
**% seit 5 Tagen nicht aktualisiert**

Der Indikator % der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden, verwendet die Formel ([[Anzahl der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden]] / [[Anzahl der offenen Security Incidents]]) * 100.

Die Registerkarte Datenqualität enthält interaktive Filter für die Kategorie des Security Incident und die Stufen Risiko, Priorität und Schweregrad. Diese Filter werden gleichzeitig auf die folgenden Indikatoren angewendet:

**Security Incidents offen für mehr als 30 Tage nach Zuweisungsgruppe und Status**

Die Anzahl der offenen Security Incidents, gefiltert nach einem Alter von 30 Tagen und aufgeschlüsselt nach Zuweisungsgruppe und Status.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incidents mit Beauftragtem, der nicht aktiv ist**

Die Anzahl der offenen Security Incidents ohne Beauftragten oder mit einem Beauftragten, der nicht aktiv ist.

**Security Incidents offen für mehr als 30 Tage nach Zuweisungsgruppe und Status**

Der Indikator „Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden“ aufgeschlüsselt nach Zuweisungsgruppe und Status.

Die Registerkarte „KPI“ enthält die folgenden zusätzlichen Indikatoren:

- % der neuen kritischen Security Incidents
- Durchschnittliches Alter offener Security Incidents
- Durchschnittliche Abschlusszeit von Security Incidents
- % der Security Incidents, die neu zugewiesen wurden
- % der Security Incidents, die bei der ersten Zuweisung geschlossen wurden
- % der per Selfservice geschlossenen Security Incidents
- % der nicht gelösten Security Incidents
- Durchschnittliche Abschlusszeit von Security Incident-Aufgaben

## BreakdownsAufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

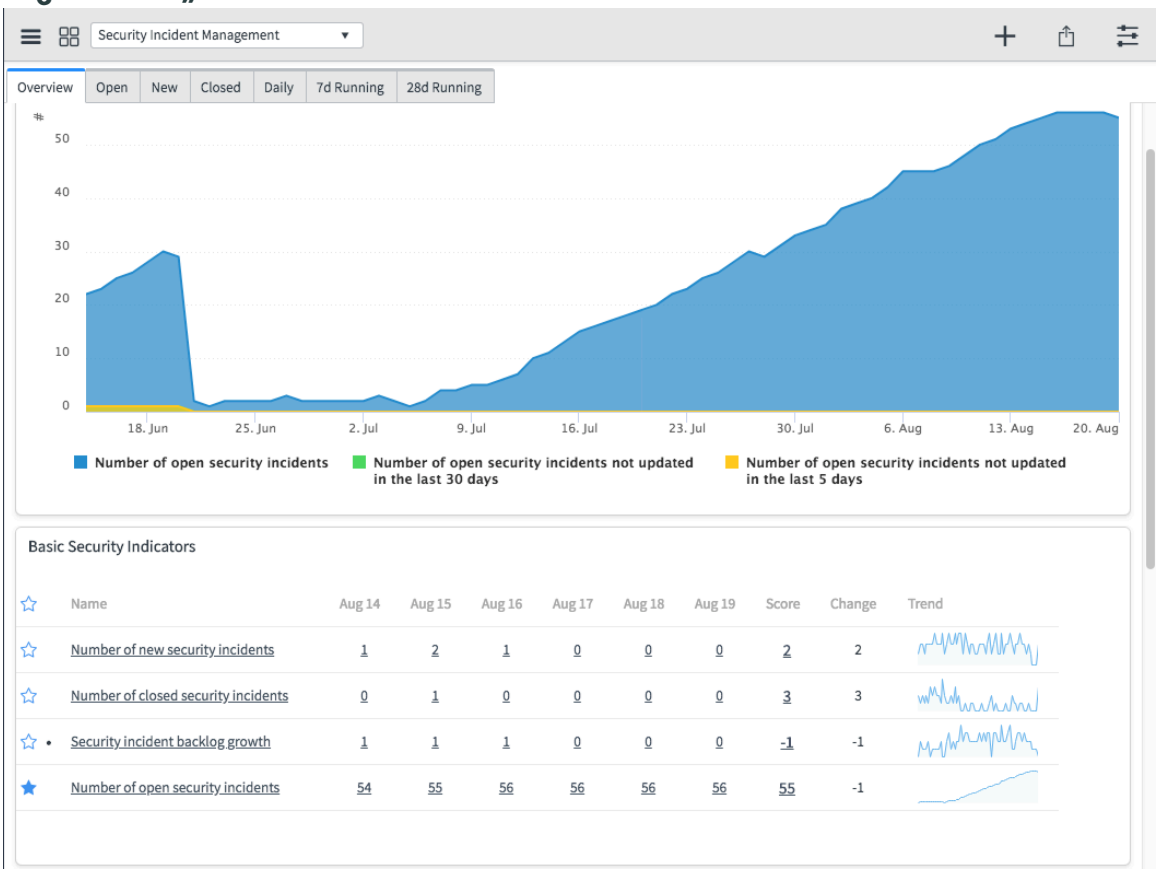
### Security Incident Management-Dashboard

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung einfach nachverfolgen.

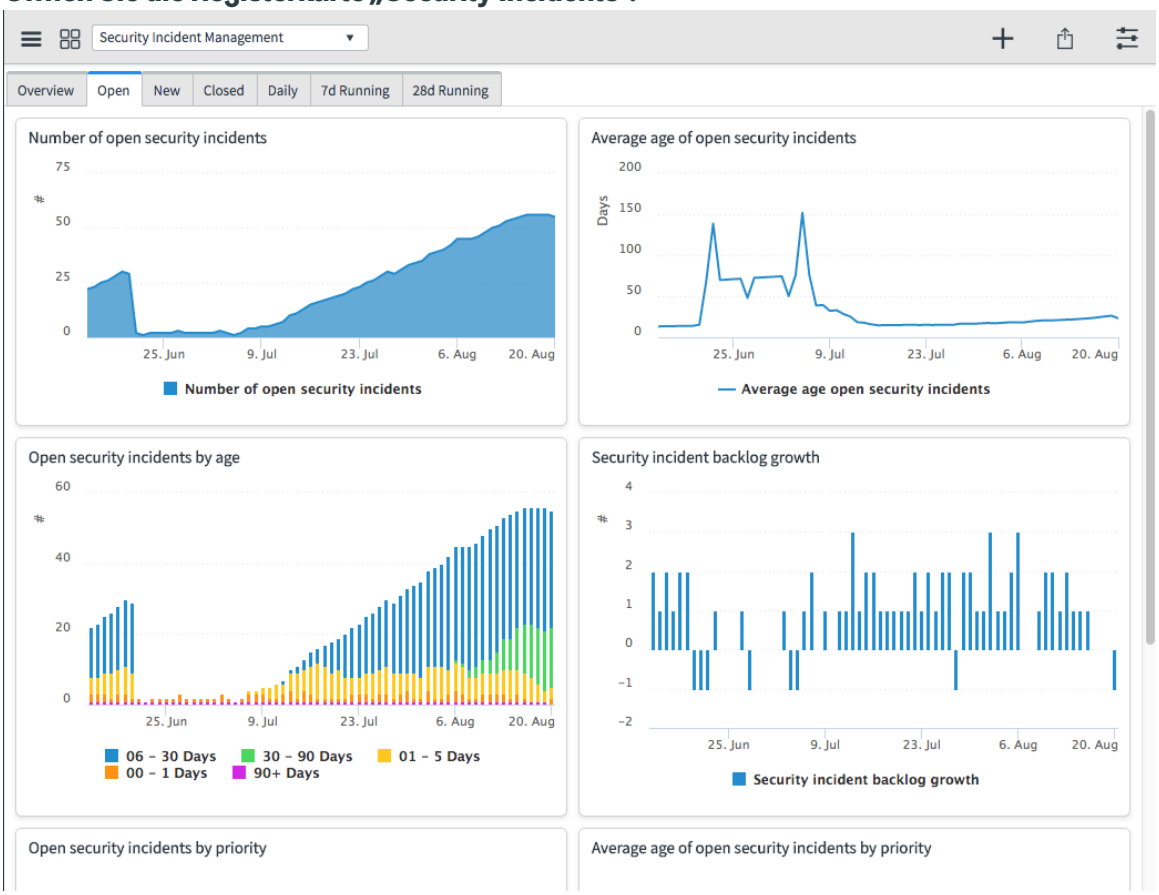


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Übersicht“



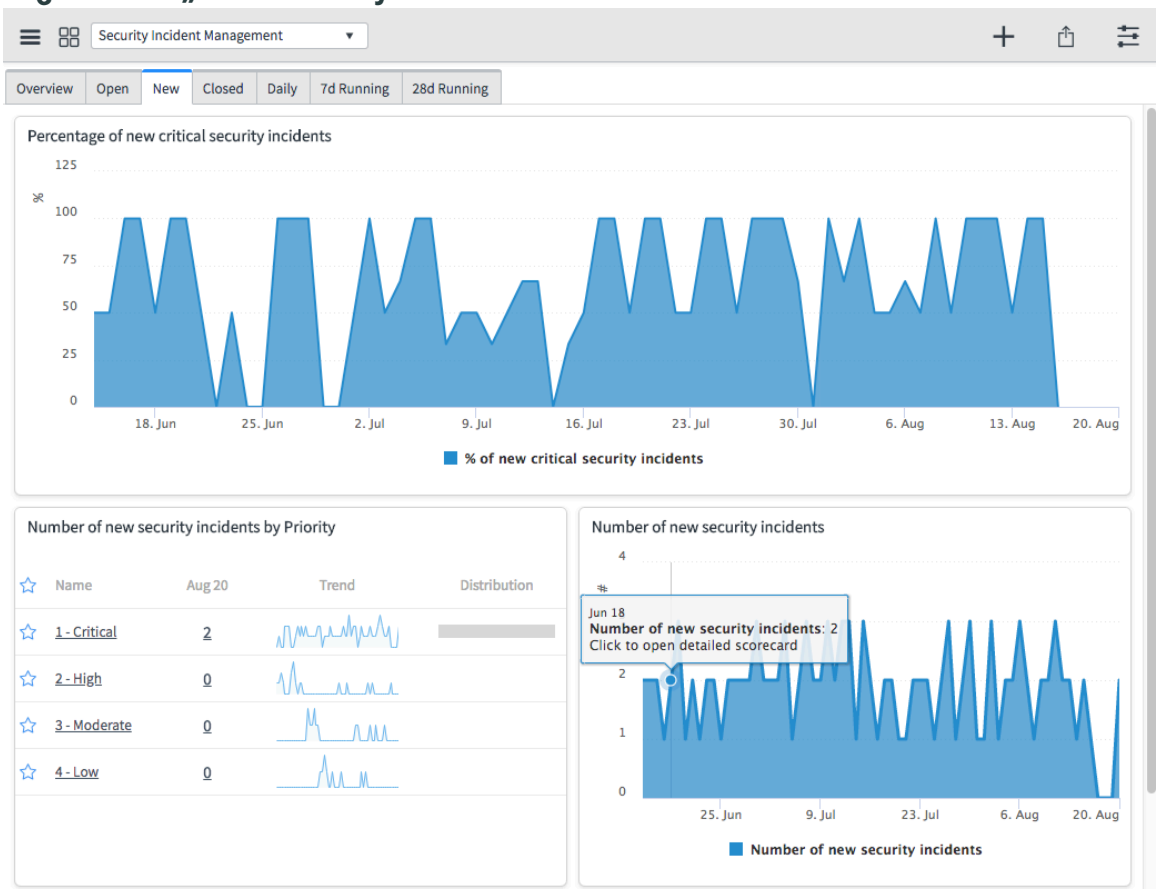

## Öffnen Sie die Registerkarte „Security Incidents“.



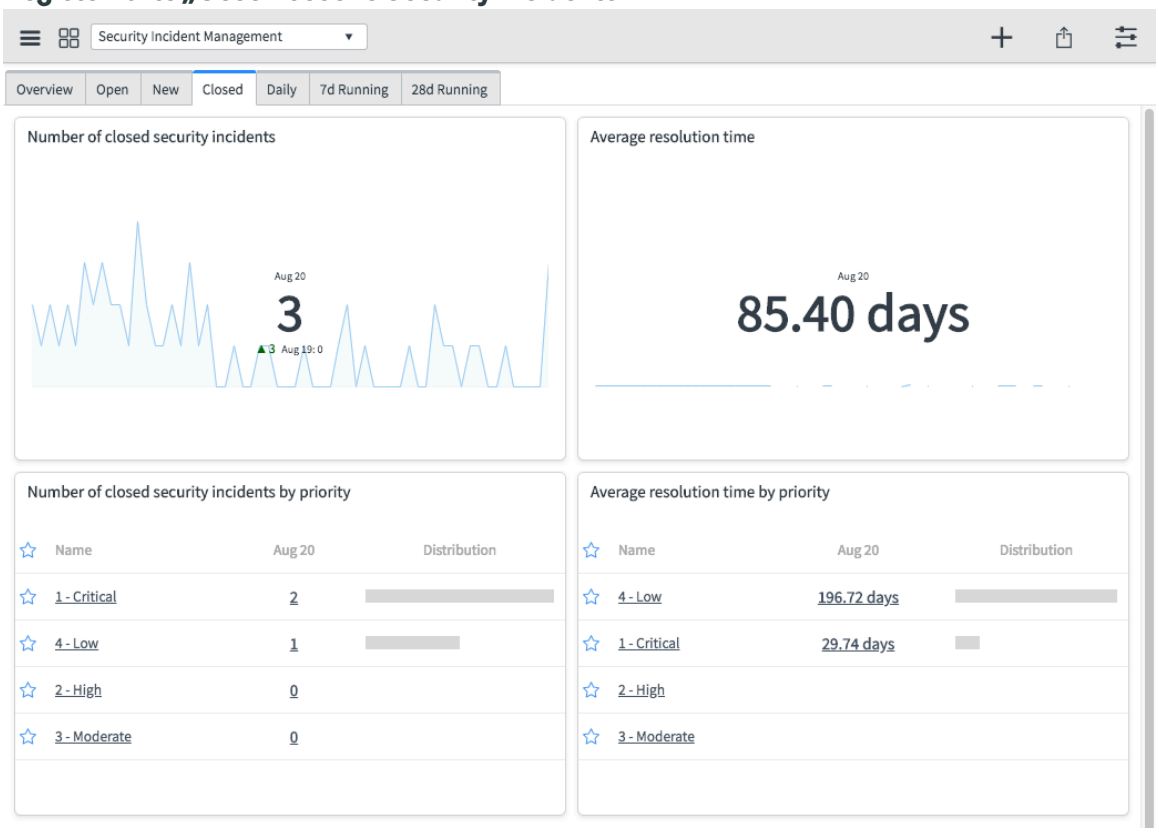

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Neuer Security Incident“.



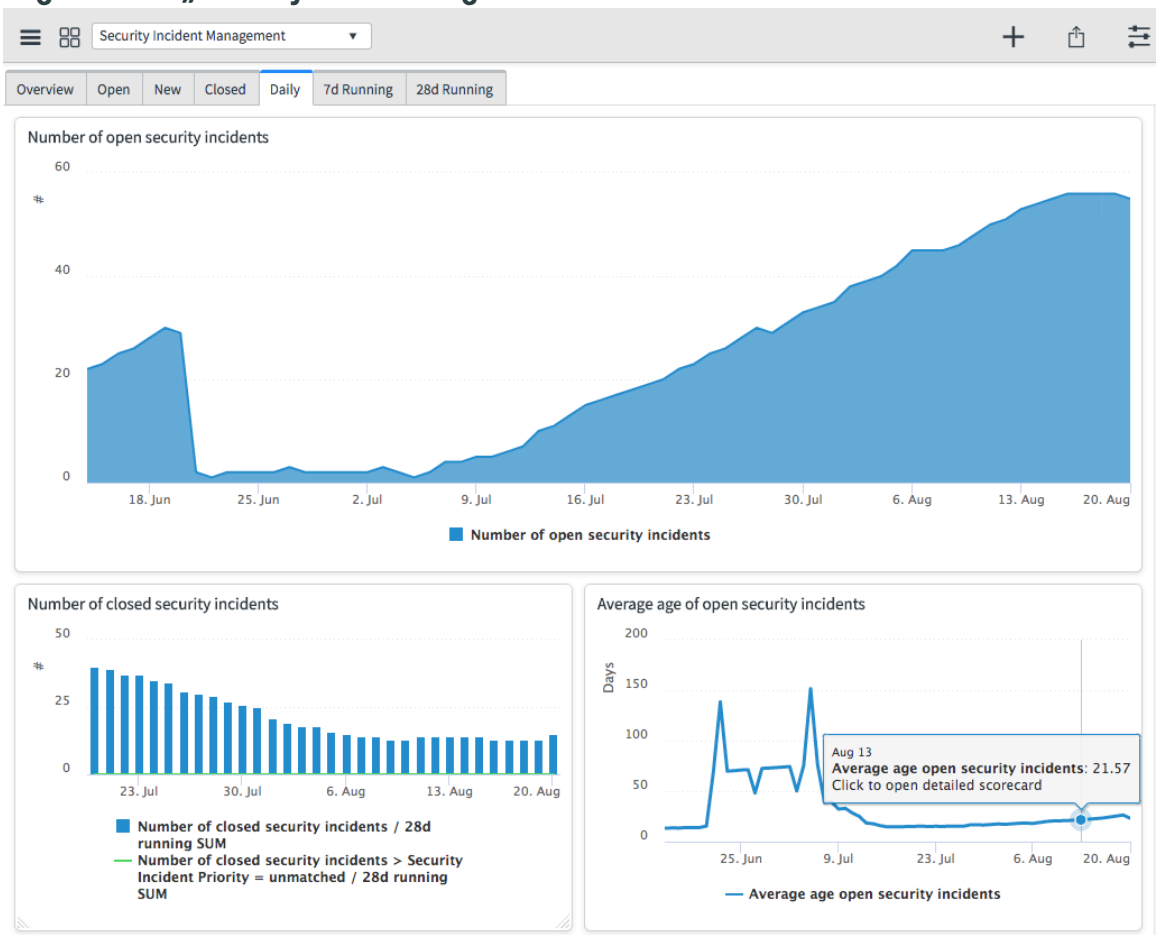

## Registerkarte „Geschlossene Security Incidents“




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Security Incidents täglich“.**




Die Registerkarten „ **7 Tage** ausgeführt“ und **„28** Tage ausgeführt“ folgen dem Format der Registerkarte „ **Täglich** “.

## Endbenutzer und Rollen

| Endbenutzer und Ziel | Erforderliche Rolle | Vorteile |
|---|---|---|
| Security Response Manager: Benötigt klare Transparenz in Bezug auf den Gesamtstatus und das Volumen von Security Incidents im Zusammenhang mit Anwendungen und Services. | sn_si.manager | Kann die allgemeine Sicherheitslage überprüfen und die Mitglieder von Zuweisungsgruppen anpassen. |
| Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben, während er nach Bedarf Gebiete und Kompetenzen verwaltet. | sn_si.admin | Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden. |
| Security Response-Analysten: Müssen schnell priorisieren, auf welche Schwachstellen der Schwerpunkt basierend auf der | sn_si.analyst | Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Endbenutzer und Ziel | Erforderliche Rolle | Vorteile |
|---|---|---|
| Relevanz für die Organisation gelegt werden soll. | | Änderungen und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren. |

## Security Incident Management-Indikatoren

Das Security Incident Management-Dashboard enthält die folgenden Leistungskennzahlen:

**Neue Security Incidents**

Ein Diagramm der Anzahl der neuen Security Incidents.

**Offene Security Incidents**

Ein Diagramm, in dem Sie die Anzahl der offenen Security Incidents, die Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden, und die Anzahl der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden, vergleichen können.

**Indikatoren für einfache Sicherheit**

Die letzten 6 Tage der Punktzahlen der Anzahl der neuen Security Incidents, der Anzahl der geschlossenen Security Incidents, des Wachstums des Rückstands von Security Incidents und der Indikatoren „Anzahl der offenen Security Incidents“.

**Neue Security Incidents nach Priorität**

Die Anzahl der neuen Security Incidents, aufgeschlüsselt nach Priorität.

## BreakdownsAufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

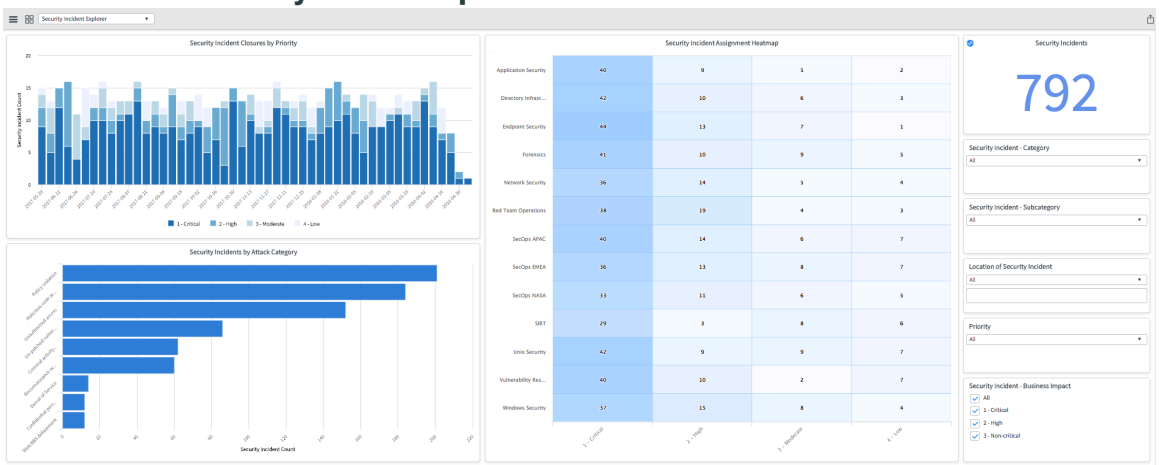
### Security Incident Explorer-Dashboard

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen. Mit diesen Ansichten erhalten Manager schnell Einblick in die Häufigkeit, mit der Angriffe auftreten, und darüber, welche Business Services betroffen sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Teilansicht des Security Incident Explorer-Dashboards




## Endbenutzer und Rollen

| Endbenutzer und Ziel | Erforderliche Rolle | Vorteile |
|---|---|---|
| Security Response Manager: Benötigt klare Transparenz in Bezug auf den Gesamtstatus und das Volumen von Security Incidents im Zusammenhang mit Anwendungen und Services. | sn_si.manager | Kann die allgemeine Sicherheitslage überprüfen und die Mitglieder von Zuweisungsgruppen anpassen. |
| Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben, während er nach Bedarf Gebiete und Kompetenzen verwaltet. | sn_si.admin | Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden. |
| Security Response Analyst: Müssen schnell priorisieren, auf welche Schwachstellen sie sich konzentrieren sollen, basierend auf der Relevanz für die Organisation. | sn_si.analyst | Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Änderungen und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren. |

## Security Incident Explorer-Indikatoren

Das Security Incident Explorer-Dashboard enthält die folgenden Leistungskennzahlen:

**Security Incidents**

Gesamtvolumen offener und ausstehender Security Incidents.

**Security Incident-Abschlüsse nach Priorität**

Die Anzahl der geschlossenen Security Incidents, aufgeschlüsselt nach Priorität.

**Security Incidents nach Angriffskategorie**

Die Anzahl der offenen Security Incidents aufgeschlüsselt nach Kategorie.

**Security Incident-Zuweisungs-Heatmap**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine zweistufige Aufgliederung der Anzahl offener Security Incidents nach Zuweisungsgruppe und Priorität.

**Security Incident-Heatmap**

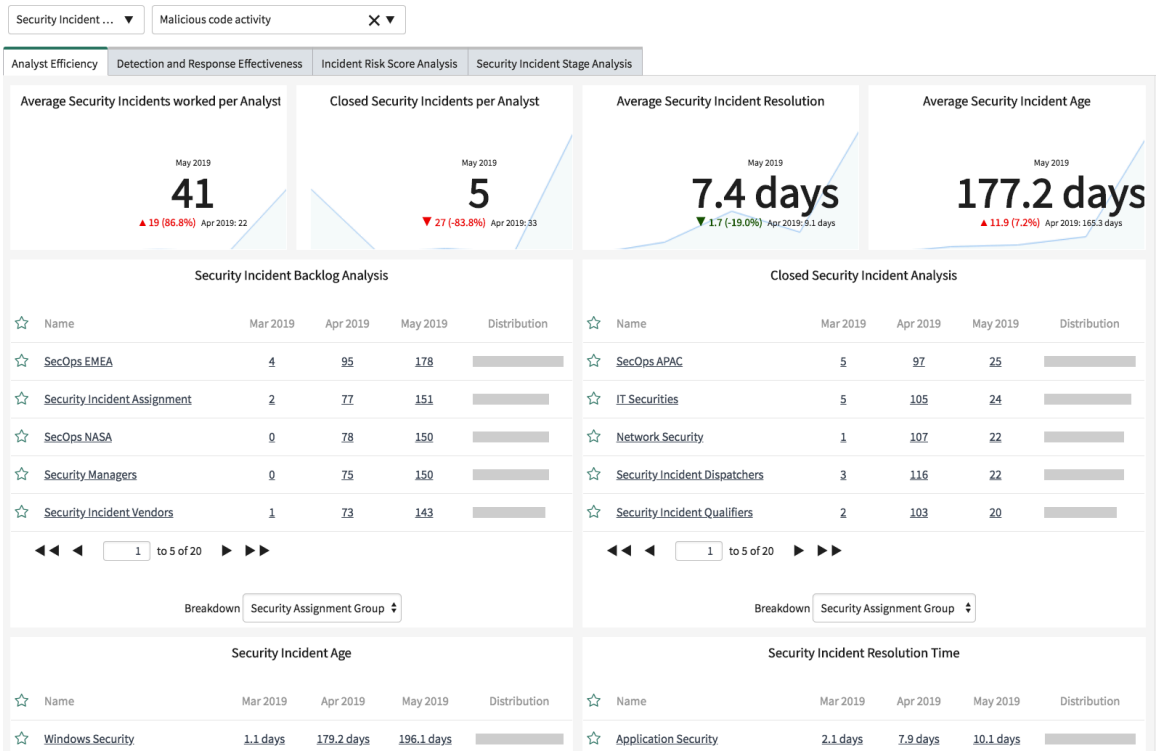
Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land zeigt.

## Dashboard „Effizienz von Sicherheitsvorgängen“.

SOC-Manager (Security Operations Center) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

SOC-Manager können das Performance Analytics-Dashboard verwenden, um die Effizienz zu verbessern und sich ein Bild von der Leistung von SOC in allgemeinen und spezifischen Bereichen im Laufe der Zeit zu machen.

## Registerkarte „Analyseneffizienz“.

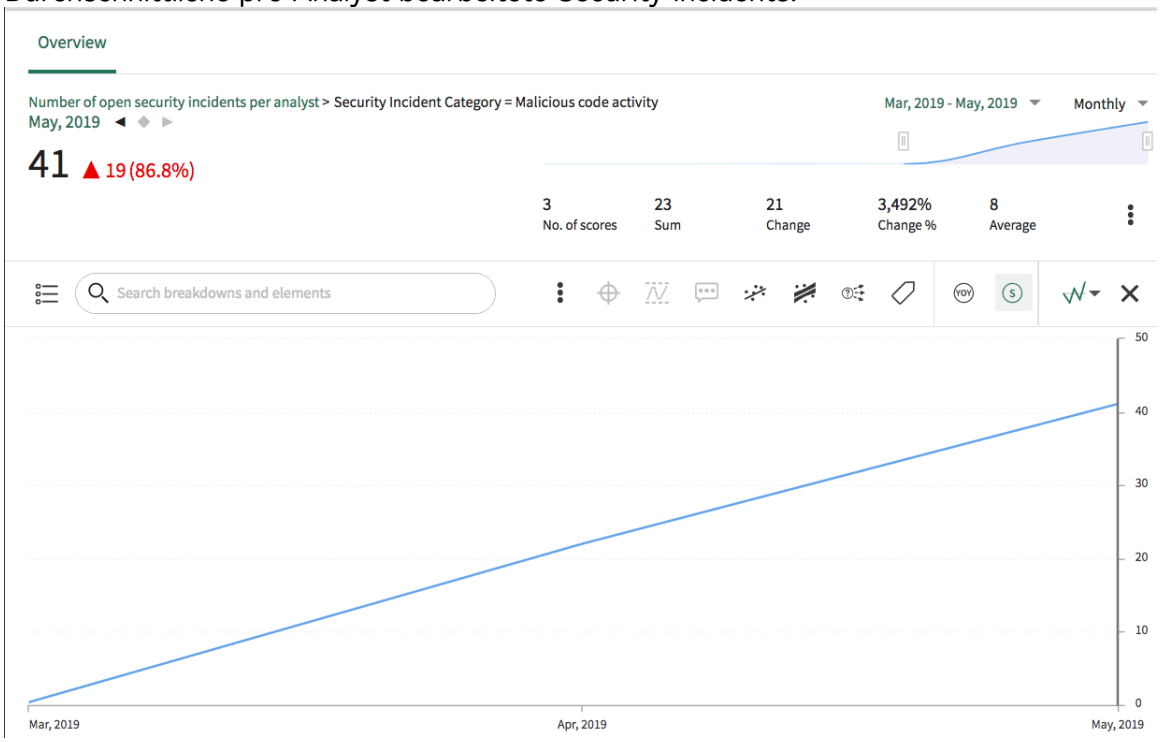



Klicken Sie auf einen der Indikatoren, um weitere Details anzuzeigen.
Klicken Sie beispielsweise auf den Indikator im Abschnitt



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durchschnittliche pro Analyst bearbeitete Security Incidents.




Das Diagramm zeigt, dass die Anzahl der offenen Security Incidents von 0 im März auf über 40 im Mai gestiegen ist. Beachten Sie die im Header angezeigten Daten:

- Trendindikator: Zeigt die Änderung der Anzahl offener Incidents im letzten Zeitraum an, für den die Daten erfasst wurden. Dieses Diagramm zeigt Daten für den Zeitraum März 2019 bis Mai 2019, und die Anzahl der offenen Incidents ist im Mai um 19 gestiegen. Die Effizienz der Analysten ist besser, wenn die Anzahl der offenen Incidents im Laufe der Zeit abgenommen hat.
- Anzahl der Punktzahlen: Der Zeitraum, für den die Daten gesammelt wurden (März bis Mai 2019).
- Summe: Die Anzahl der neuen offenen Incidents im Zeitraum zwischen März und Mai.
- Change: Die Anzahl der neuen offenen Incidents zwischen März und April.
- Durchschnitt: Die durchschnittliche Anzahl offener Incidents pro Analyst für den ausgewählten Zeitraum.

**Registerkarte „Analyseneffizienz“.**

| Indikator | Beschreibung |
|---|---|
| Durchschnittliche Anzahl der pro Analyst bearbeiteten Security Incidents | Durchschnittliche Anzahl der offenen Security Incidents pro Analyst für den angegebenen Zeitraum. Die verwendete Formel lautet [[Anzahl der offenen Security Incidents / Pro Monat - Durchschnitt +]]/[[Anzahl der Security-Service Desk-Mitarbeiter]] |
| Geschlossene Security Incidents pro Analyst | Die Gesamtzahl der Incidents, die von jedem Analysten in der ausgewählten Kategorie im angegebenen Zeitraum geschlossen wurden. Die verwendete Formel lautet [Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie =“.<category_name> / Pro Monat SUM +]]/[[Anzahl der Security-Service Desk-Mitarbeiter / Pro Monat - Durchschnitt +]] |
| Durchschnittliche Lösung von Security Incidents | Die durchschnittliche Zeit, die jeder Analyst benötigt, um Security Incidents im angegebenen Zeitraum zu schließen. Die Formel zum Anzeigen des Ergebnisses |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

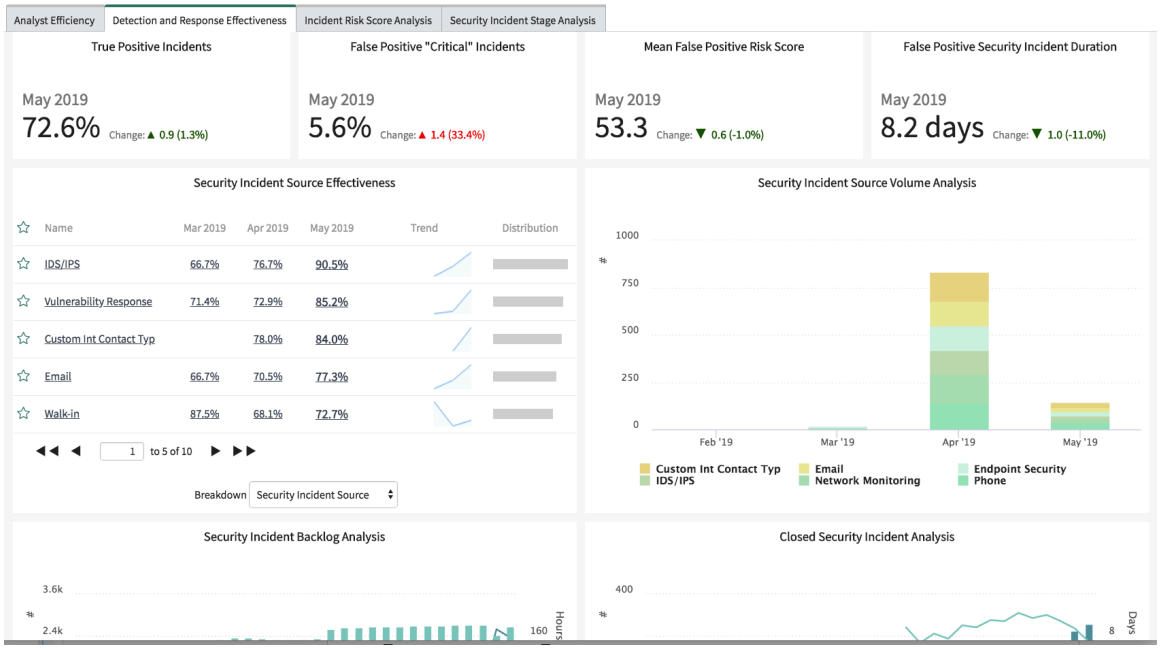
**Registerkarte „Analysteneffizienz". (Fortsetzung)**

| Indikator | Beschreibung |
|---|---|
| | in Tagen lautet ([[Summierte Dauer der geschlossenen Security Incidents > Security Incident-Kategorie =<category_name> / Pro Monat - Durchschnitt +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = / Pro Monat - Durchschnitt +]]) / 24 |
| Durchschnittliches Alter von Security Incidents | Die durchschnittliche Anzahl von Tagen, für die Security Incidents für jeden Analysten offen bleiben. Die Formel zum Anzeigen des Ergebnisses in Tagen lautet ([[Summiertes Alter der offenen Security Incidents > Security Incident-Kategorie =<category_name> / Pro Monat - Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Security Incident-Kategorie = / Pro Monat - Durchschnitt +]]) / 24 |
| Rückstandanalyse von Security Incidents | Die Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum. Wählen Sie eine Option aus der Liste Aufgliederung aus, um den Rückstand für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen. |
| Analyse geschlossener Security Incidents | Die Gesamtzahl der Security Incidents, die im angegebenen Zeitraum geschlossen wurden. Wählen Sie eine Option aus der Liste Aufgliederung aus, um die Anzahl für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der Security Incidents vergleichen, die in zwei ausgewählten Monaten geschlossen wurden. |
| Security Incident-Alter | Die durchschnittliche Anzahl der offenen Tage für Security Incidents im angegebenen Zeitraum. Wählen Sie eine Option aus der Liste Aufgliederung aus, um das Alter der Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel zum Anzeigen des Ergebnisses in Tagen lautet ([[Summiertes Alter der offenen Security Incidents > Security Incident-Kategorie =<category_name> > Sicherheitszuweisungsgruppe =<group_name> / Pro Monat - Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Security Incident-Kategorie = > Sicherheitszuweisungsgruppe = / Pro Monat - Durchschnitt +]]) / 24 |
| Lösungszeit für Security Incidents | Die durchschnittliche Anzahl von Tagen, die für die Lösung von Security Incidents während des angegebenen Zeitraums benötigt wurden. Wählen Sie eine Option aus der Liste Aufgliederung aus, um die Lösungszeit für Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel, die verwendet wird, um das Ergebnis in Tagen anzuzeigen, lautet ([[Summierte Dauer der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität > Sicherheit zugewiesen an = Johnashby / Pro Monat - Durchschnitt +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität > Sicherheit zugewiesen an = John Shaby / Pro Monat - Durchschnitt +]]) / 24 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Erkennungs- und Antworteffektivität“




### Registerkarte „Erkennungs- und Antworteffektivität“

| Indikator | Beschreibung |
|---|---|
| Richtig positive Incidents | Prozentsatz der wirklich positiven Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel lautet (1-([[Anzahl der falsch positiven Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität / Pro Monat SUM +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität / Pro Monat SUMME +]])) * 100 |
| Falsch positive kritische Incidents | Prozentsatz der falsch positiven kritischen Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel lautet ([[Anzahl der falsch positiven Security Incidents > Security Incident-Risikopunktzahl = Kritisches Risiko > Security Incident-Kategorie = Böswillige Codeaktivität / Pro Monat SUM +]]/[[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillig“. Codeaktivität / Pro Monat SUM +]]) * 100<br><br>**Hinweis:**<br>Alle Security Incidents, bei denen der Geschlossen-Code = Ungültige Schwachstelle oder Falsch positive Werte als falsch positive Incidents behandelt werden |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Erkennungs- und Antworteffektivität“ (Fortsetzung)**

| Indikator | Beschreibung |
|---|---|
| Mittlere falsch positive Risikopunktzahl | Durchschnittliche monatliche Risikopunktzahl geschlossener Security Incidents, die als falsch positive Incidents identifiziert wurden Eine niedrigere Risikopunktzahl zeigt an, dass die Sicherheitsanalysten weniger Zeit für die Analyse falsch positiver Incidents aufgewendet haben. Die verwendete Formel lautet ([[Anzahl der falsch positiven Security Incidents > Security Incident-Risikopunktzahl = Kritisches Risiko > Security Incident-Kategorie = Böswillige Codeaktivität / Pro Monat SUM +]]/[[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillig“. Codeaktivität / Pro Monat SUM +]]) * 100 |
| Dauer des falsch positiven Security Incidents | Durchschnittliche Anzahl der Tage, die Sicherheitsanalysten für die Untersuchung falsch positiver Incidents aufgewendet haben. Die verwendete Formel lautet ([[Summierte Dauer der falsch positiven Security Incidents]] / [[Anzahl der falsch positiven Security Incidents]]) / 24 |
| Effektivität der Security Incident-Quelle | Prozentsatz der wirklich positiven Security Incidents, die von einer bestimmten Quelle für den angegebenen Zeitraum identifiziert wurden. Die Quelle kann E-Mail, Netzwerkaktivität, Kundensupport usw. sein. Anhand dieser Daten kann die Effektivität der Security Incident-Quelle gemessen werden. Die verwendete Formel lautet (1-([[Anzahl der falsch positiven Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität > Security Incident-Quelle = IDS/IPS / Pro Monat SUM +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident Kategorie = Böswillige Codeaktivität > Security Incident Source = IDS/IPS / Pro Monat SUM +]])) * 100 |
| Quellvolumenanalyse des Security Incident | Anzahl der geschlossenen Security Incidents für den aktuellen Monat für jede Security Incident-Quelle. Sie können auch die Anzahl der Security Incidents für jeden Quelltyp zwischen zwei ausgewählten Monaten vergleichen. |
| Rückstandanalyse von Security Incidents | Die Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum und die durchschnittliche Anzahl von Tagen, für die die Incidents offen bleiben. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen. Die Formel zur Berechnung des durchschnittlichen Rückstandszeitraums lautet ([[Summiertes Alter offener Security Incidents |

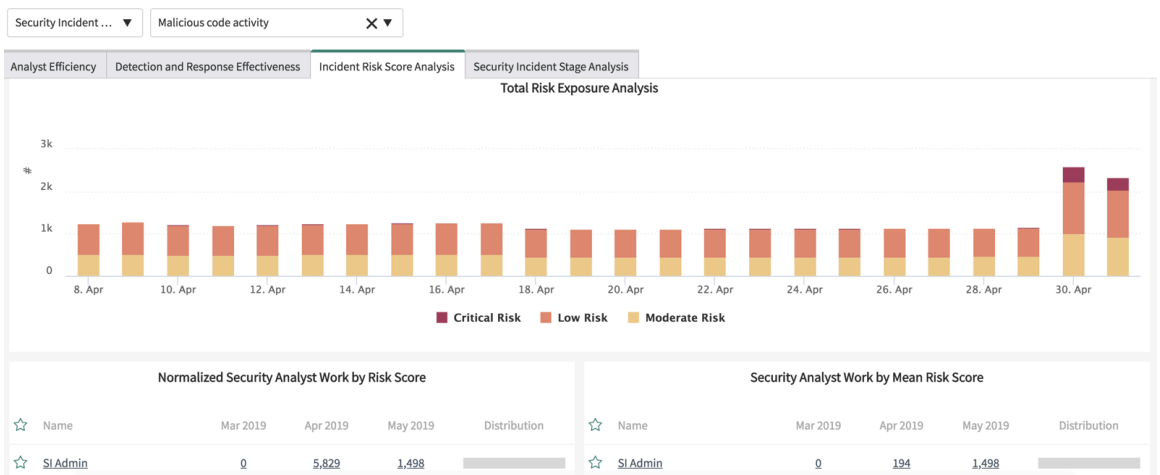


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Erkennungs- und Antworteffektivität“ (Fortsetzung)

| Indikator | Beschreibung |
|---|---|
| | > Security Incident-Kategorie = Böswillige Codeaktivität]]/[[Anzahl offener Security Incidents > Security Incident-Kategorie = Böswillige Code-Aktivität]]) / 24 |
| Analyse geschlossener Security Incidents | Die Gesamtzahl der geschlossenen Security Incidents im angegebenen Zeitraum und die durchschnittliche Lösungszeit für diese Incidents. Die Formel zur Berechnung der durchschnittlichen Lösungszeit lautet ([[Summierte Dauer der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität]]) / 24 |

## Registerkarte „Analyse der Incident-Risikopunktzahl“




### Registerkarte „Analyse der Incident-Risikopunktzahl“

| Indikator | Beschreibung |
|---|---|
| Analyse des Gesamtrisikos des Gefahrenpotenzials | Gesamtzahl der offenen Incidents in jeder Risikokategorie (niedrig, mittel und kritisch) im angegebenen Zeitraum. Sie können auch die Anzahl der Incidents in den verschiedenen Risikokategorien zwischen zwei Monaten vergleichen. |
| Normalisierte Arbeit von Sicherheitsanalysten nach Risikopunktzahl | Die Gesamtrisikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Dies wird basierend auf der Anzahl der echten positiven Security Incidents berechnet, die der Sicherheitsanalyst geschlossen hat. Die verwendete Formel lautet [[Summierte Risikopunktzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität > Sicherheit zugewiesen |

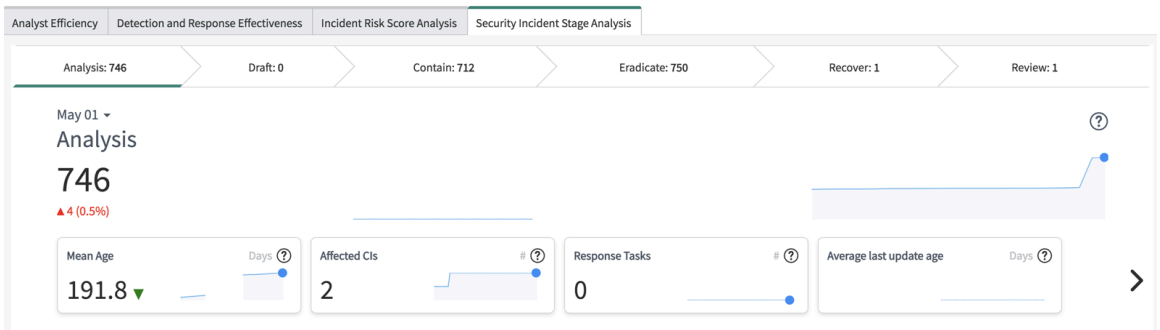


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Analyse der Incident-Risikopunktzahl“ (Fortsetzung)**

| Indikator | Beschreibung |
|---|---|
| | an = SI-Administrator / Pro Monat SUM +]] - [[Summierte Risikopunktzahl der falsch-positiven Security Incidents > Security Incident-Kategorie“. = Böswillige Codeaktivität > Sicherheit zugewiesen an = SI-Administrator / Pro Monat SUM +]] |
| Sicherheitsanalysten arbeiten nach durchschnittlicher Risikopunktzahl | Die durchschnittliche Risikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Die verwendete Formel lautet [[Summierte Risikopunktzahl der geschlossenen Security Incidents > Security Incident-Kategorie = Böswillige Codeaktivität > Sicherheit zugewiesen an = SI-Administrator / Pro Monat - Durchschnitt +]] - [[Summierte Risikopunktzahl der falsch-positiven Security Incidents > Security Incident-Kategorie“. = Böswillige Codeaktivität > Sicherheit zugewiesen an = SI-Administrator / Pro Monat - Durchschnitt +]] |

## Registerkarte „Security Incident-Phasenanalyse“




Sie können die Anzahl der offenen Incidents an einem bestimmten Tag und den Status (Analyse, Entwurf, Eindämmen, Beseitigen, Wiederherstellen oder Überprüfen) dieser Incidents anzeigen. In jeder Phase können Sie das durchschnittliche Alter, betroffene CIs, Antwortaufgaben usw. anzeigen. Klicken Sie auf einen Link, um zusätzliche Details oder die Aufgliederung dieser Incidents anzuzeigen.

# Arbeitsbereich für Security Incident Response

ServiceNow® Arbeitsbereich für Security Incident Response ist eine neu konzipierte Benutzeroberfläche, die Sicherheitsanalysten und SOC-Managern eine Benutzer-Experience der nächsten Generation bietet. Damit können Sicherheitsanalysten den Lebenszyklus von Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung verwalten.

## Erste Schritte mit SIR Workspace

Wählen Sie eine Kachel aus, um mit den ersten Schritten zu beginnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| **Erkunden Sie den Arbeitsbereich**<br> <br>Erfahren Sie mehr über die Konzepte und Funktionen von SIR Workspace | **Administratoren, die Arbeitsbereich verwenden**<br> <br>Konfigurieren Sie SIR Workspace und -Funktionen |
| **Analysten, die Workspace verwenden**<br> <br>Erfahren Sie, wie Analysten SIR Workspace verwenden | **Zeigen Sie SIR-Dashboards an**<br> <br>SIR-Arbeitsbereich-Dashboards anzeigen |

## Fordern Sie Apps im Store an

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Durch die Installation von Arbeitsbereich für Security Incident Response (sn_si_aw) werden alle abhängigen Anwendungen von ServiceNow Storeautomatisch installiert. Weitere Details zu den abhängigen Anwendungen finden Sie im Abschnitt SIR Workspace -Plugins und -Rollen.

## Weitere Ressourcen

Besuchen Sie das Security Incident Response Forum auf der ServiceNow Community.

## SIR Workspace erkunden

Erkunden Sie Arbeitsbereich für Security Incident Response, um zu verstehen, wie Sicherheitsanalysten und -manager ihre täglichen Vorgänge mit einer verbesserten Benutzer-Experience durchführen, eine vollständige Incident-Untersuchung durchführen und sich einen Überblick über die Security Incidents, Reaktionsaufgaben und SLAs verschaffen, die dem Sicherheitsanalysten und zugewiesen sind Team.

In diesem Abschnitt wird Folgendes beschrieben:

- SIR Workspace -Plugins und erforderliche Rollen.
- Wichtige Funktionen von SIR Workspace.

### SIR Workspace -Plugins und -Rollen

Im Folgenden finden Sie die erforderlichen Anwendungen für das Plugin Arbeitsbereich für Security Incident Response (sn_si_aw).

## Anwendungen

- Enterprise Security Case Management PAD Commons [sn_escm_pad_cmn]
- Security Operations Common Workspace [sn_escm_ws_cmn]



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- UI-Kartenkomponente für Security Incidents [sn_sirw_evam]
- Security Operations-Spoke [sn_sec_spoke]
- Security Incident Response [sn_si]

**Enterprise Security Case Management PAD Commons** erfordert das Plugin „Playbook Experience“ [playbook_experience].

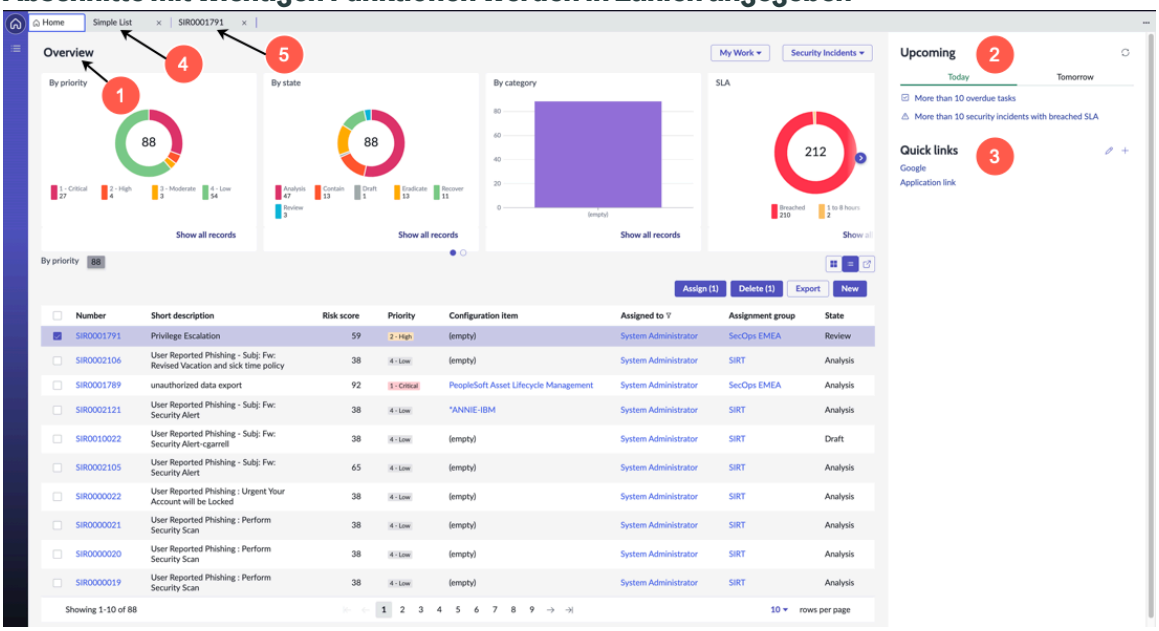
Weitere Informationen zu den Rollen, Tabellen, Eigenschaften und geplanten Aufgaben von Security Incident Response ] finden Sie unter Mit Security Incident Response installierte Komponenten.

### SIR-Arbeitsbereichsfunktionen

Arbeitsbereich für Security Incident Response besteht aus den folgenden Hauptfunktionen.

1. Übersichtsbereich
2. Abschnitt „Bevorstehend“
3. Quick-Links
4. Listenansicht
5. Schnittstelle mit mehreren Registerkarten, die das Öffnen mehrerer Security Incident-Incidents unterstützt

**Abschnitte mit wichtigen Funktionen werden in Zahlen angegeben**




### SIR Workspace -Schnittstellenübersicht

Die Übersichtsseite SIR Workspace besteht aus den Details zu Security Incidents und Antwortaufgaben, die sich unter Sicherheitsanalysten und ihrem Team befinden.

Unter jedem Filter sind verschiedene Widgets vorhanden, gruppiert nach Priorität, Kategorie, Status und SLA, die sich in den Warteschlangen der Sicherheitsanalysten und in der Warteschlange des Sicherheitsanalystenteams befinden.

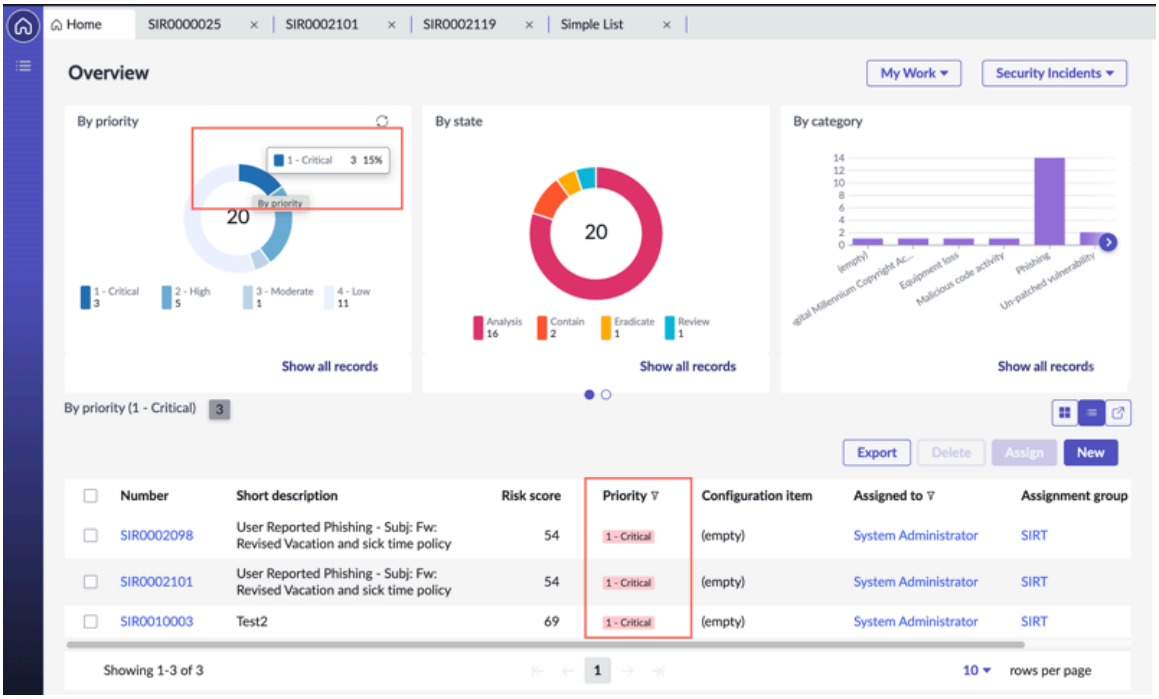
Wenn Filter auf die Widgets angewendet werden, wird die untere Hälfte der Übersichtsseite mit den entsprechenden Security Incidents oder Antwortaufgaben ausgefüllt, die als Karten oder Listenelemente dargestellt werden. Der Analyst kann nach Bedarf zwischen der Kartenansicht und der Listenansicht wechseln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

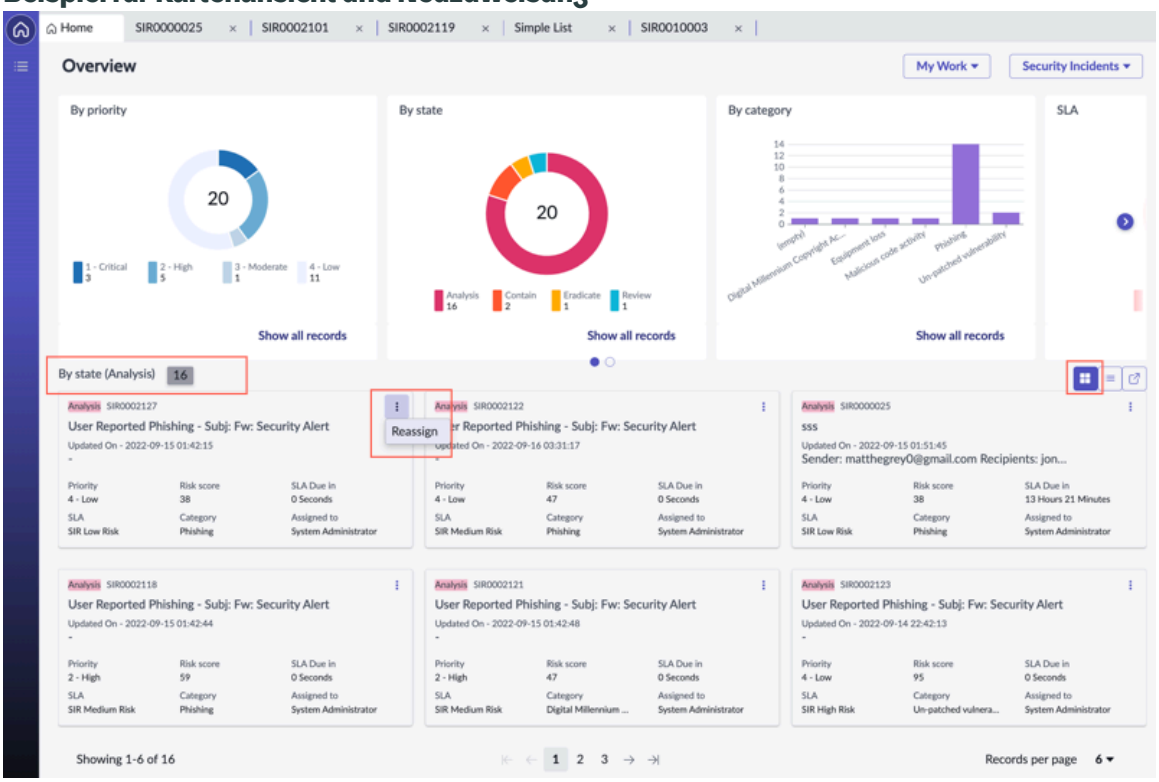
Wenn Sie beispielsweise im Widget „ **Priorität** “ alle kritischen Incidents oder Reaktionsaufgaben auswählen möchten, klicken Sie auf das Segment „ **Kritisch** “ (Beispiel-Screenshot unten) des Widgets, und die kritischen Incidents oder Reaktionsaufgaben werden in der Liste oder Karte angezeigt -Ansicht.

### Übersichtsbereich




Sie können Security Incidents oder Antwortaufgaben direkt in dieser Ansicht zuweisen oder neu zuweisen, indem Sie auf das Ellipse-Symbol klicken und **Zuweisen** (Option in Kartenansicht) oder direkt die Schaltfläche **Zuweisen** (Option in Listenansicht) auswählen, um einen Incident zuzuweisen.

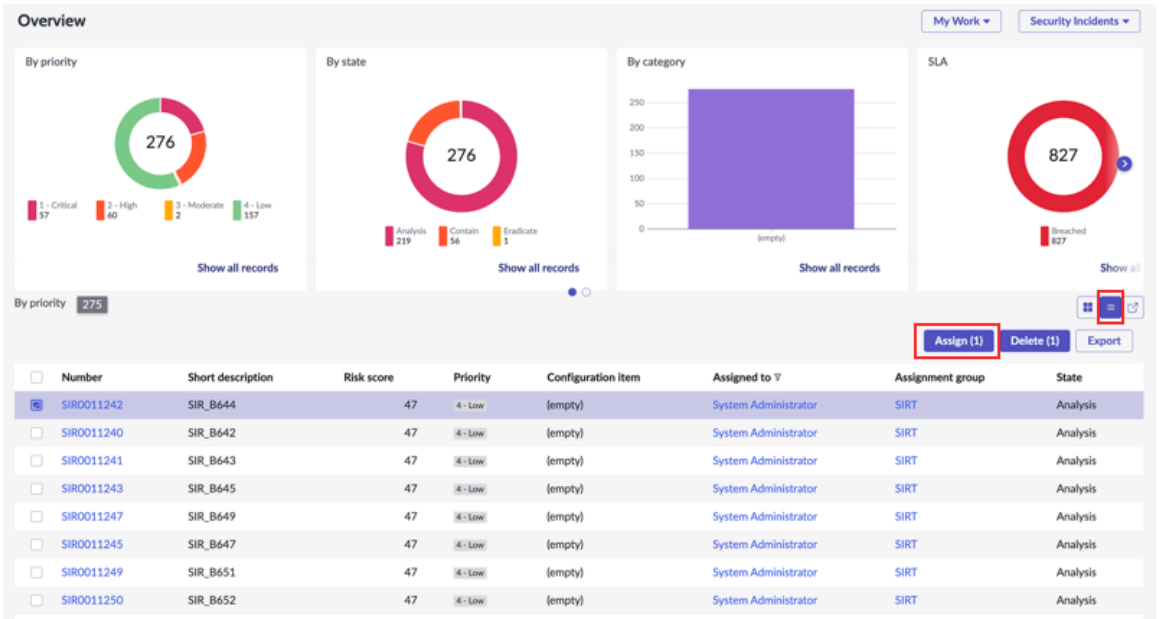
### Beispiel für Kartenansicht und Neuzuweisung





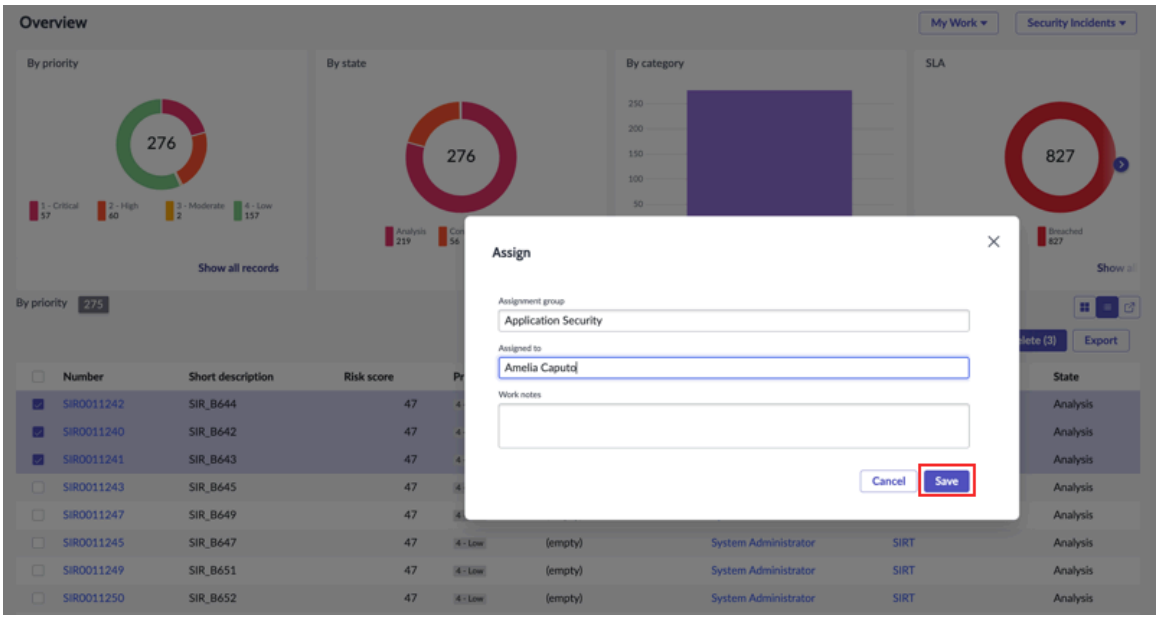

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Incident zuweisen




Hier ist ein Beispiel für die Listenansicht. Der Benutzer kann Incidents auch über die Listenansicht zuweisen.

### Incident zuweisen




**Fügen Sie** die Beauftragtendetails wie Zuweisungsgruppe und Zugewiesen an hinzu, oder ändern Sie sie, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.

**Hinweis:**

Sie können den Zuweisungsgruppen einen oder mehrere Security Incidents oder Reaktionsaufgaben zuweisen. Die ausgewählte Nummer wird auf der Schaltfläche **Zuweisen** angezeigt.

Der Benutzer kann Security Incidents aus dieser Ansicht löschen. Klicken Sie auf die Schaltfläche **Löschen**, um den Security Incident zu löschen. Der Datensatz wird aus der Listenansicht gelöscht.

Der Benutzer kann den Listeninhalt auch exportieren. Klicken Sie auf die Schaltfläche **Exportieren**, um die Liste im gewünschten Format zu exportieren.



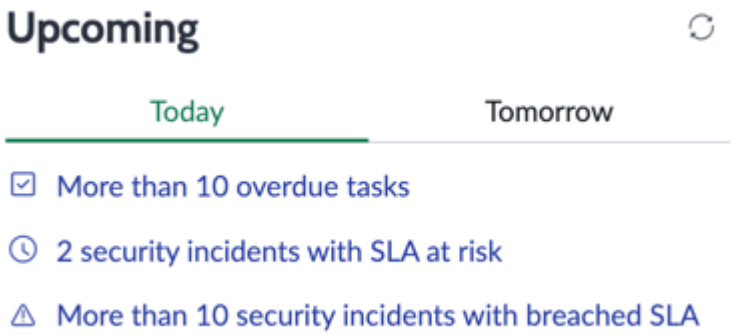
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Abschnitt „Bevorstehend“

In diesem Abschnitt werden die bevorstehenden Aufgaben angezeigt, z. B. die Security Incidents und Antwortaufgaben, die am selben Tag und am nächsten Tag fällig sind.

Die angezeigte Liste mit Security Incidents und Antwortaufgaben basiert auf dem Fälligkeitsdatumsfeld und der SLA-Definition, die für diese Datensätze definiert sind.

Wenn dieser Abschnitt mehr als einen Security Incident oder eine Antwortaufgabe enthält, werden für den Incident oder die Datensätze alle diese Datensätze auf einer neuen Registerkarte geöffnet.




### Zeigen Sie bevorstehende Aufgaben an

Der Sicherheitsanalyst kann die bevorstehenden Aufgaben im Zusammenhang mit Security Incidents und Reaktionsaufgaben anzeigen, die fällig, überfällig sind oder gegen die definierte SLA verstoßen.

#### Vorbereitungen

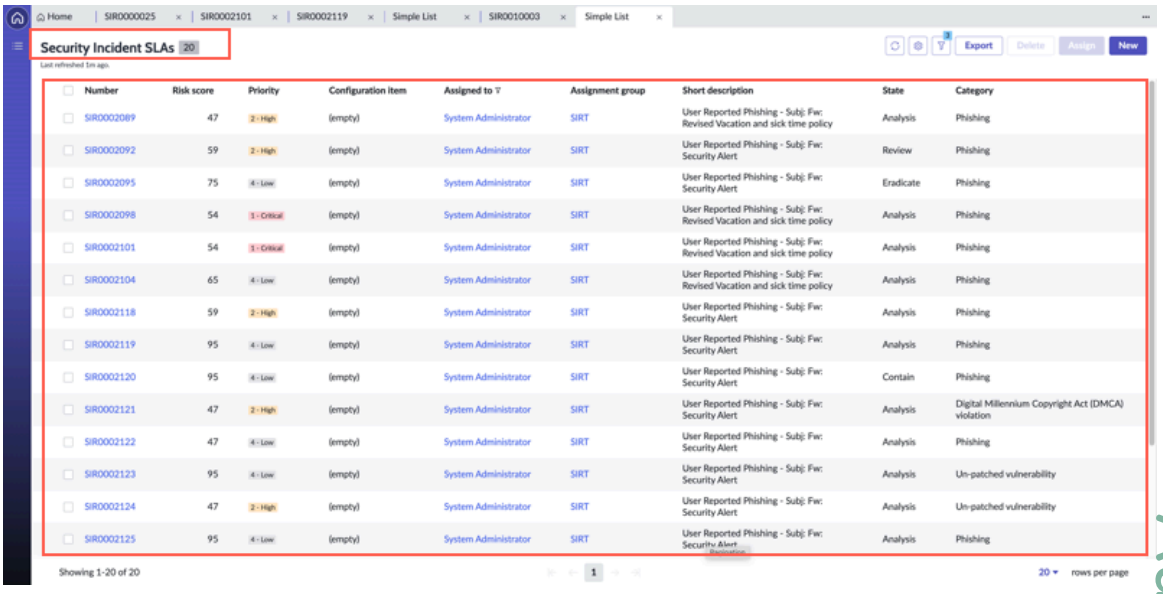
Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Bevorstehend**.
2. Klicken Sie auf die Registerkarte **Heute**, um die Aufgaben anzuzeigen, die am selben Tag fällig sind.
3. Wählen Sie die Registerkarte **Morgen** aus, um die Aufgaben anzuzeigen, die bis zum nächsten Tag überfällig sind.
   Im nächsten Abschnitt werden die Security Incidents oder Antwortaufgaben aufgelistet, die basierend auf dem Fälligkeitsdatum überfällig sind und die SLA-Definition verletzt haben.
4. **Klicken** Sie auf das Aktualisierungssymbol, um die bevorstehende Abschnittsliste zu aktualisieren.
   Wenn Sie beispielsweise auf den Link **Mehr als 10 Security Incidents mit SLA-Verstoß** klicken, wird die Liste der Incidents mit SLA-Verstoß auf einer neuen Registerkarte im Arbeitsbereich angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Sie können die Vorgänge Neu, Zuweisen, Exportieren und Löschen in jeder Listenansicht ausführen.

### Abschnitt „Quick-Links“

Quick-Links funktionieren wie Lesezeichen-Links. Sie können externe URLs hinzufügen und schnell über den Arbeitsbereich darauf zugreifen.

### Arbeiten mit Quick-Links

Fügen Sie Quick-Links hinzu, um die Referenz zu erleichtern.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

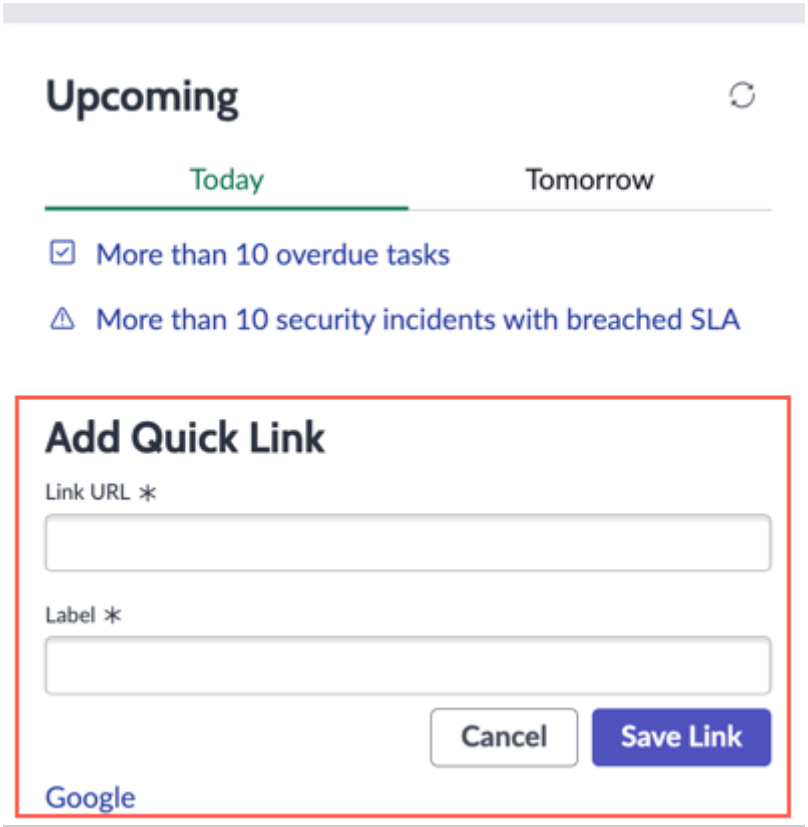
**Warum und wann dieser Vorgang ausgeführt wird**
Sie können nützliche Quick-Links hinzufügen und ändern und die Links, die bei der Incident-Lösung helfen, mit Lesezeichen versehen.

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Quick-Links**.
2. Klicken Sie auf das Symbol **Quick-Link** hinzufügen, um die Links hinzuzufügen.
3. Geben Sie den Link zur URL und zur Bezeichnung ein.
4. Klicken **Sie auf Link speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der neue Link wird unter dem Quick-Links-Abschnitt hinzugefügt.

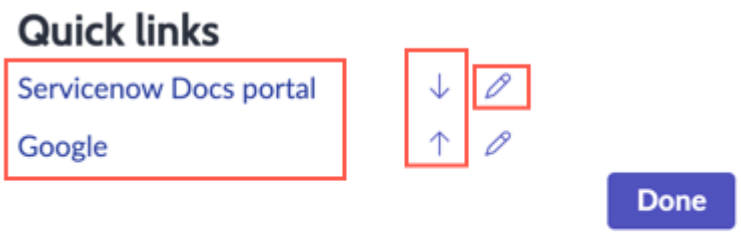
**5. So ändern oder löschen Sie die Links:**

**a.** Klicken Sie auf das Symbol **Link bearbeiten**.

**b.** Ändern Sie den gewünschten Link oder zeigen Sie den Text an, der die Bezeichnung der URL ist.

**c.** Klicken Sie auf **Speichern**.

**d.** Klicken Sie auf **Erledigt**.




**e.** Verwenden Sie die Pfeile nach oben und unten, um die Position der Links zu verschieben.

**f.** Klicken Sie auf **Löschen**, um die Links zu löschen, die beim Bearbeiten mit einem Lesezeichen versehen wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Listenansicht in SIR Workspace

Die Listenansicht besteht aus Security Incidents, Antwortaufgaben, Phishing-E-Mails und Bewertungen.

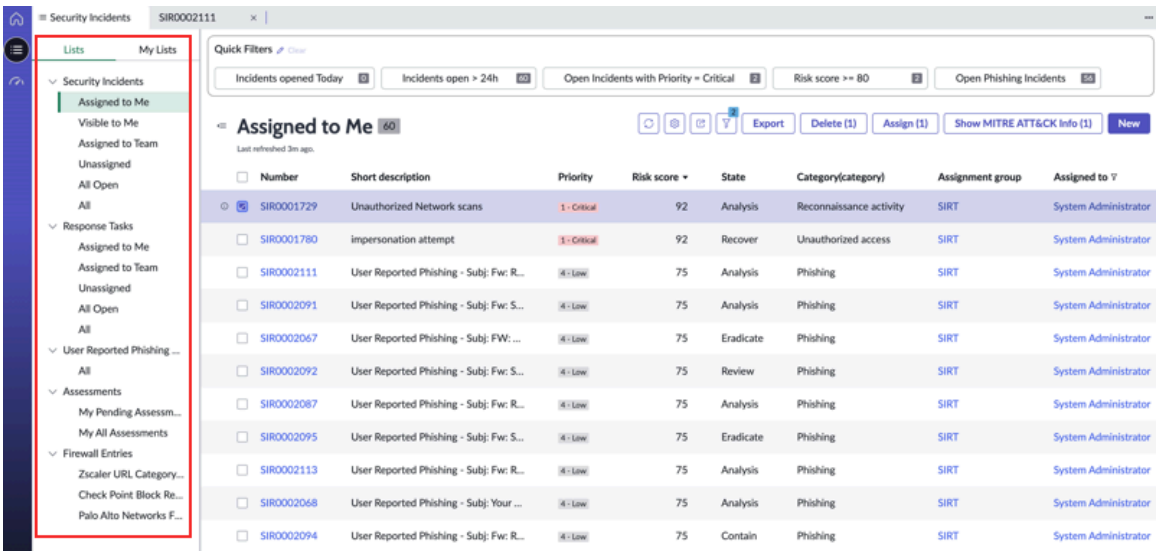
In der Listenansicht sind vorab Filter angewendet, z. B. Mir zugewiesen, Dem Team zugewiesen, Nicht zugewiesen, Alle offen, Alle usw.

Mit diesen Listenkategorien und gefilterten Listen können Analysten schnell die erforderlichen Security Incidents- und Reaktionsaufgaben-Datensätze finden, an denen sie arbeiten müssen.

Um zur Listenansicht zu gelangen, müssen Sie auf das Listensymbol ( ) klicken. Wenn Sie in einer Listenansicht auf einen Datensatz klicken, wird der Datensatz in einer neuen Registerkarte geöffnet.

## Listentypen

Im Folgenden finden Sie eine Beispielansicht der Listen.




Der Listenbereich enthält die folgenden Abschnitte:

#### Lists

| Listenelement | Beschreibung | Fähigkeit |
|---|---|---|
| Security Incidents | Zeigen Sie die Liste der Security Incidents an, und navigieren Sie zum gewünschten Incident, um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar:<br>• **Für mich sichtbar**: Security Incidents, die für den angemeldeten Benutzer sichtbar sind.<br>• **Mir zugewiesen**: Security Incidents, die dem Analysten zugewiesen sind. | • In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf das Zahnradsymbol klickt, das über den Incident-Spalten verfügbar ist.<br>• Der Analyst kann einen oder mehrere Security Incidents auswählen und diese Incidents den anderen Benutzern zuweisen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Lists (Fortsetzung)**

| Listenelement | Beschreibung | Fähigkeit |
|---|---|---|
| | • **Dem Team zugewiesen**: Security Incidents, die allen Teams zugewiesen sind, denen der Analyst angehört.<br>• **Nicht zugewiesen**: Liste der nicht zugewiesenen Security Incidents.<br>• **Alle offenen**: Liste aller offenen Security Incidents.<br>• **Alle**: Liste aller Security Incidents. | • Der Analyst kann die Security Incidents löschen.<br>• Der Analyst kann einen neuen Security Incident erstellen.<br>• Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf die Option Schnellfilter klicken, anstatt die Option „ **Erweiterter Filter“** zu verwenden. Mit den Schnellfiltern können Sie schnell die Liste der Security Incidents filtern, die sofortige Aufmerksamkeit erfordern. Weitere Informationen finden Sie unter Arbeiten mit Schnellfiltern.<br>• Die Analysten können die Liste der Incidents aktualisieren.<br>• Analysten können die Listenansicht in die Formate Excel, CSV, JSON und PDF exportieren. |
| Antwortaufgaben | Zeigen Sie die Liste der Antwortaufgaben an, und navigieren Sie zur gewünschten Antwortaufgabe, um mit der Bearbeitung zu beginnen. Die Listenansicht enthält:<br>• **Mir zugewiesen**: Antwortaufgaben, die dem Analysten zugewiesen sind.<br>• **Dem Team zugewiesen**: Antwortaufgaben, die den Teams zugewiesen sind, zu denen die Analysten gehören.<br>• **Nicht zugewiesen**: Liste der nicht zugewiesenen Antwortaufgaben. | • In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf das Zahnradsymbol klickt, das über den Incident-Spalten verfügbar ist.<br>• Der Analyst kann eine oder mehrere Antwortaufgaben auswählen und diese Aufgaben anderen Benutzern zuweisen.<br>• Der Analyst kann eine neue Antwortaufgabe erstellen.<br>• Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf die |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Lists (Fortsetzung)**

| Listenelement | Beschreibung | Fähigkeit |
|---|---|---|
| | • **Alle offenen**: Liste aller offenen Antwortaufgaben.<br>• **Alle**: Liste aller Antwortaufgaben. | Option Schnellfilter klicken, anstatt die Option „ **Erweiterter Filter“** zu verwenden. Mit den Schnellfiltern können Sie schnell die Liste der Antwortaufgaben filtern, die sofortige Aufmerksamkeit erfordern.<br>• Die Analysten können die Liste der Antwortaufgaben aktualisieren.<br>• Analysten können die Listenansicht in die Formate Excel, CSV, JSON und PDF exportieren. Weitere Informationen finden Sie unter Exportieren Sie Security Incidents oder Antwortaufgaben. |
| Phishing-E-Mails | Zeigen Sie die Liste aller Phishing-E-Mails an. Die Listenansicht wird basierend auf der letzten Aktualisierung sortiert. | • Phishing-E-Mail melden Weitere Informationen zum Melden einer Phishing-E-Mail finden Sie unter Phishing-E-Mail melden.<br>• Löschen Sie Phishing-E-Mails.<br>• Exportieren Sie die Phishing-E-Mail-Listenansicht in die Formate Excel, CSV, JSON und PDF. |
| Bewertungen | Zeigen Sie die Liste der Bewertungen an, die für die Überprüfung nach Incidents erforderlich sind.<br>• **Meine ausstehenden Bewertungen**: Liste der ausstehenden Bewertungen.<br>• **Alle meine Bewertungen**: Liste aller Bewertungen. | Nehmen Sie Bewertungen vor. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Personalisieren Sie eine Liste

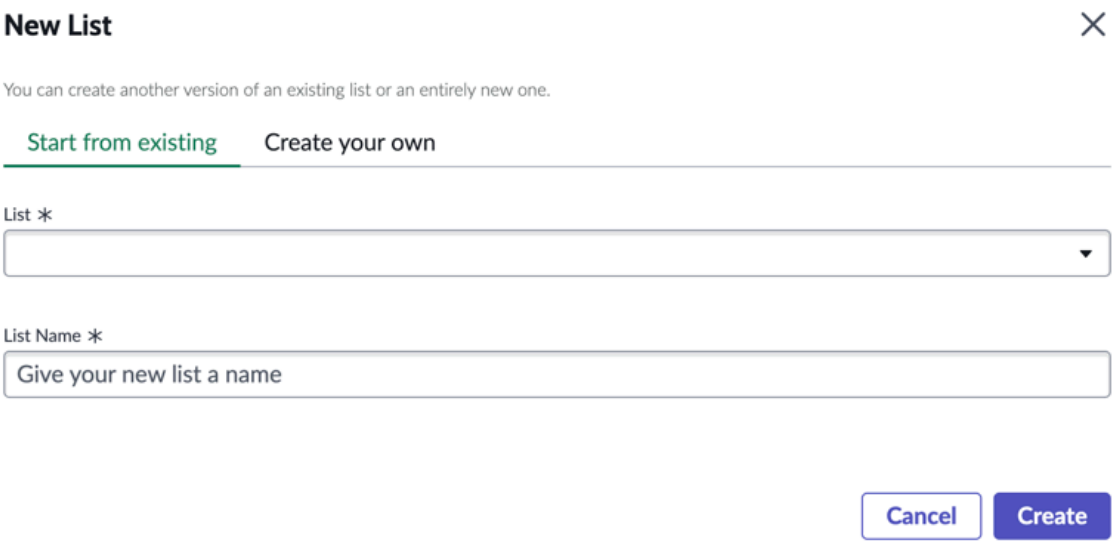
Sicherheitsanalysten oder -manager können die benutzerdefinierte Listenansicht für Security Incidents, Antwortaufgaben oder Phishing-E-Mails nach ihren individuellen Vorlieben personalisieren.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie **auf Listenansicht**.
3. Klicken **Meine Listen**.
4. Klicken Sie unten in der Ansicht **„Meine Listen**“ auf **Neue Liste** hinzufügen.




Sicherheitsanalysten können entweder eine andere Version einer vorhandenen Liste oder eine vollständig neue benutzerdefinierte Liste erstellen.

5. **So erstellen Sie aus einer vorhandenen Listenansicht:**

   a. Klicken Sie auf den Link **Aus vorhandenem starten**.

   b. Wählen Sie die **Liste** aus der Dropdown-Liste aus.

   > **Hinweis:**
   > Welche Liste Sie auch immer in der Dropdown-Liste auswählen, der Listenname ist die Kopie Ihrer Hauptliste. Wenn Sie beispielsweise im Abschnitt „Security Incidents“ die **Option Mir zugewiesen** auswählen, wird der **Listenname in Mir zugewiesen Kopie** des Abschnitts „Security Incidents“ geändert.

   c. Wählen Sie die zu personalisierenden Spalten aus, und fügen Sie Filter hinzu.
   Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und (einen) Wert/e enthalten.

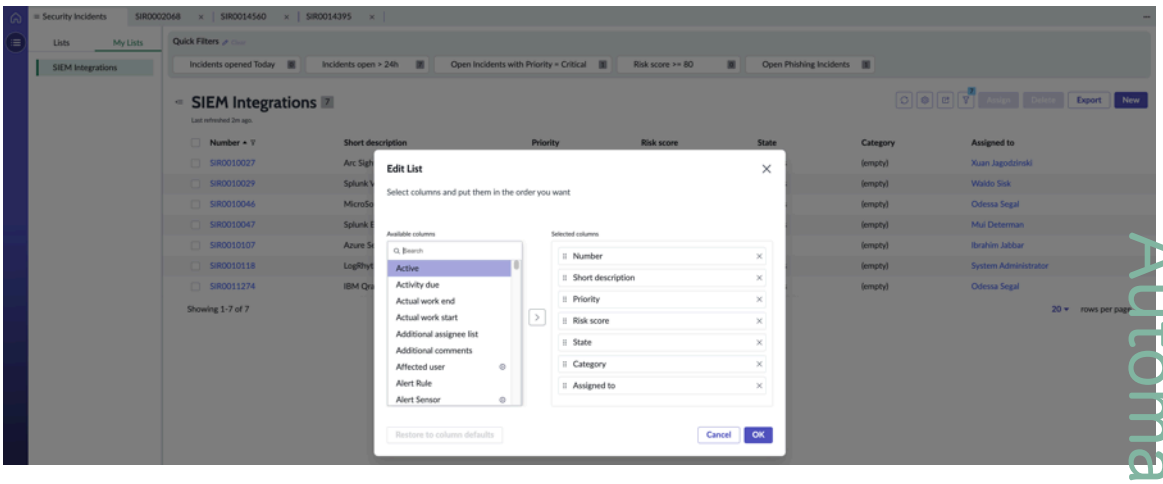
   d. Klicken Sie auf **Erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Um Ihre eigene Listenansicht anzupassen, können Sie benutzerdefinierte Spalten und Filter hinzufügen, Bedingungen festlegen und nach Bedarf nach der Reihenfolge sortieren.

**e.** Nachdem eine personalisierte Listenansicht erstellt wurde, klicken Sie auf das Zahnradsymbol, und passen Sie die Listenspalten an, indem Sie die Option **Spalten** bearbeiten auswählen, um die Spalten zu bearbeiten und in die gewünschte Reihenfolge zu bringen.




Sie haben auch die folgenden Möglichkeiten:

- **Benennen Sie** die personalisierte Listenansicht um.
- **Löschen Sie** die personalisierte Listenansicht.
- Speichern Sie die personalisierte Listenansicht wie gewünscht mit der Option **Speichern unter**.
- **Setzen Sie die Breite** der Listenansicht zurück.

**Hinweis:**
Sie können diese Vorgänge auch direkt über die anderen bereitgestellten Listenaktionsschaltflächen ausführen, z. B. Zuweisen, Löschen, Exportieren der Listenansicht.

**6. So erstellen Sie eine eigene Liste:**

**a.** Klicken Sie auf den Link Selbst **erstellen**.

**b.** Geben Sie einen **Listennamen an**.

**c.** Wählen Sie die **Quelle** und die **Spalten aus**.

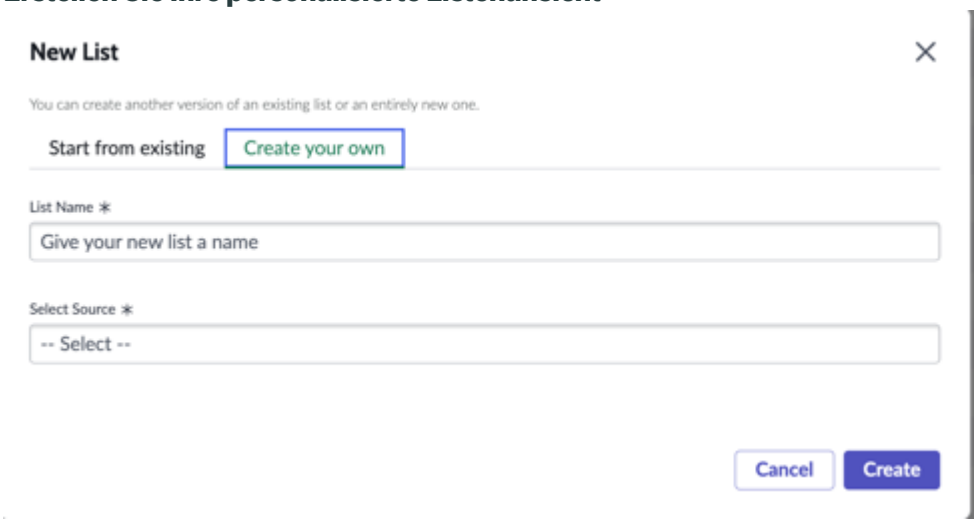
**d.** Fügen Sie Filter hinzu.
Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, und geben Sie die Reihenfolge an, in der die Liste angezeigt werden soll.

**e.** Klicken Sie auf **Erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie Ihre personalisierte Listenansicht




Unterhalb des Abschnitts „ **Meine Listen** “ wird eine neue Liste erstellt, wie von Ihnen definiert und angepasst.

**Hinweis:**
Sie können Ihre personalisierte Ansicht **neu anordnen**, indem Sie ihre Positionen verschieben.

### Weisen Sie Security Incidents zu

Weisen Sie Security Incidents zu.

**Vorbereitungen**
Erforderliche Rolle: sn_si.basic

**Prozedur**

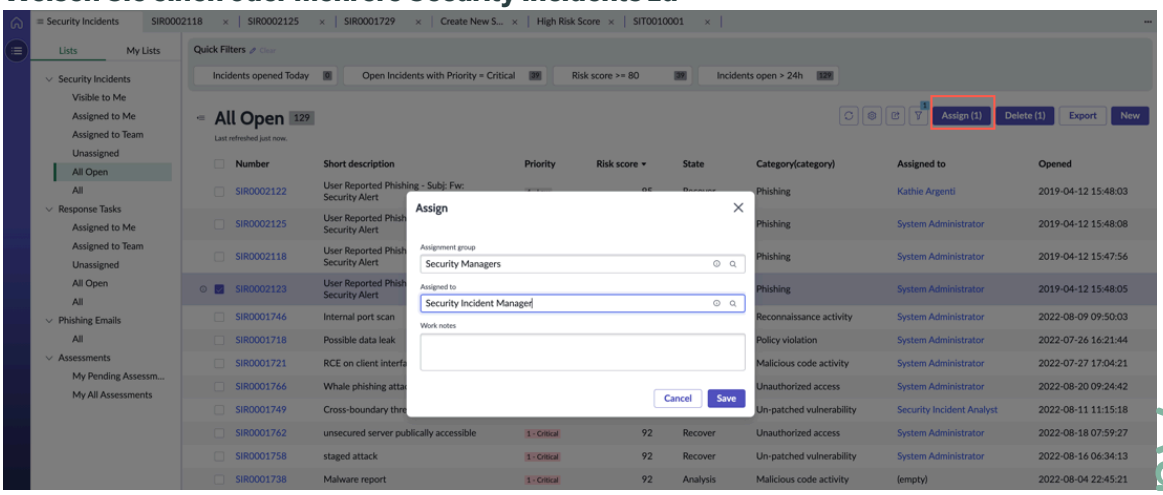
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Klicken Sie auf **Listen**.
4. Wechseln Sie beispielsweise zu **Security Incidents** > **Alle offen**.
5. Wählen Sie einen oder mehrere Security Incidents aus.
6. Klicken Sie auf **Zuweisen**.
7. Füllen Sie die Details aus, z. B. Zuweisungsgruppe, Zugewiesen an, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Benutzer zugewiesen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Speichern**.

### Weisen Sie einen oder mehrere Security Incidents zu




### Weisen Sie Antwortaufgaben zu

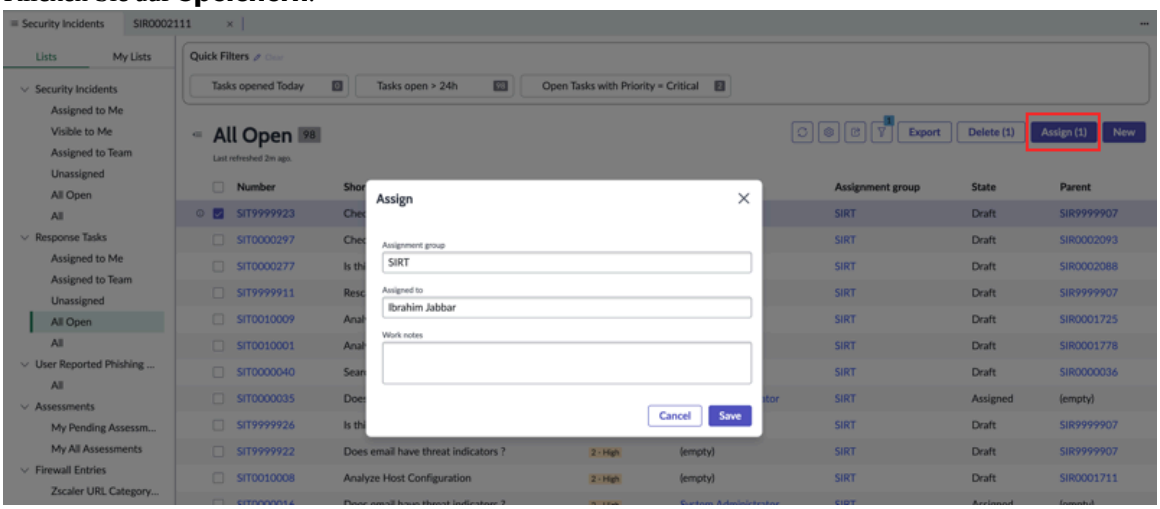
Weisen Sie Antwortaufgaben für ein Sicherheitsproblem zu.

## Vorbereitungen

Erforderliche Rolle: sn_si.basic

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Klicken Sie auf **Listen**.
   Wechseln Sie beispielsweise zu **Antwortaufgaben** > **Alle offen**.
4. Wählen Sie eine oder mehrere Antwortaufgaben aus.
5. Klicken Sie auf **Zuweisen**.
6. Füllen Sie die Details aus, z. B. Zuweisungsgruppe, Zugewiesen an, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Benutzer zugewiesen.
7. Klicken Sie auf **Speichern**.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

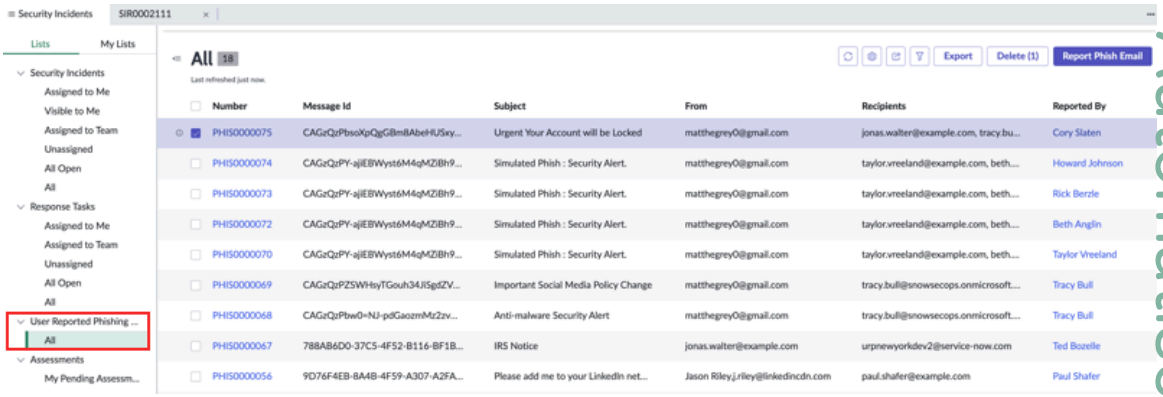
### Phishing-E-Mail melden

Phishing-E-Mails aus der Listenansicht melden.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Gehe zu **Vom Anwender gemeldete Phishing-E-Mails** > **Alle**.
   Die Liste der vom Benutzer gemeldeten Phishing-E-Mails wird angezeigt.




4. Klicken Sie auf die Schaltfläche **Phishing-E-Mail** melden.
   Melden Sie eine Phishing-E-Mail, indem Sie sie hochladen.
5. Klicken Sie auf **Datei** hinzufügen, um Anhänge hinzuzufügen.
6. Klicken Sie auf **Hochladen**.

> **Hinweis:**
> Melden Sie eine Phishing-E-Mail, indem Sie die Anhänge hochladen. Sie können jeweils nur eine Phishing-E-Mail hochladen, die im EML-Format vorliegen muss.

7. Klicken Sie auf **Absenden**.
   Die Phishing-E-Mail zur Protokollierung eines Security Incident wird erstellt.

### Arbeiten mit Schnellfiltern

Schnellfilter sind leicht zugängliche Filter, die in den Listen „“, „Security Incidents“ und „Antwortaufgaben“ verfügbar sind.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

SIR Workspace bietet eine Schnellfilterfunktion, mit der Sie die Liste der Security Incidents oder Antwortaufgaben mühelos filtern können.

Sie können Schnellfilter verwenden, um neue Filter zu konfigurieren oder vorhandene Filter zu ändern, die in diesen Listen angezeigt werden. Das Basissystem bietet die folgenden Schnellfilter für jeden Security Incident:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Heute geöffnete Incidents**
- **Offene Incidents > 24 Stunden**
- **Offene Incidents mit Priorität = Kritisch**
- **Risiko >= 80**
- **Offene Phishing-Incidents**

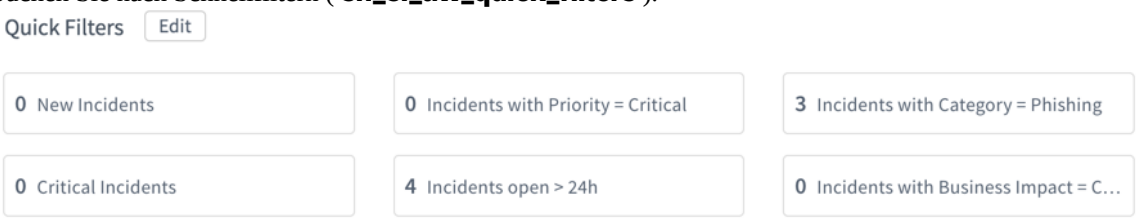
Das Basissystem bietet die folgenden Schnellfilter für jede Antwortaufgabe:

- **Aufgaben offen > 24 Stunden**
- **Offene Aufgaben mit Priorität = Kritisch**

**Hinweis:**
Ein Administrator kann die erforderliche Liste der Schnellfilter entsprechend den Anforderungen der Organisation konfigurieren.

### Prozedur

1. Navigieren zu **Systemdefinition** > **Tabellen**.
2. Suchen Sie nach Schnellfiltern ( **sn_si_aw_quick_filters** ).




3. Gehe zu **Zugehörige Links** > **Liste anzeigen** Abschnitt.
   Die **Listenseite** „Schnellfilter“ wird angezeigt. OOTB, im Folgenden finden Sie die Liste der Schnellfilter, die im Lieferumfang der Anwendung enthalten sind.

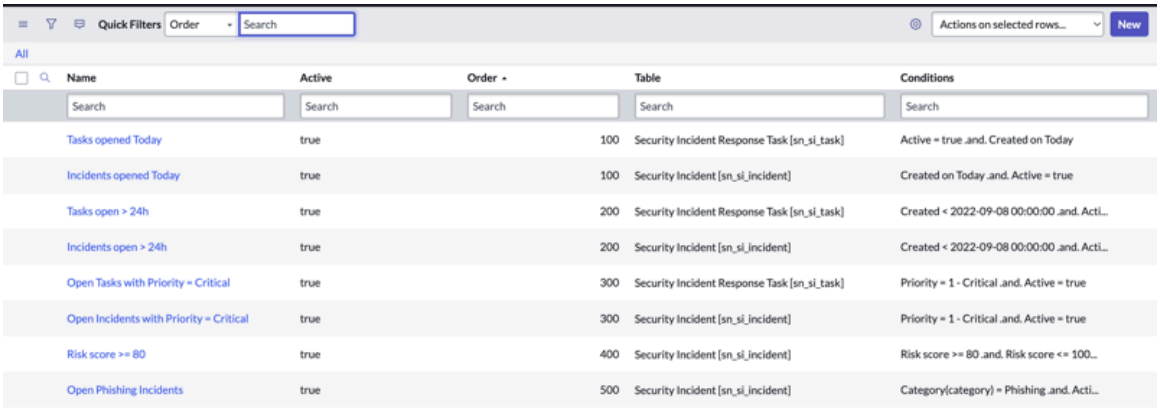
| Name | Tabelle | Wert |
|---|---|---|
| Heute geöffnete Aufgaben | Security Incident-Aufgabe [sn_si_task] | Wahr |
| Heute geöffnete Incidents | Security Incident [sn_si_incident] | Wahr |
| Aufgaben offen > 24 Stunden | Security Incident Response-Aufgabe [sn_si_task] | Wahr |
| Offene Incidents > 24 Stunden | Security Incident [sn_si_incident] | Wahr |
| Offene Aufgaben mit Priorität = Kritisch | Security Incident Response-Aufgabe [sn_si_incident] | Wahr |
| Offene Incidents mit Priorität = kritisch | Security Incident [sn_si_incident] | Wahr |
| Risikopunktzahl >= 80 | Security Incident [sn_si_incident] | Wahr |
| Offene Phishing-Incidents | Security Incident [sn_si_incident] | Wahr |

**Hinweis:**
Der Sicherheitsadministrator kann diese Schnellfilter konfigurieren. Je nach Geschäftsbedürfnis kann der Administrator den vorhandenen Wert in „falsch“ ändern und einen neuen Schnellfilter erstellen.

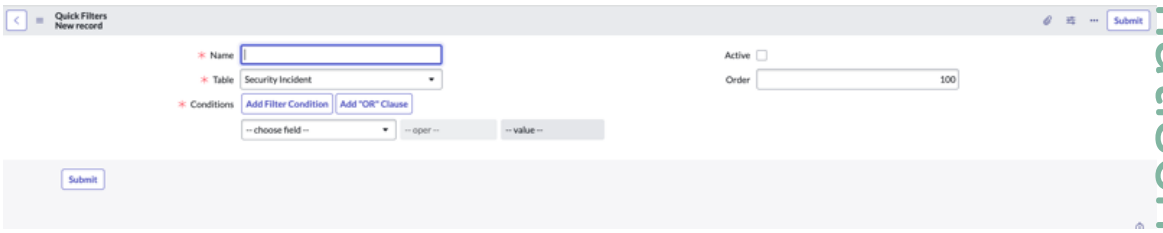


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Schnell-Filter



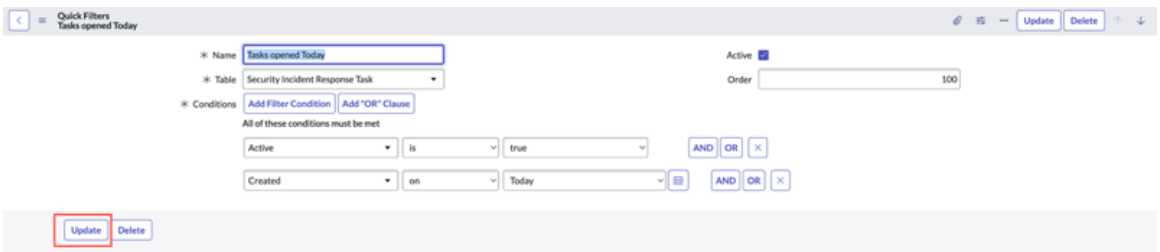

4. Klicken Sie auf **Neu**, um einen neuen Filter zu erstellen.
5. Geben Sie einen Namen für den Filter ein, wählen Sie die Tabelle aus, und geben Sie die Filterbedingung an.
6. Klicken Sie auf Absenden, um zur vorherigen **Listenseite** zurückzukehren.
   Der neu hinzugefügte Filter wird auf der Seite aufgelistet.




**Hinweis:**

- Der Schnellfilter ist nur anwendbar, wenn das Kontrollkästchen **Aktiv** aktiviert ist.
- Innerhalb des Arbeitsbereichs kann jeder angemeldete Benutzer die aktiven Schnellfilter, die in der Anwendung verfügbar sind, personalisieren. Benutzer können die neu erstellten Schnellfilter ausblenden oder einblenden. Diese Funktion basiert auf den Benutzereinstellungen.
- Wenn ein Benutzer die Voreinstellungen für Schnellfilter geändert hat und danach ein neuer Schnellfilter erstellt wird und der Schnellfilter auf „Aktiv“ gesetzt ist, wird dies nicht auf die Voreinstellung des Benutzers angewendet. Der Benutzer muss die Einstellungen in der personalisierten Ansicht manuell ändern.

7. Wählen Sie einen vorhandenen Filterdatensatz aus, um die vorhandenen Schnellfilter zu ändern.
8. Ändern Sie den Namen und die Filterbedingung.
9. Klicken Sie auf **Aktualisieren**.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie Schnellfilter hinzu, oder ändern Sie sie

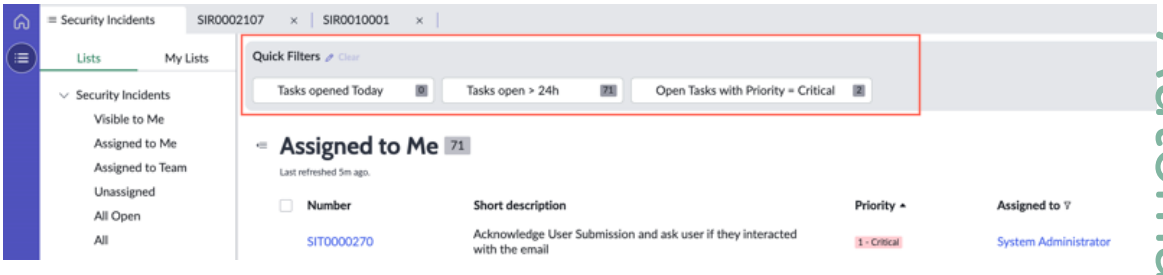
Fügen Sie Schnellfilter für Security Incidents oder Antwortaufgaben in der Listenansicht hinzu, oder ändern Sie sie.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

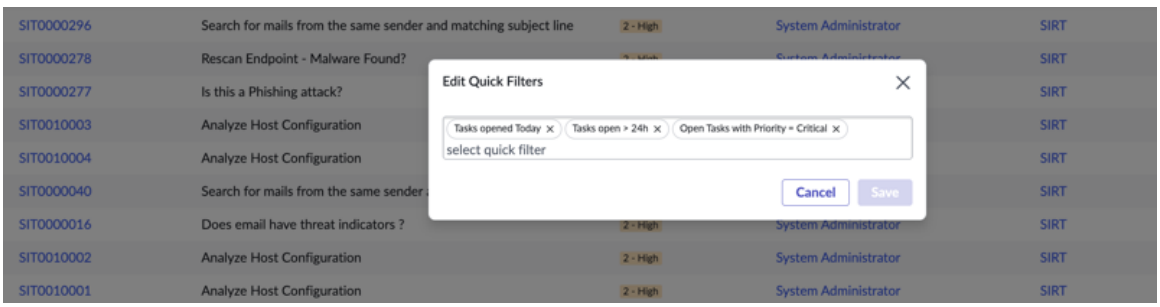
#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol ( ).
3. Wechseln Sie beispielsweise zu **Lists** > **Security Incidents** > **Schnell-Filter** Abschnitt.




4. Klicken Sie auf das Symbol **Bearbeiten**, um die Änderungen vorzunehmen.

> **Hinweis:**
> Die vorgenommene Änderung wird beibehalten, und wenn der Benutzer das nächste Mal zu dieser Seite zurückkehrt, wird die beibehaltene Einstellung angezeigt.




5. Klicken Sie auf **Speichern**.

### Exportieren Sie Security Incidents oder Antwortaufgaben

Exportieren Sie die Security Incidents oder Antwortaufgaben aus der Listenansicht.

#### Vorbereitungen

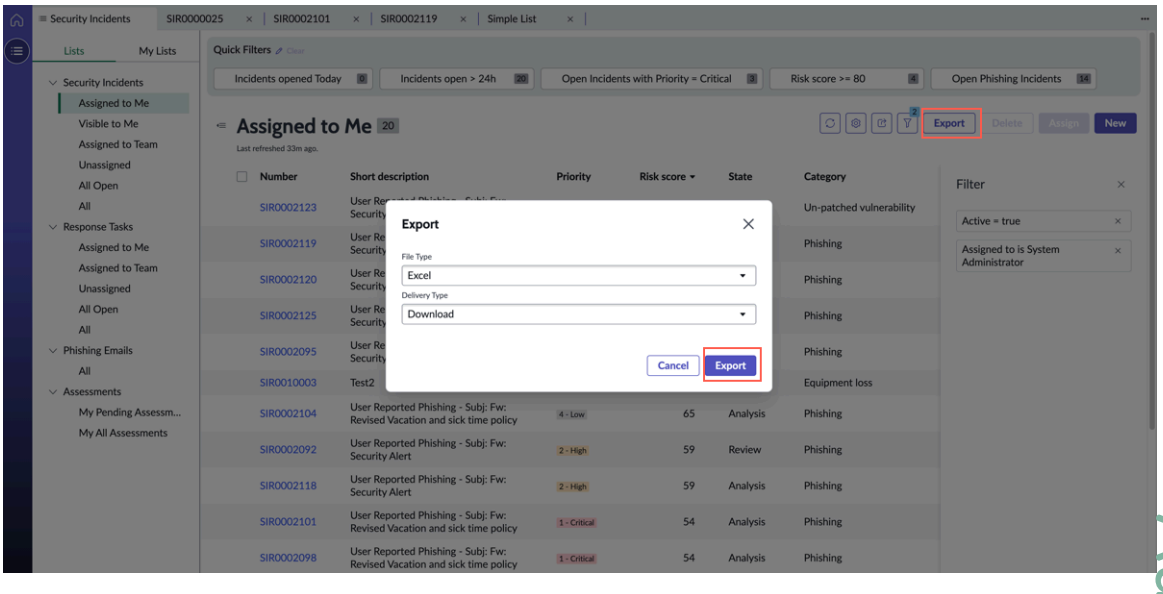
Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie auf das Listensymbol .
3. Klicken Sie auf **Listen**.
4. Gehe zu **Security Incidents oder Antwortaufgaben** > **Alle offen**.
5. Zeigen Sie die Liste an, und klicken Sie auf **Exportieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Wählen Sie den **Dateityp** und den **Bereitstellungstyp aus**.
   Beispiel: **Excel** und die Liste entweder **herunterladen** oder per E- **Mail senden**.
7. Klicken Sie auf **Exportieren**.
   Die Datei wird je nach ausgewählter Option heruntergeladen oder per E-Mail gesendet.

## SIR Workspace konfigurieren

In diesem Abschnitt werden die Konfigurationen beschrieben, die für die Arbeit mit Arbeitsbereich für Security Incident Responseerforderlich sind.

### Richten Sie die Ansicht von SIR-Datensätzen ein

In diesem Abschnitt wird beschrieben, wie die zugehörigen Listen gruppiert und auf der Registerkarte „SIR – Zugehörige Datensätze“ angezeigt werden, um die Navigation zu erleichtern.

Die Benutzer des Arbeitsbereichs können die zugehörige Liste auch einfach nach Namen durchsuchen.

### Konfigurieren Sie die SI-Entwurfszeituntersuchung

Verwenden Sie diesen Abschnitt, um die Untersuchungsseite zur Designzeit für Security Incidents so zu konfigurieren, dass mehrere Einstiegspunkte und die zugehörigen Datensätze in Arbeitsbereich für Security Incident Responsehinzugefügt werden.

Erforderliche Rolle: sn_si.admin.

Im Folgenden werden die Schritte zum Konfigurieren der Untersuchungsseite in Arbeitsbereich für Security Incident Responsebeschrieben .

- Ansicht für zugehörige Infotabellen wird erstellt
- Hinzufügen einer Einstiegspunktliste
- Zuordnungsansicht der Zuordnungsinformationen zur Einstiegspunktliste
- Konfigurieren Sie jede zugeordnete Liste in der -Ansicht für das Rendern von Laufzeitdaten

**Zugehörige Informationen**

Erkunden Sie das Untersuchungs-Canvas

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ansicht für zugehörige Infotabellen wird erstellt

Der Untersuchungsbildschirm nutzt die zugehörigen Listenansichten, die für Security Incidents erstellt wurden, um zugehörige Listen zu konfigurieren.

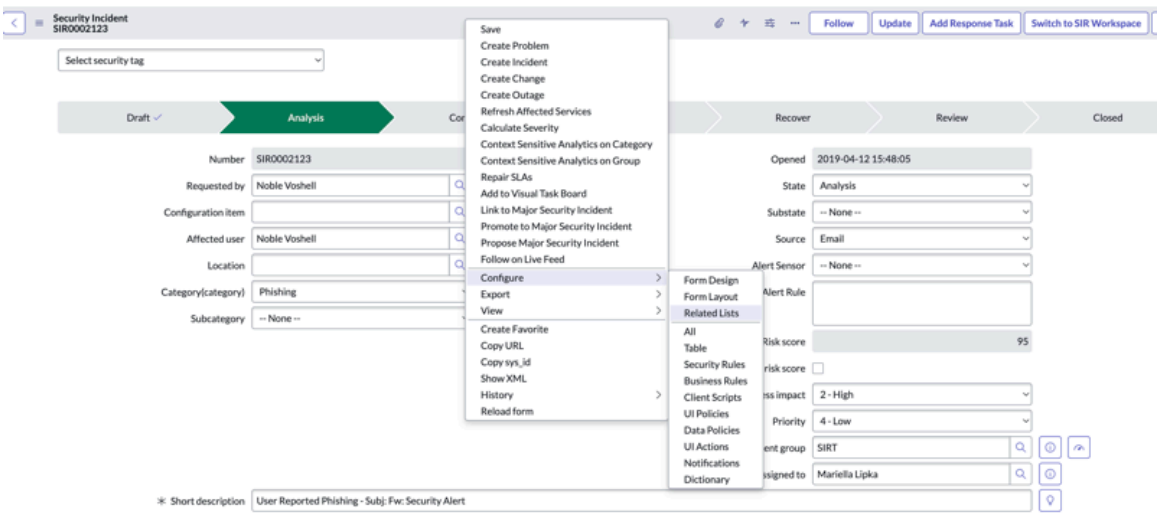
## Vorbereitungen

Erforderliche Rolle: sn_si.admin

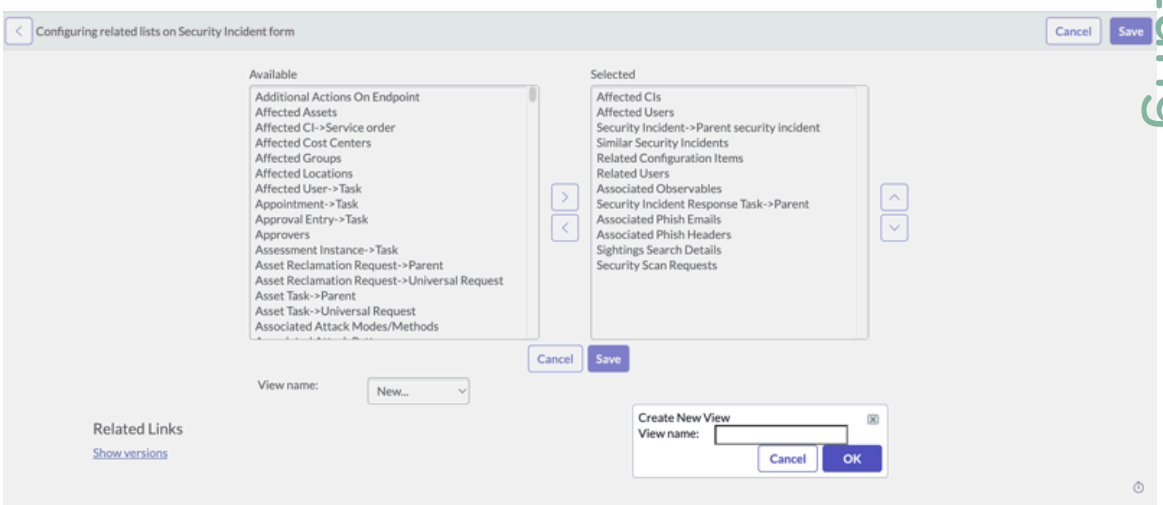
Im Folgenden finden Sie ein Verfahren zum Erstellen einer Ansicht und zum Hinzufügen zugehöriger Listen.

## Prozedur

1. Navigieren Sie zu **Security Incident** -Liste.
2. Öffnen Sie einen beliebigen Security Incident in der klassischen Benutzeroberfläche.
3. Navigieren Sie im Kontextmenü des Formulars zu **Konfigurieren** > **Zugehörige Listen**.
   Das Slushbucket-Fenster wird angezeigt.




4. Wechseln Sie zur Dropdown-Liste **Name der Ansicht**, und klicken Sie auf **Neu**, um eine neue Ansicht zu erstellen.
   Sie müssen der Ansicht einen Namen hinzufügen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Fügen Sie die gewünschten zugehörigen Listen dem rechten Bucket unter der neu erstellten Ansicht hinzu, und speichern Sie die Ansicht.
   Diese Ansicht wird verwendet, um die zugehörigen Informationen auf der Registerkarte „Untersuchung“ zu rendern.

### Hinzufügen einer Einstiegspunktliste

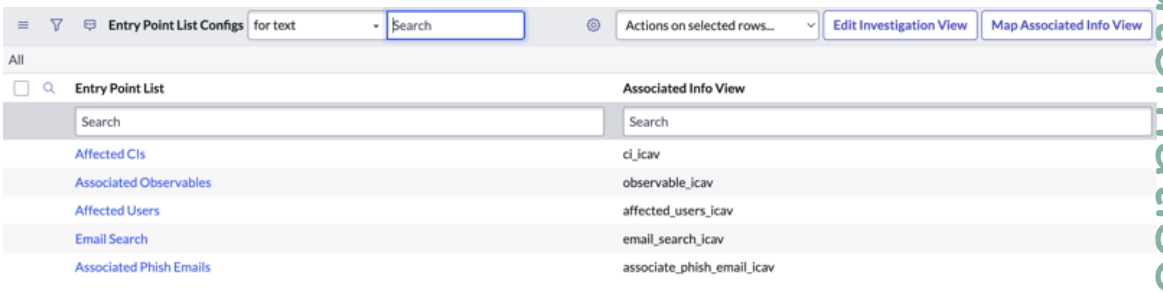
Konfigurieren Sie die neue Einstiegspunktliste, um sie der Untersuchungsseite hinzuzufügen.

## Vorbereitungen

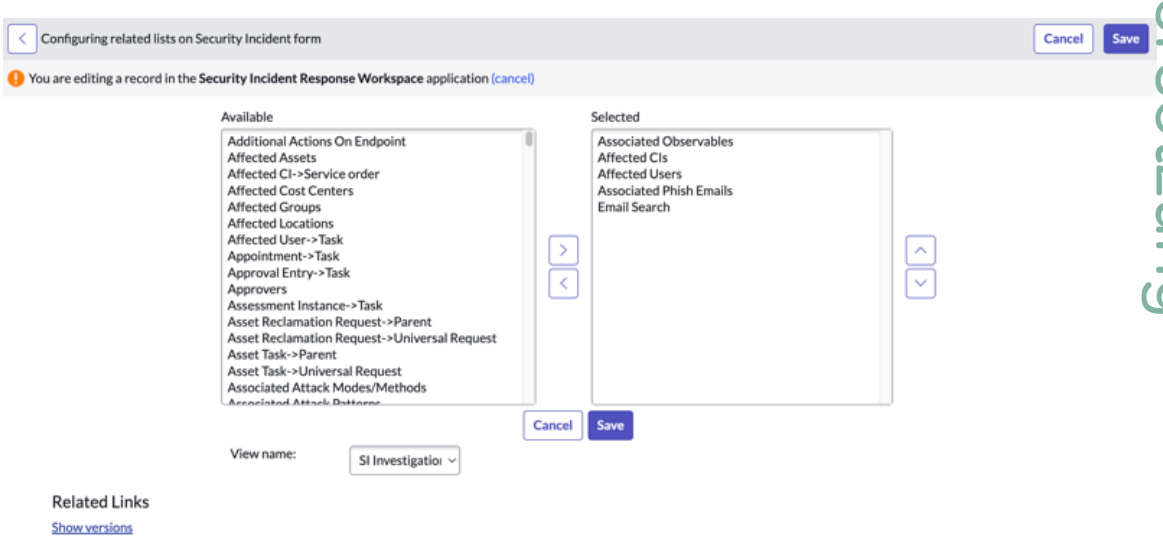
Erforderliche Rolle: admin

## Prozedur

1. Navigieren zu **sn_si_aw_entry_point_config.list**.
   Die Seite **Einstiegspunkt-Listenkonfigurationen** wird angezeigt.




2. Klicken Sie auf die Schaltfläche **Untersuchungsansicht bearbeiten**, um dem Untersuchungsbildschirm eine Einstiegspunktliste hinzuzufügen.
   Das **Formular „Zugehörige Listen in Security Incident konfigurieren“** wird angezeigt.




3. Fügen Sie der Slushbucket-Ansicht die Einstiegspunktliste hinzu, oder entfernen Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Speichern**.

**Hinweis:**
Die Ansicht, die dem Untersuchungsbildschirm mit den Einstiegspunktlisten entspricht, wird als **SI-Untersuchungsansicht** bezeichnet und ist standardmäßig ausgewählt, wenn Sie zur Seite „ **Untersuchungsansicht bearbeiten** “ navigieren.

Die Reihenfolge, in der die Einstiegspunktlisten auf der Untersuchungs-Canvas angezeigt werden, wird durch die Reihenfolge in der ausgewählten Slushbucket-Ansicht bestimmt.

### Zuordnungsansicht der Zuordnungsinformationen zur Einstiegspunktliste

Ordnen Sie die zugeordnete Infoansicht der neu hinzugefügten Einstiegspunktliste zu, indem Sie die Aktion Zugehörige Infoansicht zuordnen verwenden.

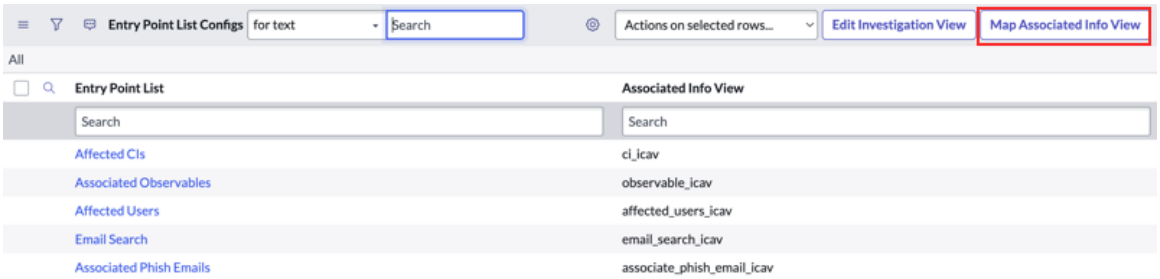
## Vorbereitungen

**Hinweis:**
Dieser Schritt ist erforderlich, damit die Einstiegspunktliste auf der Untersuchungsseite angezeigt wird. Auch wenn Sie nicht möchten, dass zugeordnete Infolisten unter einem Einstiegspunkt angezeigt werden, müssen Sie dennoch eine Dummy-Ansicht erstellen und zuordnen.

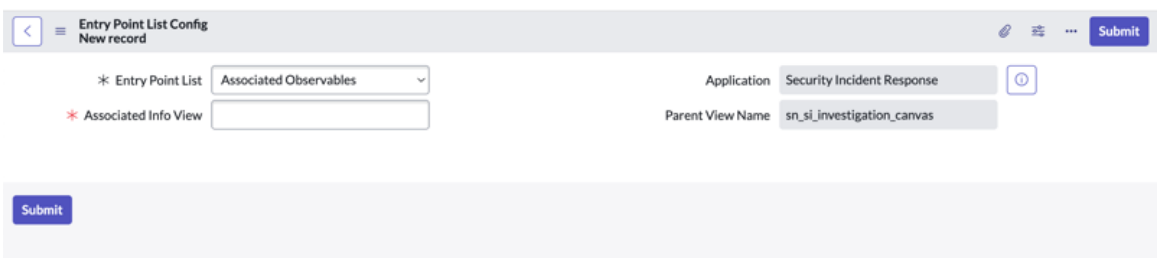
Erforderliche Rolle: admin

## Prozedur

1. Klicken Sie auf der Seite **„Einstiegspunktkonfigurationen“** auf die Schaltfläche **Map Associated Info View** (Zugeordnete Info zuordnen).




2. Wählen Sie die neu hinzugefügte Einstiegspunktliste aus der Dropdown- **Liste** „Einstiegspunktliste“ aus.
3. Geben Sie den Namen der Ansicht, die die zugehörigen Listen mit zugehörigen Informationen enthält, in das Feld **Zugeordnete** Informationsansicht ein.
Informationen zum Erstellen einer Ansicht für die zugehörigen Listen mit Informationen finden Sie unter Ansicht für zugehörige Infotabellen wird erstellt.




4. **Speichern** Sie das Formular.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Darüber hinaus können Sie bei Bedarf weitere zugeordnete Listen hinzufügen oder entfernen, indem Sie die **Ansicht „Zugehörige Informationen bearbeiten“**verwenden.
   Sie können das Layout der Einstiegspunktliste auch mit der Aktion Einstiegspunkt-Listenlayout **bearbeiten** konfigurieren. Fügen Sie dem Slushbucket nach Bedarf Spalten hinzu, oder entfernen Sie sie, und speichern Sie das Formular.

### Konfigurieren Sie jede zugeordnete Liste in der -Ansicht für das Rendern von Laufzeitdaten

Konfigurieren Sie jede zugeordnete Liste in der -Ansicht für das Rendern von Laufzeitdaten.

### Vorbereitungen

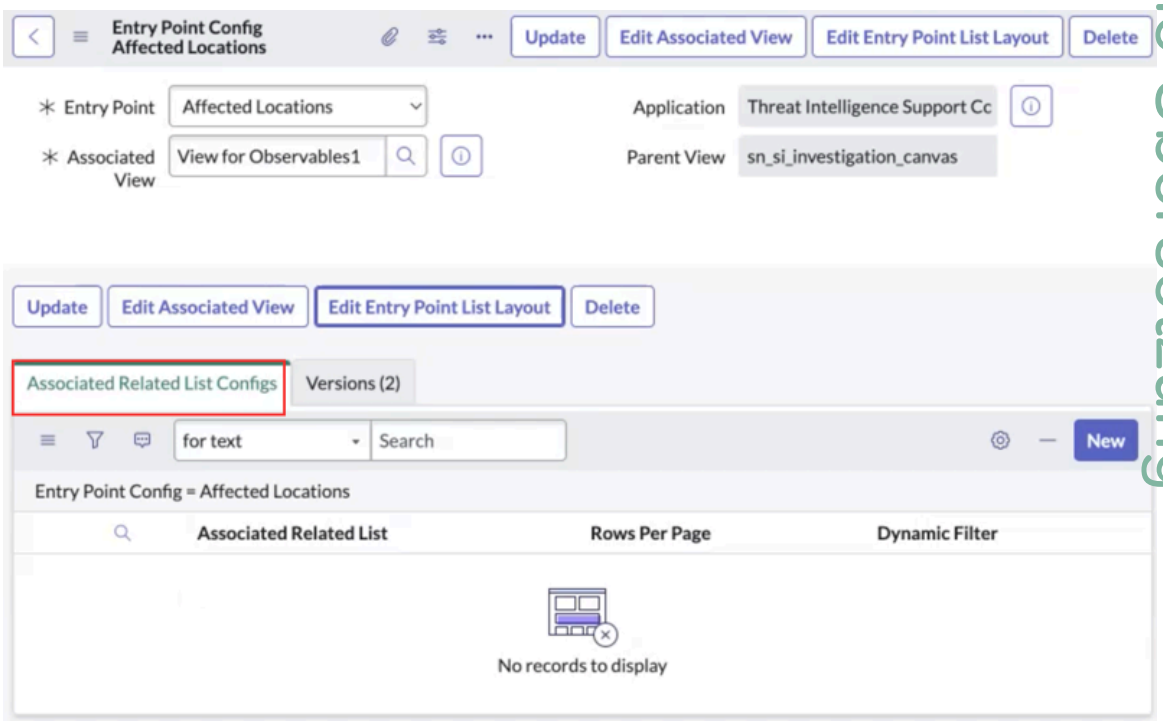
**Hinweis:**
Dieser Schritt ist für jede zugeordnete Liste obligatorisch, die in der zugehörigen Infoansicht konfiguriert ist. Andernfalls ist die zugeordnete Liste nicht auf der Untersuchungsseite verfügbar.

Jede der zugeordneten Listen, die (bei der Zuordnung einer zugeordneten Infoansicht zu einer Einstiegspunktliste) Zuordnungsansicht der Zuordnungsinformationen zur Einstiegspunktliste (oder direkt aus der Ansicht) hinzugefügt werden, erfordert eine zusätzliche Konfiguration, um die Daten in Bezug auf die Auswahl des Laufzeitdatensatzes und der Filterauswahl zu filtern.

Erforderliche Rolle: admin

### Prozedur

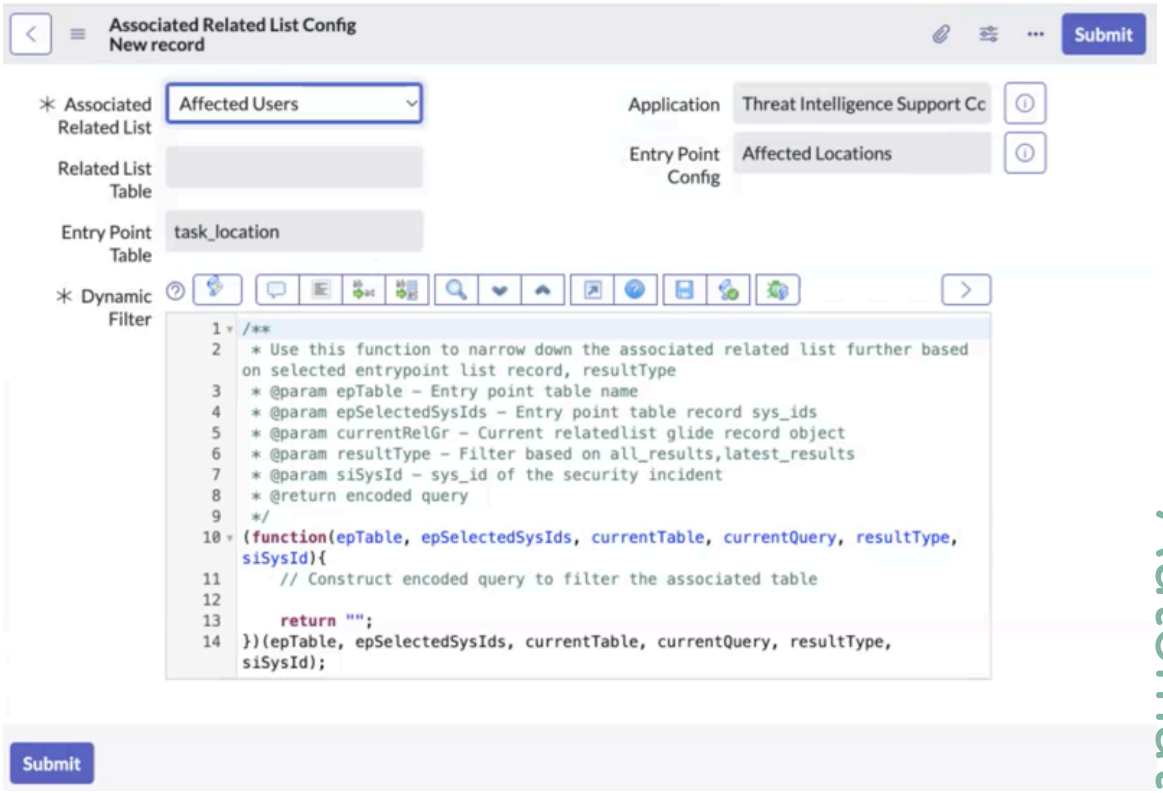
1. Klicken Sie in den **zugehörigen Listenkonfigurationen** auf **Neu**.




2. Wählen Sie den Feldwert **Zugeordnete Liste** aus.
3. Verwenden Sie die Spalte **Dynamischer Filter**, um die zugeordnete Liste basierend auf den ausgewählten Einstiegspunkt-Listendatensätzen und dem Ergebnistyp (aktuelle Ergebnisse aus jeder Lieferantenimplementierung, alle Ergebnisse) weiter zu filtern.
   Sehen Sie sich die vorhandenen Beispiele an, die im Lieferumfang des Produkts enthalten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Außerdem können Sie das zugeordnete Listenlayout mit der Aktion **Zugeordnetes Listenlayout bearbeiten** konfigurieren.
   Fügen Sie im Slushbucket-Fenster nach Bedarf Spalten hinzu, oder entfernen Sie sie.

### SIR Workspace Zugehörige Datensätze

Dieser Abschnitt besteht aus den zugehörigen Listenelementen, die in Abschnitte wie zugeordnete erkennbare Elemente und Konfigurationselemente gruppiert sind.

Die folgenden zugehörigen Listengruppen sind als Teil des Basissystems verfügbar. Sie können diese Gruppen ändern oder Gruppen innerhalb der Anwendung und ihrer jeweiligen Aktionen erstellen.

Sie können diese Gruppen ändern oder neue Gruppen erstellen. Weitere Informationen zum Konfigurieren und Gruppieren der zugehörigen Liste für Security Incidents und Antwortaufgaben finden Sie unter Konfigurieren Sie die zugehörige Liste „Security Incident“.. Jede zugehörige Liste ist innerhalb der SIR Workspacevoll funktionsfähig.

| Zugehörige Liste | Gruppiertes Element |
|---|---|
| Geschäftsauswirkung | • Configuration Items<br>• Betroffene Benutzer<br>• Zugehörige Configuration Items<br>• Zugehörige Benutzer<br>• Betroffene Services |

Automatische Übersetzung

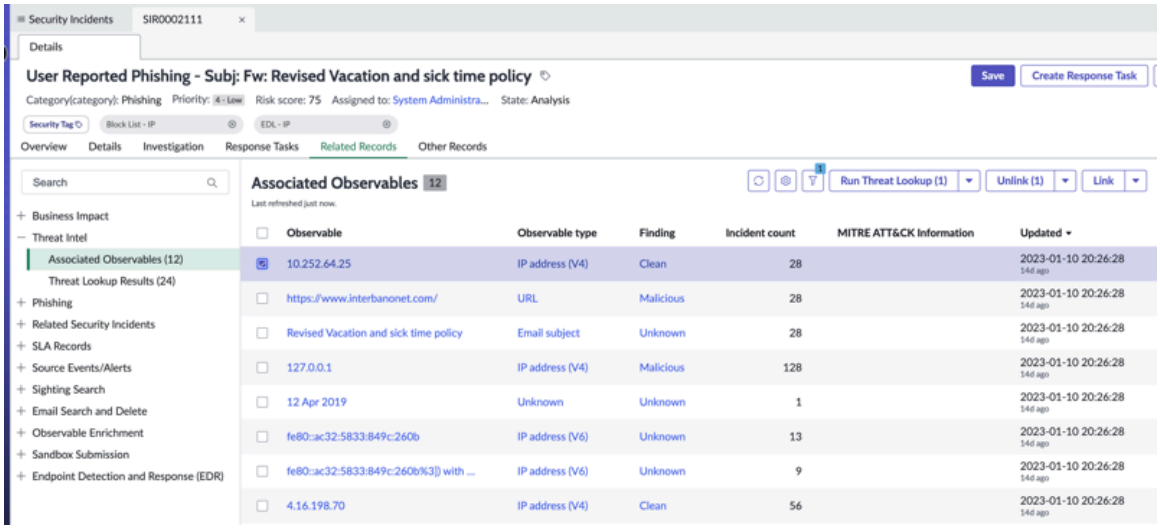
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Liste | Gruppiertes Element |
|---|---|
| Bedrohungsinformationen | • Zugehörige erkennbare Elemente<br>• Suche nach Bedrohungen – Ergebnisse |
| Phishing | • Zugeordnete Phishing-E-Mails<br>• Zugehörige Phishing-Header |
| Zugehörige Security Incidents | • Übergeordneter Security Incident<br>• Untergeordneter Security Incident<br>• Ähnlicher Security Incident |
| SLA-Datensätze | Aufgaben-SLAs |
| Quell-Ereignisse/-warnungen | Quell-Events oder -Warnungen sind die zugehörige Liste mit aktivierter SIEM-Integration, z. B. Quell-E-Mail, LogRhythm-Drilldown-Protokolle, LogRhythm-Ereignisse, zusammengefasster IBM QRadar-Angriff usw.<br>**Hinweis:**<br>Diese Liste ist vollständig von der Integration abhängig, die Sie in Ihrer Instanz haben. Um die relevante zugehörige SIEM-Integrationsliste anzuzeigen, müssen Sie die neueste Version installieren. |
| Sichtungssuche | • Ergebnisse von Sightings Search<br>• Details einer Sichtungssuche<br>• Sichtung |
| Anreicherung erkennbarer Elemente | • Ergänzung erkennbarer Elemente – Ergebnisse<br>• Zugeordnete MISP-Ereignisse<br>• MISP-Anreicherungsergebnisse |
| Endpunkterkennung und -reaktion (EDR). | • Hostdetails<br>• Laufende Prozesse<br>• Laufende Services<br>• Angemeldete Anwender<br>• Netzwerkstatistiken<br>• Datei abrufen<br>• Hosteinträge isolieren |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Liste | Gruppiertes Element |
| --- | --- |
| | • Zusätzliche Aktion für Endpunkt<br>• Details zu Microsoft Defender für endpunktbezogene Computer |




**Hinweis:**
Im Allgemeinen können Sie neue Datensätze erstellen, vorhandene Datensätze oder neue Datensätze mit der zugehörigen Listengruppe verknüpfen oder die Verknüpfung aufheben.

### Zugehörige Informationen

Konfigurieren Sie die zugehörige Liste „Security Incident“.

## Konfigurieren Sie die zugehörige Liste „Security Incident“.

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die im SIR Workspaceangezeigt werden.

### Vorbereitungen

Die zugehörige Liste „Security Incident“ wird gruppiert und als gruppenbezogene Listenelemente auf der Registerkarte „ **Zugehörige Datensätze** “ im Arbeitsbereich angezeigt.

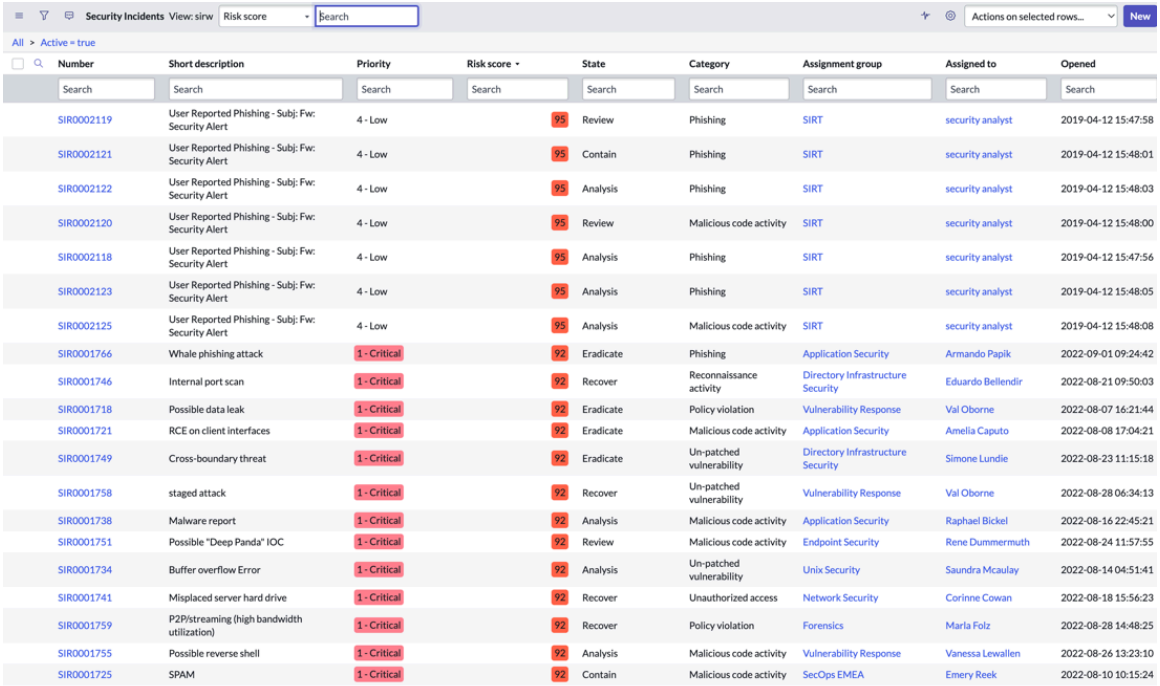
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

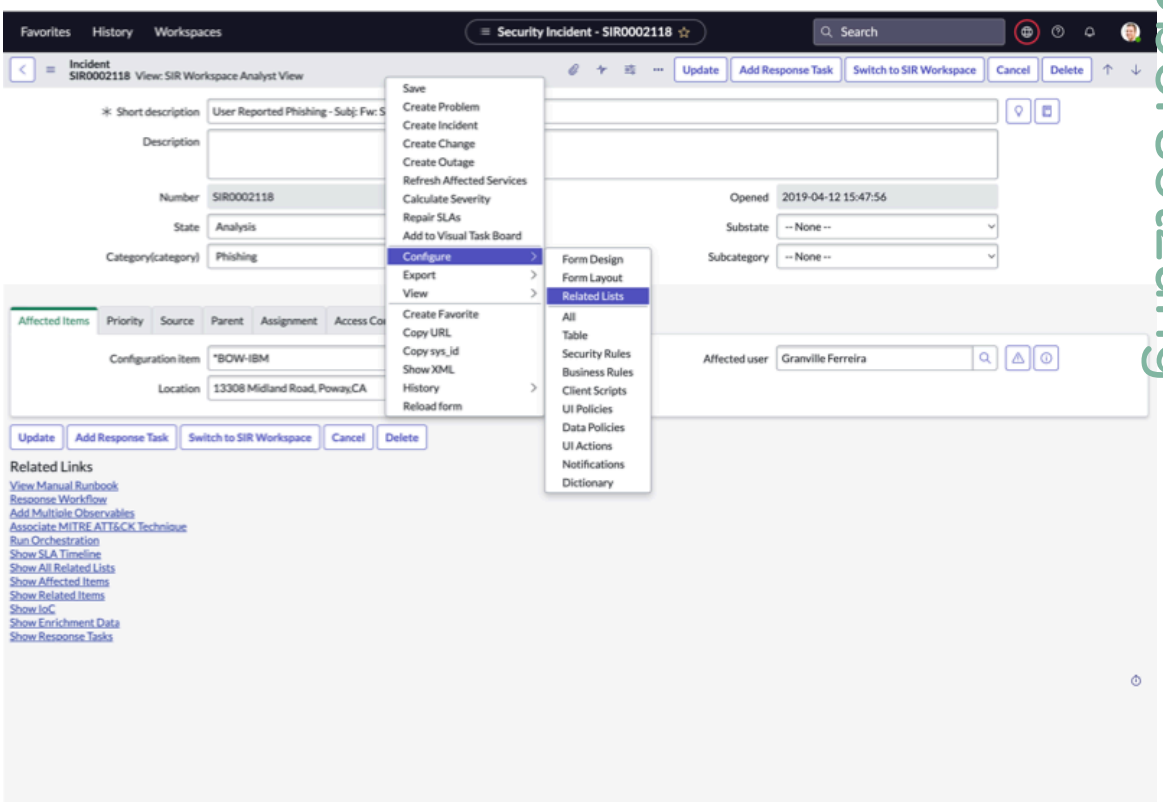
## Prozedur

1. Navigieren Sie in der klassischen Benutzeroberfläche zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.



| Number | Short description | Priority | Risk score | State | Category | Assignment group | Assigned to | Opened |
|---|---|---|---|---|---|---|---|---|
| SIR0002119 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Review | Phishing | SIRT | security analyst | 2019-04-12 15:47:58 |
| SIR0002121 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Contain | Phishing | SIRT | security analyst | 2019-04-12 15:48:01 |
| SIR0002122 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Analysis | Phishing | SIRT | security analyst | 2019-04-12 15:48:03 |
| SIR0002120 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Review | Malicious code activity | SIRT | security analyst | 2019-04-12 15:48:00 |
| SIR0002118 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Analysis | Phishing | SIRT | security analyst | 2019-04-12 15:47:56 |
| SIR0002123 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Analysis | Phishing | SIRT | security analyst | 2019-04-12 15:48:05 |
| SIR0002125 | User Reported Phishing - Subj: Fw: Security Alert | 4 - Low | 95 | Analysis | Malicious code activity | SIRT | security analyst | 2019-04-12 15:48:08 |
| SIR0001766 | Whale phishing attack | 1 - Critical | 92 | Eradicate | Phishing | Application Security | Armando Papik | 2022-09-01 09:24:42 |
| SIR0001746 | Internal port scan | 1 - Critical | 92 | Recover | Reconnaissance activity | Directory Infrastructure Security | Eduardo Bellendir | 2022-08-21 09:50:03 |
| SIR0001718 | Possible data leak | 1 - Critical | 92 | Eradicate | Policy violation | Vulnerability Response | Val Oborne | 2022-08-07 16:21:44 |
| SIR0001721 | RCE on client interfaces | 1 - Critical | 92 | Eradicate | Malicious code activity | Application Security | Amelia Caputo | 2022-08-08 17:04:21 |
| SIR0001749 | Cross-boundary threat | 1 - Critical | 92 | Eradicate | Un-patched vulnerability | Directory Infrastructure Security | Simone Lundie | 2022-08-23 11:15:18 |
| SIR0001758 | staged attack | 1 - Critical | 92 | Recover | Un-patched vulnerability | Vulnerability Response | Val Oborne | 2022-08-28 06:34:13 |
| SIR0001738 | Malware report | 1 - Critical | 92 | Analysis | Malicious code activity | Application Security | Raphael Bickel | 2022-08-16 22:45:21 |
| SIR0001751 | Possible "Deep Panda" IOC | 1 - Critical | 92 | Review | Malicious code activity | Endpoint Security | Rene Dummermuth | 2022-08-24 11:57:55 |
| SIR0001734 | Buffer overflow Error | 1 - Critical | 92 | Analysis | Un-patched vulnerability | Unix Security | Saundra Mcaulay | 2022-08-14 04:51:41 |
| SIR0001741 | Misplaced server hard drive | 1 - Critical | 92 | Recover | Unauthorized access | Network Security | Corinne Cowan | 2022-08-18 15:56:23 |
| SIR0001759 | P2P/streaming (high bandwidth utilization) | 1 - Critical | 92 | Recover | Policy violation | Forensics | Marla Folz | 2022-08-28 14:48:25 |
| SIR0001755 | Possible reverse shell | 1 - Critical | 92 | Analysis | Malicious code activity | Vulnerability Response | Vanessa Lewallen | 2022-08-26 13:23:10 |
| SIR0001725 | SPAM | 1 - Critical | 92 | Contain | Malicious code activity | SecOps EMEA | Emery Reek | 2022-08-10 10:15:24 |

2. Wählen Sie einen beliebigen Incident-Datensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Incident-Kontextmenü.
4. Gehe zu **Konfigurieren** > **Zugehörige Liste**.

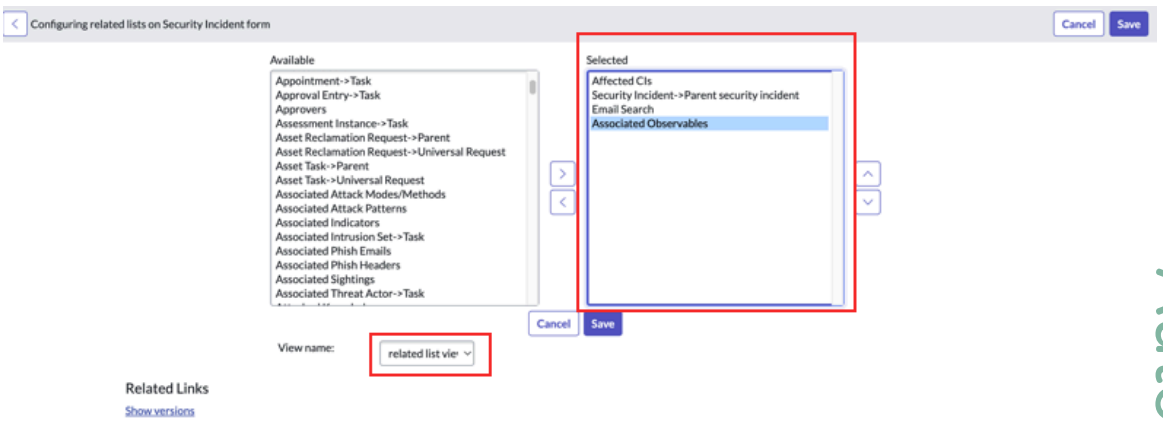


Das **Formular „Zugehörige Listen in Security Incident konfigurieren“** wird angezeigt.

Automatische Übersetzung

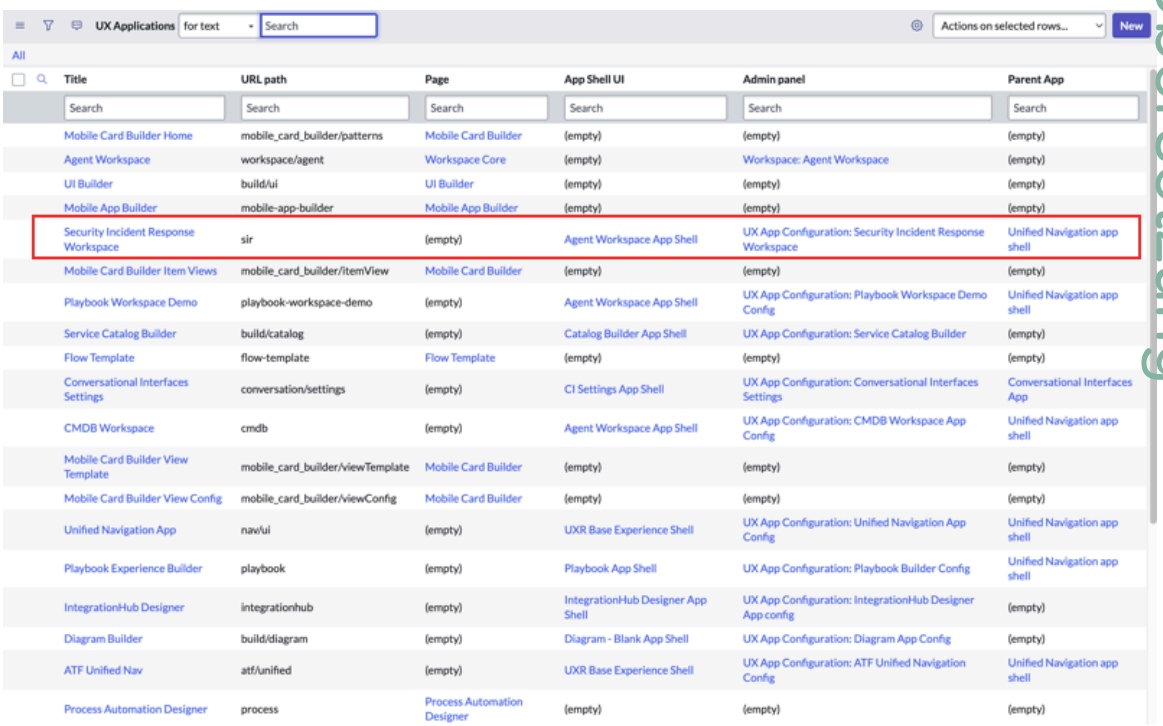
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wechseln Sie zu **Name** anzeigen, und wählen Sie **Neu**.
6. Geben Sie einen Namen für die Ansicht ein.
7. Wählen Sie die neu erstellte Ansicht aus.
   Nachdem Sie die Ansicht ausgewählt haben, wählen Sie die erforderlichen zugehörigen Listenfelder aus dem Slushbucket aus.




**Hinweis:**
Wenn Sie etwas ändern möchten, wählen Sie die Ansicht aus, und entfernen oder fügen Sie die Elemente hinzu.

8. Klicken Sie auf **Speichern**.
9. Navigieren Sie in der linken Navigation zu **Alle** > **Now-Experience-Framework** > **Erfahrungen**.
10. Wählen Sie **Security Incident Response Workspace aus**.

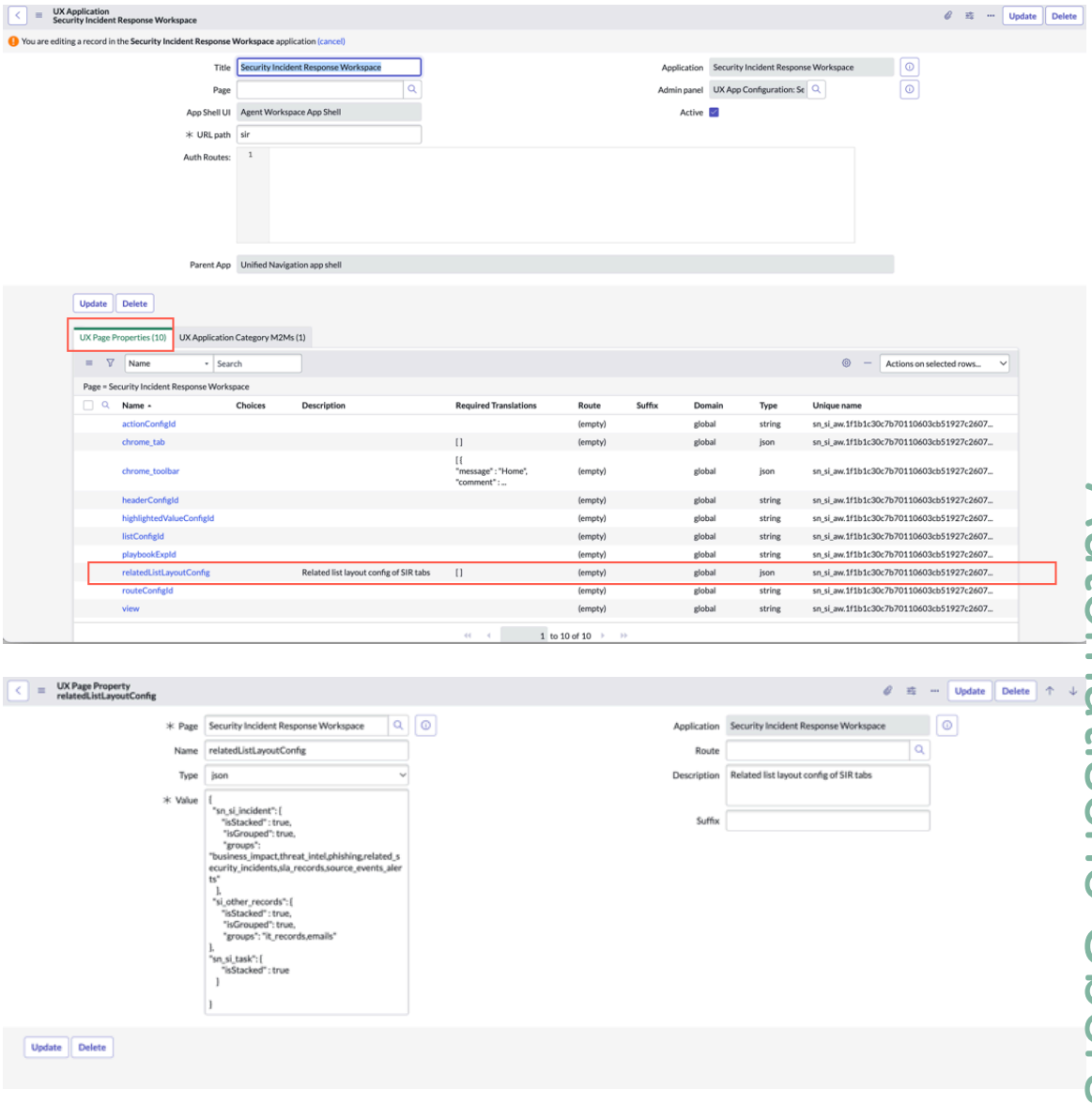



Die Seite „ **UX Application Security Incident Response Workspace** “ wird angezeigt.

11. Wechseln Sie zur Registerkarte „ **UX** -Seiteneigenschaften“, und wählen Sie in der Listenansicht die Option **relatedListLayoutConfig** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

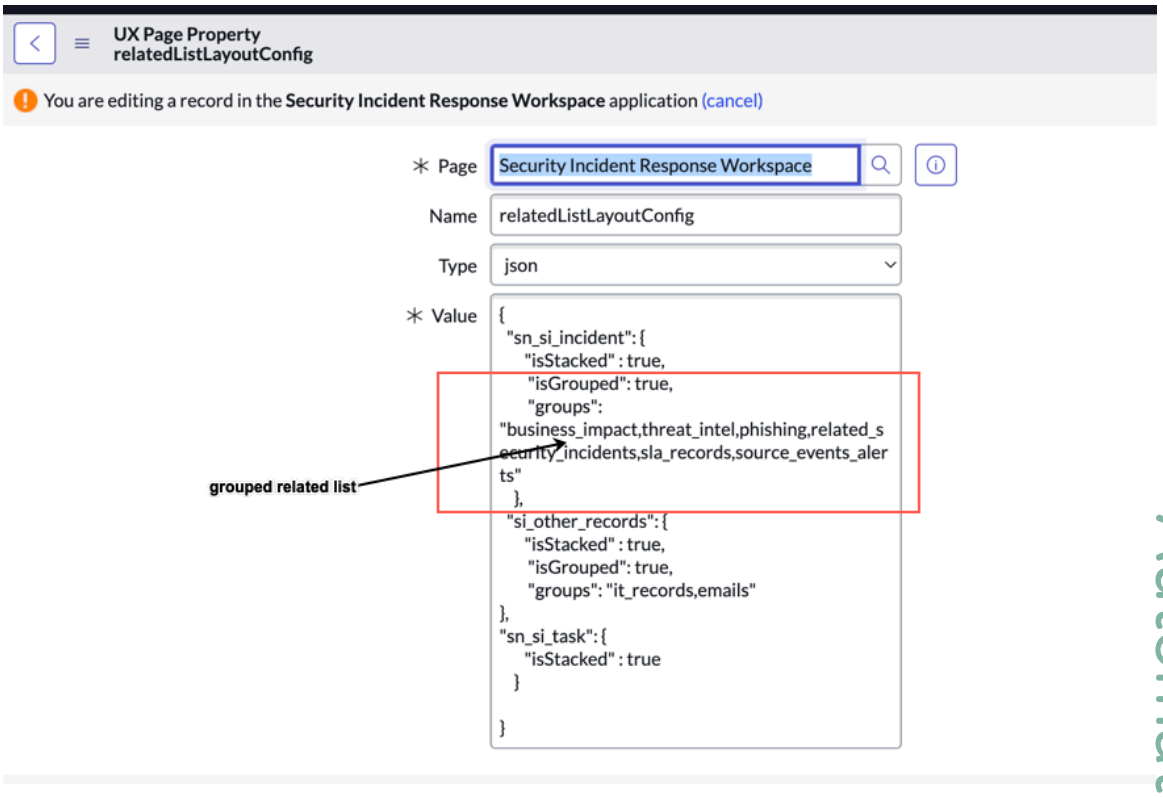

Automatische Übersetzung




**12.** Fügen Sie den neu erstellten Ansichtsnamen, getrennt durch ein Komma, einer bereits vorhandenen Liste von Werten im Textfeld **Wert** unter dem Feld **sn_si_incident.viewsUsedForGrouping hinzu**.
Wenn Sie beispielsweise einen neuen Ansichtsnamen mit dem Namen **Geschäftsauswirkung** erstellt haben, müssen Sie ihn im Textfeld **Wert** als **business_impact** (durch Unterstrich innerhalb des Ansichtsnamens und durch ein Komma nach einem vorhandenen Wert getrennt) unter sn_si_incident angeben :Gruppenfeld.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

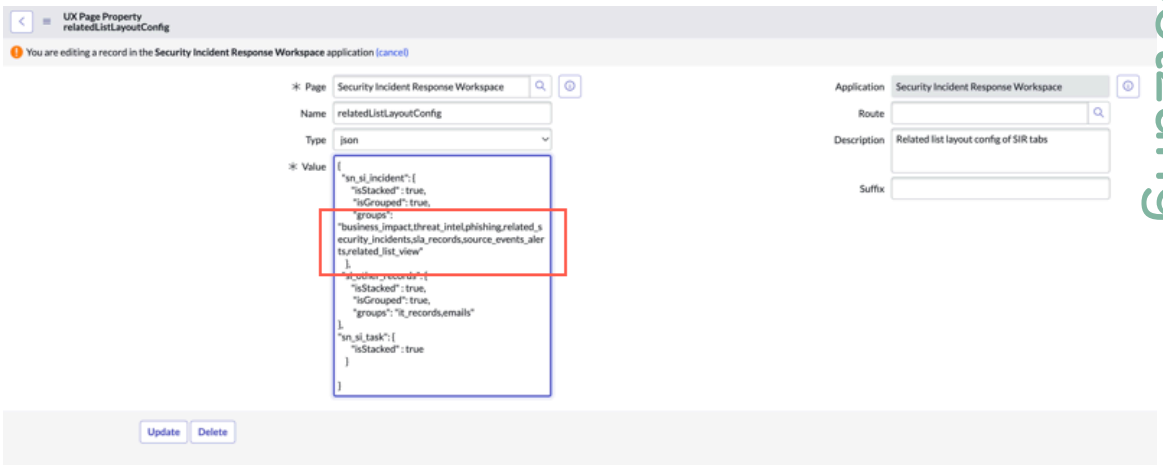



**Hinweis:**

Wenn Sie den neuen Ansichtsnamen unter dem Feld **„sn_si_incident.viewsUsedForGrouping** “ hinzufügen, wird der Eintrag auf der Registerkarte „ **Zugehörige Datensätze** “ des Arbeitsbereichs erstellt.

Wenn Sie den Ansichtsnameneintrag in **si_other_records.viewsUsedForGrouping aktualisieren**, wird die zugehörige Listengruppe auf der Registerkarte „ **Andere Datensätze** “ des Arbeitsbereichs hinzugefügt.

Unten sehen Sie eine Beispielansicht, in der die neu erstellten Ansichten hinzugefügt werden.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
„**requiredRolesForGrouping** “ enthält kommagetrennte sys_user_role-Datensatznamen. SIR-Arbeitsbereichsbenutzer müssen über mindestens eine dieser Rollen verfügen, um die gruppierten zugehörigen Listen zu verwenden. Wenn ein Benutzer keine dieser Rollen hat, wird die für die aktuelle Benutzerrolle konfigurierte zugehörige Listenansicht mithilfe der Ansichtsregelkonfiguration vertikal ohne Gruppierung dargestellt. Diese Eigenschaft wird ignoriert, wenn die Eigenschaft **isGrouped** auf „false“ festgelegt ist. Wenn diese Eigenschaft leer ist, kann jeder Benutzer auf die gruppierten zugehörigen Listen zugreifen.

13. Klicken Sie auf **Speichern**.
14. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
15. Wählen Sie einen bestimmten Security Incident aus.
16. Wechseln Sie zur Registerkarte **Zugehörige Datensätze** des Arbeitsbereichs.
    Die gruppierten zugehörigen Listen werden angezeigt.

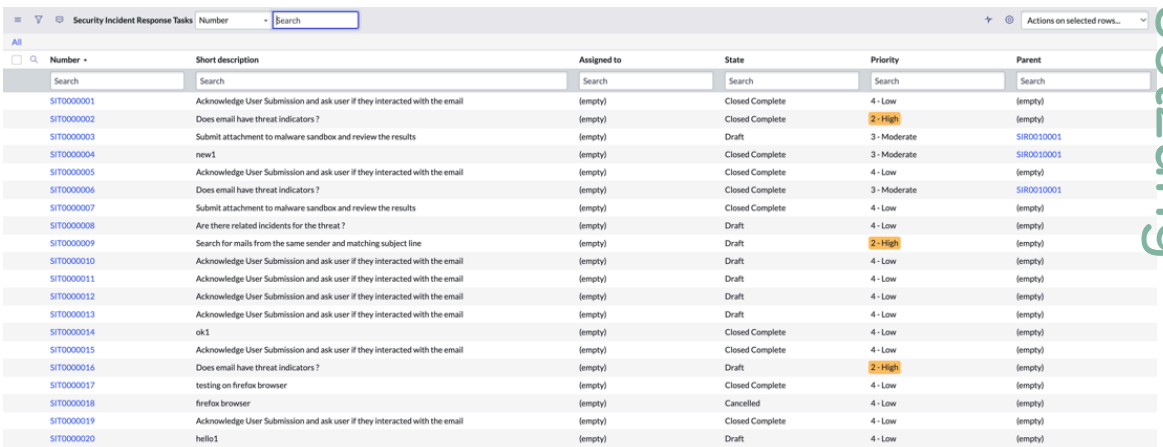
### Konfigurieren Sie die zugehörige Liste für Antwortaufgaben

Verwenden Sie diesen Abschnitt, um neue zugehörige Listen für Antwortaufgaben zu konfigurieren, die in der Security Incident Response-Anwendung angezeigt werden.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Die zugehörige Liste der Antwortaufgaben wird nicht gruppiert, sondern als einzelne zugehörige Listenelemente angezeigt, da nur wenige Standardlisten vorhanden sind. Zeigen Sie die mit den Antwortaufgaben verbundenen Elemente auf der Registerkarte **„Antwortaufgaben** “ des Security Incident-Datensatzes des Arbeitsbereichs an.

#### Prozedur
1. Navigieren zu **Alle** > **Security Incident** > **Antwortaufgaben** > **Alle Aufgaben anzeigen**.



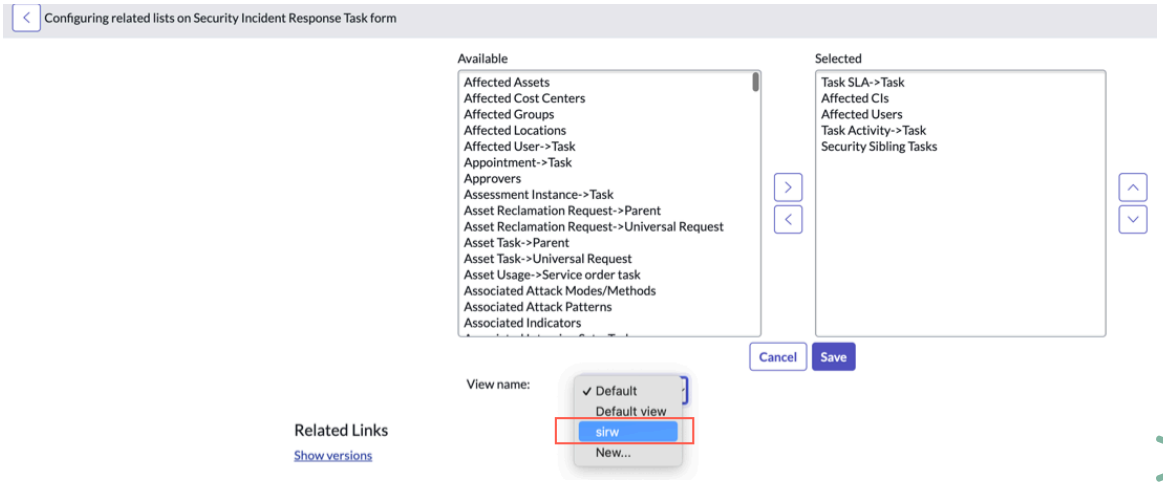

| Number | Short description | Assigned to | State | Priority | Parent |
|---|---|---|---|---|---|
| SIT0000001 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000002 | Does email have threat indicators ? | (empty) | Closed Complete | 2 - High | (empty) |
| SIT0000003 | Submit attachment to malware sandbox and review the results | (empty) | Draft | 3 - Moderate | SIR0010001 |
| SIT0000004 | new1 | (empty) | Closed Complete | 3 - Moderate | SIR0010001 |
| SIT0000005 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000006 | Does email have threat indicators ? | (empty) | Closed Complete | 3 - Moderate | SIR0010001 |
| SIT0000007 | Submit attachment to malware sandbox and review the results | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000008 | Are there related incidents for the threat ? | (empty) | Draft | 4 - Low | (empty) |
| SIT0000009 | Search for mails from the same sender and matching subject line | (empty) | Draft | 2 - High | (empty) |
| SIT0000010 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Draft | 4 - Low | (empty) |
| SIT0000011 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Draft | 4 - Low | (empty) |
| SIT0000012 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Draft | 4 - Low | (empty) |
| SIT0000013 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Draft | 4 - Low | (empty) |
| SIT0000014 | ok1 | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000015 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000016 | Does email have threat indicators ? | (empty) | Draft | 2 - High | (empty) |
| SIT0000017 | testing on firefox browser | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000018 | firefox browser | (empty) | Cancelled | 4 - Low | (empty) |
| SIT0000019 | Acknowledge User Submission and ask user if they interacted with the email | (empty) | Closed Complete | 4 - Low | (empty) |
| SIT0000020 | hello1 | (empty) | Draft | 4 - Low | (empty) |

2. Wählen Sie einen beliebigen Antwortaufgabendatensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Kontextmenü der Security Incident Response-Aufgabe.
4. Navigieren zu **Konfigurieren** > **Zugehörige Liste**.
   Das **Formular „Zugehörige Listen in Sicherheitsreaktionsaufgabe konfigurieren“** wird angezeigt.

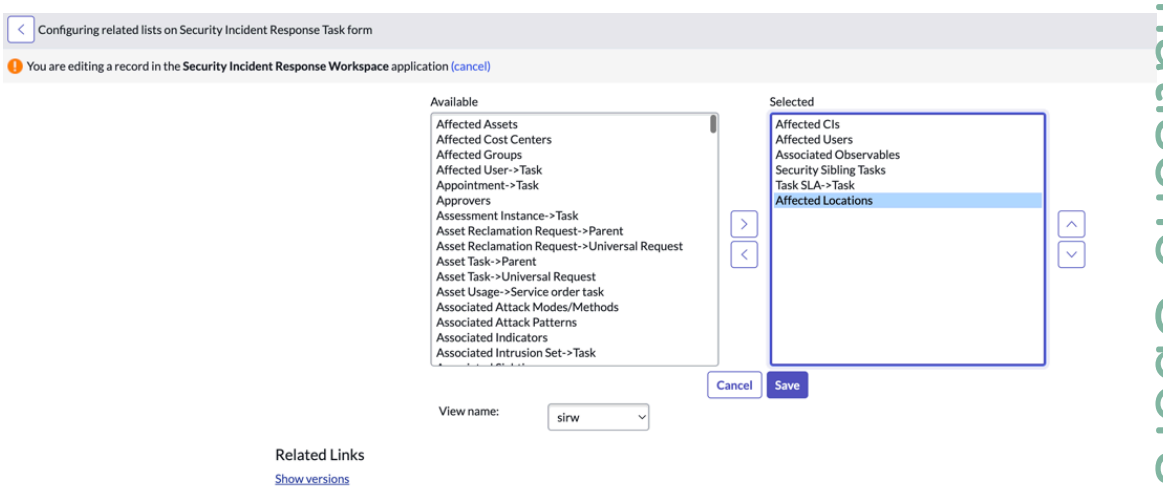


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wechseln Sie zu Ansichtsname, und wählen Sie die Ansicht sirwaus**.




6. Wählen Sie die gewünschten zugehörigen Listenfelder aus dem Slushbucket aus.
   Beispiel: Betroffene Standorte.

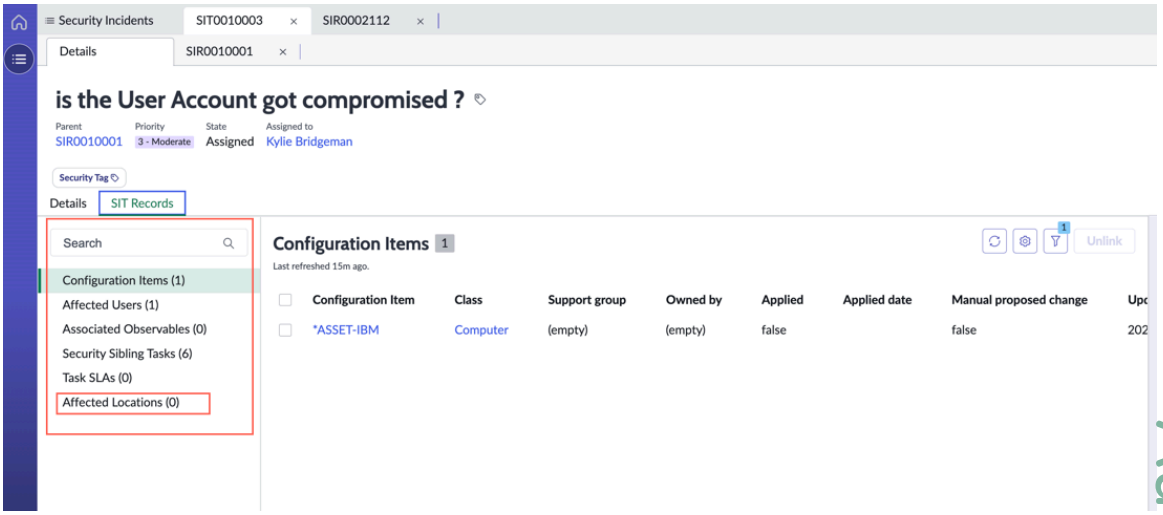



7. Klicken Sie auf **Speichern**.
8. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Antwortaufgaben** > **SIT-Datensätze**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die konfigurierten zugehörigen Listen (z. B. „Betroffene Standorte“, wie ausgewählt) werden in der SIT-Datensatzliste aufgelistet.




## Arbeiten mit SIR Workspace

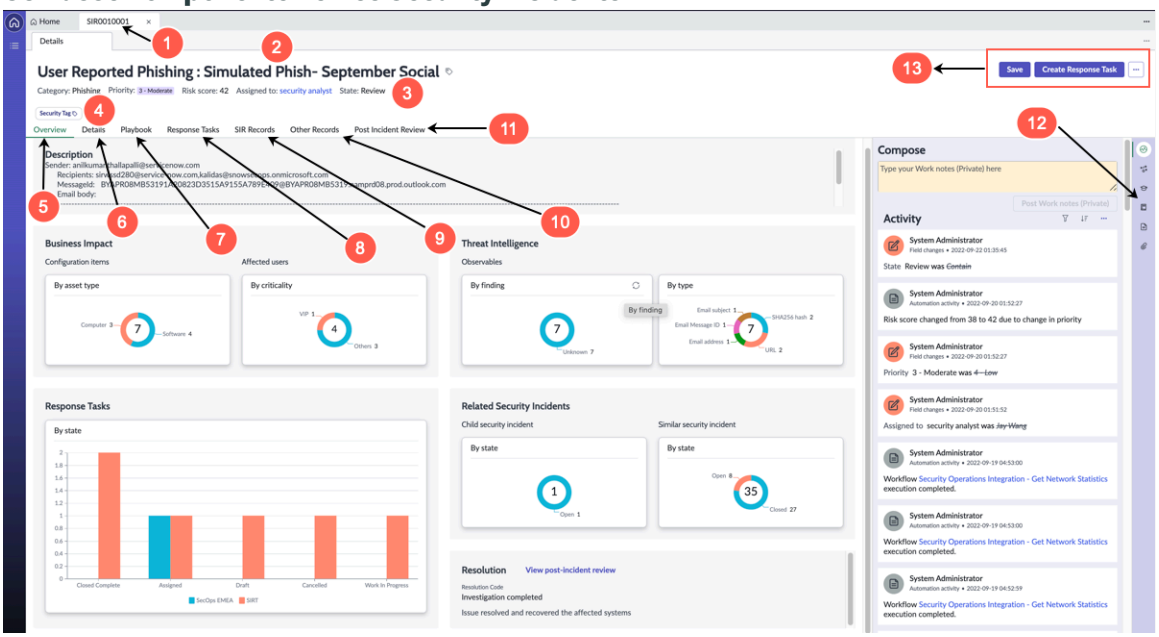
Sicherheitsanalysten und -manager verwenden SIR Workspace, um alltägliche Vorgänge mit einer verbesserten Benutzer-Experience durchzuführen, Incident-Untersuchungen durchzuführen und sich einen Überblick zu verschaffen.

### Arbeiten mit Security Incident-Datensätzen

Der Security Incident-Datensatz besteht aus Folgendem.

Schlüsselkomponenten, die in einem Security Incident-Datensatz verfügbar sind:

#### Schlüsselkomponenten eines Security Incidents




| Nummer | Name | Beschreibung |
|---|---|---|
| 1 | Security Incident-Nummer | Die Security Incident-Nummer ist für den Registerkartennamen verfügbar. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Nummer | Name | Beschreibung |
|---|---|---|
| 2 | Kurzbeschreibung | Kurzbeschreibung des Security Incident, der über dem Formularbanner angezeigt wird. |
| 3 | Formularbanner | Dies ist ein schreibgeschützter Abschnitt, der die Schlüsselfelder wie Kategorie, Priorität, Risikopunktzahl, Status und die Incident-Zuweisungsdetails enthält.<br>**Hinweis:**<br>Die regulären Plattform-Tags können auch hier angewendet werden. |
| 4 | Sicherheits-Tags | Zeigt die Sicherheits-Tags an, die einem Security Incident zugeordnet sind. |
| 5 | Übersicht | Bietet eine Snapshot-Übersicht über den Security Incident, z. B. Beschreibung, Geschäftsauswirkung bestehend aus Asset-Details nach Typ, betroffene Benutzer nach Relevanz, Threat Intelligence-Elemente bestehend aus erkennbaren Elementen nach Suche und Typ, Antwortaufgaben, zugehörige Security Incidents bestehend aus untergeordneten Security Incidents und ähnliche Security Incidents. |
| 6 | Details | Auf der Registerkarte „Details“ wird das Security Incident-Formular angezeigt. |
| 7 | Ermittlung | Die Registerkarte Untersuchung zeigt die Incident-Untersuchungs-Experience an. |
| 8 | Playbook | Playbook wird über Process Automation Designer (PAD) ausgelöst. Ob ein Prozess erstellt wird und ob eine Auslöserbedingung festgelegt ist, um das Playbook für einen Security Incident auszulösen. Dann wird ein Playbook angezeigt. |
| 9 | Antwortaufgaben | Die Antwortaufgaben erfasst alle Antwortaufgaben, die einem Security Incident zugeordnet sind. |
| 10 | Zugehörige Datensätze | Die Registerkarte „Zugehörige Datensätze“ besteht aus allen zugehörigen Listen der klassischen Benutzeroberfläche in diesem Abschnitt. Die zugehörigen Listen sind zur einfachen Navigation in verschiedene Abschnitte gruppiert, z. B. „Geschäftsauswirkung“, „Bedrohungsinformationen“ usw. |
| 11 | Andere Datensätze | Die Registerkarte „Andere Datensätze“ besteht aus IT-Datensätzen wie Change-Anforderungen, Incidents und E-Mails, die in diesem Abschnitt gruppiert und angezeigt werden. |
| 12 | Registerkarte „Überprüfung nach Incident“ | Wenn der Security Incident in den Überprüfungsstatus übergeht, wird die Registerkarte „Überprüfung nach Incident“ mit den Bewertungen und Berichten nach Incidents auf der Registerkarte angezeigt. |
| 13 | Kontextmenü | Bietet einfachen Zugriff auf Schnellaktionen und ist auf allen Registerkarten verfügbar, auf die Analysten bei Bedarf zugreifen können. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Nummer | Name | Beschreibung |
|---|---|---|
| | | Das Kontextmenü bietet eine einfache Navigation zu den verschiedenen Ressourcen, z. B.:<br><br>**1.** Aktivitätenstrom<br>**2.** Playbook<br>**3.** Analyst Assist<br>**4.** Runbook<br>**5.** Vorlagen<br>**6.** Anlagen |
| 14 | Formular-UI-Aktionen | Die verschiedenen UI-Aktionen für Security Incident-Formulare werden oben rechts im Incident-Formular angezeigt. Folgende Formular-UI-Aktionen sind verfügbar:<br>• Speichern<br>• Antwortaufgabe erstellen<br>• E-Mail erstellen<br>• Playbook hinzufügen<br>• Verknüpfte(n) Workflow(s) öffnen<br>• Incident erstellen<br>• Problem erstellen<br>• Change-Anforderung erstellen<br>• Ausfall erstellen<br>• Schweregrad berechnen<br>• Link zu Major Security Incident<br>• Vorschlagen als Major Security Incident<br>• Heraufstufen zu Major Security Incident<br>• Zusätzliche Aktion(en) für Endpunkt ausführen<br>• Ordnen Sie die MITRE ATT&CK-Technik zu<br>• Zu klassischer UI wechseln<br>• Dem Sicherheitsfall hinzufügen<br>• Löschen<br><br>Weitere Informationen finden Sie unter Arbeiten mit Formular-UI-Aktionen. |

**Abschnitt „Security Incident – Übersicht“.**

Im Arbeitsbereich „Übersicht“ werden die wichtigsten Informationen zum Security Incident angezeigt.

Für Ringdiagramme sind Drilldown-Funktionen aktiviert. Wenn ein Analyst auf eines der Diagrammelemente klickt, navigiert er zum jeweiligen Datensatz mit einer gefilterten



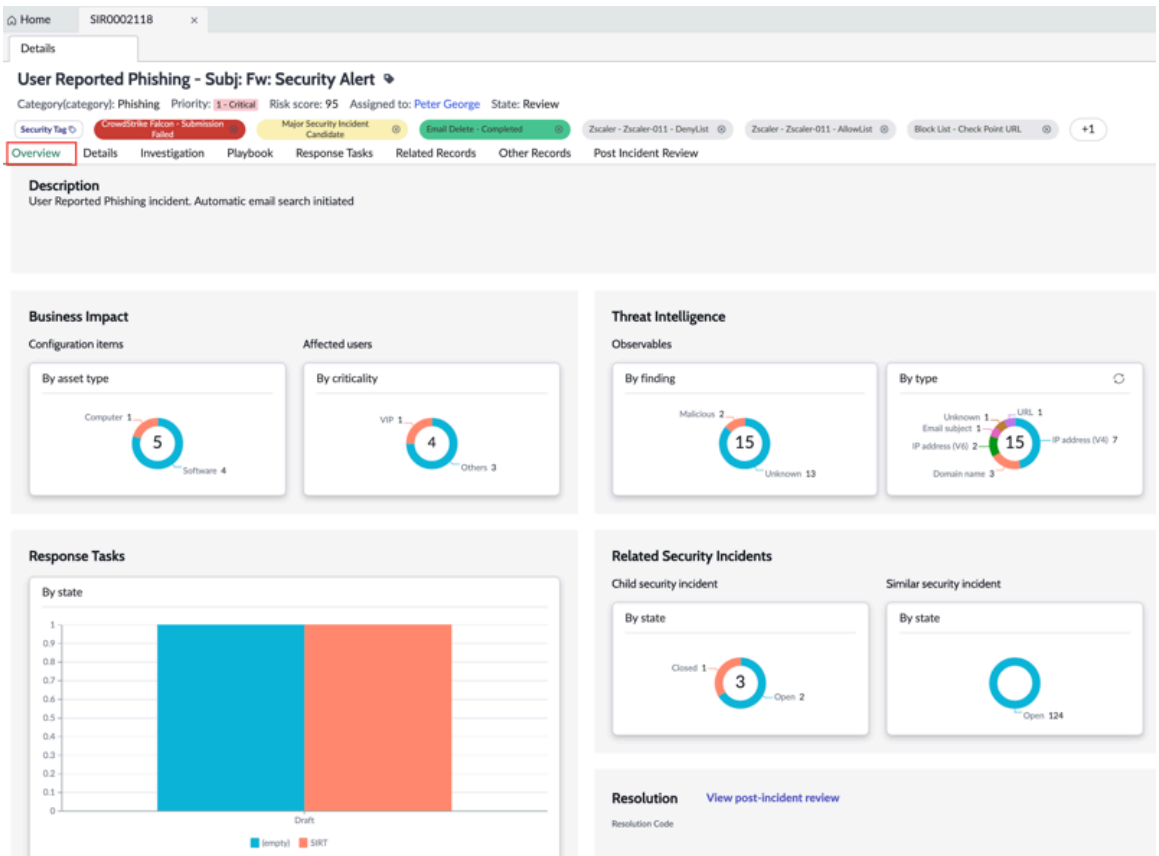
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenansicht der Elemente auf der entsprechenden Registerkarte. Wenn Sie beispielsweise auf „ **Böswillige erkennbare Elemente** “ klicken, gelangen Sie zu den erkennbaren Elementen mit einer gefilterten Listenansicht der schädlichen erkennbaren Elemente auf der Registerkarte „ **Zugehörige Datensätze** “.

Im Abschnitt „Übersicht“ wird Folgendes angezeigt:

- Beschreibung des Security Incident
- Geschäftsauswirkungsdetails, z. B. Konfigurationselemente nach Asset-Typ und betroffene Benutzer nach Relevanz, ob VIP-Benutzer oder andere Benutzer.
- Threat Intelligence-Elemente wie erkennbare Elemente, indem Sie feststellen, ob die erkennbaren Elemente böswillig oder unbekannt sind, und nach Typ.
- Antwortaufgaben nach Status und Zuweisungsgruppe.
- Zugehörige Security Incidents, bestehend aus untergeordneten Security Incidents nach Status (offen oder geschlossen) und ähnlichen Security Incidents nach Status (offen oder geschlossen).
- Der Abschnitt „Lösung“ wird angezeigt, wenn ein Incident in den Status „Überprüfung“ verschoben wird. Anschließend wird der Abschnitt „Lösung“ im Abschnitt „ **Übersicht** “ angezeigt, mit der Möglichkeit, die Überprüfung nach dem Incident anzuzeigen.
- Lösung – Überprüfung nach Incident anzeigen: Klicken Sie auf den Link, um zur Seite „ **Überprüfung nach Incident“** zu navigieren.
- Nachdem der Incident geschlossen wurde, werden im Abschnitt „Auflösung“ der Lösungscode, Lösungsnotizen und Gelöst von (Benutzer) zusammen mit den Details zur Überprüfung nach Incidents angezeigt.

**Übersichtsbereich**






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident Abschnitt „Details“.

In diesem Abschnitt werden die Formularfelder für Security Incidents angezeigt, die aus der klassischen Benutzeroberfläche des Security Incident gerendert werden.

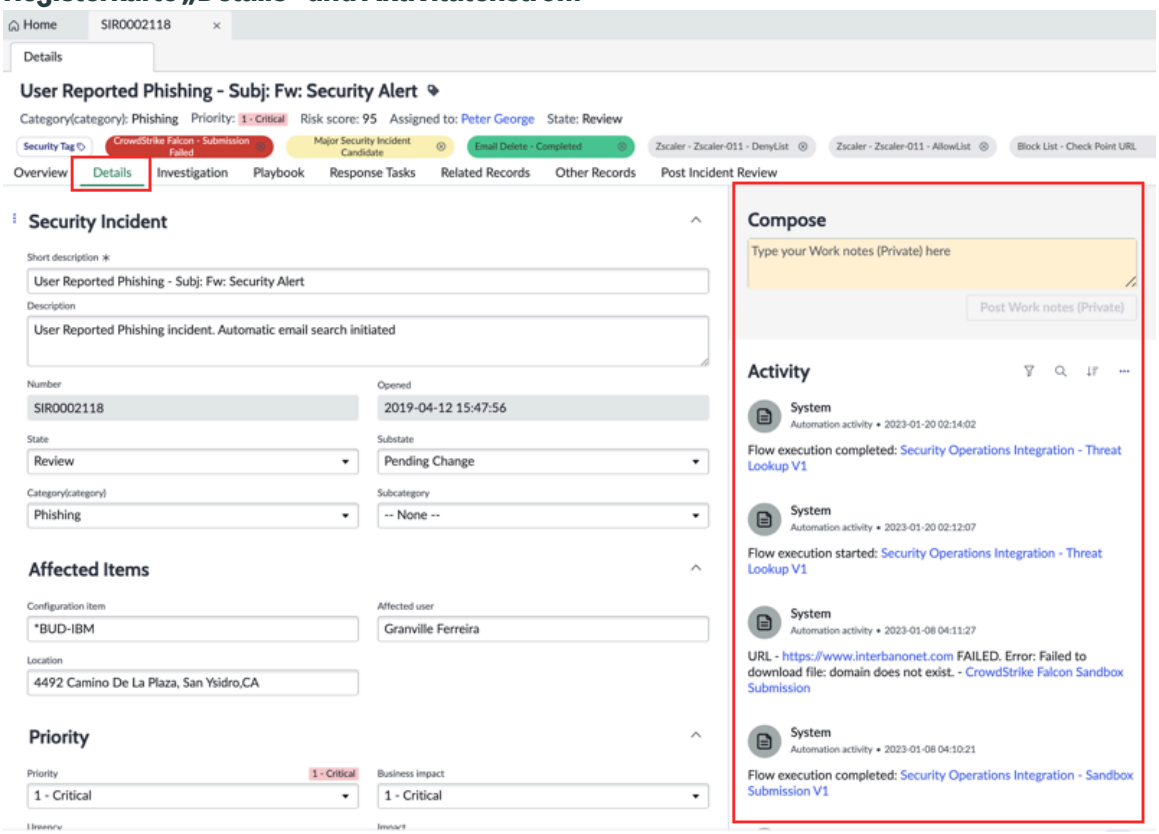
Für die klassische UI wurde eine Ansicht namens **SIRW-** Ansicht erstellt. Diese Ansicht wird der Registerkarte „ **Details** “ im neuen Arbeitsbereich zugeordnet. Alle erforderlichen Anpassungen müssen in dieser Ansicht implementiert werden.

Die Formularfelder sind in die folgenden Abschnitte gruppiert und werden in der Formularansicht der Registerkarte „Details“ angezeigt. Klicken Sie auf einen der Abschnitte, oder wechseln Sie zum entsprechenden Abschnitt im Formular:

- Security Incident
- Priorität
- Quelle
- Übergeordnet
- Zuweisung
- Zugriffssteuerungen
- Betroffene Elemente
- Lösung

Die Registerkarte „ **Details** “ enthält den Abschnitt „ **Aktivitätsstream** “ innerhalb des Detailformulars selbst, um den Sicherheitsanalysten einen schnellen Zugriff zu ermöglichen, um Kommentare hinzuzufügen und zu veröffentlichen.

**Registerkarte „Details“ und Aktivitätenstrom**

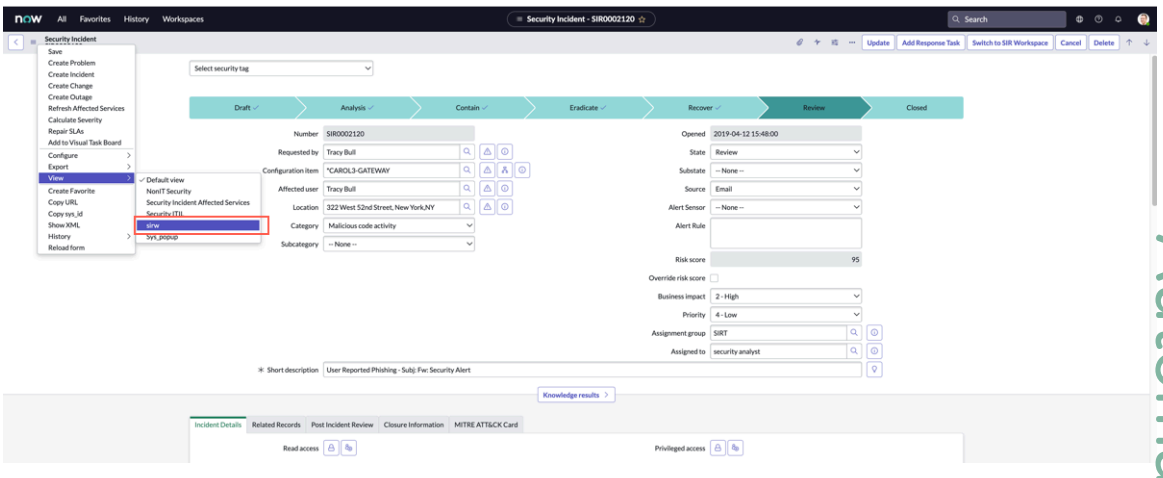



**Ansicht „SIR Analyst Workspace“ anzeigen:**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

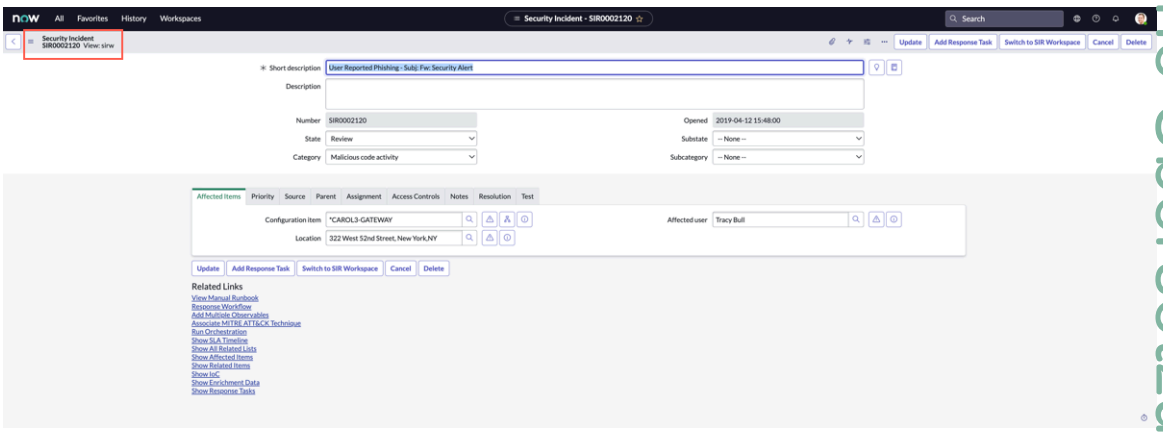
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Wählen Sie einen beliebigen Security Incident-Datensatz aus.
3. Klicken Sie auf das Kontextmenü, und wählen Sie **Ansicht** > **sirw**.

**Hinweis:**
Sie können die **sirw-** Arbeitsbereichsansicht im klassischen UI-Formular anpassen.




4. Die Security Incident-Arbeitsbereichsansicht wird wie unten dargestellt gerendert.

**SIR-Arbeitsbereichsansicht**

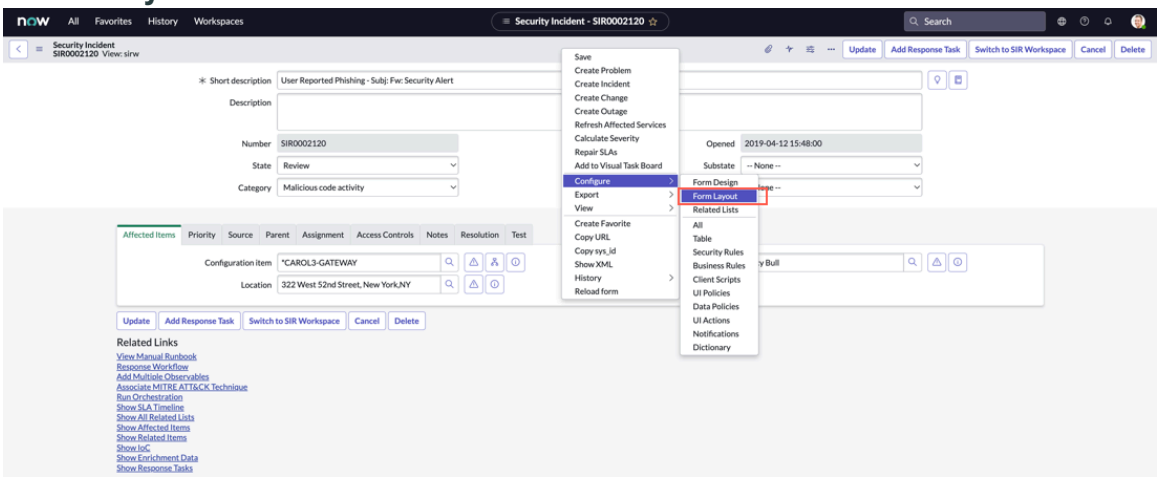



5. Klicken Sie im Security Incident-Datensatz mit der rechten Maustaste, und wechseln Sie zu **Konfigurieren** > **Formularlayout**.

Automatische Übersetzung

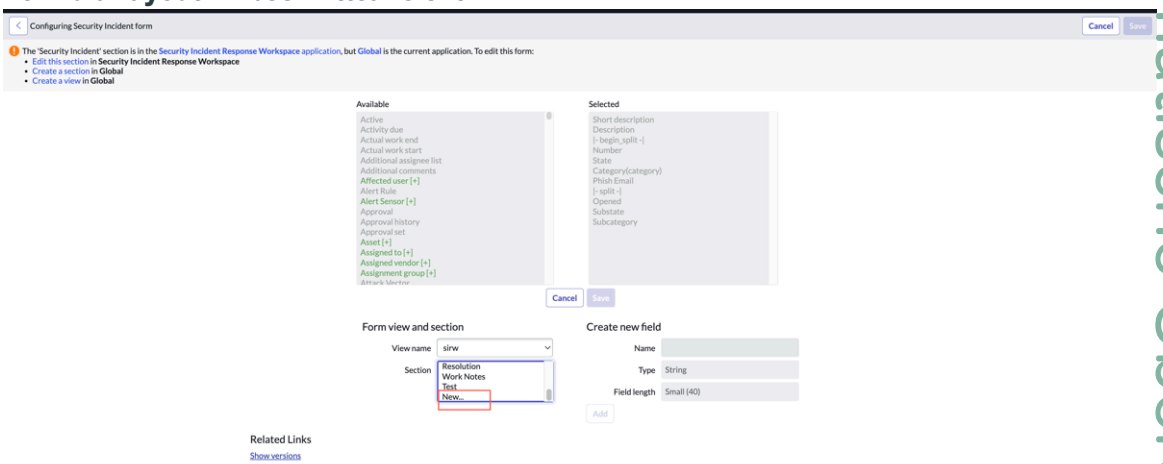
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formularlayout**




6. Führen Sie einen Drilldown zur **Formularansicht und zum Abschnitt** durch, und wählen Sie **Neu** unter **Abschnitt** aus, um einen neuen Abschnitt zu erstellen.

**Formularlayout – Abschnittsansicht**



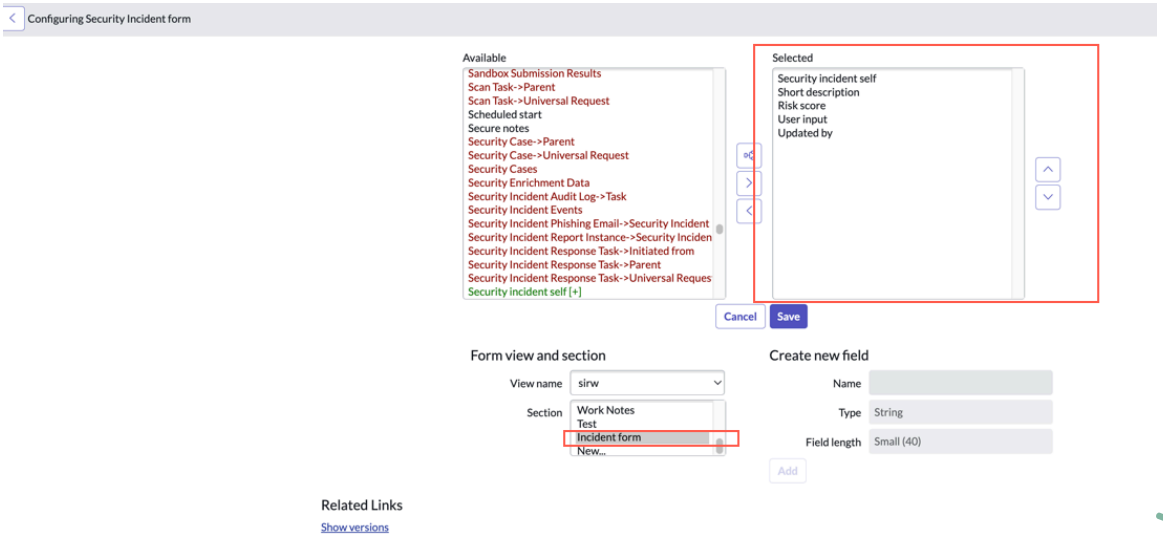

7. Geben Sie den neuen Abschnittsnamen ein, und klicken Sie auf **OK**.

   Beispiel: Incident-Formular.

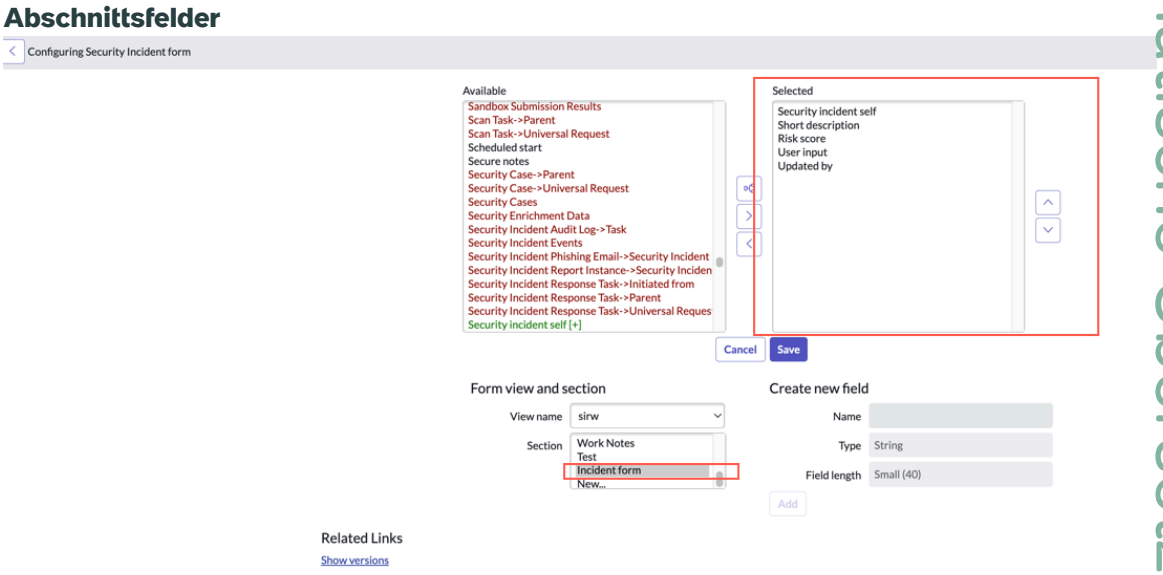
8. Der neue Abschnitt wird erstellt und dem **Abschnitt**hinzugefügt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



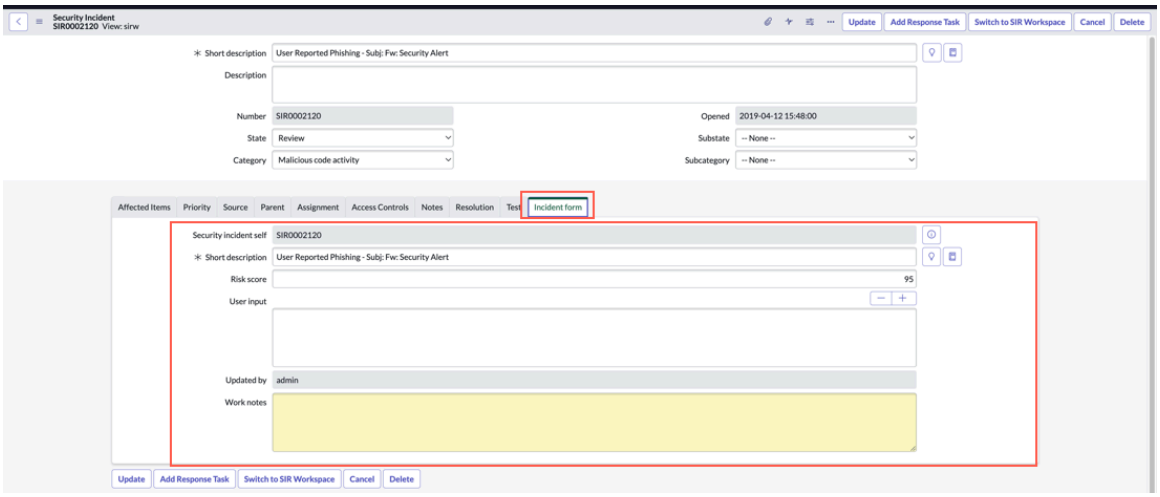

9. Wählen Sie Ihren neuen Abschnitt aus, fügen Sie dem Slushbucket die erforderlichen Abschnittsfelder hinzu, und klicken Sie auf **Speichern**.




10. Der neu hinzugefügte Abschnitt wird zusammen mit dem vorhandenen Abschnittslayout im Security Incident-Formular angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




11. Klicken Sie nun **auf Zu SIR-Arbeitsbereich wechseln**, um zum Security Incident-Formular und dem benutzerdefinierten Abschnitt auf der Registerkarte „ **Details** “ des Arbeitsbereichs zu wechseln.

### SIR Workspace Orchestration

Arbeitsbereich für Security Incident Response Orchestration-Aktivitäten helfen Sicherheitsanalysten, die Untersuchungs-Canvas anzuzeigen und verschiedene zutreffende Aktionen auszuführen.

### SIR Workspace Untersuchungs-Canvas

Arbeitsbereich für Security Incident Response ermöglicht es Sicherheitsanalysten, die wichtigsten Informationen anzuzeigen, die dem Security Incident während des Incident-Korrekturprozesses zugeordnet sind. Die wichtigsten Informationen umfassen auch die zugehörigen Listen wie „Erkennbare Elemente“, „Ergebnisse der Bedrohungssuche“, „Sichtungssuche“, „Anreicherung erkennbarer Elemente“ usw.

In der klassischen Benutzeroberfläche sind die meisten Orchestration-Aktionen, die mit den vordefinierten Integrationen verknüpft sind, für die zugehörigen Listen verfügbar. Zum Beispiel sind „Bedrohungssuche ausführen“, „Anreicherung erkennbarer Elemente ausführen“ usw. in der zugehörigen Liste „Zugeordnete erkennbare Elemente“ vorhanden. Ebenso sind „Hostdetails abrufen“, „Netzwerkstatistiken abrufen“ usw. für die zugehörige Liste „Konfigurationselemente“ verfügbar.

Wenn ein Sicherheitsanalyst diese Aktionen ausführt, werden die Ergebnisse in eine andere zugehörige Liste eingetragen. Wenn ein Benutzer beispielsweise eine Bedrohungssuche ausführt, sind die Ergebnisse in der Tabelle „Ergebnisse der Bedrohungssuche“ verfügbar. Manchmal sind Ergebnisse in mehreren verschiedenen Tabellen verfügbar. Während dieses Prozesses haben die Sicherheitsanalysten eine unzusammenhängende und unorganisierte Benutzer-Experience, wenn sie die Informationen von mehreren Stellen in Beziehung setzen.

Im überarbeiteten neuen SIR Workspacebietet die **Untersuchungs** -Canvas (Registerkarte) alle erforderlichen Informationen, die logisch an einem Ort gruppiert sind, damit der Analyst die Untersuchung durchführen kann.

### Erkunden Sie das Untersuchungs-Canvas

Das Hauptziel der Untersuchungs-Canvas besteht darin, die erforderlichen Security Incident-Daten an einem gemeinsamen Ort darzustellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Innerhalb von SIR Workspacekonzentriert sich die Untersuchung von Security Incidents hauptsächlich auf einige wichtige Einstiegspunkte.

Im Folgenden sind einige wichtige Einstiegspunkte aufgeführt, die für Sicherheitsanalysten im Basissystem bereitgestellt werden:

- Zugehörige erkennbare Elemente
- Configuration Items
- Betroffene Benutzer
- Zugeordnete Phishing-E-Mails
- E-Mail-Suche

Sie können die oben genannten Einstiegspunkte auch konfigurieren, indem Sie die Einstiegspunkte nach Bedarf hinzufügen, ändern oder entfernen. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung.

Auf der Registerkarte „ **Untersuchung** “ fungiert die Einstiegspunkttabelle als übergeordnete Tabelle. Alle Tabellen, die die Ergebnisse einer für die übergeordnete Tabelle ausgeführten Orchestration-Aktion enthalten, werden innerhalb des Einstiegspunkts als untergeordnete Tabelle dargestellt.

Zum Beispiel ist für den Einstiegspunkt **Zugeordneteerkennbare Elemente** die Tabelle „Erkennbare Elemente zuordnen“ die übergeordnete Tabelle, und andere Tabellen wie Ergebnisse der Bedrohungssuche, Ergebnisse der Sandbox-Übermittlung usw. sind die untergeordneten Tabellen.

Der Sicherheitsanalyst kann alle Orchestration-Aktionen in der Tabelle „Zugeordnete erkennbare Elemente“ ausführen und alle zugehörigen Informationen auf derselben Seite anzeigen, ohne zwischen mehreren Stellen navigieren zu müssen.

**Hinweis:**
Wenn ein Benutzer auf der **Übersichtsseite** auf die interaktiven Diagramme klickt, z. B. auf schädliche erkennbare Elemente, wird der Benutzer zur gefilterten Ansicht der schädlichen erkennbaren Elemente innerhalb der Untersuchungs-Canvas weitergeleitet. Alternativ kann der Benutzer die Untersuchung direkt starten, indem er zur Untersuchungs-Canvas navigiert, die alle Daten enthält.

Die Liste der untergeordneten Tabellen unter einem Einstiegspunkt ist ebenfalls konfigurierbar. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung.

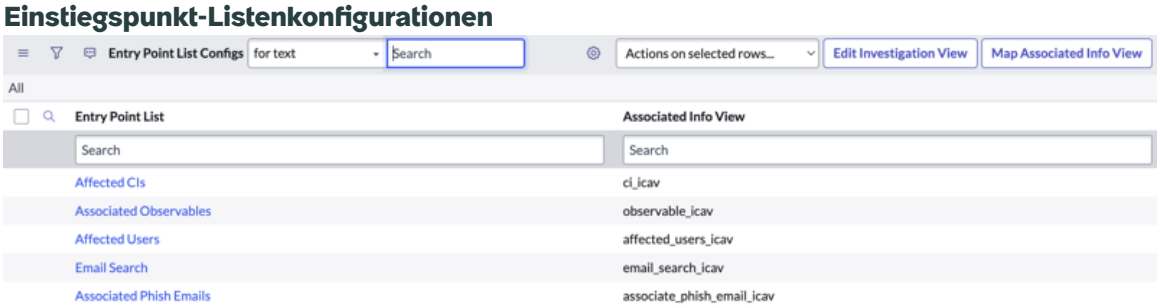
Im Folgenden finden Sie ein detailliertes Beispiel für einen Einstiegspunkt (zugeordnetes erkennbares Element), der im Basissystem konfiguriert und bereitgestellt wird:

1. Wählen Sie in der Dropdown-Liste den Einstiegspunkt **Zugeordnete erkennbare Elemente** aus.

   Hier ist die übergeordnete Tabelle auch **Zugeordnetes erkennbares Element**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




2. Wählen Sie ein oder mehrere erkennbare Elemente aus der übergeordneten Tabelle aus.
3. Führen Sie die gewünschte Fähigkeit aus.

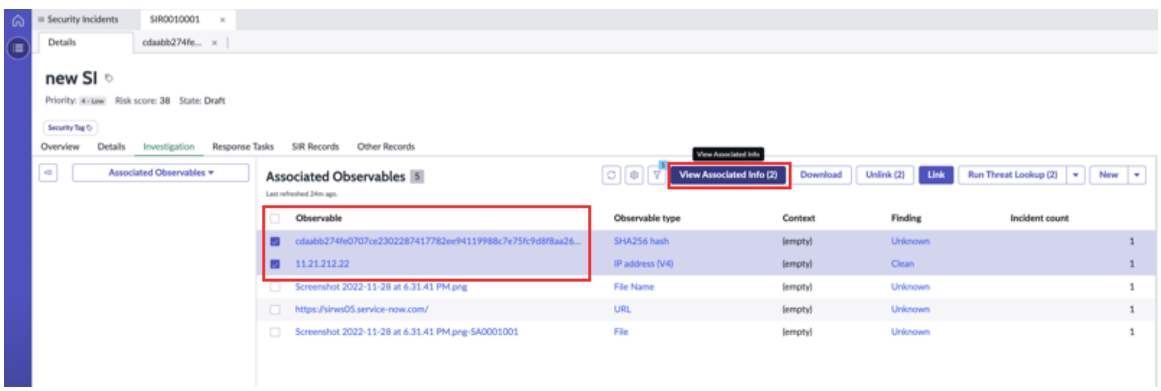
   Wählen Sie beispielsweise **Bedrohungssuche ausführen** aus, um die Ergebnisse der Bedrohungssuche für ein ausgewähltes erkennbares Element abzurufen.

   **Hinweis:**
   Wenn eine entsprechende Aktion für erkennbare Elemente ausgeführt wird, wird der Prozess im Back-End ausgeführt, und die Ergebnisse werden unter der Liste der erkennbaren Elemente angezeigt.

4. Klicken Sie auf **Zugehörige Informationen** anzeigen, um die Ergebnisse der erkennbaren Elemente anzuzeigen. Die Ergebnisse werden auf derselben Seite angezeigt.

   **Hinweis:**
   Sie können die Ergebnisse anzeigen, indem Sie nach Ergebnissen filtern. Wählen Sie entweder **Alle Ergebnisse** oder **Neueste Ergebnisse**aus, je nachdem, welche Ansicht die gewünschte ist. Standardmäßig werden die neuesten Ergebnisse angezeigt. Wenn mehrere Implementierungen (von Integrationen) vorhanden sind, werden die neuesten Ergebnisse pro Implementierung angezeigt.

   Darüber hinaus können Sie die Ergebnisse **nach zugeordneten zugehörigen Listen** filtern, bei denen es sich um die Ergebnisse der untergeordneten Tabelle handelt. Standardmäßig werden alle konfigurierten zugehörigen Listen der untergeordneten Tabelle angezeigt. Weitere Informationen finden Sie unter Konfigurieren Sie die SI-Entwurfszeituntersuchung. Sie können jedoch nur die untergeordneten Tabellen auswählen, die erforderlich sind.

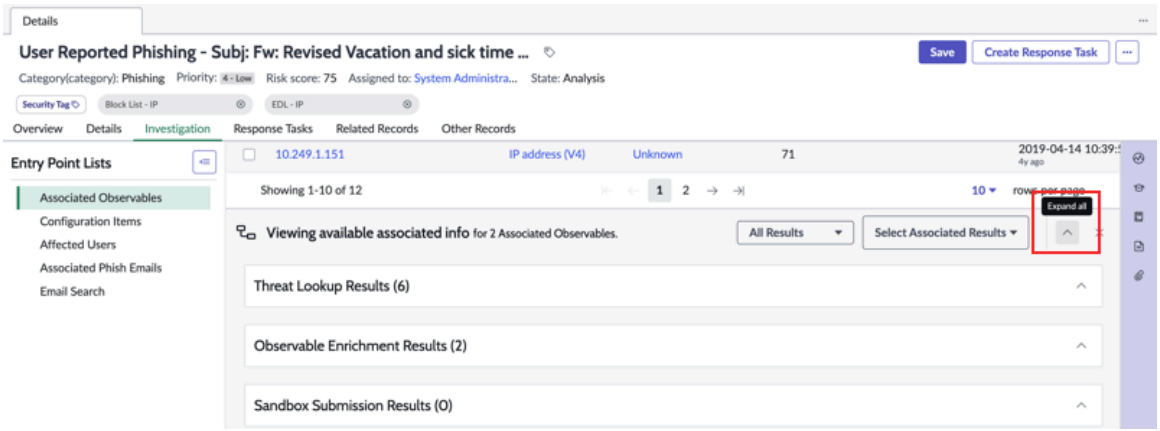



5. Durch Klicken auf **Zugehörige Informationen** anzeigen können Sie alle zugeordneten untergeordneten Tabellendaten an einem Ort anzeigen. Sie können jedoch die Ansicht der zugehörigen Listen schließen, indem Sie auf die Schaltfläche **Ansicht** schließen klicken. Sobald Sie die Ansicht geschlossen haben, können Sie nur die übergeordnete Tabelle der erkennbaren Elemente wie zuvor anzeigen.

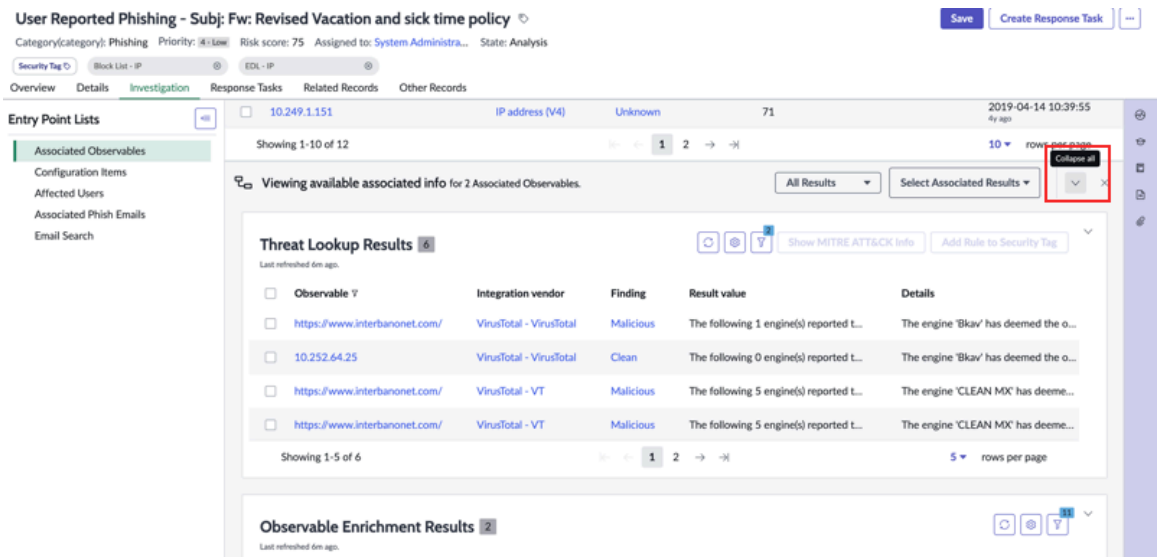


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie in der Ergebnistabelle **Verfügbare zugeordnete Informationen** anzeigen auf das Symbol **Alle** nach oben erweitern, um alle untergeordneten Tabellendaten der zugehörigen Listen zu erweitern.



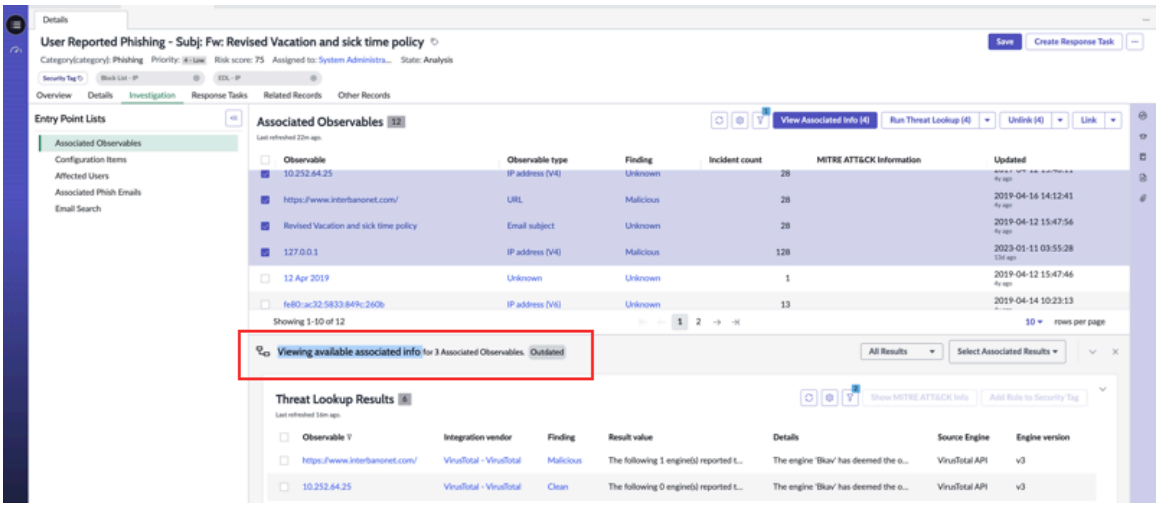

7. Klicken Sie auf das Symbol **Alle** nach unten reduzieren, um alle untergeordneten Tabellendaten der zugehörigen Listen zu reduzieren.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Banner über dem zugeordneten Infoabschnitt, der alle untergeordneten Tabellendaten enthält, zeigt an, wie viele zugehörige Informationen zu erkennbaren Elementen dem Benutzer angezeigt werden. Wenn Sie beispielsweise anfänglich zwei erkennbare Elemente auswählen und auf Zugehörige Informationen anzeigen **klicken**, wird im Banner Folgendes **angezeigt: Verfügbare zugeordnete Informationen für 2 zugeordnete erkennbare Elemente werden angezeigt.**. Wenn Sie beispielsweise ein anderes erkennbares Element auswählen, wird im Banner darauf hingewiesen, dass die Informationen veraltet sind (Screenshot unten). Sie müssen erneut auf **Zugehörige Informationen anzeigen** klicken, um die neuesten Daten zu erhalten.




Wenn Sie zusätzlich zu der obigen umfassenden Ansicht der den erkennbaren Elemente zugeordneten Informationen weitere Informationen zu einem Datensatz in der übergeordneten Tabelle anzeigen möchten, klicken Sie auf das erkennbare Element. Das Datensatzformular der übergeordneten Tabelle wird auf einer anderen Registerkarte mit einer detaillierteren Ansicht der geöffnet ausgewählten Datensatz. Alle zugeordneten untergeordneten Tabellendaten dieses bestimmten ausgewählten Datensatzes werden auch im Abschnitt **Zugeordnete Informationen** angezeigt.

Im zugehörigen Infoabschnitt werden jedoch nur die neuesten Ergebnisse der untergeordneten Tabelle angezeigt, wie im Untersuchungs-Canvas im schreibgeschützten Modus zu sehen ist. In dieser Ansicht sind keine Aktionen möglich. Die Formularseite der untergeordneten Tabelle kann in einer neuen Registerkarte geöffnet werden, die die voll funktionsfähige Seite mit Aktionen (falls vorhanden) darstellt.

Sie können mithilfe der Dropdown-Liste zwischen den verschiedenen Tabellen wechseln. Sie können auch jedes Formular unter dem zugehörigen Infoabschnitt erweitern oder reduzieren.

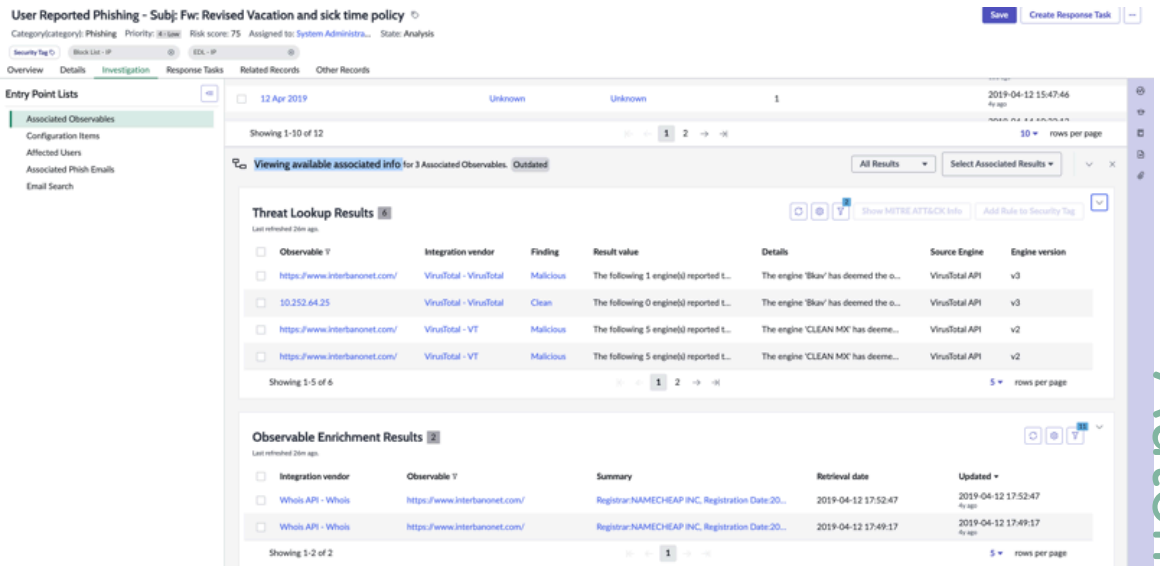
Auf der **Formularseite** „Erkennbares Element“ (Datensatzformularseite der übergeordneten Tabelle) können Sie bestimmte Aktionen ausführen, sofern verfügbar. Wenn Sie eine Aktion ausführen, können Sie im zugehörigen Infobanner auf Aktualisieren klicken, um die Daten zu aktualisieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Alle** erweitern, um alle untergeordneten Tabellen der zugehörigen Listen zu erweitern. Standardmäßig werden alle untergeordneten Elemente erweitert.

**Erweiterte Ansicht der erkennbaren Elemente**




### Zugehörige Informationen

Konfigurieren Sie die SI-Entwurfszeituntersuchung

## Einheitliches Experience-Framework für Integrationen, die auf dem Fähigkeits-Framework basieren

In der klassischen Benutzeroberfläche ist die Experience bei der Ausführung von Orchestration-Aktivitäten wie der Ausführung der Bedrohungssuche, der Sichtungssuche usw. unzusammenhängend. Jede Fähigkeit hat ihre eigene Experience bei der Ausführung. Im neuen Arbeitsbereich gibt es eine einheitliche Experience für alle Fähigkeiten.

Die einheitliche Experience gilt nur für die Integrationen und Orchestration-Aktivitäten, die in das Fähigkeits-Framework fallen. Es kann Aktionen geben, die für die Integration spezifisch sind, z. B. Indikatoren in Microsoft Defender erstellen. Diese Aktionen haben je nach Anwendungsfall eine eigene Experience.

Das neue Framework besteht aus modalen Bildschirmen mit drei Schritten, wie unten erläutert.

1. **Implementierungen**: Der erste Schritt umfasst die Auswahl einer oder mehrerer Implementierungen, die für die ausgewählte Fähigkeit vorhanden sind.

   Wenn der Analyst beispielsweise auf **Bedrohungssuche**ausführen klickt, kann der Analyst eine oder mehrere Implementierungen auswählen, die für die **Fähigkeit „Bedrohungssuche ausführen“**vorhanden sind.

   Jede Implementierung enthält die Details der Integrationsquelle. Weitere Informationen finden Sie in der folgenden Tabelle. Zusätzliche Informationen werden auch für jede Implementierung angezeigt.

   Zusätzliche Informationen können beispielsweise Informationen zu Filtern, Typen der unterstützten erkennbaren Elemente usw. enthalten. Die zusätzlichen Informationen können nach Bedarf konfiguriert werden. Weitere Informationen finden Sie unter technisches Konfigurationsverfahren für UX-Framework.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

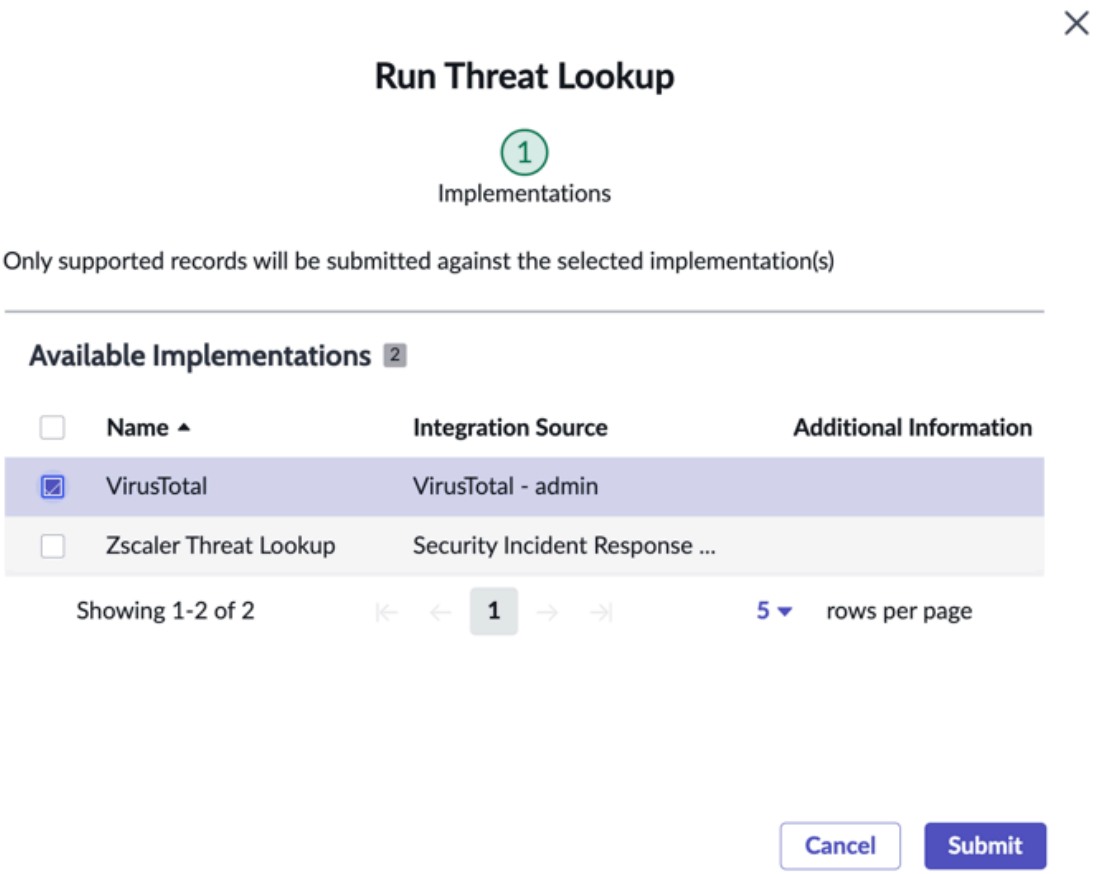
### Modales Element für einheitliches Implementierungs-Framework

| Implementierung | Beschreibung |
|---|---|
| Name | Name der Implementierung. |
| Integrationsquelle | Die Quelle der Implementierung, z. B. die verwendete Konfiguration. |
| Zusätzliche Information | Diese Spalte erfasst die statischen Informationen, die dem Sicherheitsanalysten mehr Kontext für die ausgewählten Implementierungen hinzufügen, um mit einer Aktion fortzufahren. Zum Beispiel Supportbarkeit oder gefilterte Informationen. Wenn eine Implementierung nur einen bestimmten Typ von erkennbaren Elementen unterstützt, z. B. Domäne oder URL, können Sie diese zusätzlichen Informationen hier in dieser Spalte hinzufügen, um dem Benutzer den Kontext bereitzustellen.<br><br>**Hinweis:**<br>Das UI-Framework würde im Grunde die Auswahl jeder Art von Implementierung und jeder Art von erkennbaren Elementen ermöglichen. Während der Übermittlung übernehmen die vorhandenen Basissystemintegrationen, die im Lieferumfang enthalten sind, die Filterung im Back-End und übermitteln nur den unterstützten Typ von erkennbaren Elementen. Die restlichen Datensätze, die nicht mit der Unterstützbarkeit übereinstimmen, werden ignoriert. Daher wird eine UI-Informationsmeldung angezeigt, während Sie die Fähigkeit auswählen: **Nur unterstützte Datensätze werden für die ausgewählte(n) Implementierung(en) übermittelt.** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bildschirm 1: Implementierung(en)**

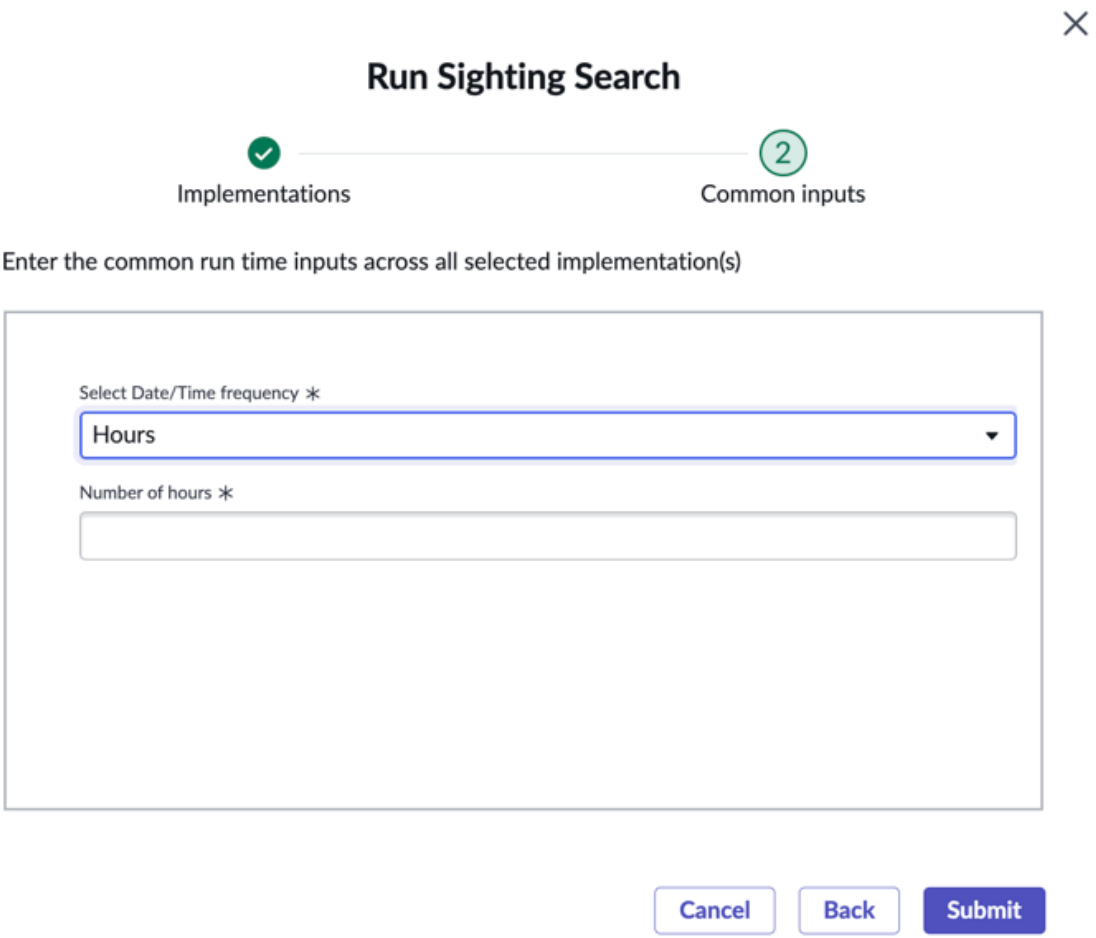



2. **Allgemeine Eingaben**: Fügen Sie allgemeine Eingaben für die ausgewählten Implementierungen oder für alle ausgewählten zutreffenden Implementierungen hinzu. Dies ist der Bildschirm 2 Ihrer Implementierung. Zum Beispiel verfügt ab sofort nur die **Sichtungssuche** über den gemeinsamen Eingabebildschirm. Diese Implementierung ist eine Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 2 (allgemeine Eingaben).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bildschirm 1 + Bildschirm 2**



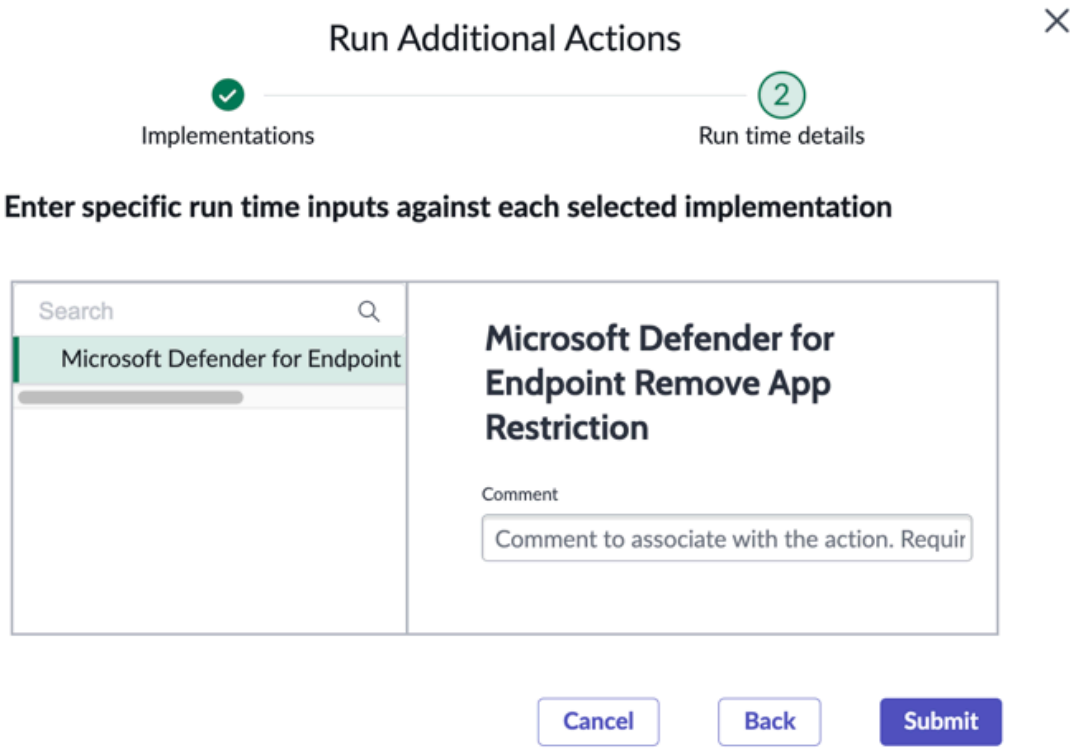

3. **Ausführungszeitdetails**: Fügen Sie bestimmte Ausführungszeiteingaben für die ausgewählten Implementierungen hinzu, die sich voneinander unterscheiden. Dies ist

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Bildschirm 3 Ihrer Implementierung. Diese Implementierung ist eine Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 3 (spezifische Laufzeiteingaben).

**Bestimmte Eingaben**




**Hinweis:**
Nicht alle drei Schritte sind immer erforderlich. Abhängig von der Fähigkeit und der Art der erforderlichen Eingaben sind der Schritt „Laufzeitdetails“ und der Schritt „Allgemeine Eingaben“ sichtbar.

### Unified Experience-Funktionen und modale Bildschirme

In der folgenden Tabelle werden die Fähigkeiten und die entsprechenden Bildschirme beschrieben.

### Beispiel für eine einheitliche Experience

In diesem Beispiel werden die Fähigkeiten von Unified Experience Framework veranschaulicht.

### Beispiel 1: Wählen Sie Implementierungen aus: Bedrohungssuche

Das folgende Beispiel zeigt die Implementierung(en).

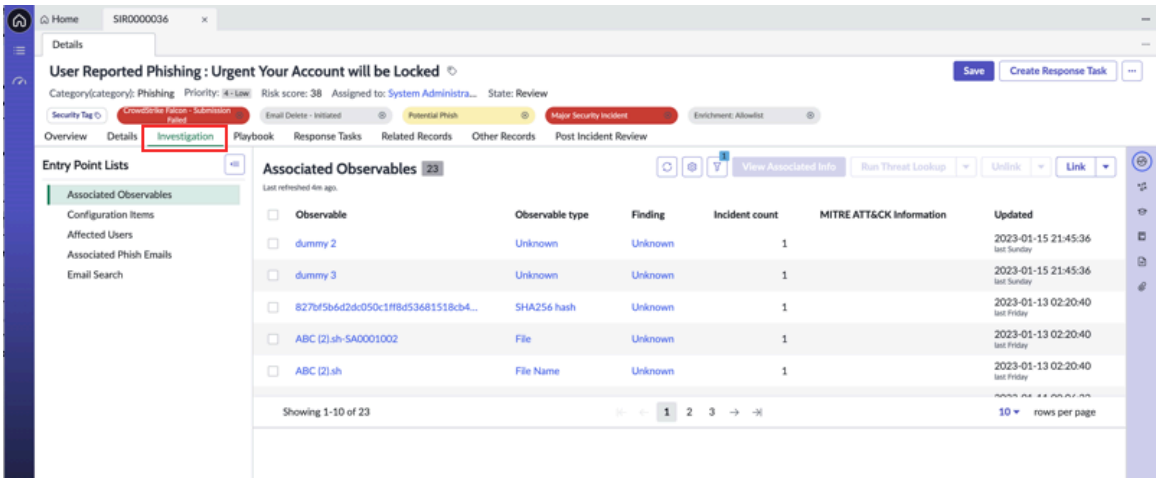
## Beispiel 1: Nur Bildschirm 1: Bedrohungssuche

Sie können die Aktion „ **Bedrohungssuche** ausführen“ im Zusammenhang mit Integrationsfähigkeiten über die Registerkarte „ **Untersuchung** “ im SIR Workspaceausführen.

1. Navigieren Sie auf der Registerkarte „ **Untersuchung** “ zum Abschnitt „ **Einstiegspunktlisten** “, der links auf der Seite angezeigt wird.
2. Wählen Sie einen beliebigen Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Sie können auch zur Registerkarte „ **Zugehörige Datensätze** “ im Arbeitsbereich navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

**Die Bedrohungssuche** ist eines der Beispiele, in dem detailliert beschrieben wird, wie die Integrationen durchgeführt werden.

### Wählen Sie Implementierungen aus

Wählen Sie eine oder mehrere Implementierungen nach Bedarf aus.

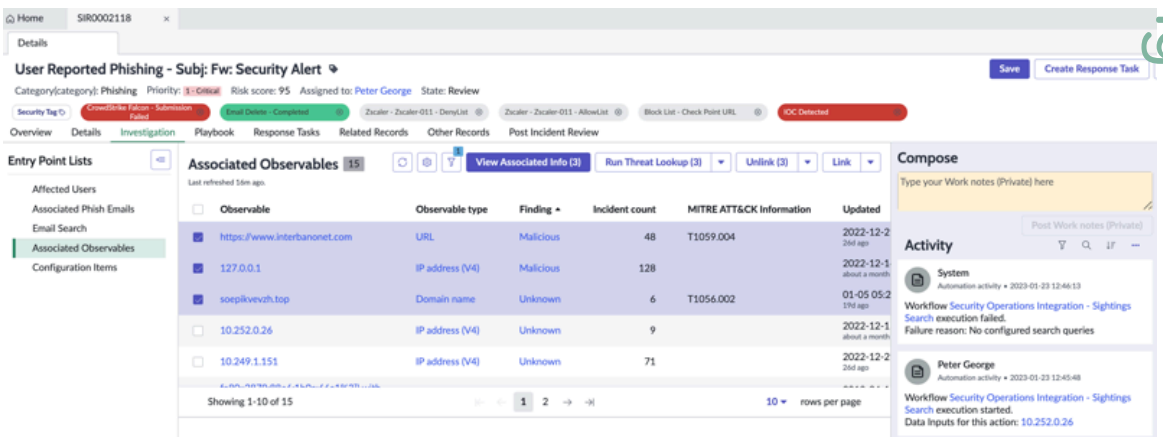
### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nach der Auswahl werden nur die unterstützten Datensätze für die ausgewählte(n) Implementierung(en) übermittelt.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Untersuchung** des Arbeitsbereichs.
   Die Registerkarte „Untersuchung“ mit den Einstiegspunktlisten wird angezeigt.



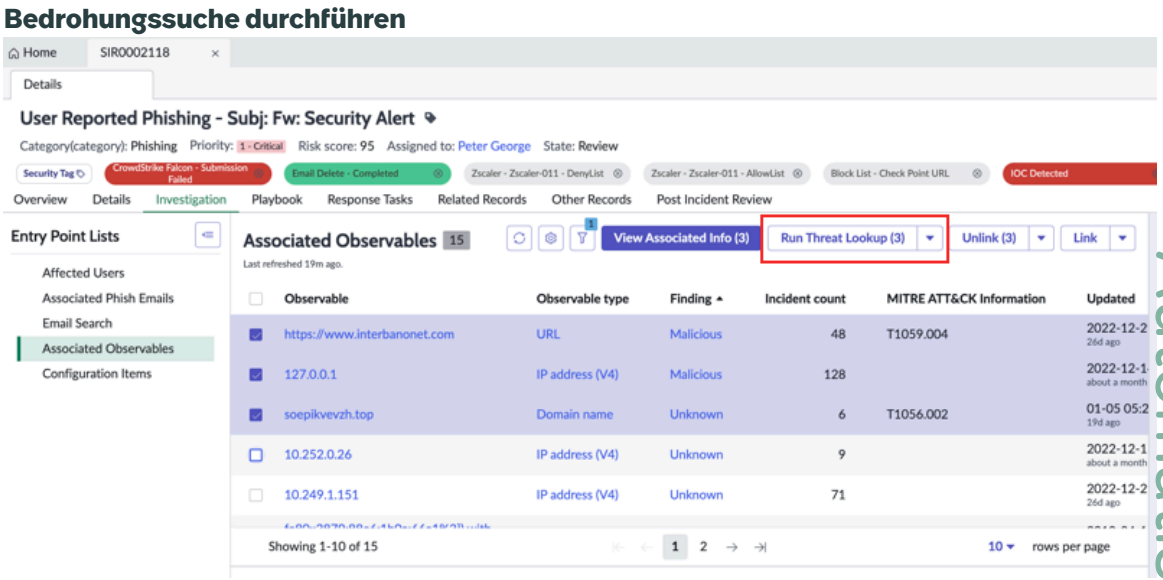

4. Wählen Sie das zugeordnete erkennbare Element aus den Einstiegspunktlisten aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie beispielsweise **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze für erkennbare Elemente werden angezeigt.

**Hinweis:**
Sie können eine Implementierung auswählen, um eine Suche für die ausgewählten erkennbaren Elemente durchzuführen, oder Sie können die Suche durchführen, indem Sie alle Implementierungen auswählen.




5. Aktivieren Sie das Kontrollkästchen eines erkennbaren Elements, für das Sie die Bedrohungssuche durchführen möchten.
6. Navigieren Sie zur Dropdown-Liste Aktionen für zugehörige Listen, die oben auf der Seite „Zugehörige Listen“ angezeigt wird.
7. Wählen **Sie Bedrohungssuche** ausführen aus, um die Aktion für Integrationsfunktionen im Zusammenhang mit Bedrohungsinformationen auszuführen.

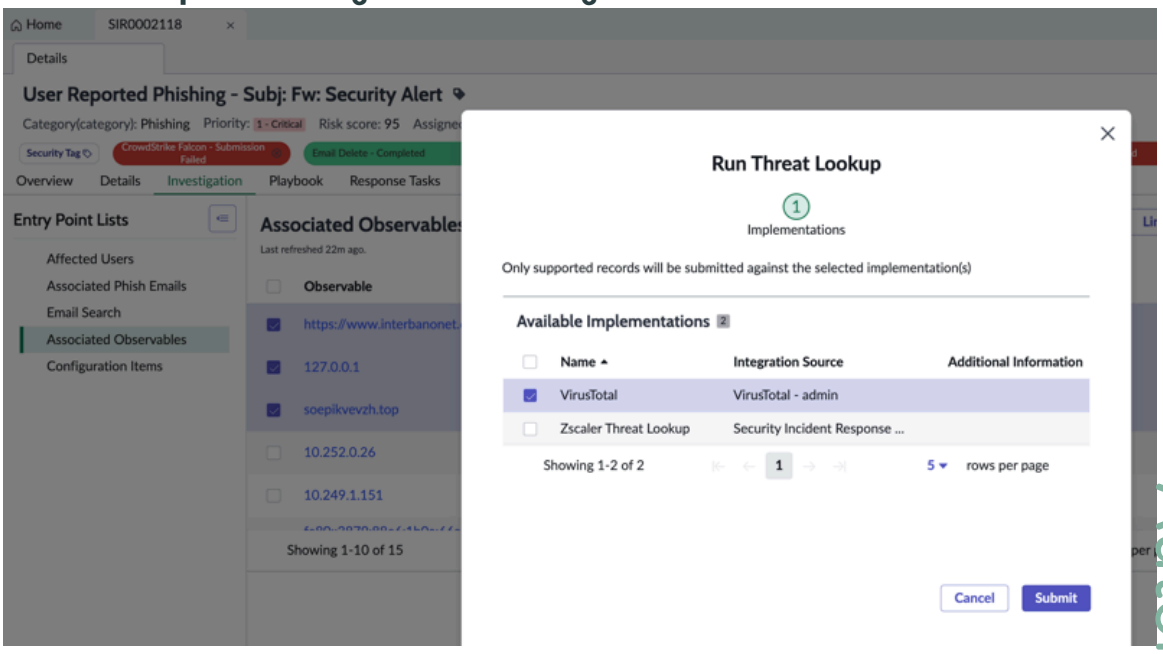
**Hinweis:**
Die Fähigkeit „Bedrohungssuchen ausführen“ führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsbedrohungen zugeordnet sind.

Der modale Bildschirm **„Implementierungen der Bedrohungssuche ausführen“** wird angezeigt.



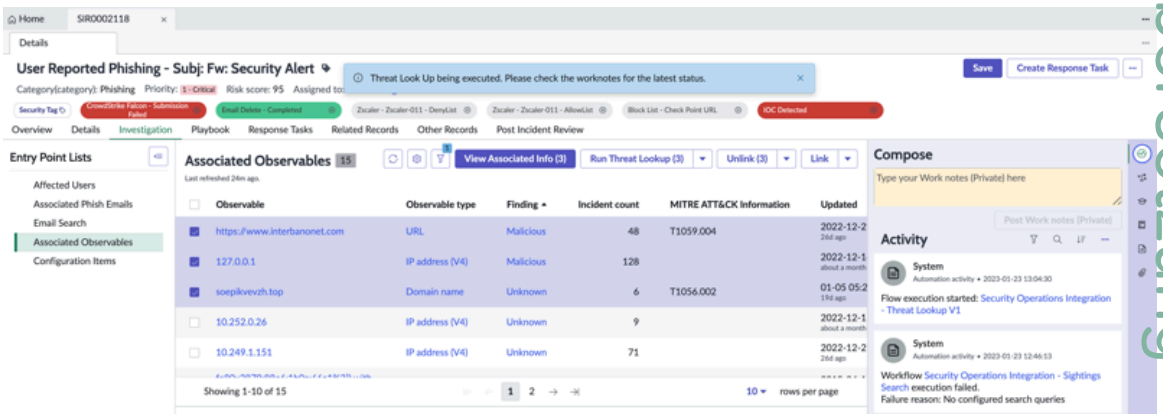
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Führen Sie Implementierungen der Bedrohungssuche aus




8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.

9. Klicken Sie auf **Absenden**.
   Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Suche ausgeführt wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen **Listenabschnitt „Ergebnisse der Bedrohungssuche** “ angezeigt. Außerdem wird die entsprechende Implementierungsaktivität im Abschnitt „ **Aktivität** “ angezeigt. Es werden zwei Aktivitäten angezeigt: eine, wenn die Implementierungsausführung gestartet wird, und eine zweite, wenn die Ausführung abgeschlossen ist.




**Hinweis:**
Die zugehörigen Listen für **Bedrohungsinformationen** wie die zugehörigen zugehörigen Listen für erkennbare Elemente werden im Abschnitt „ **Ergebnisse der Bedrohungssuche** “ angezeigt, und die zugehörigen Listen „ **Sichtungssuche** “ werden im Abschnitt „ **Sichtungssuchergebnisse** “ unter den zugehörigen Datensätzen angezeigt.

### Beispiel 2: Allgemeine Eingaben: Sichtungssuche

Das folgende Beispiel zeigt die Aktion für allgemeine Eingabefunktionen.

Sie können die Aktion „ **Sichtungssuche** ausführen“ im Zusammenhang mit Integrationsfähigkeiten über die Registerkarte „ **Untersuchung** “ in SIR Workspaceausführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren Sie auf der Registerkarte „ **Untersuchung** “ zum Abschnitt „ **Einstiegspunktlisten** “, der links auf der Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.

**Hinweis:**
Sie können auch zur Registerkarte „ **Zugehörige Datensätze** “ im Arbeitsbereich navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

### Fügen Sie einer Implementierung allgemeine Eingaben hinzu

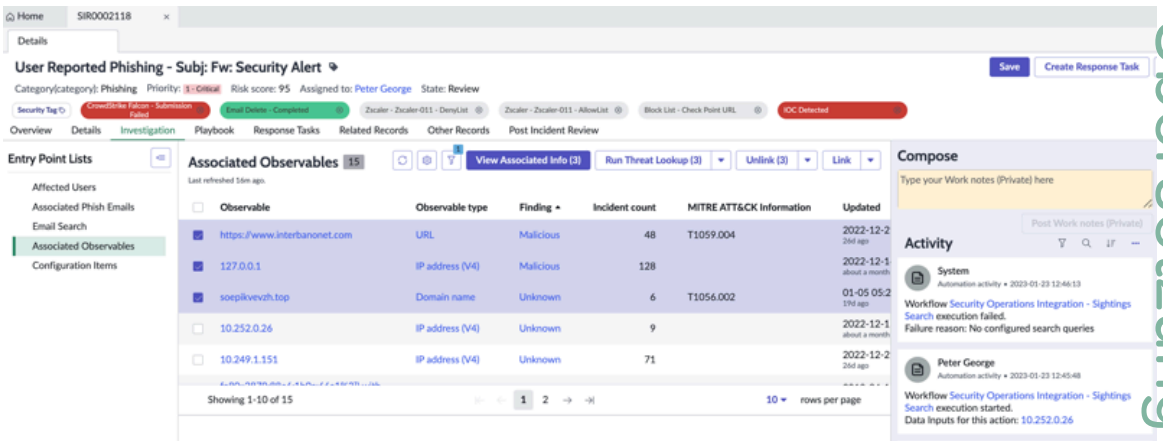
Fügen Sie allgemeine Laufzeiteingaben hinzu, die für alle ausgewählten Implementierungen gelten.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nach der Auswahl werden nur die unterstützten Datensätze für die ausgewählte(n) Implementierung(en) übermittelt.

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Untersuchung** des Arbeitsbereichs.
   Die Registerkarte „Untersuchung“ mit den Einstiegspunktlisten wird angezeigt.



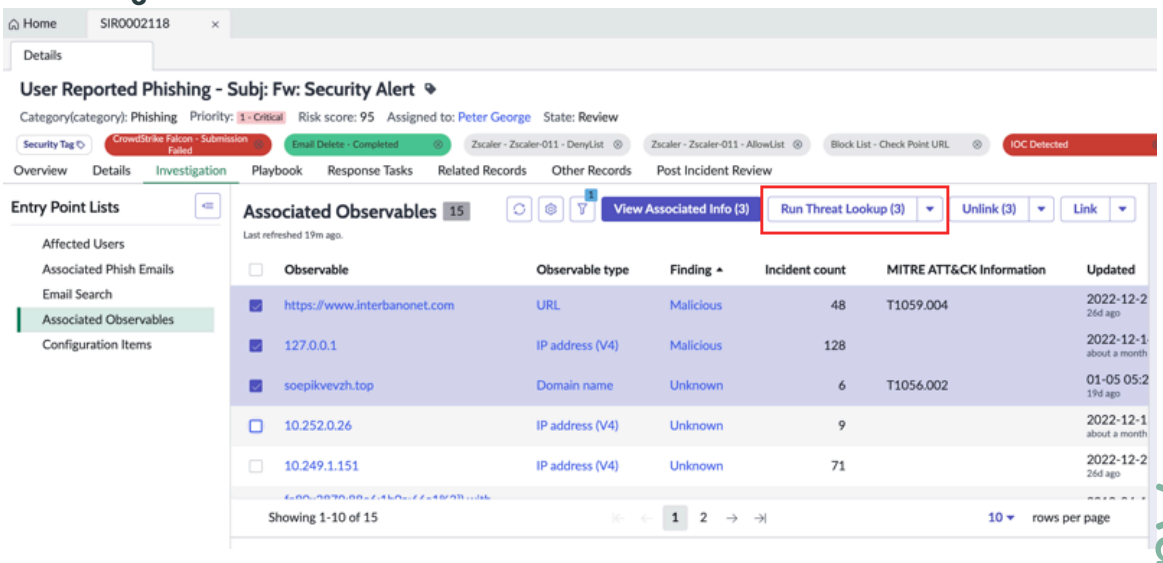

4. Wählen Sie das zugeordnete erkennbare Element aus den Einstiegspunktlisten aus.
   Wählen Sie beispielsweise **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze für erkennbare Elemente werden angezeigt.

**Hinweis:**
Sie können eine Implementierung auswählen, um eine Sichtungssuche für die ausgewählten erkennbaren Elemente durchzuführen, oder mehrere Implementierungen auswählen.



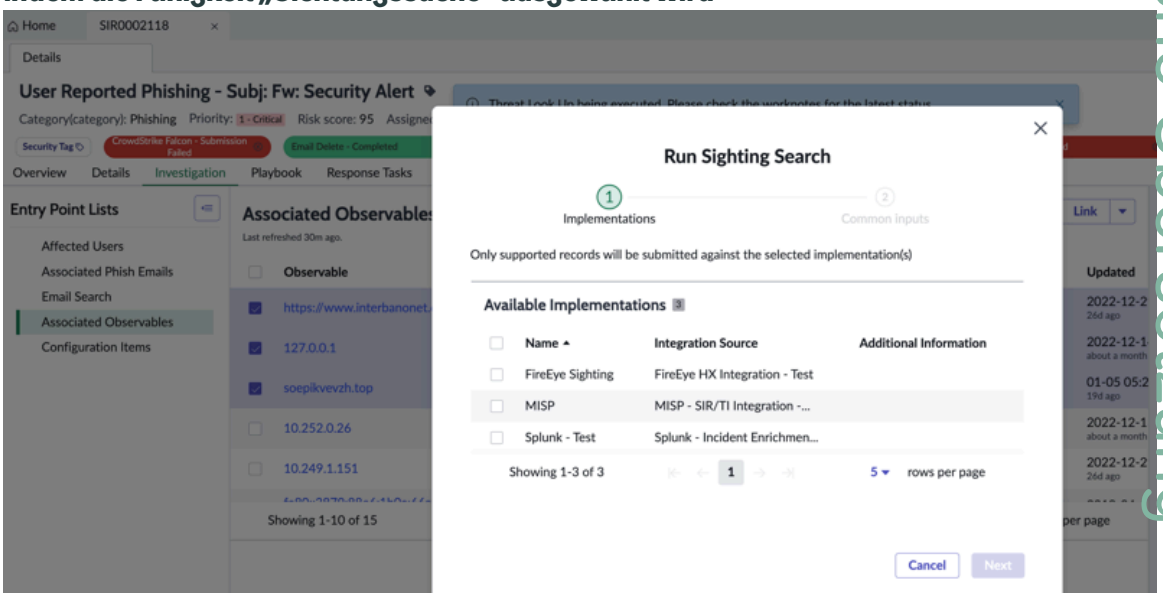
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Bedrohungssuche durchführen




5. Aktivieren Sie das Kontrollkästchen eines erkennbaren Elements, für das Sie die Bedrohungssuche durchführen möchten.
6. Wählen **Sie Sichtungssuche** ausführen aus, um eine E-Mail-Suche durchzuführen.
   Das Dialogfeld „Sichtungssuchimplementierungen ausführen“ wird angezeigt.

### Ein Beispiel, das zeigt, wie allgemeine Laufzeiteingaben hinzugefügt werden, indem die Fähigkeit „Sichtungssuche“ ausgewählt wird

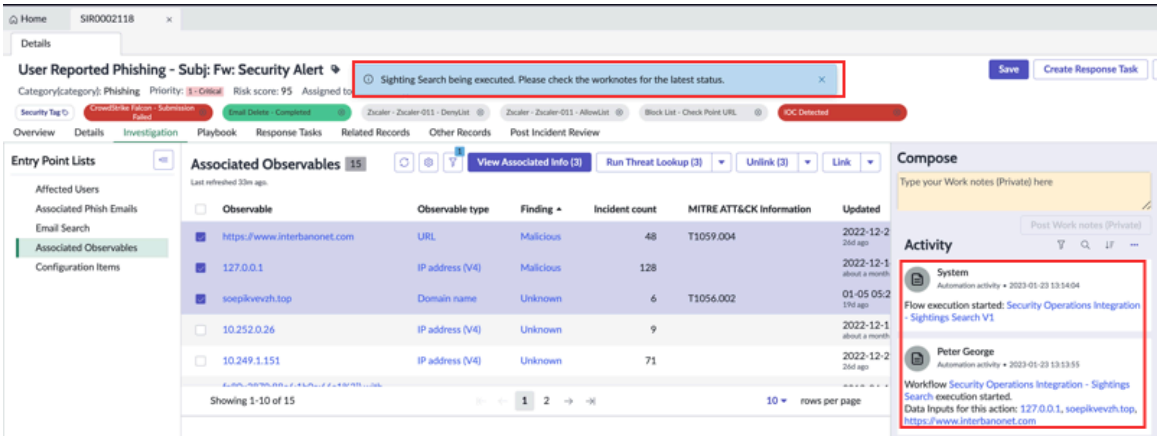



7. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.
8. Klicken Sie auf **Next (Weiter)**.
   Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen Listenabschnitt „ **Sichtungssuche** “ angezeigt. Außerdem wird die jeweilige Implementierungsaktivität im Abschnitt „Aktivität“ angezeigt. Es werden zwei Aktivitäten angezeigt: eine, wenn die Implementierungsausführung gestartet wird, und eine zweite, wenn die Ausführung abgeschlossen ist.
9. Wählen Sie den allgemeinen Eingabewert für die Laufzeit aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **Absenden**.




Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im zugehörigen Listenabschnitt „ **Sichtungssuchergebnisse** “ angezeigt. Außerdem wird der Verarbeitungsstatus der jeweiligen Implementierungsaktivität im Abschnitt „ **Aktivität** “ angezeigt.

### Beispiel 3: Bestimmte Eingaben für Laufzeitdetails zu einer Implementierung hinzufügen: Zusätzliche Aktionen ausführen

Fügen Sie einer Implementierung bestimmte Eingaben für Laufzeitdetails hinzu, Zusätzliche Aktionen ausführen.

Sie können die Aktion „ **Zusätzliche Aktionen** ausführen“ im Zusammenhang mit Integrationsfähigkeiten über die Registerkarte „ **Untersuchung** “ in SIR Workspaceausführen.

1. Navigieren Sie auf der Registerkarte „ **Untersuchung** “ zum Abschnitt „ **Einstiegspunktlisten** “, der links auf der Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion für die Integrationsfähigkeit aus.

**Hinweis:**
Sie können auch zur Registerkarte „ **Zugehörige Datensätze** “ im Arbeitsbereich navigieren, um die Aktion „Integrationsfunktionen“ auszuführen.

### Fügen Sie einer Implementierung bestimmte Eingaben hinzu

Fügen Sie für jede der ausgewählten Implementierungen nach Bedarf spezifische Laufzeiteingaben hinzu.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

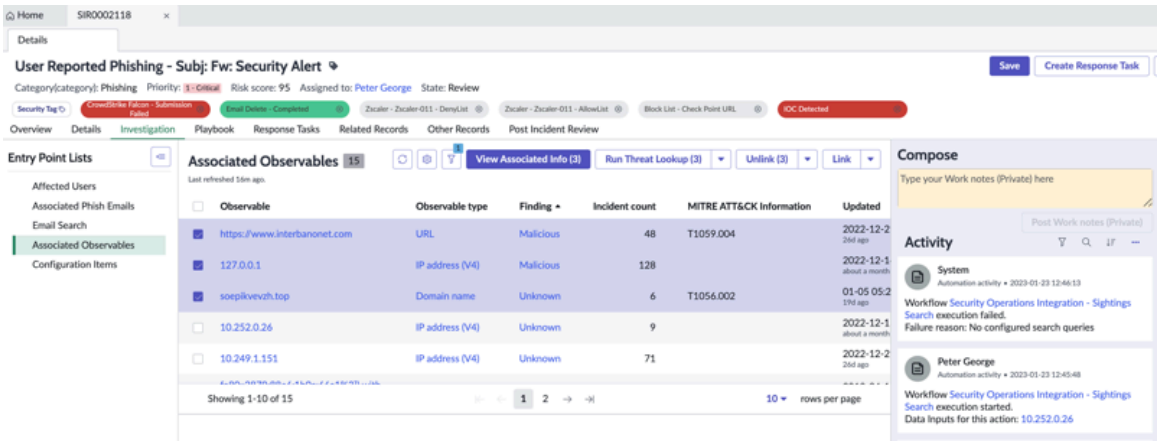
Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nach der Auswahl werden nur die unterstützten Datensätze für die ausgewählte(n) Implementierung(en) übermittelt.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Wechseln Sie zur Registerkarte **Untersuchung** des Arbeitsbereichs.
   Die Registerkarte „Untersuchung“ mit den Einstiegspunktlisten wird angezeigt.

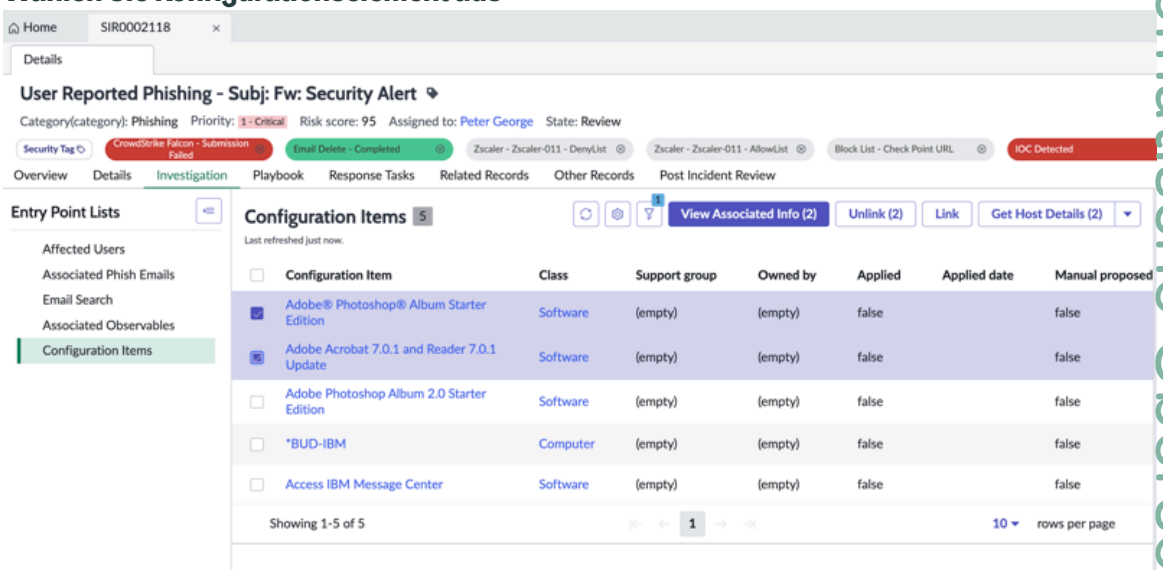


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wählen Sie das Konfigurationselement aus der Einstiegspunktliste aus.
   Wählen Sie beispielsweise die Liste der **Konfigurationselement** -Einstiegspunkte aus. Die entsprechenden Configuration Items-Datensätze werden angezeigt.

**Wählen Sie Konfigurationselement aus**



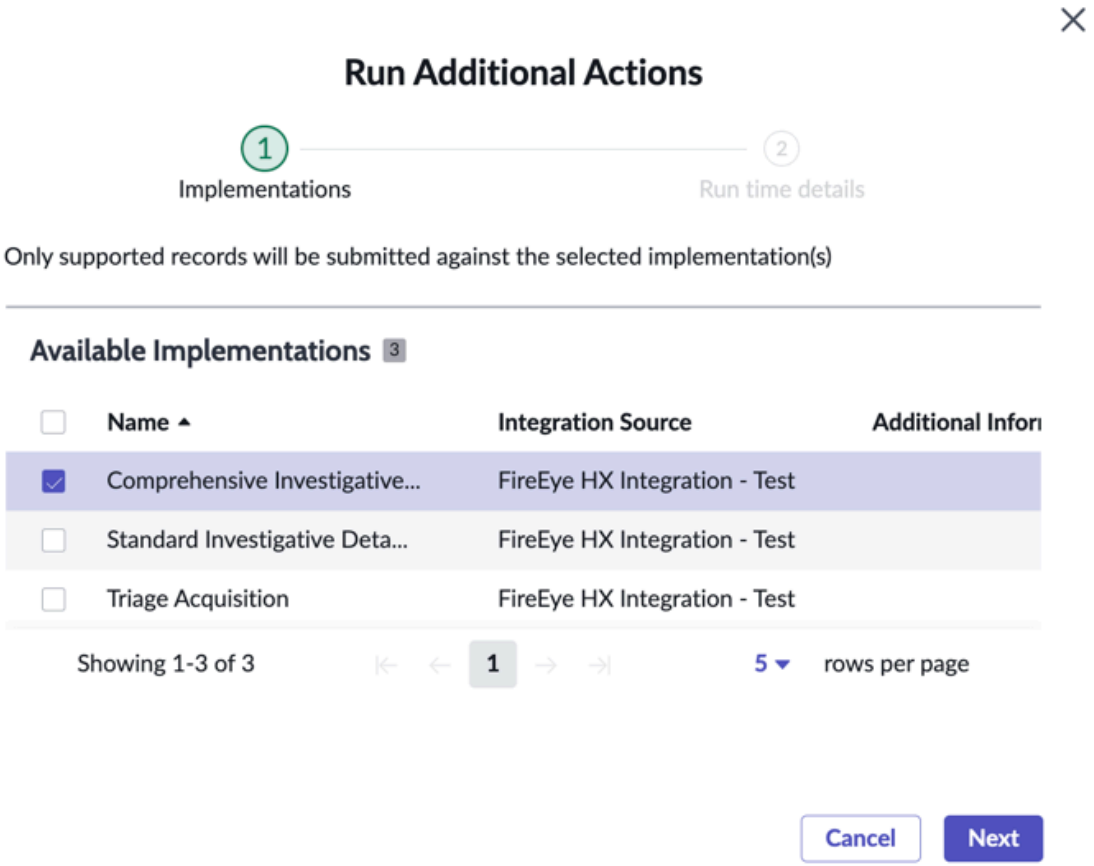

5. Wählen Sie ein beliebiges **Konfigurationselement aus**.
6. Navigieren Sie zur Dropdown-Liste „Zugehörige Listen“, die oben auf der Seite angezeigt wird.
   Für Security Incident-Konfigurationselemente (CIs) enthalten die Dropdown-Listen die folgende Liste von Fähigkeiten-Aktionen. Die aufgelisteten CI-Aktionen erfassen die Ergebnisse und speichern sie als Ergänzungsdaten zu einem Security Incident:
   - Datei abrufen: Diese Fähigkeit führt die Aktion aus, um Dateien mit einem bestimmten Hashwert oder Dateinamen abzurufen.
   - Host isolieren: Diese Fähigkeit schränkt Systemverbindungen zu anderen Geräten ein.
   - Hostdetails abrufen: Mit dieser Funktion werden die Hostdetails, Details der angemeldeten Benutzer und andere Ergänzungsfunktionen abgerufen.
   - Zusätzliche Aktionen ausführen: Diese Fähigkeit führt die zusätzlichen Aktionen aus, die über die Standardaktionen hinausgehen.
   - Netzwerkstatistiken abrufen: Mit dieser Funktion werden die Netzwerkstatistiken für eine betroffene Ressource abgerufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Laufenden Prozess abrufen: Diese Fähigkeit ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (CI) von einem Host ab.
- Angemeldete Benutzer abrufen: Mit dieser Funktion werden die Daten der angemeldeten Benutzer erfasst und mit dem Security Incident verknüpft.

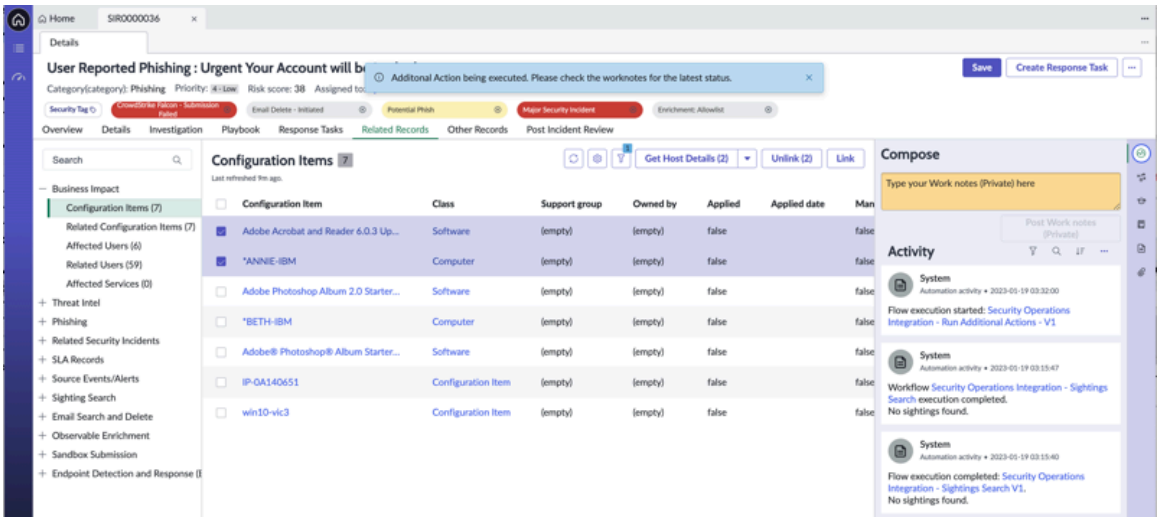
7. Wählen **Sie Zusätzliche Aktionen** ausführen aus, um die Aktion für Integrationsfunktionen im Zusammenhang mit Bedrohungsinformationen auszuführen.
   Das Dialogfeld „Zusätzliche Implementierungen ausführen“ wird angezeigt.
8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.




9. Klicken Sie auf **Next (Weiter)**.
   Sie gelangen nun zum nächsten Schritt, um die Ausführungszeitdetails hinzuzufügen.
10. Geben Sie einen Kommentar ein, der der Aktion zugeordnet werden soll.
11. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Meldung angezeigt, dass die Anforderung „Zusätzliche Aktion“ ausgeführt wird. Außerdem wird der Fortschritt der jeweiligen Implementierungsaktion im Abschnitt „ **Aktivität** “ angezeigt.

**12.** Zeigen Sie die Ergebnisse aus dem zugehörigen Listenabschnitt EDR an.

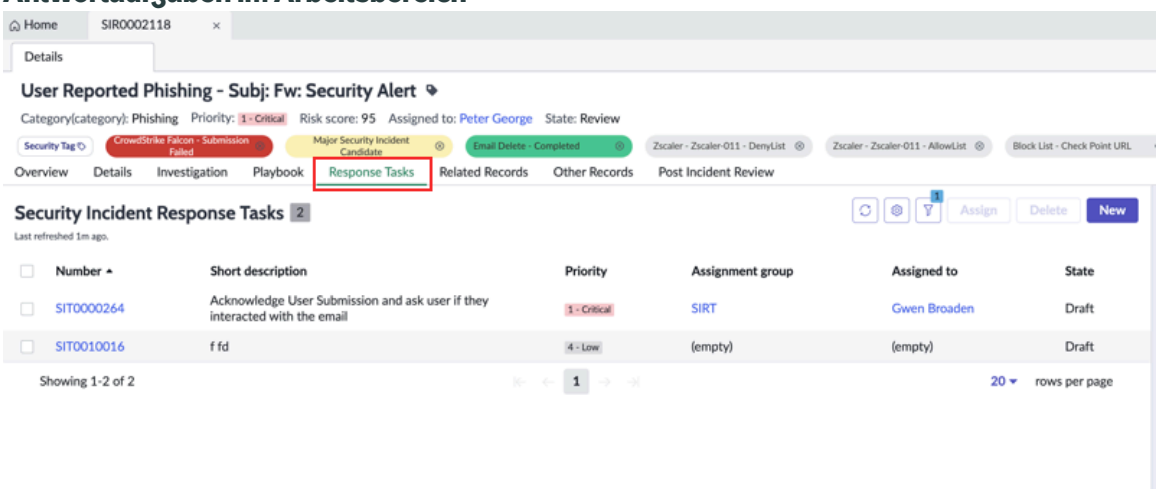
### Security Incident Response-Aufgaben

Alle einem Security Incident zugeordneten Antwortaufgaben werden im Abschnitt „Antwortaufgaben“ angezeigt.

Der Analyst kann:

- Erstellen Sie eine neue Antwortaufgabe
- Antwortaufgaben sich selbst oder anderen zuweisen
- Antwortaufgaben löschen

### Antwortaufgaben im Arbeitsbereich




**Hinweis:**
So nehmen Sie schnelle Änderungen an den Antwortaufgaben vor: Wählen Sie die Antwortaufgabe aus, und eine Liste der Antwortaufgaben wird angezeigt. Wählen Sie den Datensatz aus, nehmen Sie Änderungen vor, und speichern Sie die Antwortaufgabe.

### Erstellen Sie eine Antwortaufgabe

Erstellen Sie Antwortaufgaben, um einzelne Aktionen nachzuverfolgen, die als Reaktion auf das Sicherheitsproblem ausgeführt werden sollen.



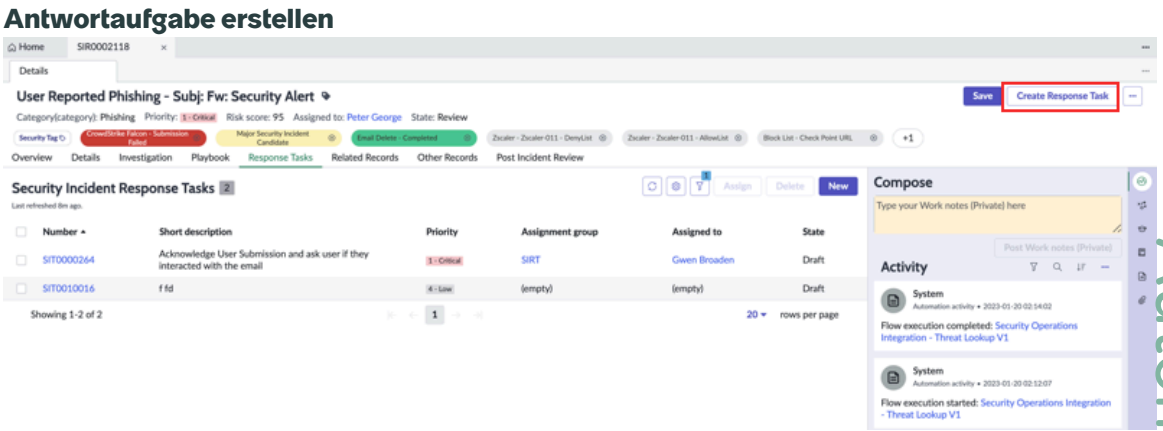
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Klicken Sie in den UI-Aktionen auf **Antwortaufgabe erstellen**.



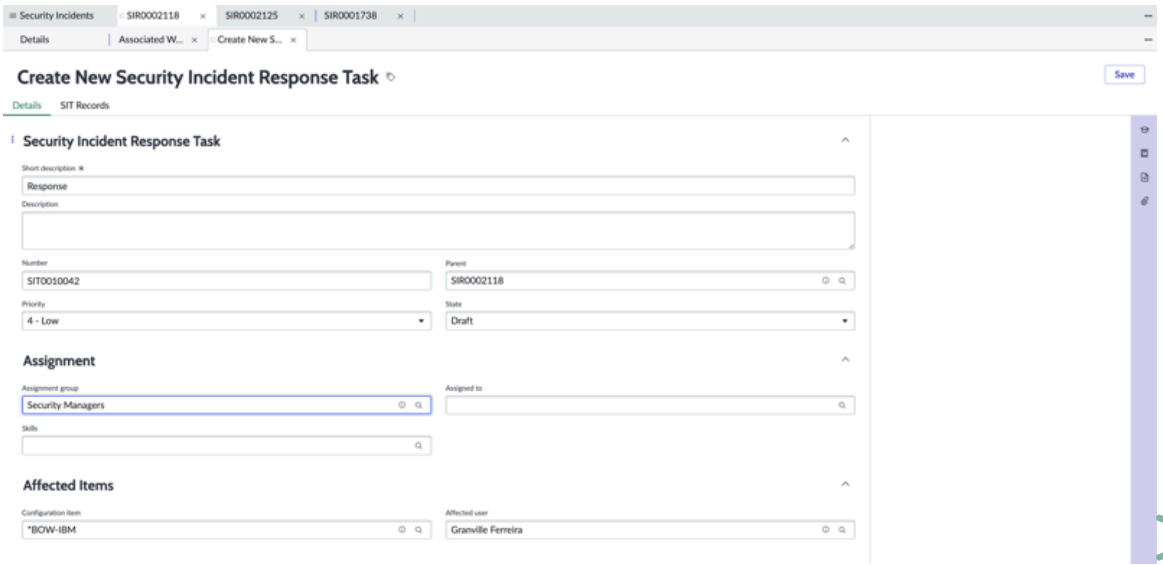

3. Füllen Sie die entsprechenden Felder im Formular aus.

#### Sicherheitsvorfall

| Feld | Beschreibung |
|---|---|
| Kurzbeschreibung | Eine Beschreibung der Aufgabe Security Incident Response. |
| Beschreibung | Eine Beschreibung für die ausgewählte Aufgabe. |
| Nummer | Eindeutige Nummer, die für einen Security Incident automatisch generiert wird. |
| Übergeordnet | Die Nummer des zugehörigen Security Incidents. |
| Priorität | Die Priorität, anhand derer bestimmt wird, wann diese Aufgabe ausgeführt wird. |
| Status | Aktueller Status der Sicherheitsreaktionsaufgabe Standardmäßig lautet der Anfangsstatus **Entwurf**. |
| Zuweisungsgruppe | Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird. |
| Zugewiesen an | Die Person, der die Aufgabe zugewiesen wurde. |
| Kompetenzen | Die zum Ausführen dieser Aufgabe erforderliche Kompetenz. Suchen Sie in der Suche, und wählen Sie die erforderliche Kompetenz aus. |
| Betroffene Elemente | Die vom Sicherheitsproblem betroffenen Elemente. |
| Konfigurationselement | Das vom Sicherheitsproblem betroffene Konfigurationselement. |
| Betroffener Anwender | Die vom Sicherheitsproblem betroffene Person. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



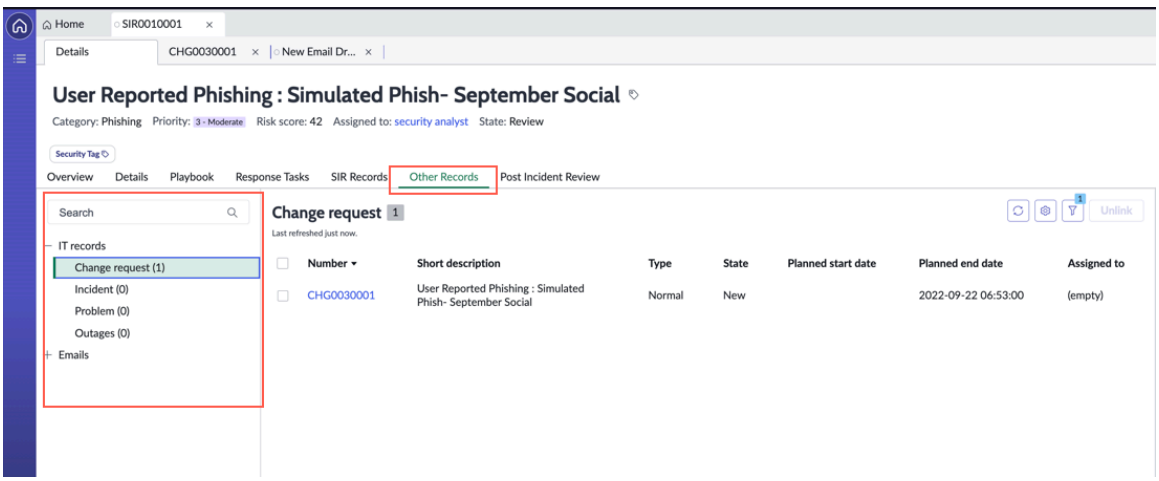

4. Klicken Sie auf **Speichern**.
   Die neue Antwortaufgabe (SIT) wird erstellt.

### Security Incident Response – Sonstige Datensätze

In diesem Abschnitt werden die anderen Datensätze angezeigt, z. B. IT-bezogene Datensätze und E-Mail-Datensätze. Unter den IT-Datensätzen werden Incident, Change-Anforderung, Problem und Ausfälle angezeigt.

Unter E-Mail werden Entwurf, gesendete E-Mails und empfangene E-Mails angezeigt.

### Andere Datensätze




### Incident erstellen

Erstellen Sie einen Incident innerhalb eines Security Incident.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

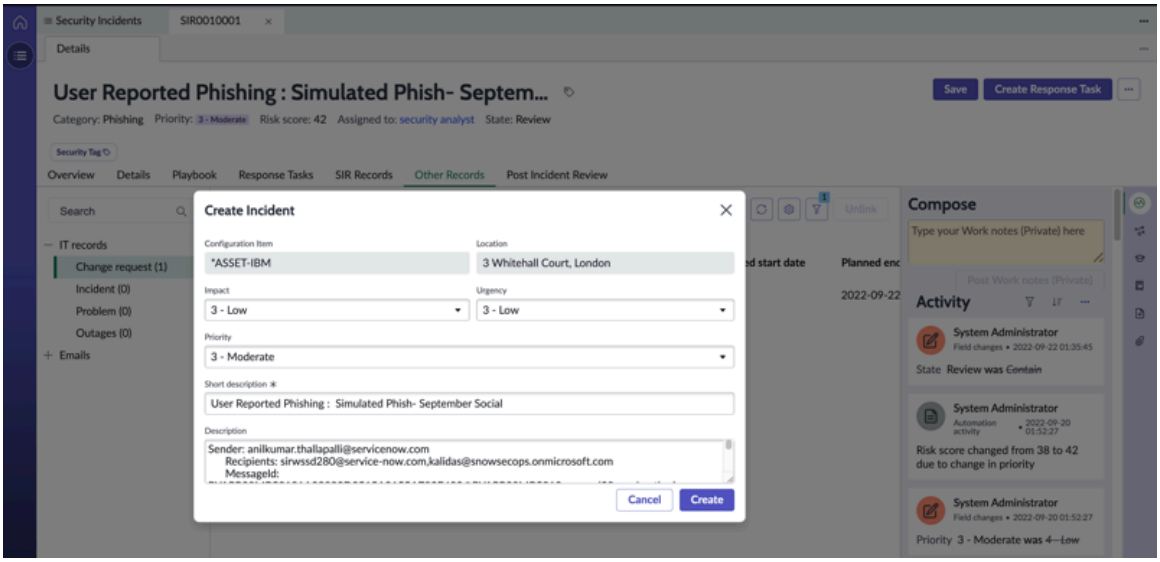
### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.

Automatische Übersetzung

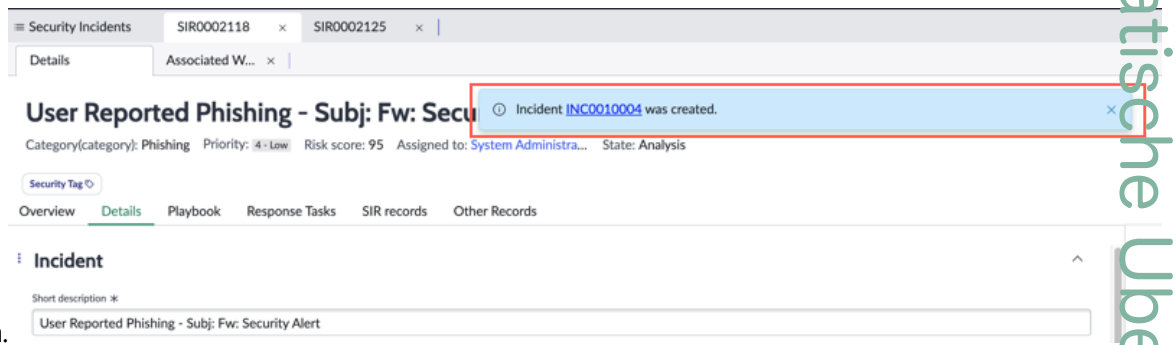
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Incident erstellen**.




4. Geben Sie Details wie Konfigurationselement, Auswirkung, Dringlichkeit, Standort, Priorität und Kurzbeschreibung ein.

5. Klicken Sie auf **Erstellen**.




6. Ein Incident wird erstellt.

### Problemaufgaben erstellen

Erstellen Sie eine Problemaufgabe.

### Vorbereitungen

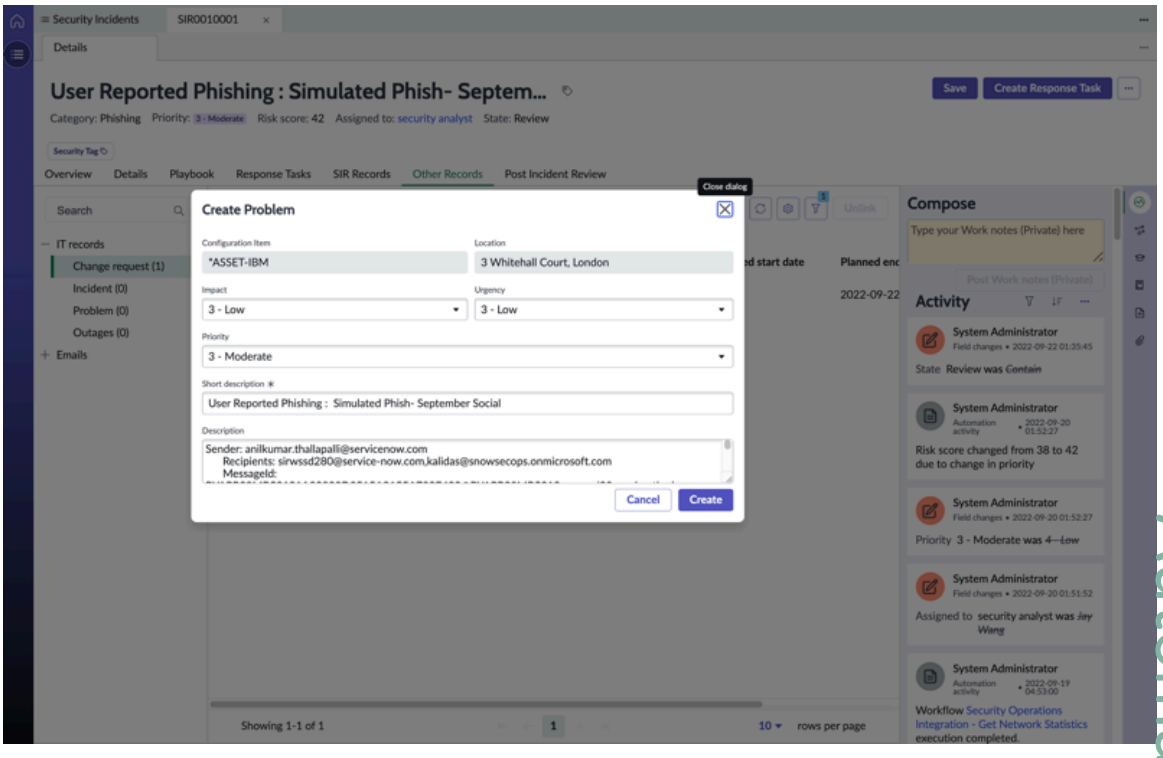
Erforderliche Rolle: sn_si.analyst

### Prozedur

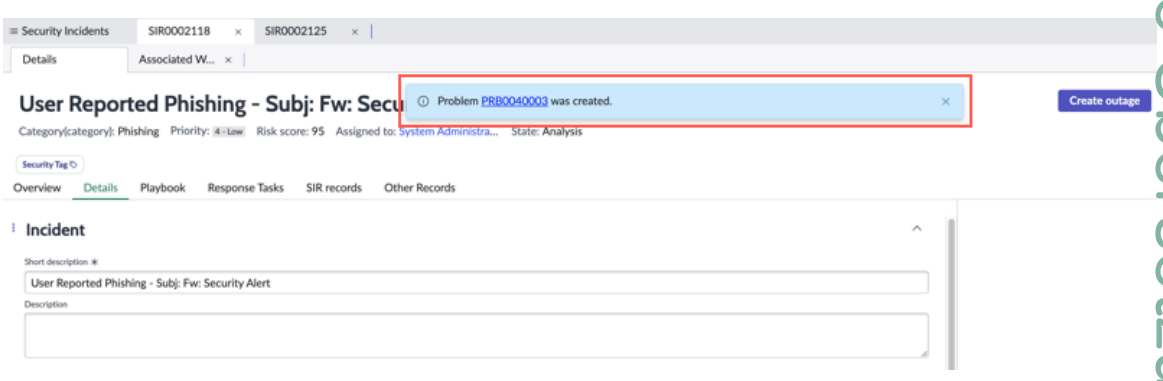
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken **Sie auf Problem erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie Details wie Konfigurationselement, Standort, Auswirkung, Dringlichkeit, Priorität und Kurzbeschreibung ein.
5. Klicken Sie auf **Erstellen**.




6. Eine Problemaufgabe wird erstellt.

## Change Requests erstellen

Erstellen Sie eine Change-Anforderung.

### Vorbereitungen

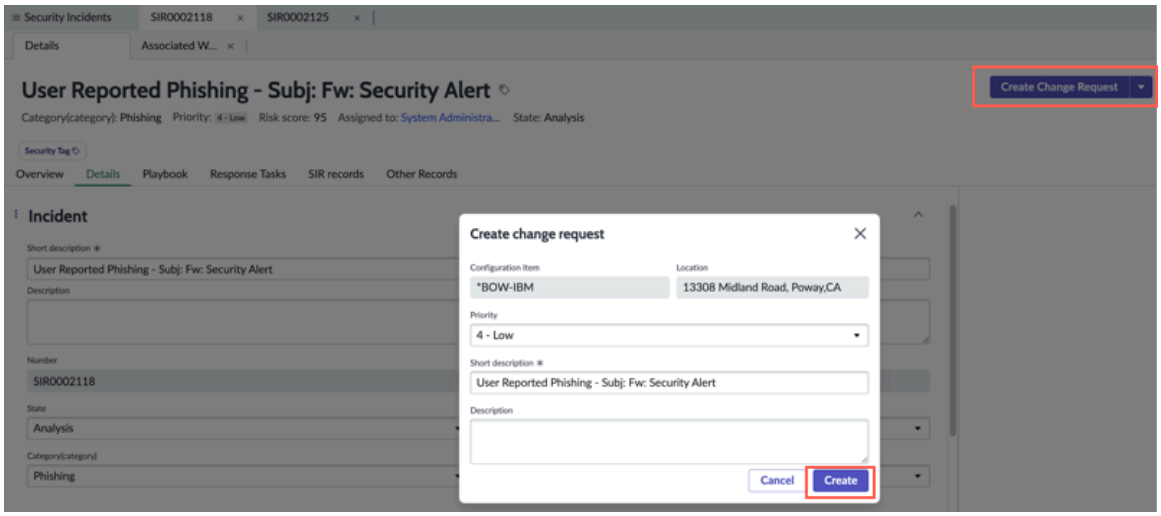
Erforderliche Rolle: sn_si.analyst.

### Prozedur

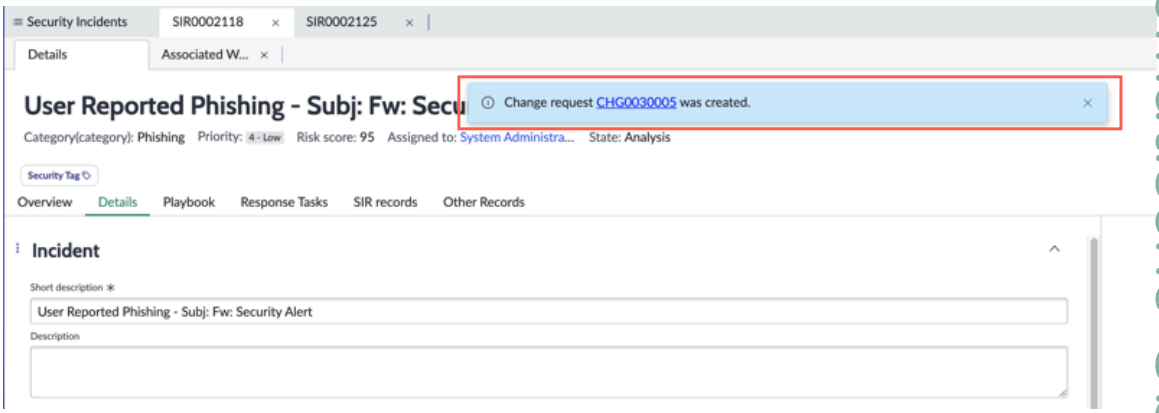
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken **Sie auf Change-Anforderung erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie Details wie Konfigurationselement, Standort, Priorität und Kurzbeschreibung ein.
5. Klicken Sie auf **Erstellen**.




6. Eine Change-Anforderung wird erstellt.

## Nichtverfügbarkeit erstellen

Erstellen Sie einen Ausfall aus einem Incident, um die Ausfallzeit eines Konfigurationselements nachzuverfolgen.

### Vorbereitungen

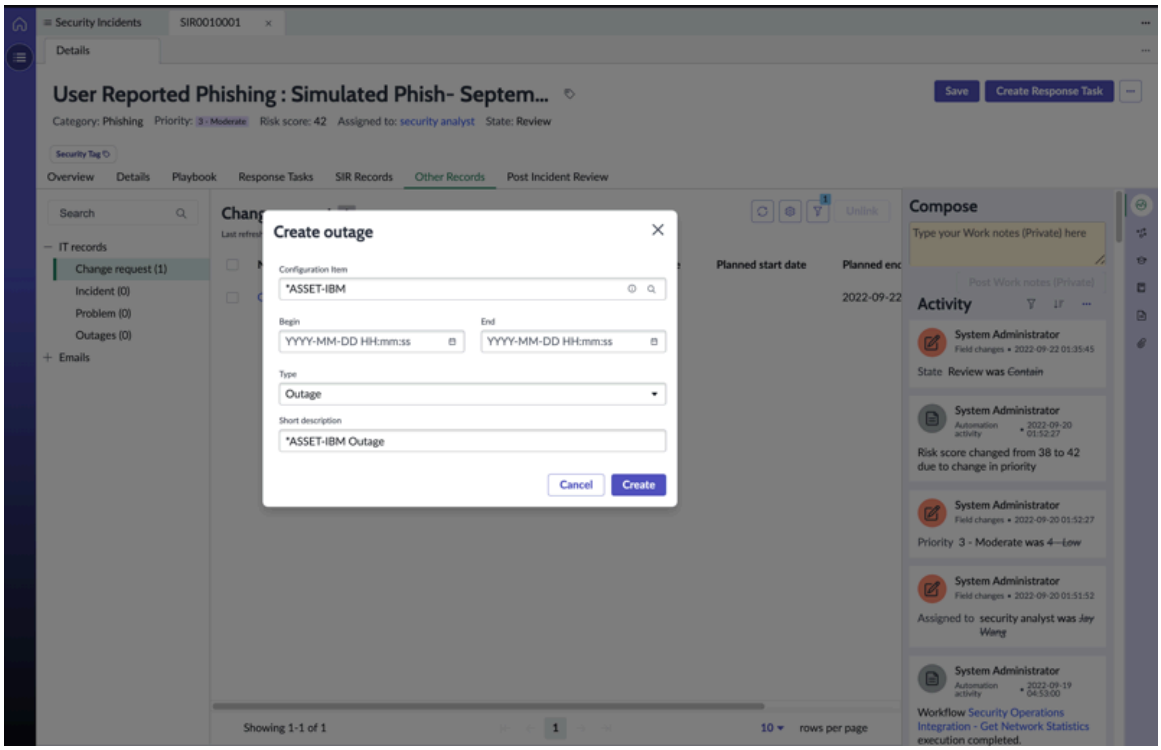
Erforderliche Rolle: sn_si.analyst

### Prozedur

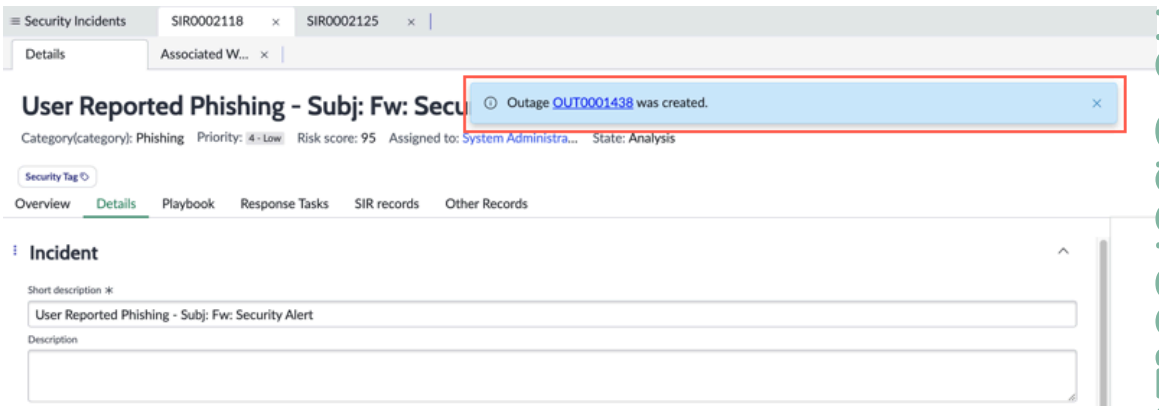
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken **Sie auf Ausfall erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie Details wie Konfigurationselement, Startdatum, Enddatum, Typ und Kurzbeschreibung ein.
5. Klicken Sie auf **Erstellen**.




## E-Mails verfassen

Als Analyst können Sie E-Mails direkt aus Security Incidents verfassen.

### Vorbereitungen

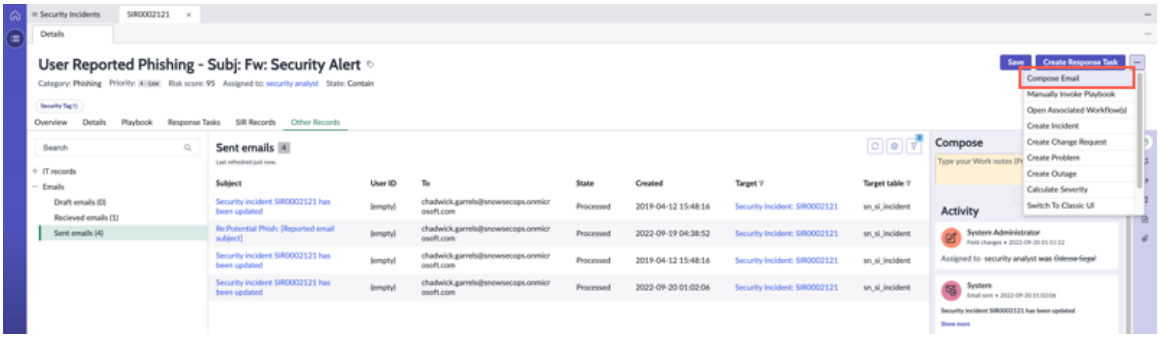
Erforderliche Rolle: sn_si.analyst

### Prozedur

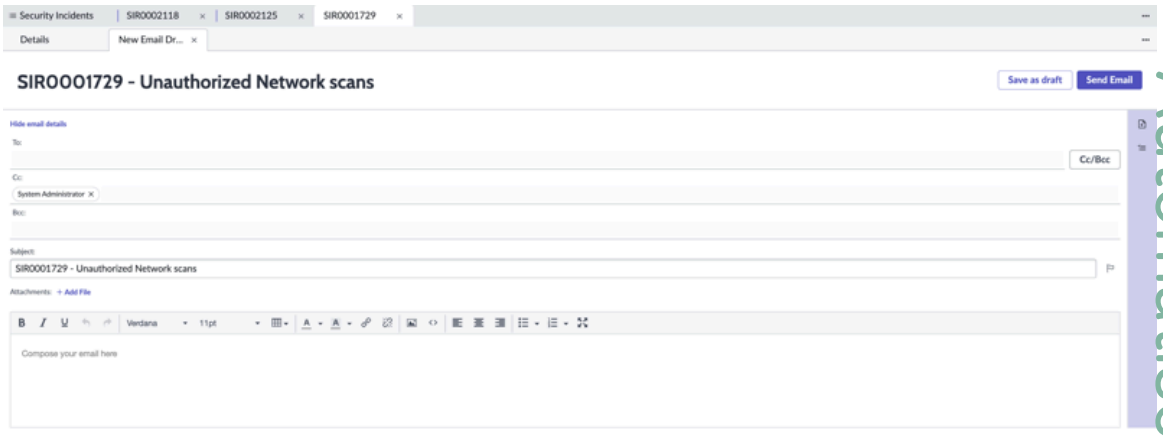
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen und öffnen Sie den Incident, für den Sie eine E-Mail verfassen möchten.
3. Klicken Sie auf den Überlauf, und wählen Sie **E-Mail erstellen**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

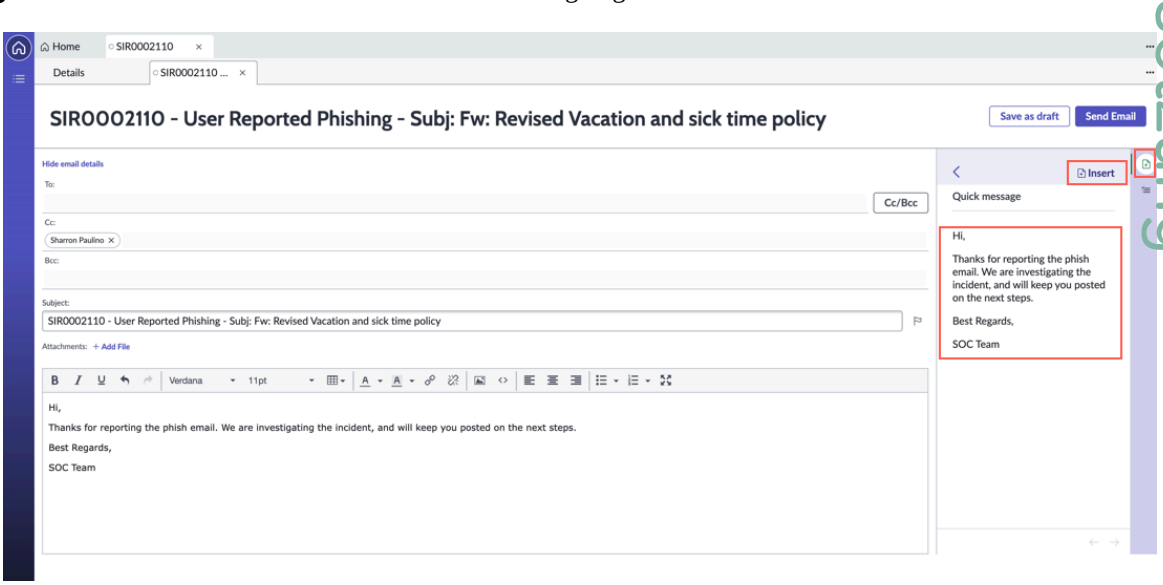



**4.** Geben Sie die Felder **An** und **CC** ein.




**5. Fügen Sie** Anhänge hinzu, falls vorhanden.

**6.** Klicken Sie im E-Mail-Formular auf **Schnellnachrichten**, um die Schnellnachrichten anzuzeigen, die auf der rechten Seite des Abschnitts „E- **Mails verfassen** “ angezeigt werden.
Die verfügbaren Schnellnachrichten werden angezeigt. Wählen Sie die Nachricht aus, und klicken Sie auf **Einfügen**. Die Nachrichten werden in den E-Mail-Text eingefügt.




**7.** Verfassen Sie Ihre E-Mail, und klicken Sie auf E-Mail **senden**.

Automatische Übersetzung

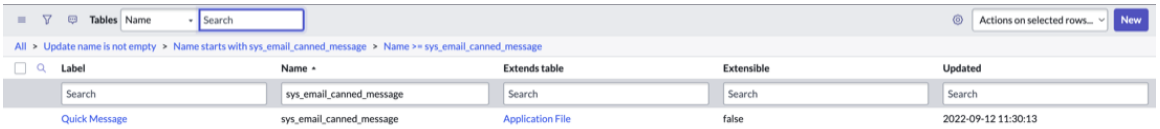
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können eine E-Mail als Entwurf speichern. Diese E-Mail-Entwürfe sind auf der Registerkarte Sonstige Datensätze verfügbar.

**So konfigurieren Sie Schnellnachrichten:**

**a.** Navigieren zu **Systemdefinitionen** > **Tabellen**.

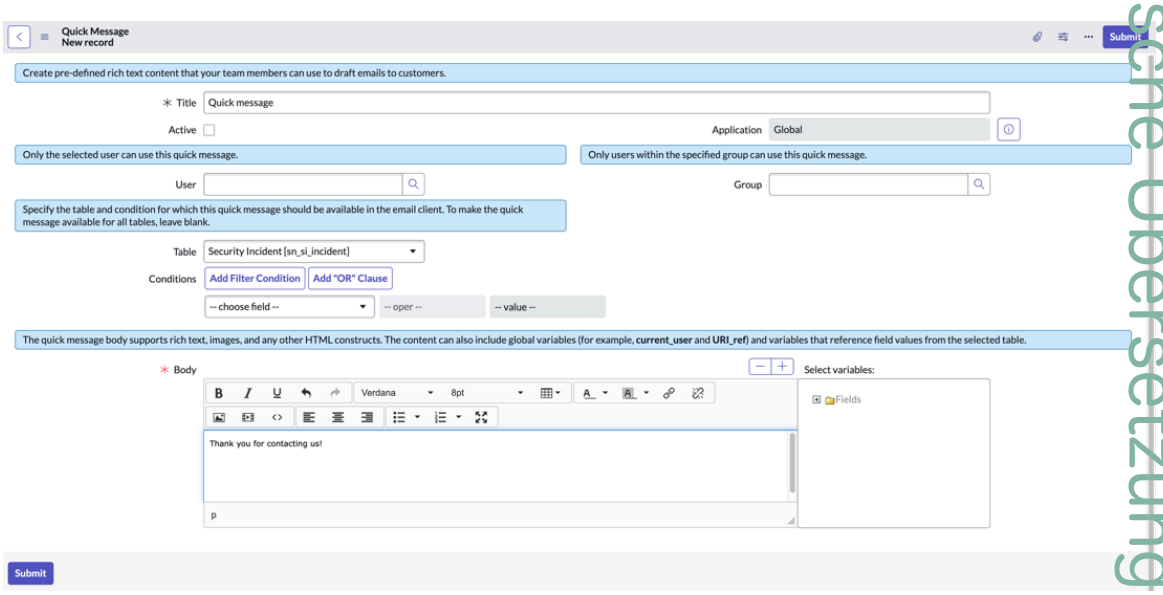
**b.** Suchen Sie nach der Tabelle **„Schnellnachricht" (sys_email_canned_message**).




**c.** Gehe zu **Zugehörige Links** > **Liste anzeigen**.

**d.** **Neue**erstellen.

**e.** Geben Sie den **Titel**und den Text **der Nachricht**ein, aktivieren Sie die **Tabelle: Security Incident (sn_si_incident)** und das Kontrollkästchen **Aktiv**.



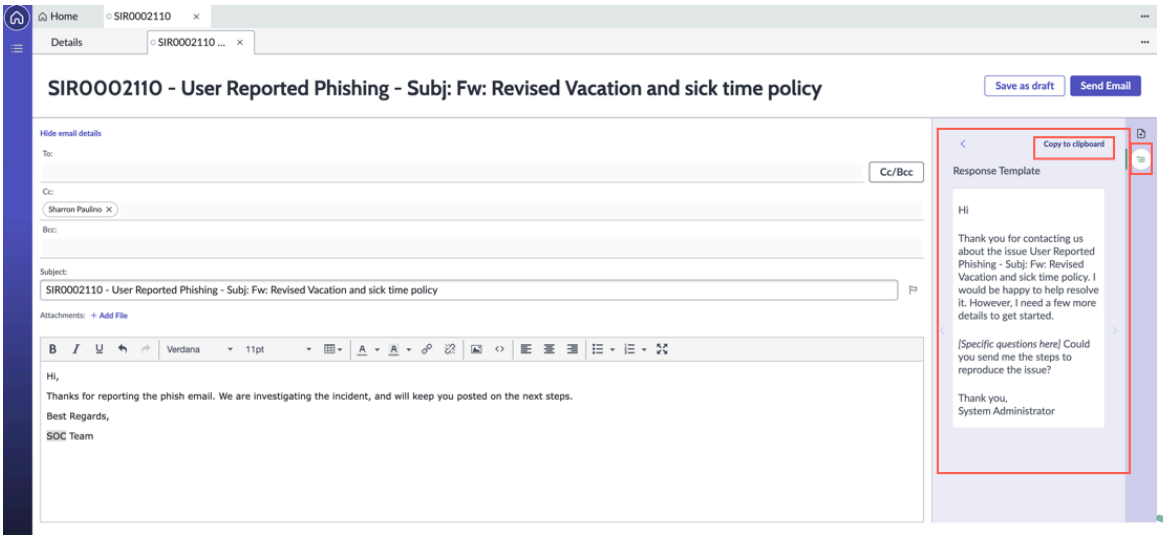

**f.** Klicken Sie auf **Absenden**.
Nachdem ein neuer Eintrag in der Tabelle erstellt wurde, wird die Schnellnachricht im Kontextmenü angezeigt.

**8.** Klicken Sie auf Vorlagen, um bei Bedarf eine **Vorlage** hinzuzufügen.

**9.** Wählen Sie die **Antwortvorlage** aus, klicken Sie **auf In Zwischenablage kopieren,** und wenden Sie die Vorlage bei Bedarf an.

Automatische Übersetzung

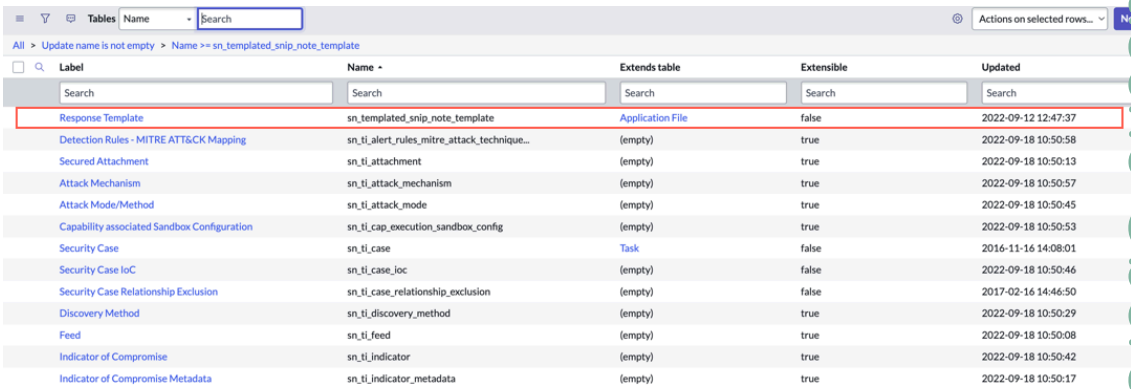
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**So konfigurieren Sie Antwortvorlagen:**

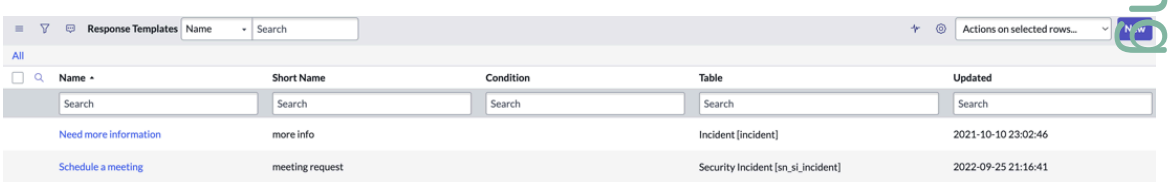
**a.** Navigieren zu **Systemdefinitionen** > **Tabellen**.

**b.** Suchen Sie nach der Tabelle **„Antwortvorlage“ (sn_templated_snip_note_template)**.




**c.** Gehe zu **Zugehörige Links** > **Liste anzeigen**.

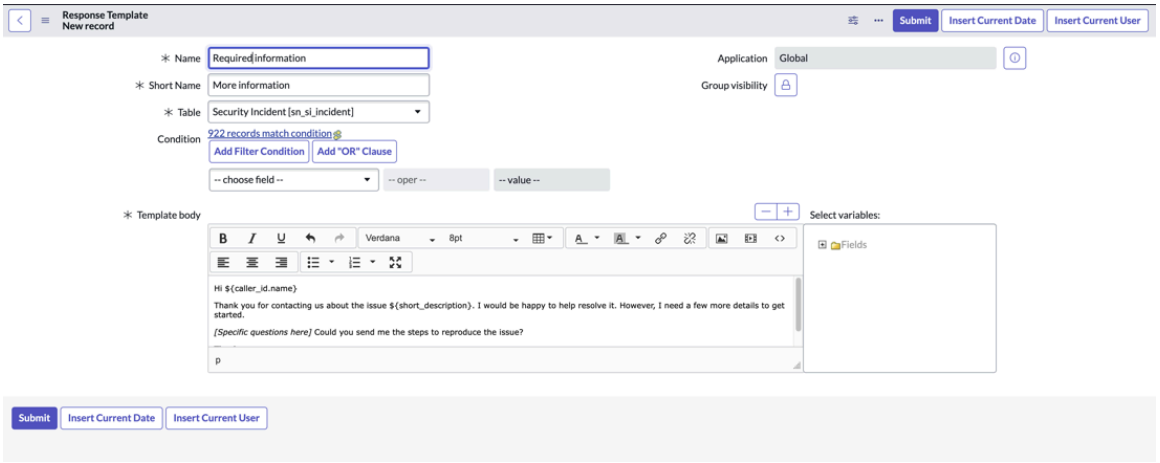
**d. Neue**erstellen.




**e.** Geben Sie den **Namen**und den **Kurznamen**ein, und wählen Sie die **Tabelle „Security Incident“ (sn_si_incident)** und den **Vorlagentext aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**f.** Klicken Sie auf **Absenden**.
Nachdem ein neuer Eintrag in der Tabelle erstellt wurde, wird die neue Vorlage im Kontextmenü angezeigt.

### Security Incident Response – Überprüfung nach Incident

Die Überprüfung nach Incidents wird angezeigt, wenn ein Incident in den Status Überprüfen verschoben wird.

Ausführlichere Informationen zur Durchführung von Aktivitäten nach Incidents finden Sie unter Überprüfungsbericht nach Incident

Die Überprüfung nach Incidents besteht aus den folgenden Abschnitten:

1. Bewertungen
2. Berichte

Im Security Incident Response-Arbeitsbereich können Sie mit diesen beiden neuen UI-Aktionen Bewertungen anfordern und durchführen.

| Name | Beschreibung |
|---|---|
| Bewertungen | Bewertung zeigt alle Bewertungen an, die den anderen Bewertungen des Security Incident zugeordnet sind. Der Analyst kann Bewertungen vornehmen und Bewertungen anfordern.<br><br>• **Bewertungen**vornehmen: Klicken Sie auf „ **Bewertungen durchführen** “, um die Bewertungen (falls zutreffend) vorzunehmen und die Bewertung abzuschließen. Vor Abschluss der Bewertung lautet der Status des Security Incident „Bereit“ und das Fälligkeitsdatum des Incident wird in Rot angezeigt.<br>• Bewertungen anfordern: Klicken Sie auf **„Bewertung anfordern** “ für zusätzliche Bewertungen, und Sie können die neuen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Beschreibung |
|---|---|
| | Benutzer hinzufügen, die Sie anfordern möchten.<br><br>**Hinweis:**<br>Benutzer, die bereits angefordert haben, werden in diesem Abschnitt nicht angezeigt.<br><br>Jede Bewertung für diesen Incident wurde basierend auf den in der Überprüfung nach Incidents festgelegten Bedingungen konfiguriert. Sie kann entweder obligatorisch oder optional sein. |
| Berichte | Ändern Sie die Laufzeitkonfigurationen, und generieren Sie den Bericht.<br><br>Wählen Sie die Berichtsinstanz aus, ändern Sie die Filter, und speichern Sie den Bericht. Der Analyst kann eine Vorschau des PIR-Berichts anzeigen und herunterladen. |

### Security Incident-Playbook

Rufen Sie den Security Incident-Playbook-Flow automatisch oder manuell auf.

Ein Playbook ist nur sichtbar, wenn mindestens ein Playbook einem Security Incident zugeordnet ist. Die Playbook-Komponente funktioniert nur für die mit PAD (Process Automation Designer) erstellten Prozesse und nicht für die mit Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert sie weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Es gibt zwei Möglichkeiten, das Playbook dem Security Incident zuzuordnen:

- Playbook automatisch aufrufen
- Fügen Sie das Playbook manuell hinzu

## Playbook automatisch aufrufen

Damit ein Playbook automatisch aufgerufen wird, muss ein Prozess mit **Process Automation Designer (PAD)**definiert werden. Wenn die Auslöserbedingung erfüllt ist, wird automatisch die Playbook-Registerkarte mit den angezeigten Playbook-Aktivitäten gerendert.

## Fügen Sie das Playbook manuell hinzu

Um ein Playbook manuell aufzurufen, navigieren Sie zur Dropdown-Liste der Formular-UI-Aktion, und wählen **Sie Playbook hinzufügen**aus. Weitere Informationen finden Sie unter. Playbook hinzufügen

**Hinweis:**
Wenn bereits ein Playbook verfügbar ist, werden die neu hinzugefügten Playbooks parallel zu den vorhandenen Playbooks ausgeführt.

- Innerhalb des Playbooks kann der Analyst die Playbook-Karten nach Status filtern.
- Der Analyst kann ein Playbook abbrechen, indem er es über das Ellipse-Symbol auswählt.



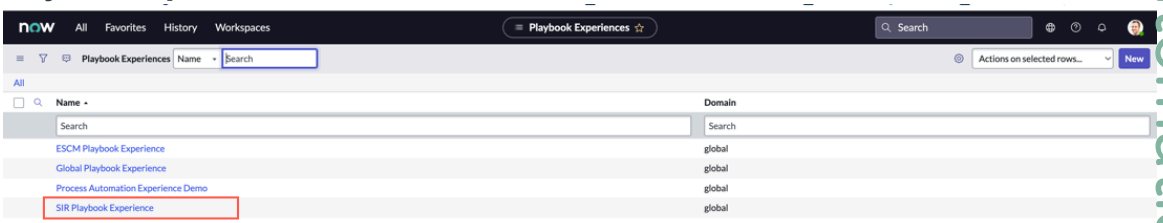
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Innerhalb jeder Aktivität kann der Analyst die in den Aktivitätskarten definierten Aktionen ausführen, z. B. Überspringen, Als abgeschlossen markieren, Abbrechen, oder Orchestration-Aktionen wie An Sandbox senden, E-Mails durchsuchen usw.
- Jede dieser Aktionen wird in der Aktivitätsdefinition definiert, und die vollständige sichtbare Karte kann zum Zeitpunkt der Erstellung der Aktivitätsdefinition selbst angepasst werden.

**Hinweis:**
Alle zukünftigen Aktivitätsdefinitionen und die nächsten auszuführenden Schritte werden mit einem Sperrsymbol angezeigt und befinden sich für den Benutzer im schreibgeschützten Modus. Der Playbook-Anzeigemodus wird durch eine Konfiguration gesteuert, wie unten erläutert.

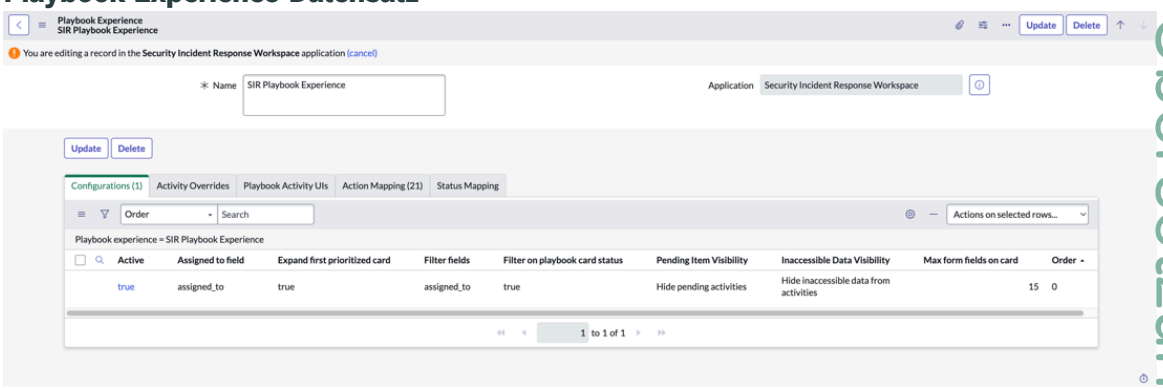
1. Navigieren zu **Alle** > **Playbook Experiences**.
2. Wählen Sie auf der Seite „Playbook-Experiences“ eine **SIR-Playbook-Experience**aus.

**Playbook-Experience**

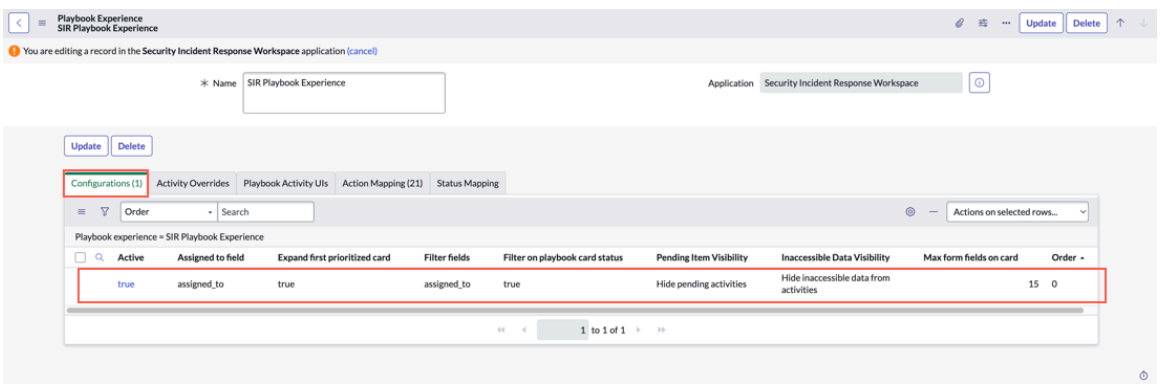



Die Seite **„Playbook-Experience – SIR-Playbook-Experience** “ wird angezeigt.

**Playbook-Experience-Datensatz**




3. Klicken Sie auf den **Konfigurationsdatensatz**.

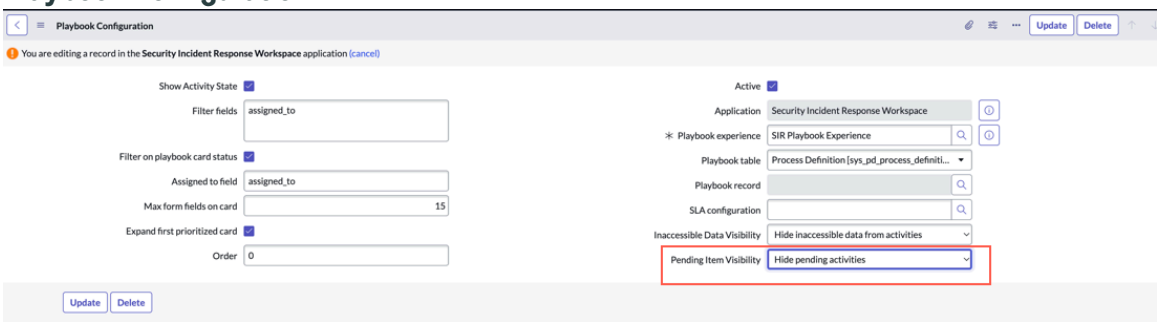





© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

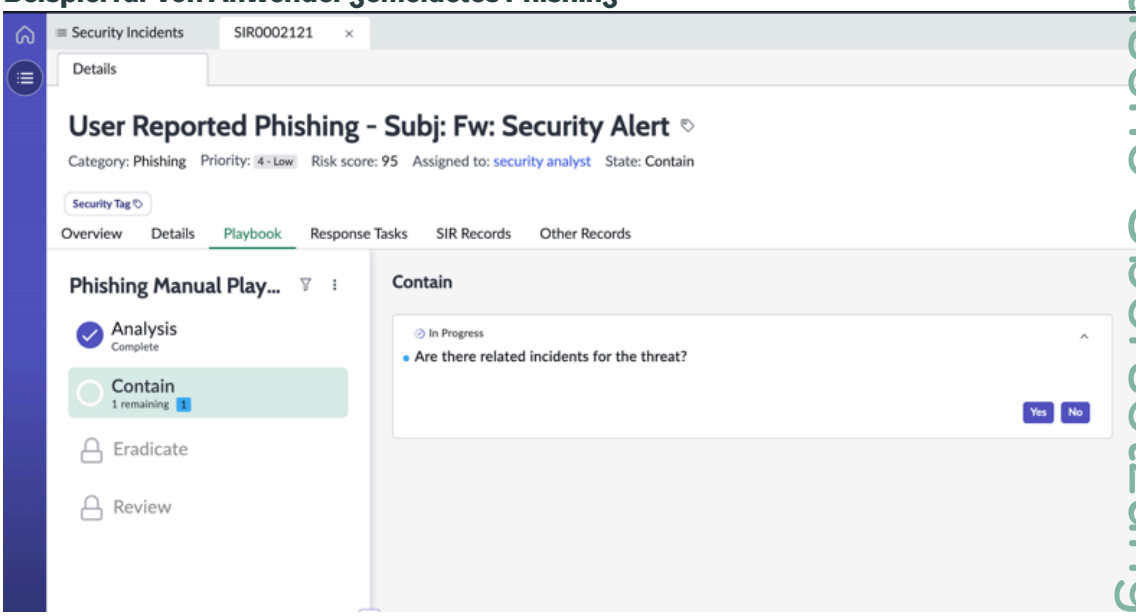
4. Klicken Sie auf der Registerkarte Konfiguration auf die SIR-Playbook-Experience-Konfiguration.

**Playbook-Konfiguration**




5. Navigieren Sie zur Dropdown-Liste des Felds **Sichtbarkeit ausstehender Elemente**, wählen Sie die gewünschte Option aus, und speichern Sie den Datensatz. Wählen Sie eine der folgenden Optionen aus:
   - **Ausstehende Aktivitäten ausblenden**: Wählen Sie diese Option aus, um die ausstehenden Aktivitäten auszublenden, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

**Beispiel für von Anwender gemeldetes Phishing**

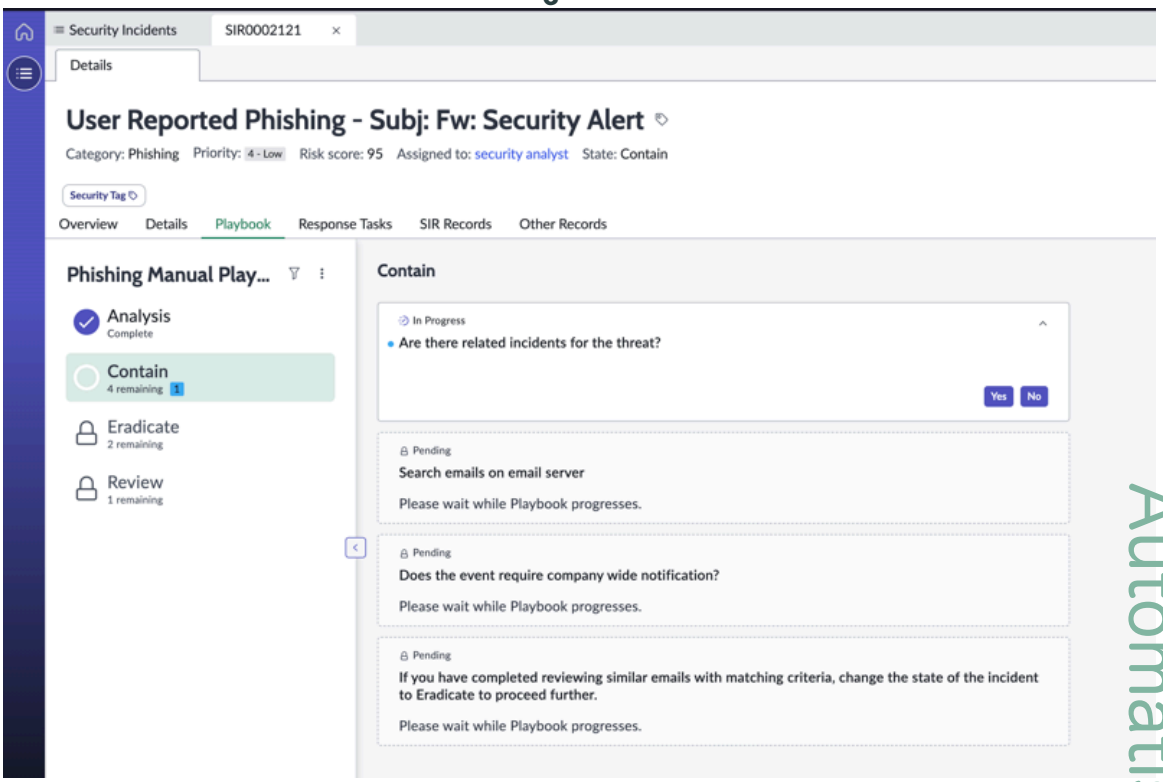



   - **Ausstehende Phasen und Aktivitäten**anzeigen: Wählen Sie diese Option aus, um ausstehende Phasen und Aktivitäten anzuzeigen, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

Automatische Übersetzung

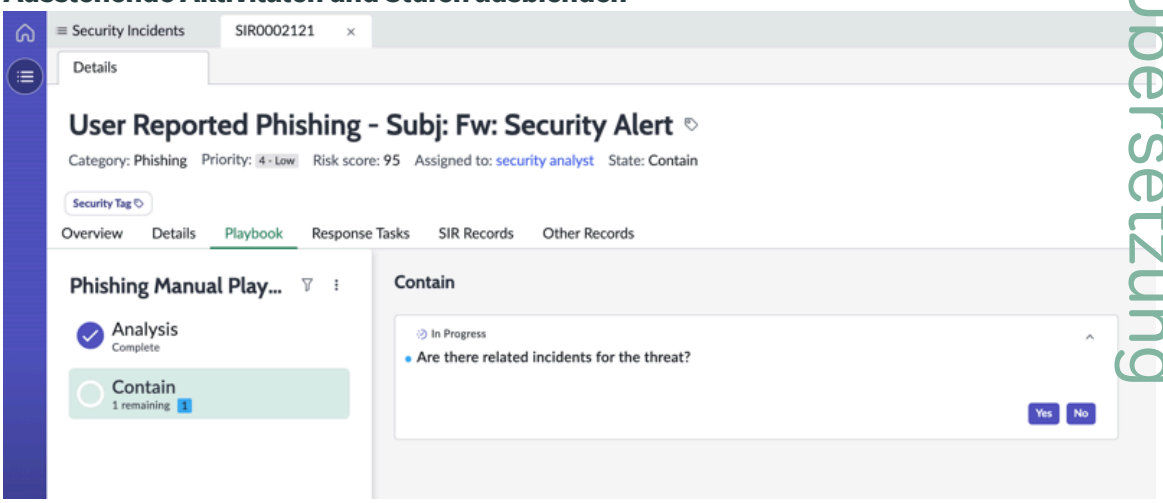
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausstehende Stufen und Aktivitäten anzeigen**




- **Ausstehende Aktivitäten und Phasen**ausblenden: Wählen Sie diese Option aus, um ausstehende Aktivitäten und Phasen auszublenden, die im Playbook-Abschnitt des Arbeitsbereichs angezeigt werden sollen.

**Ausstehende Aktivitäten und Stufen ausblenden**

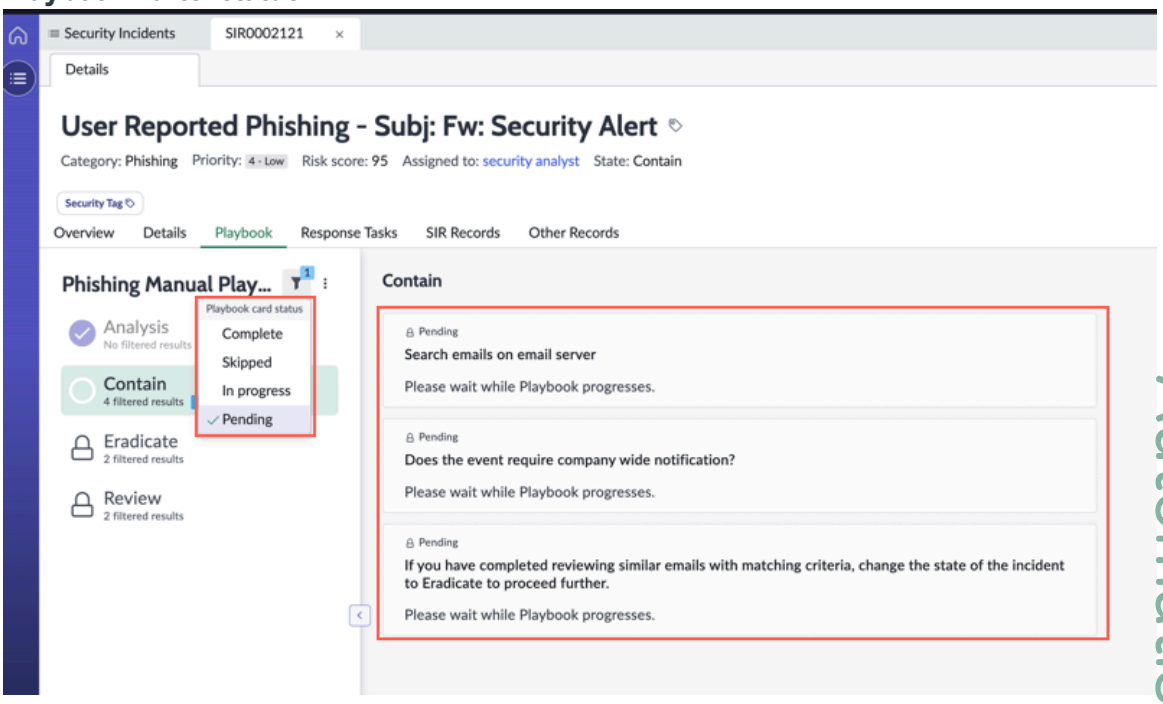



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verwenden Sie im Abschnitt „Playbook“ die Filteroption, um die Aktivitäten nach Playbook-Kartenstatus (Aktivitätsdefinition) zu filtern.

**Playbook-Kartenstatus**




## Playbook hinzufügen

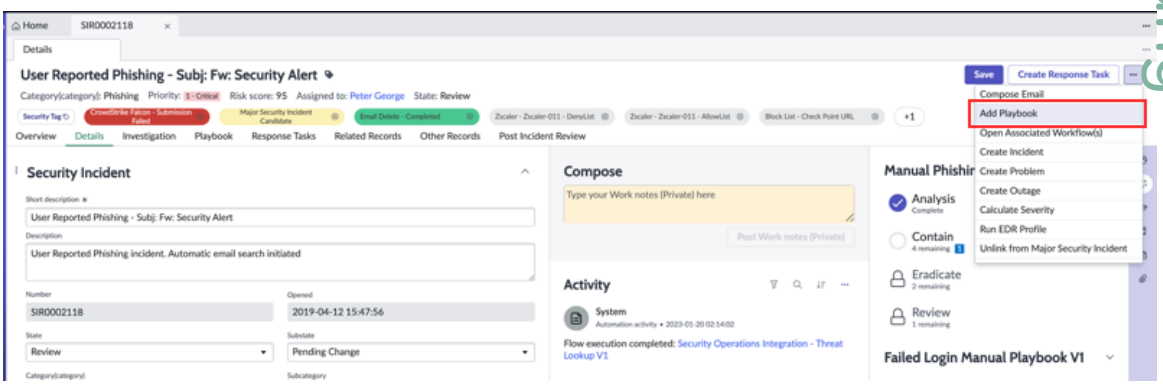
Verwenden Sie diesen Abschnitt, um das Playbook manuell hinzuzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Prozedur

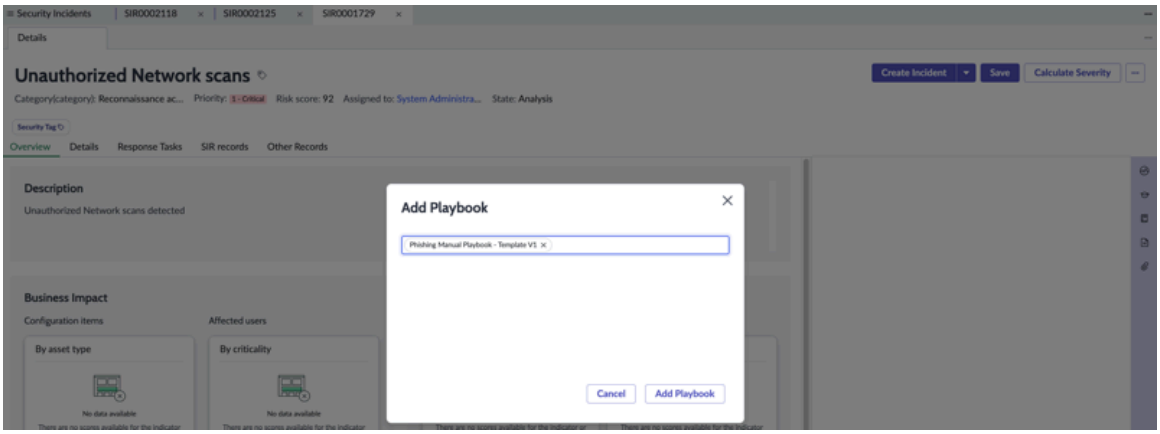
1. Navigieren zu **Alle** > **Security Incident** > **Security Analyst Workspace**.
2. Öffnen Sie einen Incident-Datensatz.
3. Klicken **Sie auf Playbook hinzufügen**.



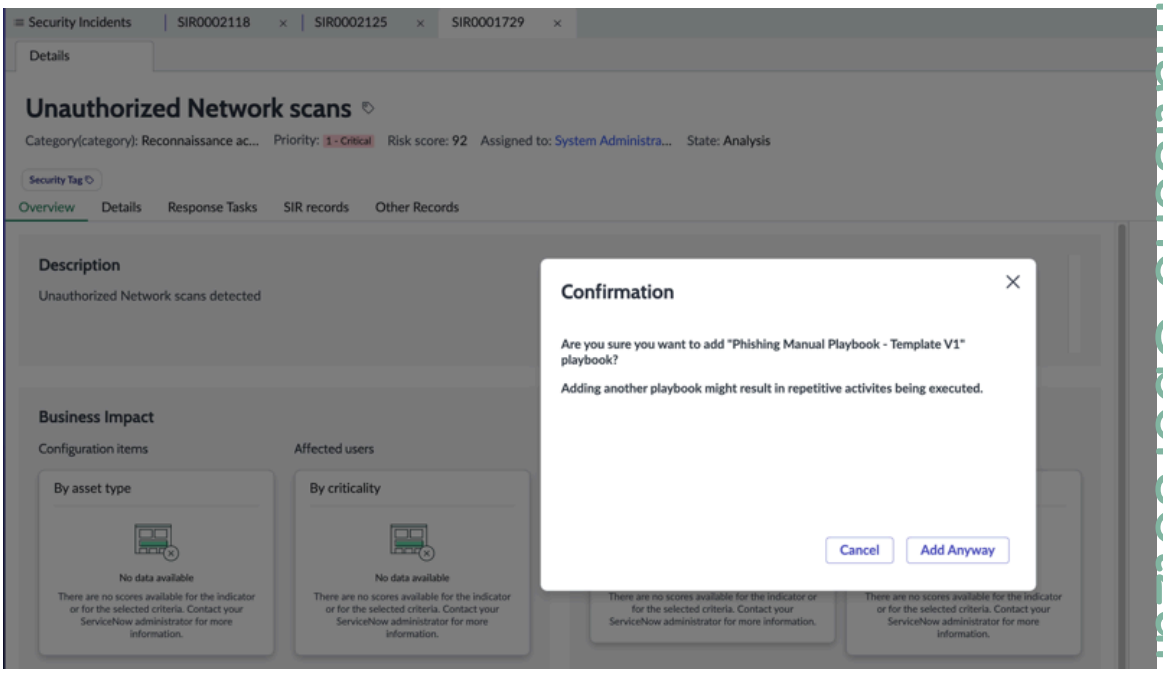

Das Dialogfeld „ **Playbook** hinzufügen“ wird angezeigt.

Automatische Übersetzung

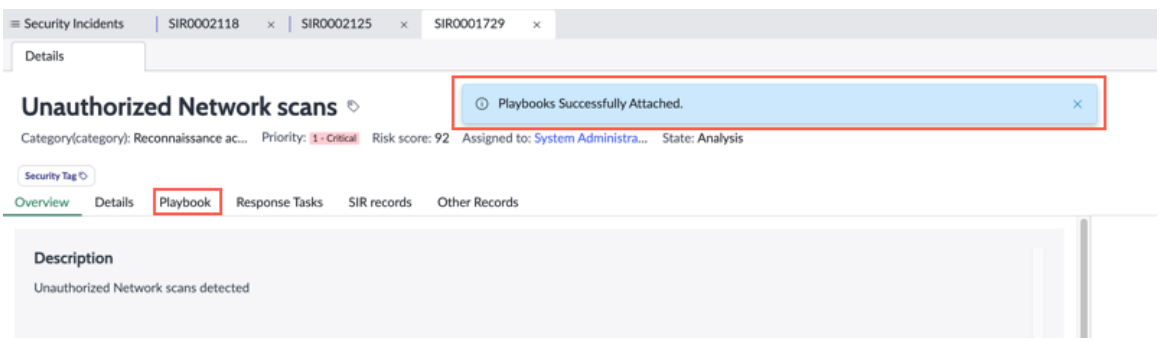
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wählen Sie die Playbook-Vorlage aus.
5. Klicken **Sie auf Playbook hinzufügen**.
   Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie bestätigen müssen.
6. Klicken Sie **auf Trotzdem hinzufügen**.



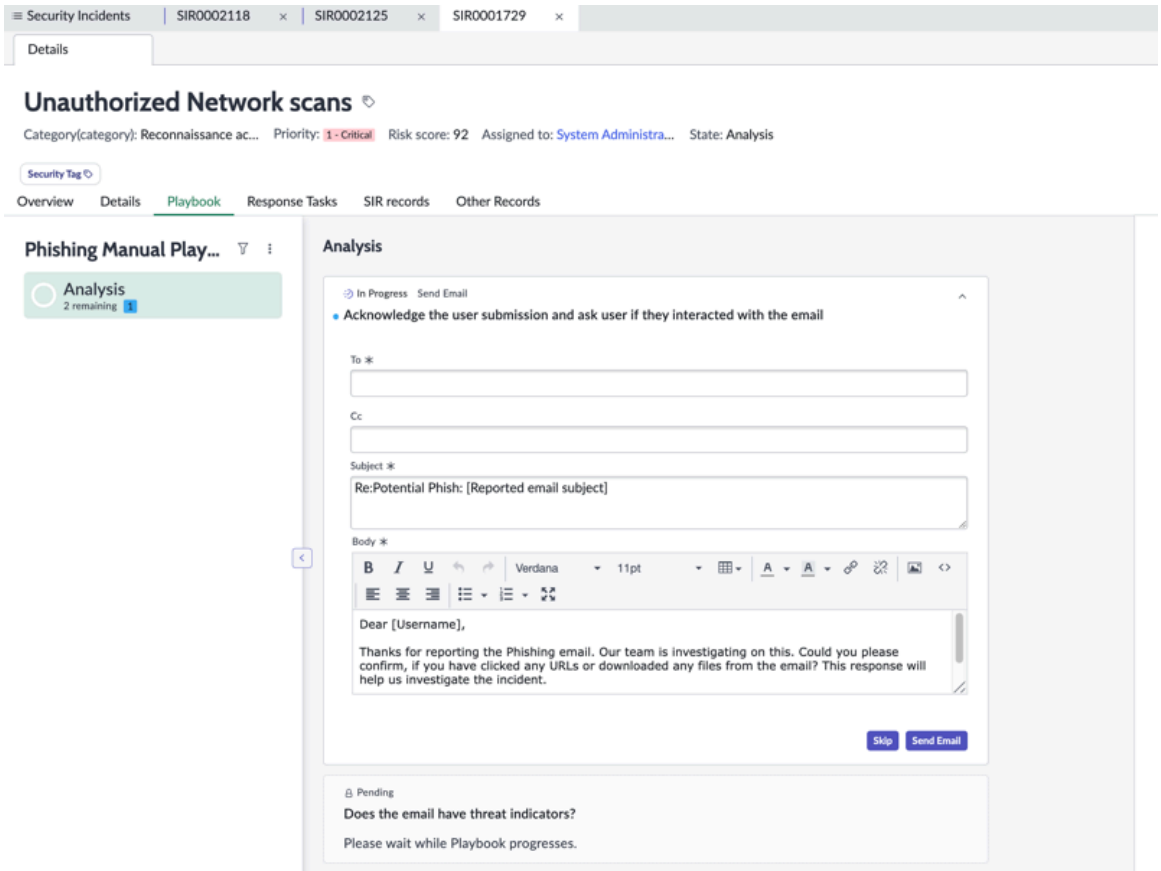

7. Das **Playbook** wird neben der Registerkarte „ **Details** “ hinzugefügt.




8. Klicken Sie auf die Registerkarte **Playbook**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




9. Führen Sie die Reihe der aufgeführten Aktivitäten aus, um zur nächsten Ebene zu gelangen.

> **Hinweis:**
> Wenn ein Security Incident einem Playbook zugeordnet ist, kann der Benutzer bis zum Schließen oder Abbrechen des zugeordneten Playbooks dasselbe Playbook nicht erneut demselben Security Incident zuordnen.

### Voraussetzungen für die Playbooks

Sie benötigen die folgenden Rollen und Plugins, um die Playbooks zu erstellen.

Erforderliche Rolle: admin.

- Aktivieren Sie das Plugin „Process Automation Designer (PAD)“ [com.glide.pad.license].
- Aktivieren Sie die folgenden Plugins für eine Playbook-Experience:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Aktivieren Sie die Security Operations-Spoke, um auf Flows zuzugreifen [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Commons.

Stellen Sie sicher, dass Sie die Plattformdokumentation zu Playbook Experience und Process Automation Designer (PAD) gelesen haben, bevor Sie mit diesem Leitfaden beginnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorhandene Playbooks werden auf PAD neu erstellt

Sie können vorhandene Flows nicht direkt in Prozesse in PAD konvertieren. Jeder Flow Designer-Schritt, der eine Antwortaufgabe zur Anleitung des Analysten erstellt, muss in separate Aktionen oder Subflows unterteilt werden.

Sie dürfen vorhandene Flows nicht direkt in Prozesse in PAD konvertieren. Jeder Flow Designer-Schritt, der eine Antwortaufgabe zur Anleitung des Analysten erstellt, muss in separate Aktionen oder Subflows unterteilt werden. Wenn Sie diese granularen Subflows oder Aktionen verwenden, müssen Sie Aktivitätsdefinitionen erstellen. Nachdem Sie diese Aktivitätsdefinitionen erstellt haben, werden sie als Aktivitäten innerhalb einer Spur in der Prozessdefinition hinzugefügt. Sie können Aktivitätsdefinitionen in mehreren Playbooks wiederverwenden.

Sie können jede Aktivität anpassen, um die darin enthaltenen erforderlichen Aktionen darzustellen und festzulegen, wie die Karte beim Erstellen der Aktivitätsdefinition aussehen soll. Die Aktivität kann E-Mail-Clients, Tabellen, Aktionen, KB-Artikel, URLs usw. anzeigen. Sie können definieren, wie die Aktivitätsdefinition und die zugrunde liegenden Aktionen oder Subflows erstellt werden.

Weitere Informationen finden Sie in den folgenden Abschnitten.

- Aktivitätsdefinitionen
- Process Automation Designer

### Aktivitätsdefinitionen

Now Platform enthält einige Aktivitätsdefinitionen innerhalb des Basissystems. Darüber hinaus sind für die Playbooks im Basissystem von SIR Workspace einige Aktivitätsdefinitionen im Basissystem unter der Anwendung Enterprise Security Case Management PAD Commons definiert.

Erforderliche Rolle: sn_si.admin.

Hier ist die Liste der Aktivitätsdefinitionen, die Teil des Basissystems sind:

| Aktivitätsdefinition | Tabelle | Beschreibung | Anwendung |
|---|---|---|---|
| Warten-auf-Bedingung ohne Experience | Global [global] | Warten auf Bedingung ohne Experience | Enterprise Security Case Management PAD Commons |
| An CSF X Sandbox übermitteln | Security Incident [sn_si_incident] | An Sandbox senden | Enterprise Security Case Management PAD Commons |
| E-Mail senden | Security Incident [sn_si_incident] | Aktivität „E-Mail senden“ für SIR-Playbooks. | Enterprise Security Case Management PAD Commons |
| E-Mail durchsuchen | Security Incident [sn_si_incident] | Durchsuchen Sie E-Mails auf dem E-Mail-Server | Enterprise Security Case Management PAD Commons |
| Aufgabenstatus aktualisieren | Security Incident [sn_si_incident] | Aktualisieren Sie den Aufgabenstatus | Enterprise Security Case Management PAD Commons |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktivitätsdefinition | Tabelle | Beschreibung | Anwendung |
|---|---|---|---|
| E-Mail löschen | Security Incident [sn_si_incident] | Löschen Sie E-Mails | Enterprise Security Case Management PAD Commons |
| Ja/Nein-Ergebnis | Aufgabe [task] | Erwartetes Ergebnis | Enterprise Security Case Management PAD Commons |

### Beispiel-Aktivitätsdefinition: E-Mail senden

Das folgende Beispiel zeigt die Definition der Aktivität „E-Mail senden“.

## Standard

Die grundlegenden Details umfassen Name (Bezeichnung), Anwendung, Beschreibung, Tabelle und alle Anwendungen, von denen aus darauf zugegriffen werden kann.

Fügen Sie den Automatisierungsplan und die Aktivitäts-Experience hinzu, und übermitteln Sie sie. Bearbeiten Sie das Dokument nach dem Absenden, um weitere Details für jede Registerkarte hinzuzufügen.

## Automatisierungsplan

Der Automatisierungsplan ordnet die Back-End-Aktion oder die Subflows zu, die mit dem Flow Designer erstellt wurden. In diesem Beispiel wird Folgendes verwendet: Subflow „E-**Mail senden – ESCM-Aktivität** “.

Dieser Subflow ermöglicht das Senden einer E-Mail. Es verfügt über die Kernlogik zum Senden einer E-Mail. Es sind alle Eingabefelder und Ausgabefelder definiert.

Alle Eingabefelder werden im Automatisierungsplanabschnitt angezeigt. Jedes Eingabefeld kann so aktiviert werden, dass es nur für den Administrator im standardmäßigen modalen Fenster, im standardmäßigen modalen Fenster und im Konfigurationsbereich sichtbar ist:

- **Nur**Administratorsichtbarkeit: Wenn dies auf Administrator festgelegt ist, kann nur der Administrator sie anzeigen.
- **In Standardmodell einbeziehen**: Wenn die Ansicht im Standardmodal festgelegt ist, wird sie nur im Dialogfeld „Eigenschaften“ angezeigt.
- **In Standardmodell und Konfigurationsbereich einbeziehen**: Wenn die Ansicht im standardmäßigen modalen Fenster und im Konfigurationsbereich festgelegt ist, wird sie im PAD-Konfigurationsbereich sowie im modalen Fenster „Eigenschaften“ angezeigt. Weitere Informationen finden Sie unter Aktivitätsdefinitionen

Sie können die Eingabefelder zum Zeitpunkt der Aktivitätsdefinition selbst definieren, sofern Sie diese Werte zum Zeitpunkt der Konfiguration nicht ändern müssen. Dies hilft dem Geschäftsprozessverantwortlichen, beim Konfigurieren einer Aktivität innerhalb eines Prozesses Zeit zu sparen.

## Aktivitäts-Experience

Die Registerkarte „Aktivitäts-Experience“ definiert, wie die Aktivitätskarte zur Laufzeit gerendert wird. Das Basissystem bietet die folgenden Experience-Typen:

- Freigabe
- Katalogelement



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datensatz erstellen
- Instruktion
- Wissen
- Liste
- Benachrichtigung
- Datensatz

Basierend auf der Art der von Ihnen ausgewählten Experience werden die weiteren Felder ausgefüllt. Weitere Informationen finden Sie in der Now Platform-Dokumentation.

In diesem Beispiel ist **Datensatztyp** ausgewählt.

**Hinweis:**
Wenn Sie beispielsweise eine Tabelle rendern möchten, können Sie „Liste“ als Experience-Typ auswählen.

### Zugeordneter Datensatz

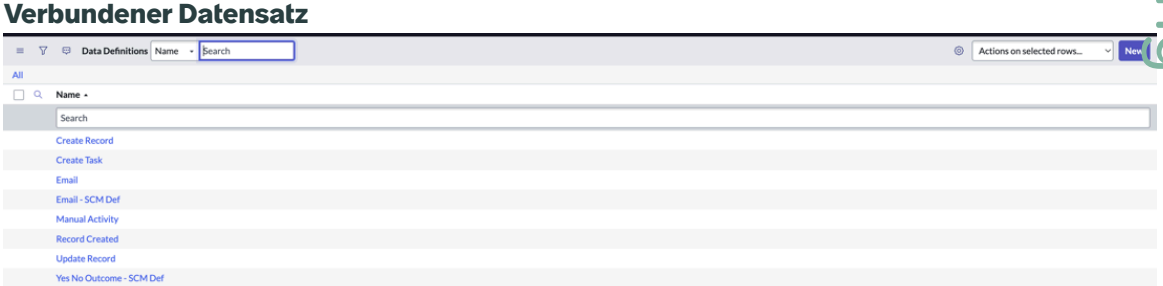
Verwenden Sie diesen Datensatz, um die zugehörigen Daten zur aktuellen Aktivität zu speichern. Dadurch werden die Ausführungszeitdaten sowie der Status der Experience erfasst.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Experience-Statustabelle: Flow-Daten
- Experience-Statusdatensatz: VL

In diesem Beispiel wird die Flow-Datentabelle verwendet, um die Laufzeitdaten zu erfassen. Die Laufzeitdaten können je nach Anwendungsfall variieren. In diesem Beispiel handelt es sich bei den Ausführungszeitdaten um Felder wie „An“, „CC“, „Betreff“ und „Text“. Für jeden Anwendungsfall muss eine Flow-Datendefinition erstellt werden, um den Typ der Laufzeitdaten zu definieren.

1. Navigieren Sie zum linken Bereich, und geben **Sie sys_flow_data_definition.list**ein. Zeigt die Liste der Definitionen an, die für die Flow-Datentabelle erstellt wurden.

### Verbundener Datensatz

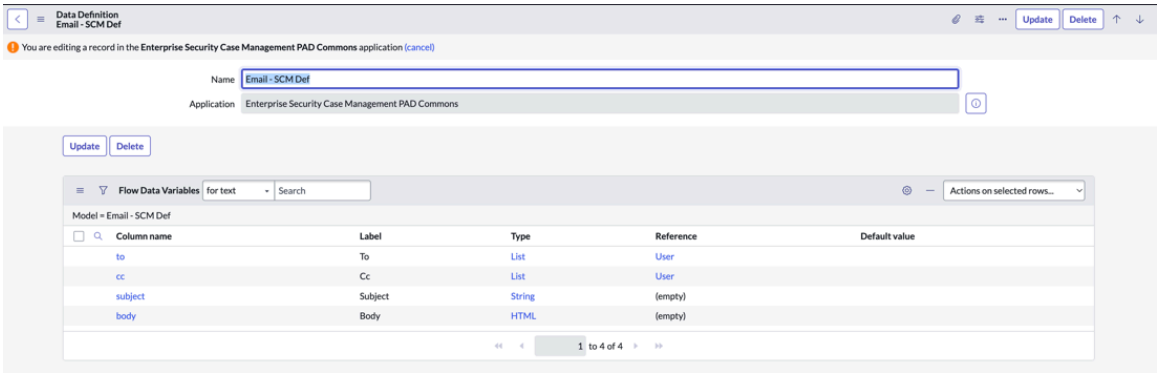



2. Öffnen **Sie E-Mail – SCM-** Definition, um die Definition für dieses Beispiel anzuzeigen.



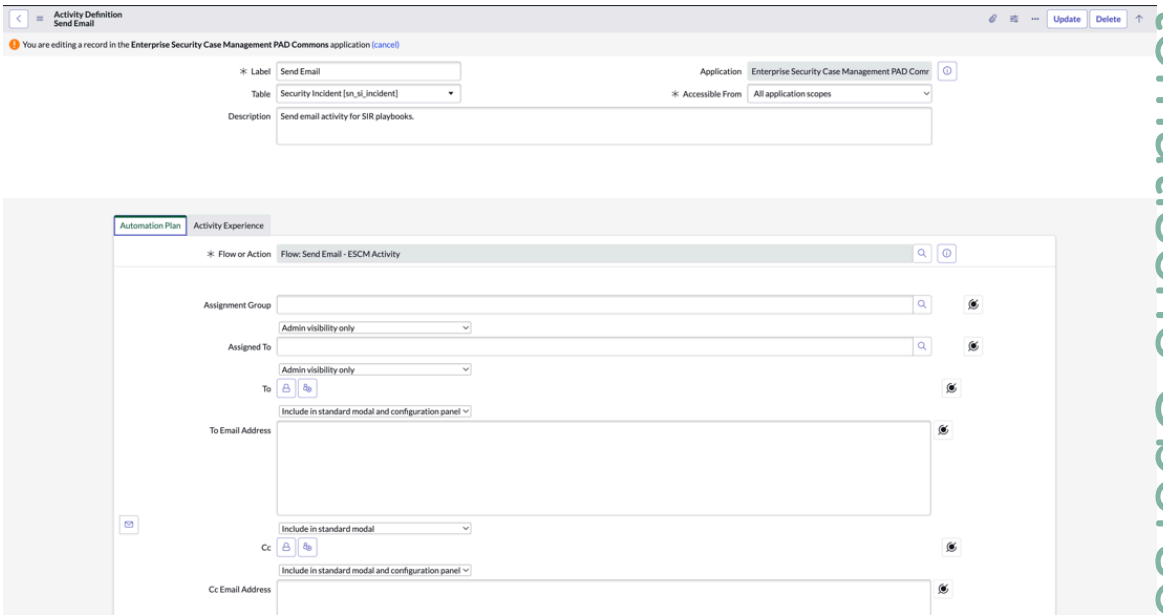
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### E-Mail – SCM-Definition




Diese Flow-Datendefinition muss vom Subflow oder der Aktion, die dieser Aktivitätsdefinition (Siehe Automatisierungsplan) zugeordnet ist, verwendet werden, um die Laufzeitdaten zu erfassen.

### Aktivitätsdefinitionen



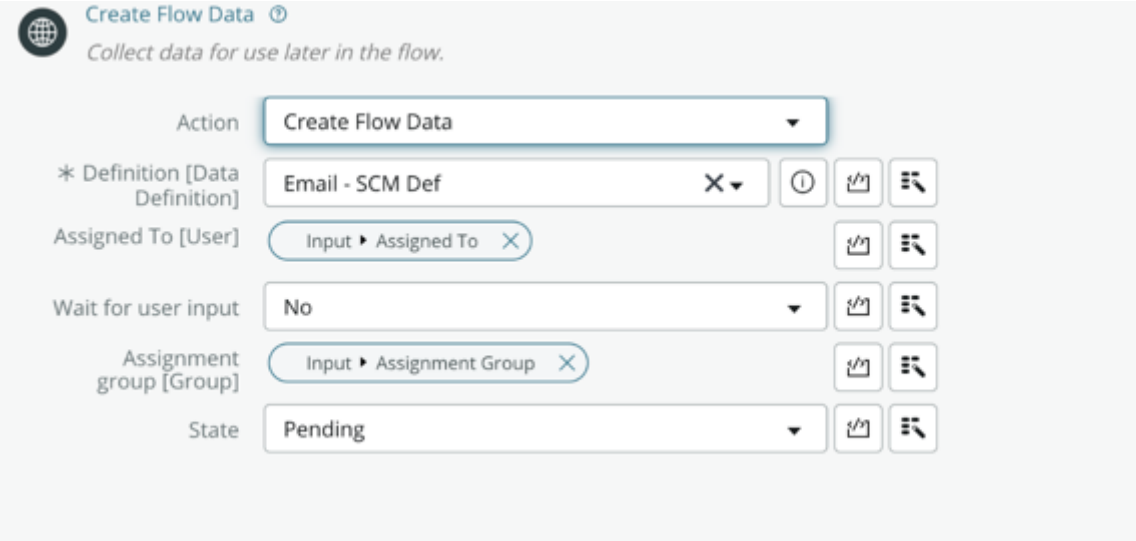

3. Öffnen Sie in diesem Beispiel den folgenden Subflow: E- **Mail senden – ESCM-Aktivität**. Unter dem Schritt **Flow-Daten erstellen** wird die von Ihnen erstellte Flow-Datendefinition dem Feld **Definition** zugeordnet. Dieser Flow-Datensatz wird im gesamten Subflow



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet. In diesem Beispiel wird der Aktivitätskartenstatus (Experience-Status) in der Flow-Datentabelle erfasst.

**E-Mail senden – ESCM-Aktivität**




**Hinweis:**

Wenn Sie die Laufzeitdaten in einem anderen Tabellendatensatz als der Flow-Datentabelle erfassen möchten, z. B. in einer Antwortaufgabe. Sie können die zugeordnete Tabelle als Antwortaufgabentabelle auswählen. Der zugeordnete Datensatz sollte auf den vom Subflow erstellten Antwortaufgabendatensatz festgelegt werden.

Ebenso wird in der Experience-Statustabelle der Status der Aktivitätskarte erfasst. Im Basissystem wird das Statusfeld der Flow-Datentabelle dem Aktivitätskartenstatus zugeordnet. Wenn also die Flow-Datentabelle zum Erfassen des Experience-Status verwendet wird, wird der Aktivitätskartenstatus automatisch aktualisiert. Sie können auch eine andere Tabelle als die Flow-Datentabelle verwenden, um den Experience-Status zu erfassen.

Wenn Sie beispielsweise den Status der Antwortaufgabe dem Status der Aktivitätskarte zuordnen möchten, ist dies möglich. Gehen Sie dazu wie folgt vor:

1. Navigieren zu **Alle** > **Playbook Experiences**.

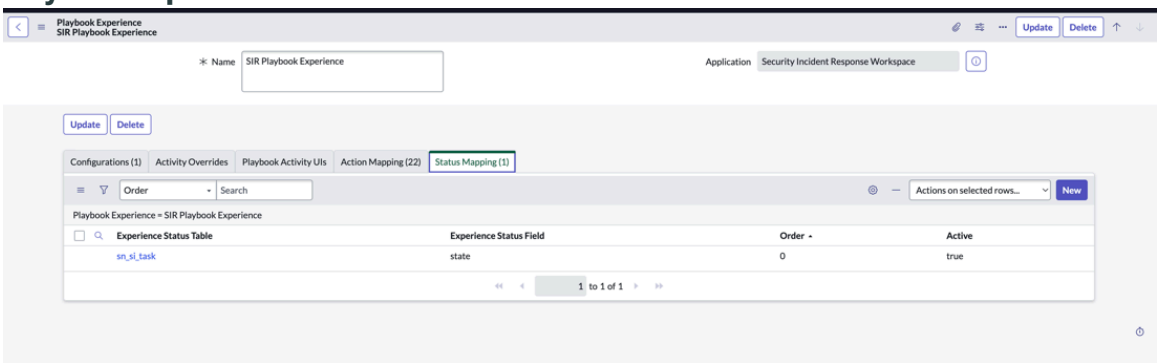
**Playbook Experiences**

2. Öffnen **Sie die SIR-Playbook-Experience**.
3. Öffnen Sie die zugehörige Liste **„Statuszuordnung“**.

Automatische Übersetzung

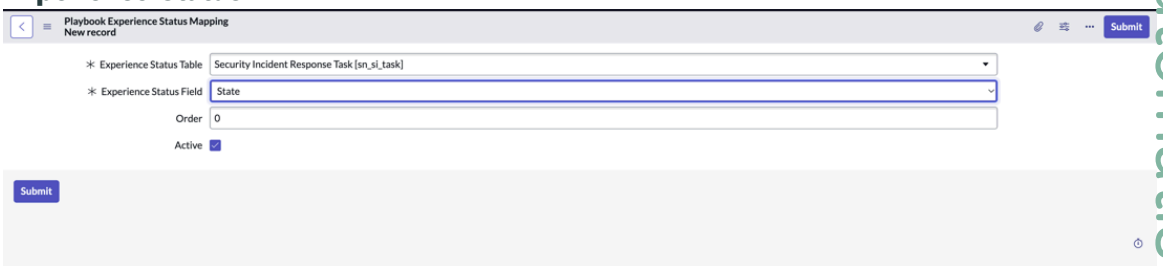
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook-Experience**



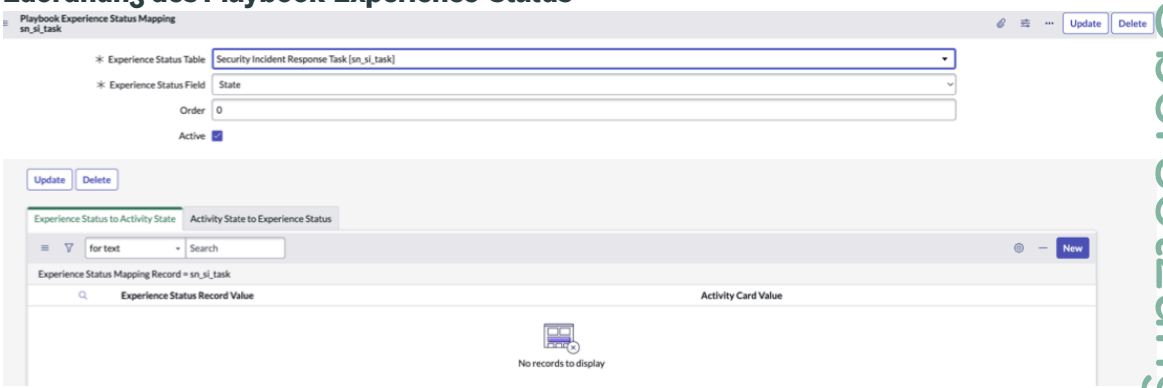

4. Geben Sie das Feld **Antwortaufgabe** für Experience-Statustabelle ein.
5. **Geben** Sie das Feld Status für Experience-Status ein.

**Experience-Status**



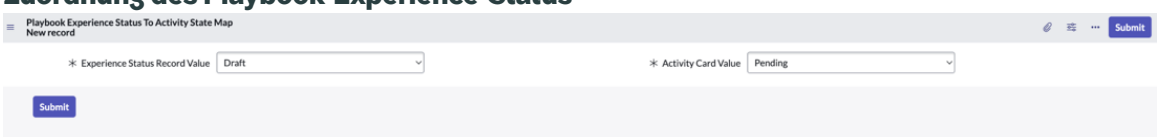

6. Klicken Sie auf **Absenden**. Der Datensatz wird erstellt.

**Zuordnung des Playbook-Experience-Status**




7. Ordnen Sie unter Experience-Status zu Aktivitätsstatus die Status der Antwortaufgabe dem Aktivitätskartenstatus zu.
8. Auf der linken Seite werden die Status der Antwortaufgabe und auf der rechten Seite der Status der Aktivitätskarte angezeigt.

**Zuordnung des Playbook-Experience-Status**

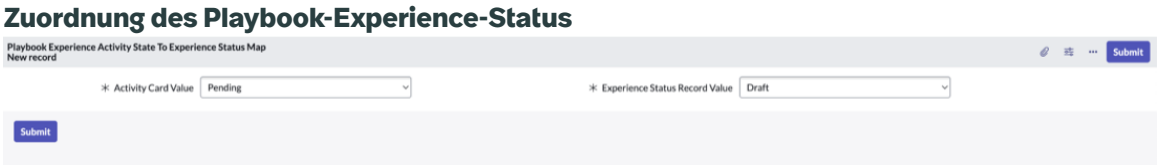



9. Die Zuordnung kann bidirektional sein. Ordnen Sie die Status auch unter der zugehörigen Liste „Aktivitätsstatus“ zu „Experience“ zu. Dieser Schritt ist die Umkehrung des

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorherigen Schritts. In diesem Fall wird auf der linken Seite der Status der Aktivitätskarte und auf der rechten Seite der Status der Antwortaufgabe angezeigt.




## Details

- Tagline: E-Mail senden
- Symbol: Umschlaggliederung (in der Benutzeroberfläche nicht angezeigt)
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert dynamisch zur Laufzeit als Titel.
- Beschreibung: **Aktivität** > **Aktivitätsinstanz** > **Beschreibung**. Hier haben wir die Beschreibung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert dynamisch zur Laufzeit als Titel.
- Statustitel ausstehend: Senden Sie eine E-Mail-Benachrichtigung. Dies ist der Titel, wenn sich die Aktivität im Status „Ausstehend“ befindet.
- Beschreibung des Status „Ausstehend“: Fordert vor dem Senden zur Bestätigung von Betreff und Text der E-Mail auf. Dies ist die Beschreibung der Aktivitätskarte, wenn der Status Datensatzfelder ausstehend lautet: In diesem Beispiel wurden Datensatzfelder ausgewählt.

  Datensatzfelder sind eine durch Kommas getrennte Liste von Feldnamen, die für den zugeordneten Datensatz in einer Name-Wert-Paar-Liste angezeigt werden sollen. Daten werden vorab auf dem Server abgerufen, Dot-Walking wird unterstützt und **canRead()**-Berechtigungen werden für jedes Feld ausgewertet.

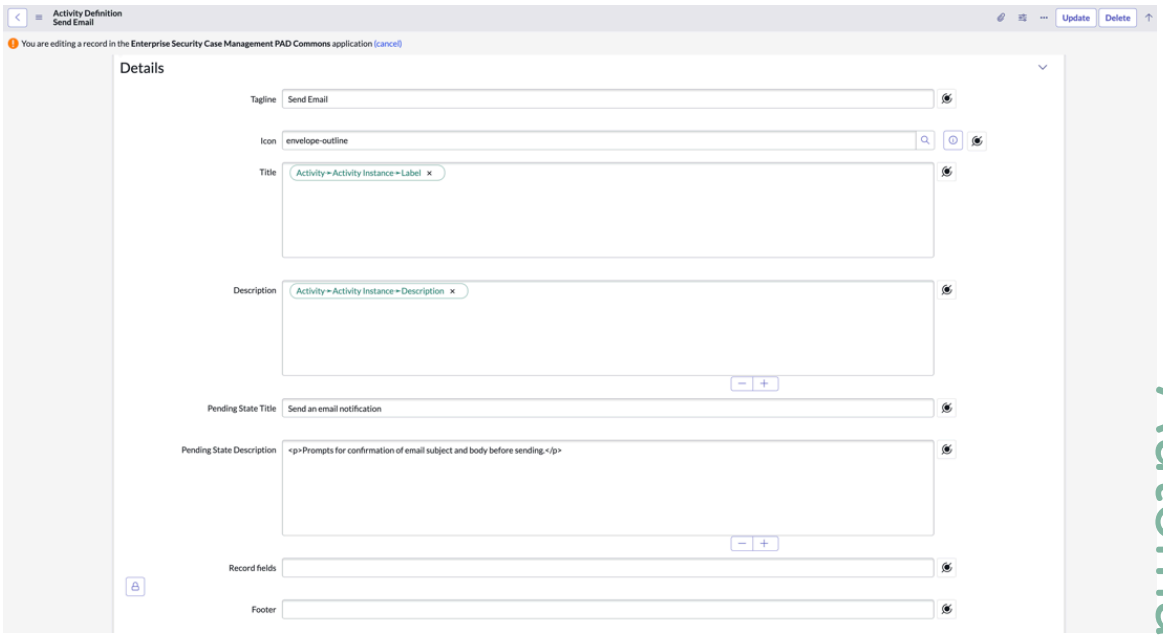
- Fußzeile: Für dieses Beispiel ist keine Fußzeile definiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fußzeile ist ein Text in einem grauen Bereich der Kartenfußzeile. Sie können der Anzeige beliebige aussagekräftige Informationen hinzufügen.

**Aktivitätsdefinition – E-Mail senden**

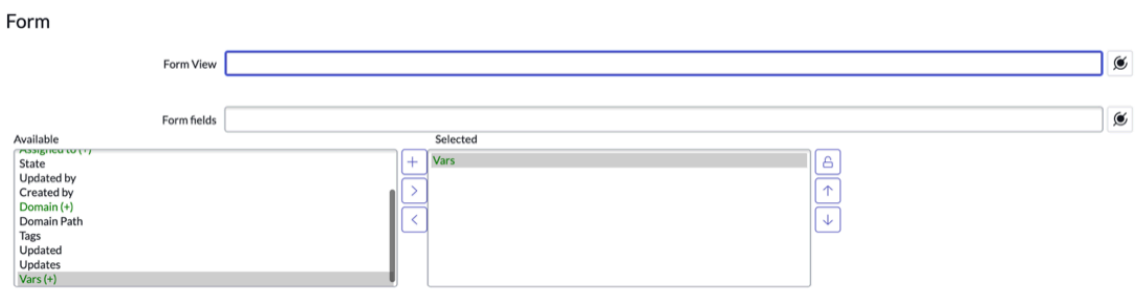



## Formular

- Formularansicht: collect_data
- Formularfelder:

In diesem Beispiel wird die Ansicht collect_data verwendet, um die Felder anzuzeigen, die dem Benutzer zur Eingabe von Eingaben angezeigt werden müssen. Die Ansicht „Collect_data“ ist eine von der Plattform bereitgestellte Ansicht, die der Flow-Datentabelle entspricht. Alternativ können Sie die Formularansicht leer lassen und Vars aus der Liste der für Formularfelder verfügbaren Werte auswählen. (Klicken Sie auf das Schlosssymbol, um die Liste der verfügbaren Werte zu öffnen.)

**Formularansicht**




## Anlagen

Beispiel:

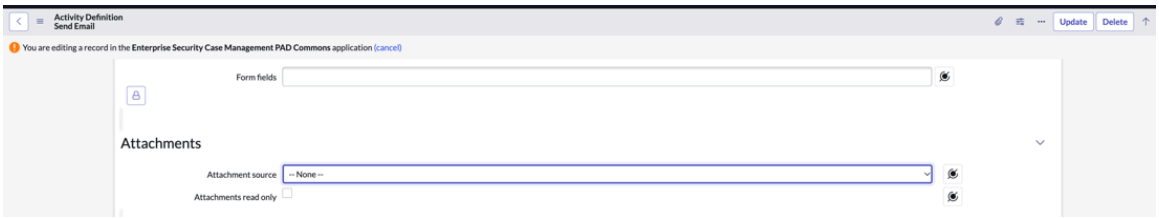
- Anhangquelle ist leer.
- Anhang „Schreibgeschützt“ nicht ausgewählt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Anhangquelle: Dropdown-Liste. Welche Anhänge auf der Karte angezeigt werden sollen: An den übergeordneten Datensatz angehängte Anhänge, Zugeordneter Datensatz oder keiner.
2. Anhang schreibgeschützt: Wahr oder Falsch. Verhindern Sie, dass der Benutzer die vorhandenen Anhänge umbenennt oder löscht.

**Aktivitätsdefinition – E-Mail senden**




## Funktionen

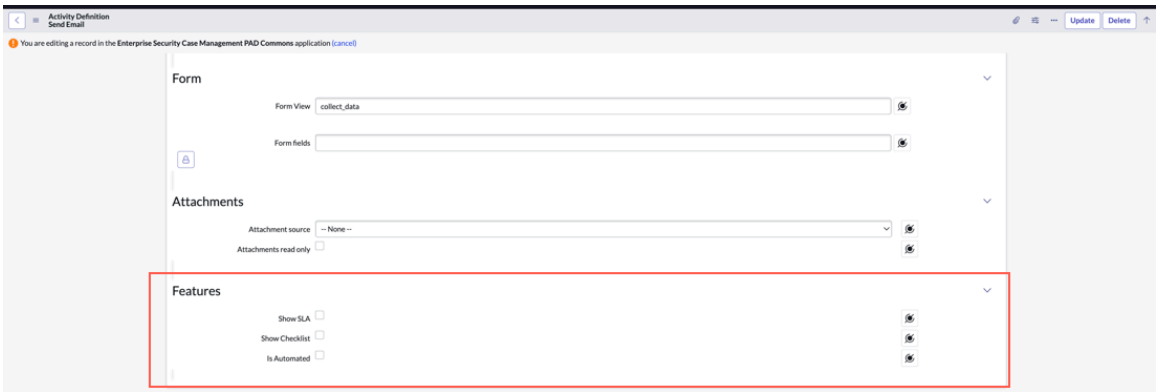
In diesem Beispiel

- SLA anzeigen – Freigegeben
- Prüfliste anzeigen – Freigegeben
- Ist automatisiert – Freigegeben

SLA anzeigen: Wahr/Falsch. Rendert einen SLA-Timer im Header der Karte für den zugeordneten Datensatz. Die SLA wird gemäß dem in der Playbook-Konfiguration angegebenen SLA-Konfigurationsdatensatz ausgewählt.

1. Prüfliste anzeigen: Wahr oder Falsch. Rendert alle Prüflisten, die an den zugeordneten Datensatz angehängt sind. Die Prüfliste kann bearbeitet werden, und Änderungen werden gespeichert, ohne dass eine deklarative Aktion erforderlich ist.
2. Ist automatisiert: Wahr oder Falsch. Bei „wahr“ werden **Tagline**und **Symbol**mit dem Text **Automatisierte Aufgabe** und einem automatisierten Symbol überschrieben.

**Aktivitätsdefinition – Formular „E-Mail senden“.**




## Playbook-Aktionen in Aktivitätsdefinition

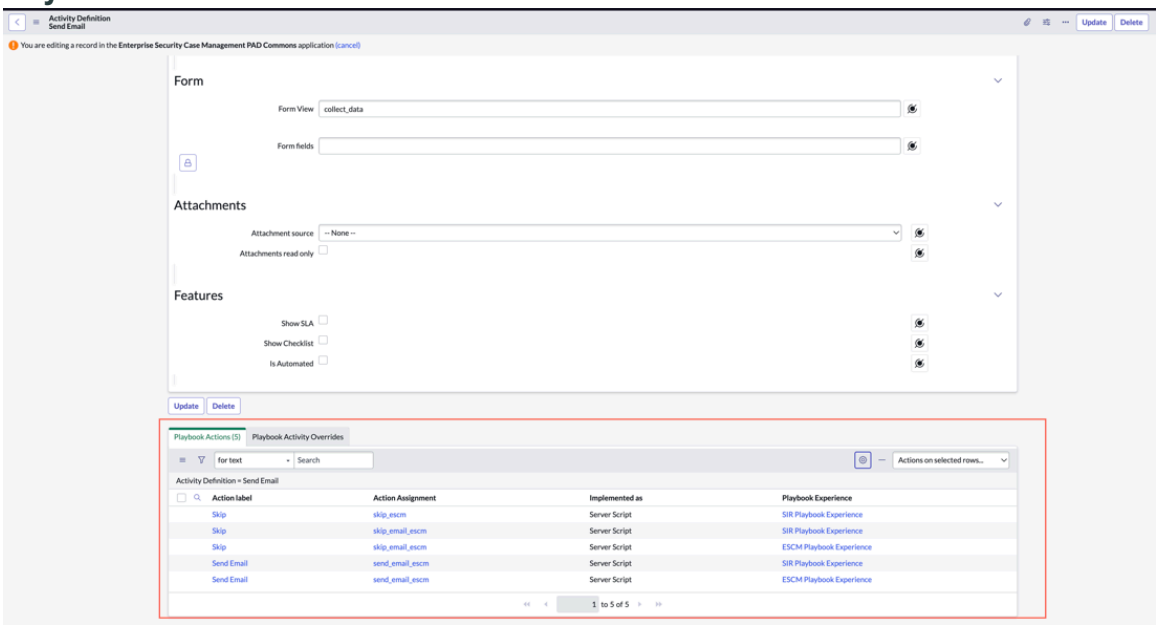
Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden. In diesem Beispiel sind die Aktionen **Überspringen**und **E-Mail** gesendet.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie einen Datensatz in der zugehörigen Liste **„Playbook-Aktionen“** am unteren Seitenrand erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Playbook-Aktionen




1. Klicken Sie auf **Neu**.
2. Wählen Sie eine vorhandene Aktivitätsaktion für das Feld „Aktionszuweisung“ aus.
3. Wählen Sie **SIR-Playbook** -Experience im Feld Playbook-Experience aus.

## Erstellen Sie eine Aktivitätsaktion

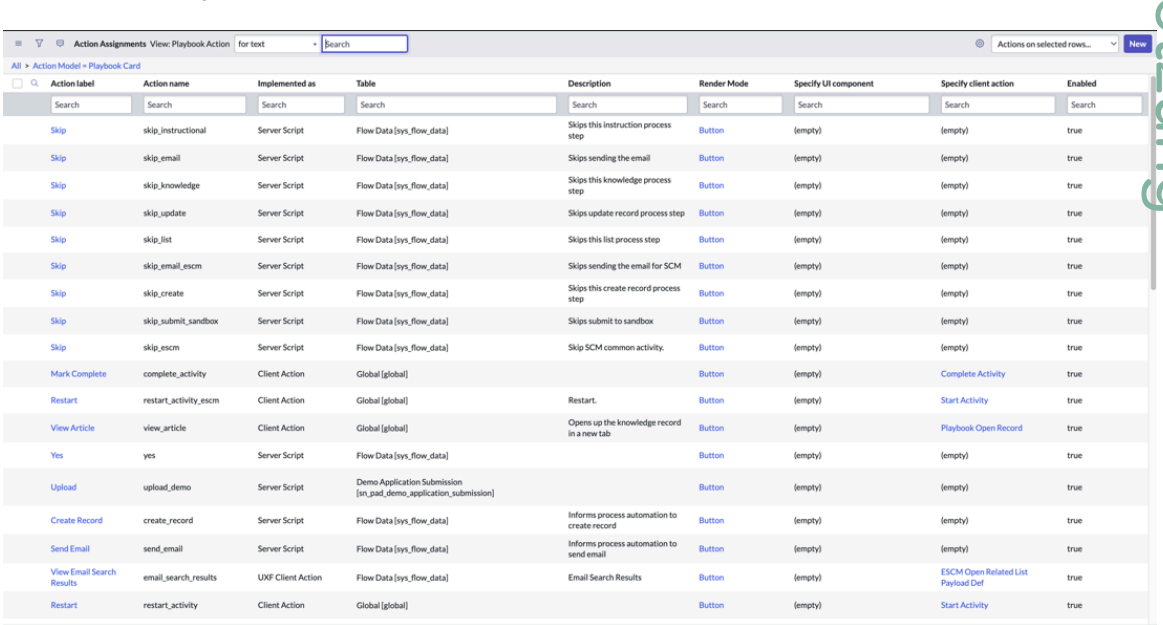
Im Folgenden finden Sie das Verfahren zum Erstellen einer Aktivitätsaktion.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Playbook Experiences** > **Aktionen** > **Aktivitätsaktionen**.




2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Now Platform-Dokumentation erfahren Sie, wie Sie diese Aktionen erstellen. In diesem Beispiel wird Überspringen als Serverskript implementiert.

3. **Playbook-Überschreibung:**

   Wenn Sie den vorhandenen Aktivitäts-Experience-Typ überschreiben möchten, ist dies möglich. Weitere Informationen finden Sie in der Now Platform-Dokumentation. Keine Playbook-Überschreibungen für dieses Beispiel.

### An CSF X Sandbox übermitteln

„An CSF X Sandbox senden“ ist ein Beispiel für einen Aktivitätsdefinitionsprozess.

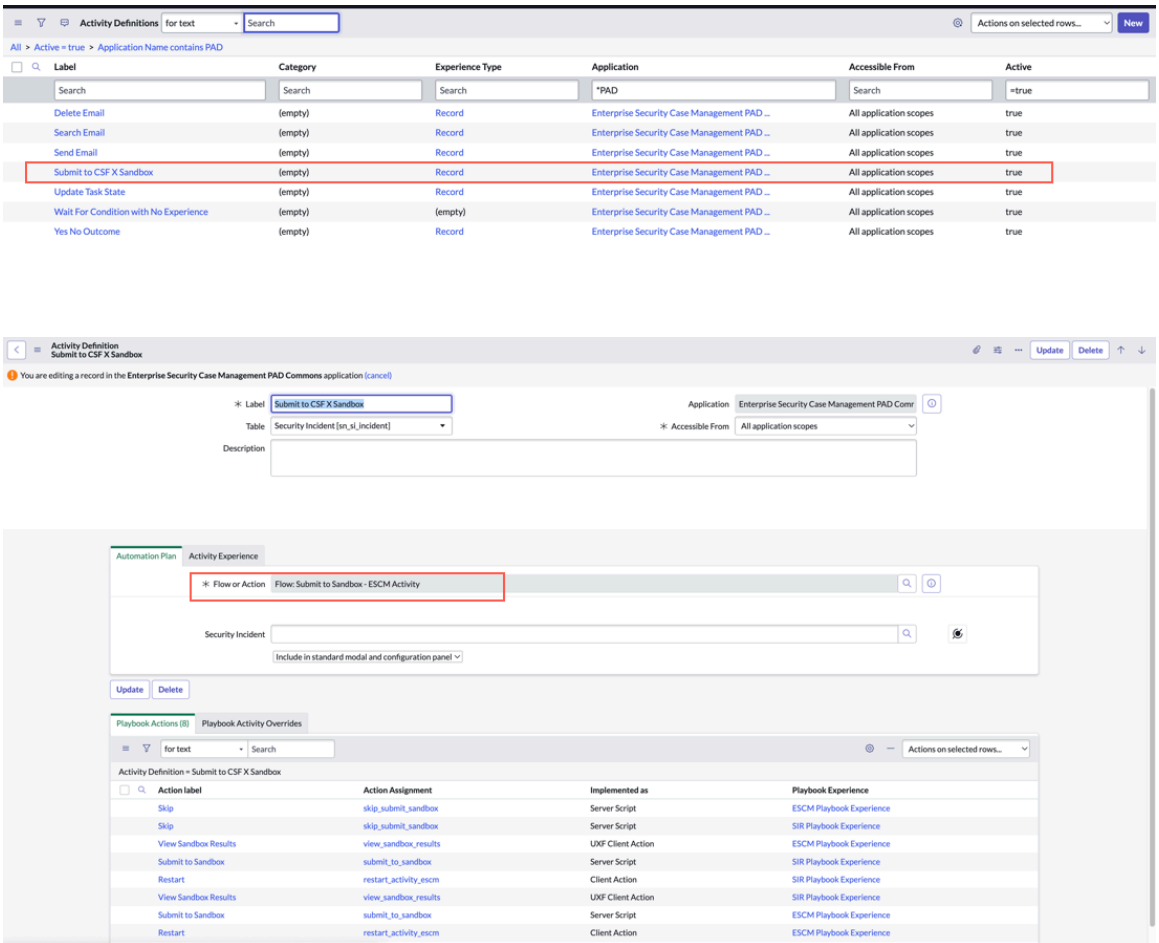
## Standard

Die grundlegenden Details umfassen den Namen (Bezeichnung), die Anwendung, die Beschreibung, die Tabelle und alle Anwendungen, von denen aus sie zugänglich sind.

Fügen Sie den Automatisierungsplan und die Aktivitäts-Experience hinzu, und übermitteln Sie sie. Bearbeiten Sie das Dokument nach der Übermittlung, um weitere Details für jede Registerkarte hinzuzufügen.

## Automatisierungsplan

Der Automatisierungsplan ordnet die mit dem Flow Designer erstellte Back-End-Aktion/den Back-End-Subflow zu. In diesem Beispiel wird der **Subflow „An Sandbox senden – ESCM-Aktivität“**verwendet.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Subflow ermöglicht das Senden der schädlichen erkennbaren Elemente an die Sandbox. Es sind alle Eingabefelder und Ausgabefelder definiert.

Security Incident ist das Eingabefeld.

### Aktivitäts-Experience

In diesem Beispiel ist **Datensatztyp** ausgewählt.

### Zugeordneter Datensatz

Der zugeordnete Datensatz dient zum Speichern der zugeordneten Daten, die sich auf die aktuelle Aktivität beziehen. Dadurch werden die Ausführungszeitdaten sowie der Status der Experience erfasst.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Experience-Statustabelle: Flow-Daten
- Experience-Statusdatensatz: VL

### Details

- Tagline: E-Mail senden
- Symbol: Umschlagkontur
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert dynamisch zur Laufzeit als Titel.
- Beschreibung: VL (Subflow-Ausgabe wird zugeordnet)
- Titel des Status „Ausstehend“: leer
- Beschreibung des Status „Ausstehend“: leer
- Datensatz-Felder
- Footer

### Formular

- Formularansicht: leer
- Formularfelder: leer

### Anlagen

Beispiel:

- Anhangquelle: Keine
- Anhang schreibgeschützt: Deaktiviert

1. Anhangquelle: Dies ist eine Dropdown-Liste. Welche Anhänge auf der Karte angezeigt werden sollen: Anhänge, die an den übergeordneten Datensatz angehängt sind, der zugeordnete Datensatz oder keine.
2. Anhang schreibgeschützt: Dies ist ein Wahr/Falsch-Wert. Verhindern Sie, dass der Benutzer die vorhandenen Anhänge umbenennt oder löscht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Funktionen

In diesem Beispiel

- SLA anzeigen: Deaktiviert
- Prüfliste anzeigen – Deaktiviert
- Ist automatisiert – Deaktiviert

## Playbook-Aktionen in Aktivitätsdefinition

Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden.

Dieses Beispiel verfügt über die Aktionen „Überspringen“, „Sandbox-Ergebnisse anzeigen“, „An Sandbox senden“ und „Neu starten“.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie einen neuen Datensatz in der zugehörigen Liste „Playbook-Aktionen“ am Ende der Seite erstellen.

## Playbook-Überschreibung

Keine Playbook-Überschreibungen für dieses Beispiel.

### Beispiel-Playbooks für SIR Workspace

Sie können Playbooks für SIR Workspace schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen Schritt für Schritt zu beheben. Sie können den Security Incident-Playbook-Flow automatisch oder manuell aufrufen.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit:

- Playbook für manuelles Phishing
- Playbook für automatisiertes Phishing
- Playbook für manuelle Malware
- Playbook für automatisierte Malware
- Playbook für fehlgeschlagene Anmeldung – manuell

### Arbeiten mit MSI-Datensätzen

Mit dem Security Incident Response-Arbeitsbereich können Sie Security Incidents als schwerwiegende Security Incidents vorschlagen, heraufstufen oder verknüpfen, wenn die Incidents als kritische Bedrohung für die Organisation identifiziert werden.

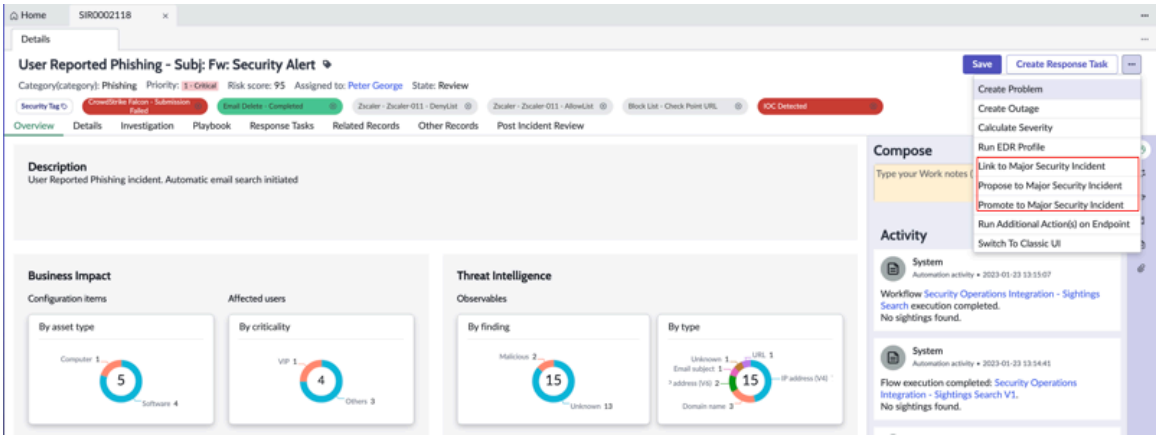
Nachdem Sie Management schwerwiegender Sicherheits-Incidents (MSIM) in Ihrer Instanz von Now Platform installiert haben, können Sie den Übergang von Security Incidents zu schwerwiegenden Incidents handhaben.

Die UI-Aktionen Management schwerwiegender Sicherheits-Incidents (MSIM) werden oben rechts im Formularbanner des Security Incident des SIR-Arbeitsbereichs angezeigt. Wählen Sie die UI-Aktion nach Bedarf aus.

**Hinweis:**
Einige Aktionen sind kontextbezogen. Beispielsweise ist die Aktion Verknüpfung aufheben nur verfügbar, wenn der Security Incident bereits vorgeschlagen, heraufgestuft oder mit einem schwerwiegenden Security Incident verknüpft wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Als schwerwiegenden Security Incident vorschlagen

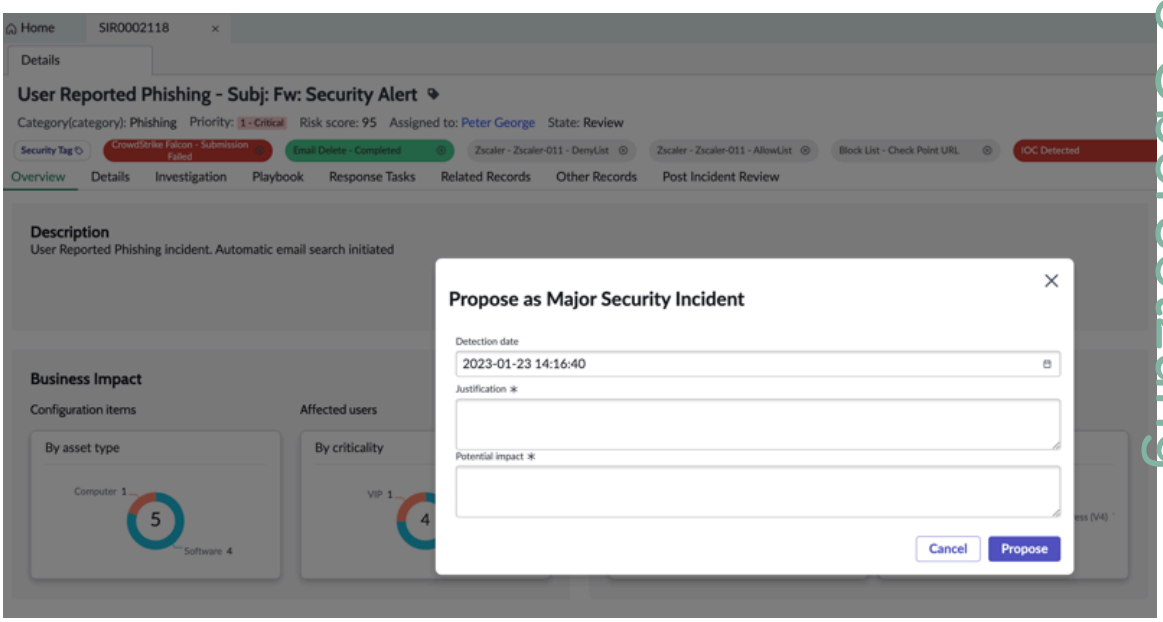
Schlagen Sie einen Security Incident als schwerwiegenden Security Incident (Major Security Incident, MSI) vor.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken **Sie auf Schwerwiegenden Security Incident vorschlagen**.




4. Füllen Sie im Formular die Felder aus, z. B. Erkennungsdatum, Begründung und Potenzielle Auswirkung.
5. Klicken Sie auf **Vorschlagen**.
   Der Incident-Datensatz wird als Kandidat für einen schwerwiegenden Security Incident vorgeschlagen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem der Incident-Datensatz als Kandidat **für schwerwiegenden Security Incident** vorgeschlagen wurde, wird das Tag Kandidat für schwerwiegenden Security Incident angewendet und im Banner des Security Incident-Formulars angezeigt.

**Hinweis:**
Klicken Sie **auf Verknüpfung mit schwerwiegendem Security Incident aufheben**, um die Verknüpfung mit dem Incident aufzuheben, den Sie nicht vorschlagen möchten oder der keine kritischen Auswirkungen hat. Die Verknüpfung des Incident wird aufgehoben und er wird dem Sicherheitsanalysten in der Listenansicht zur Korrektur angezeigt.

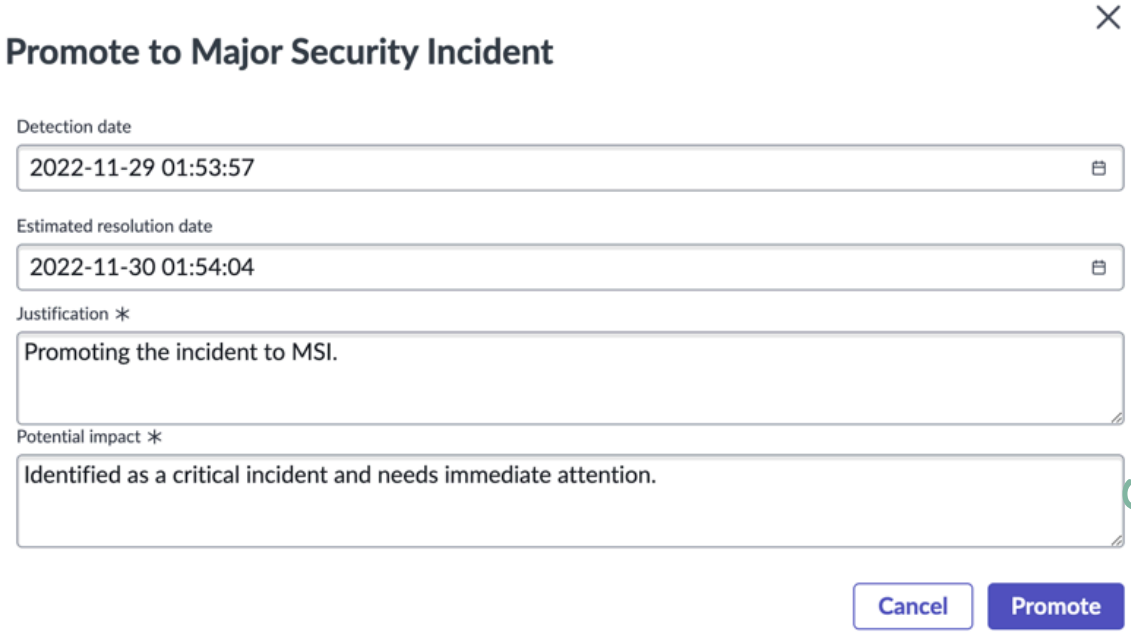
### Zu schwerwiegendem Security Incident heraufstufen

Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident herauf.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst.

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken Sie **auf Zu schwerwiegendem Security Incident heraufstufen**.
4. Füllen Sie im Formular die Felder aus, z. B. Erkennungsdatum, Geschätztes Lösungsdatum, Begründung und Potenzielle Auswirkung.




5. Klicken Sie **auf Hochstufen**.
   Der Incident-Datensatz wird als schwerwiegender Security Incident heraufgestuft.
   Nachdem der Incident-Datensatz als schwerwiegender Security Incident heraufgestuft wurde, wird das Tag **Schwerwiegender Security Incident** angewendet und im Formularbanner angezeigt.

**Hinweis:**
Sie können auch die Verknüpfung des schwerwiegenden Security Incident aufheben, wenn der Incident nicht kritisch ist. Der Incident wird dann aufgehoben und in der Listenansicht für die Korrektur durch den Sicherheitsanalysten aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

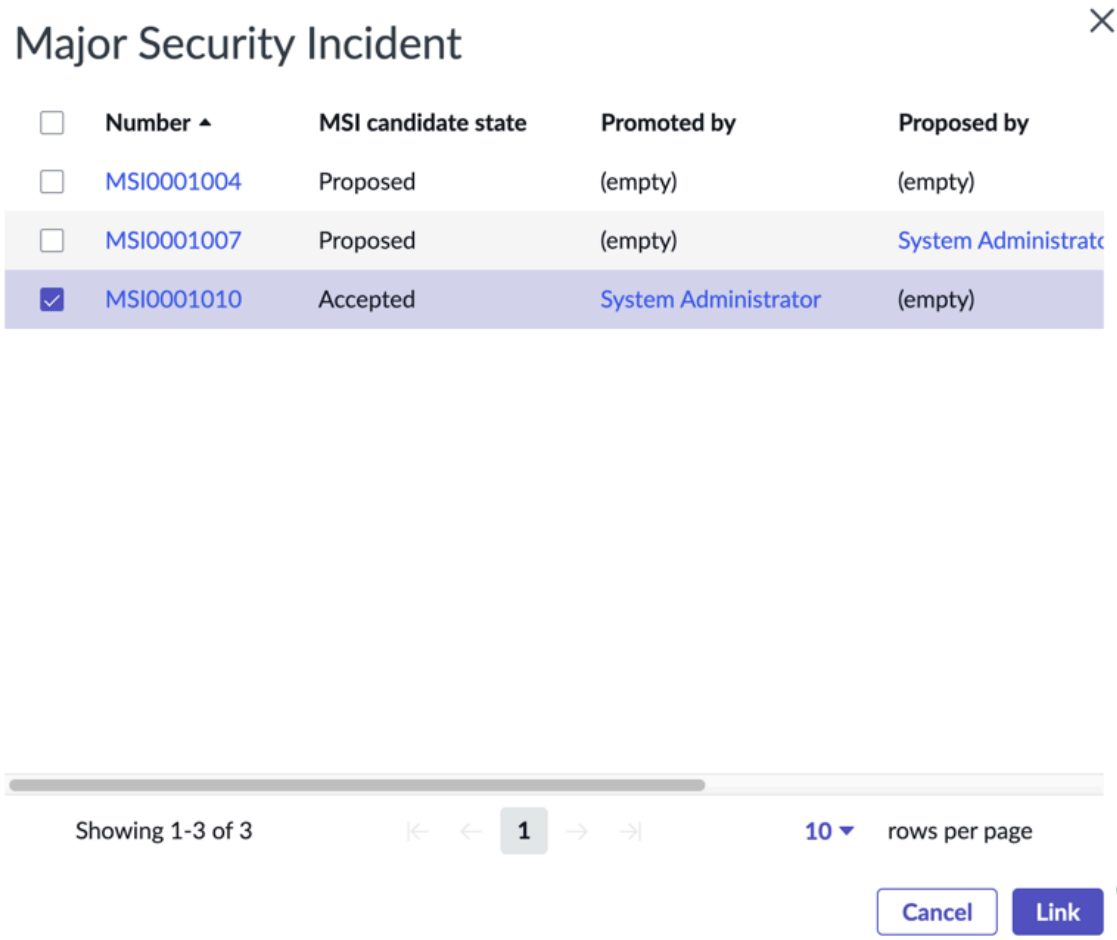
### Mit schwerwiegendem Security Incident verknüpfen

Verknüpfen Sie Security Incidents mit schwerwiegenden Security Incidents als untergeordnete Security Incidents.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst.

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Öffnen Sie einen beliebigen Security Incident.
3. Klicken Sie **auf Mit schwerwiegendem Security Incident verknüpfen**.




4. Wählen Sie die Incidents aus, die mit einem schwerwiegenden Security Incident verknüpft werden sollen.
5. Klicken Sie auf **Link**.
6. Der Incident-Datensatz ist als untergeordneter Incident des schwerwiegenden Security Incident verknüpft. Nachdem der Incident als untergeordneter Incident mit einem schwerwiegenden Security Incident verknüpft wurde, wird das Tag **Schwerwiegender Security Incident** angewendet und im Formularbanner angezeigt.

### Arbeiten mit Formular-UI-Aktionen

Im Folgenden finden Sie die UI-Aktionen, die im Security Incident-Formular angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So navigieren Sie zu den Formular-UI-Aktionen:

1. Gehe zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wählen Sie in der Listenansicht einen beliebigen Security Incident aus.
3. Alle UI-Aktionen sind in der oberen rechten Ecke des Security Incident-Formulars vorhanden.

### Arbeitsbereichsformular-UI-Aktionen

| Feldname | Beschreibung |
|---|---|
| Speichern | Speichern oder aktualisieren Sie den Security Incident Response-Datensatz, nachdem Sie Änderungen vorgenommen haben. |
| Antwortaufgabe erstellen | Erstellen Sie eine Antwortaufgabe für den Security Incident. |
| E-Mails verfassen | Verfassen Sie E-Mails für den Security Incident. |
| Playbook hinzufügen | Fügen Sie das Playbook für den Security Incident manuell hinzu. |
| Incident erstellen | Erstellen Sie einen Incident innerhalb des Security Incident. |
| Kundenservicefall erstellen | Erstellen Sie einen Kundenservicefall für den Security Incident, der vom Customer Service Management (CSM)-Team nachverfolgt wird.<br>**Hinweis:**<br>Diese Option ist nur verfügbar, wenn Customer Service Management (CSM) installiert ist. |
| Zugehörige(n) Workflow(s) öffnen | Öffnen Sie einen beliebigen Workflow-Kontext, der dem Security Incident zugeordnet ist. Diese Option ist nur sichtbar, wenn Workflows vorhanden sind. |
| Change-Anforderung erstellen | Erstellen Sie eine Change-Anforderung innerhalb des Security Incident. |
| Problem erstellen | Erstellen Sie ein Problem innerhalb des Security Incident. |
| Ausfall erstellen | Erstellen Sie einen Ausfall innerhalb des Security Incident. |
| Schweregrad berechnen | Berechnen Sie den Schweregrad eines Security Incident mit vordefinierten Rechnern. Der Schweregrad wird basierend auf den vordefinierten Regeln in den Rechnern berechnet. Der Schweregrad eines Incident basiert auf der Risikopunktzahl, den Geschäftsauswirkungen und der Priorität. |
| EDR-Profil ausführen | Wählen Sie das EDR-Profil für die erforderliche Integration aus, und führen Sie es aus.<br>**Hinweis:**<br>Diese Option ist nur verfügbar, wenn Integrationen installiert sind. |
| Mit schwerwiegendem Security Incident verknüpfen | Verknüpfen Sie einen Security Incident mit einem schwerwiegenden Security Incident. |
| Risikoereignis melden | Melden Sie diesen Security Incident als Risikoereignis an das Risikomanagement-Team. Das Risikomanagementteam analysiert das Ereignis und stellt sicher, dass solche Ereignisse und die damit verbundenen Verluste nicht erneut auftreten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

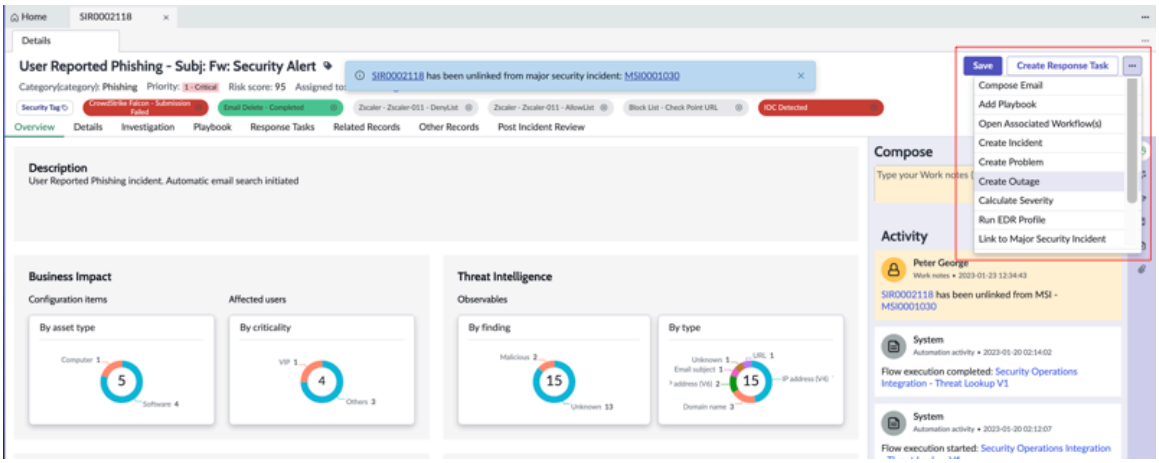
| Feldname | Beschreibung |
|---|---|
| | **Hinweis:**<br>Diese Option ist nur verfügbar, wenn Risk Management installiert ist. |
| Verknüpfung mit schwerwiegendem Security Incident aufheben | Heben Sie die Verknüpfung mit schwerwiegendem Security Incident auf. |
| Als schwerwiegenden Security Incident vorschlagen | Schlagen Sie einen Security Incident als schwerwiegenden Security Incident vor. |
| Zu schwerwiegendem Security Incident heraufstufen | Stufen Sie einen Security Incident als schwerwiegenden Security Incident herauf. |
| Zusätzliche Aktion(en) für Endpunkt ausführen | Zusätzliche Aktionen für den Endpunkt ausführen<br>**Hinweis:**<br>Diese Option ist nur verfügbar, wenn Endpunktintegrationen installiert sind. Beispiel: FireEye HX |
| Neues Ereignis in MISP erstellen | Erstellen und ändern Sie Events in MISP automatisch oder manuell.<br>**Hinweis:**<br>Diese Option ist nur verfügbar, wenn die MISP-Integration installiert ist. |
| Ordnen Sie die MITRE ATT&K-Technik zu | Ordnen Sie dem Security Incident MITRE ATT&K-Techniken zu.<br>**Hinweis:**<br>Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist. |
| MITRE ATT&K-Informationen anzeigen | Zeigt die MITRE ATT&K-Informationen an, die dem Security Incident zugeordnet sind<br>**Hinweis:**<br>Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist. |
| Dem Sicherheitsfall hinzufügen | Fügen Sie den Security Incident einem vorhandenen oder neuen Sicherheitsfall hinzu.<br>**Hinweis:**<br>Diese Option ist verfügbar, wenn Threat Intel installiert ist. |
| Zu klassischer UI wechseln | Ermöglichen Sie Analysten, zwischen klassischer und neuer UI zu wechseln, damit Analysten auch an den vorhandenen Funktionalitäten arbeiten können, die im neuen Arbeitsbereich noch nicht verfügbar sind. |
| Abbrechen | Brechen Sie einen Security Incident ab. Nachdem Sie **Abbrechen ausgewählt haben, werden** alle zugehörigen Datensätze wie Antwortaufgaben und untergeordnete Security Incidents ebenfalls abgebrochen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feldname | Beschreibung |
|---|---|
| Löschen | Löschen Sie einen Security Incident-Datensatz. |

4. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Sie sehen die UI-Aktionen oben auf der Seite.




### Workflow zum Abschluss von Security Incidents

Schließen Sie den Security Incident, indem Sie den Incident-Status aktualisieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Prozedur

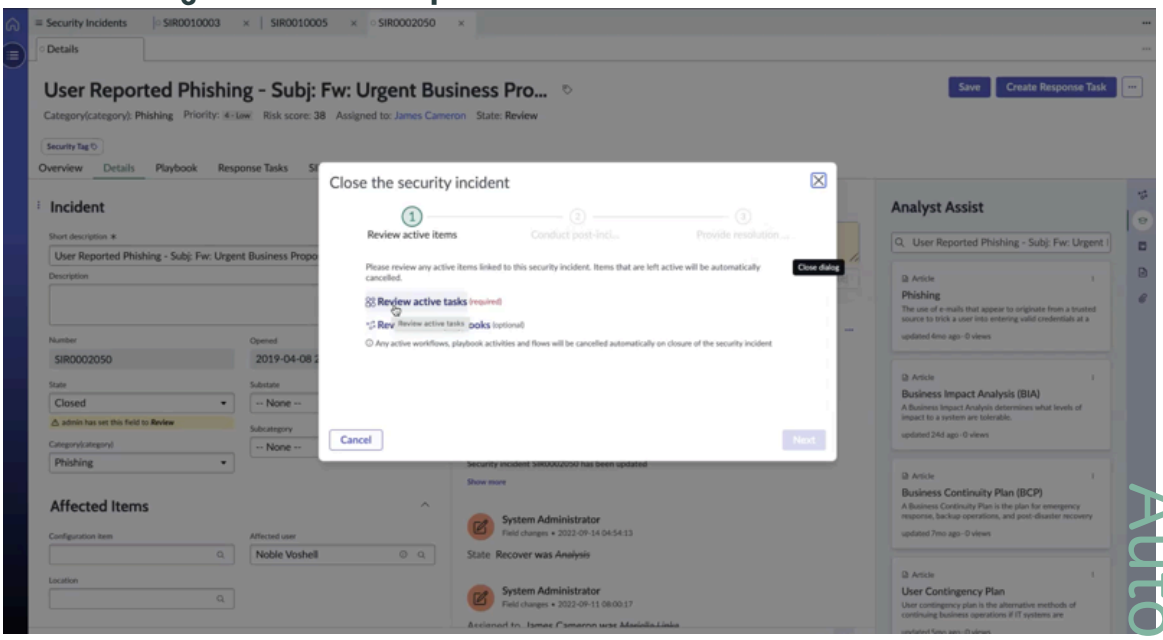
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**.
2. Wechseln Sie beispielsweise zu **Lists** > **Security Incidents** > **Offene Incidents**.
3. Öffnen Sie einen Incident, den Sie schließen möchten.
4. Wechseln Sie zur Registerkarte **Details**.
5. Führen Sie einen Drilldown zum Incident-Status durch, und wählen Sie **Schließen**aus.
6. Führen Sie die Abschlussaktivitäten aus.

   - Dies ist ein obligatorischer Schritt zur Überprüfung einer Aufgabe, bevor ein Security Incident geschlossen wird. Alle Antwortaufgaben müssen vom Analysten überprüft und geschlossen oder abgebrochen werden, bevor sie als Security Incident geschlossen werden. Wenn der Analyst auf **Aktive Aufgaben**prüfen klickt, gelangt der Benutzer zur Registerkarte **Antwortaufgaben**. Eine Sitzungsnachricht wird mit der Aufforderung angezeigt, dass Sie gerade einen Security Incident schließen. Klicken Sie auf **Fortfahren**.
   - Klicken Sie auf **Fortsetzen**. Der erste Schritt – die Überprüfung aktiver Aufgaben beim Schließen des Security Incident ist abgeschlossen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

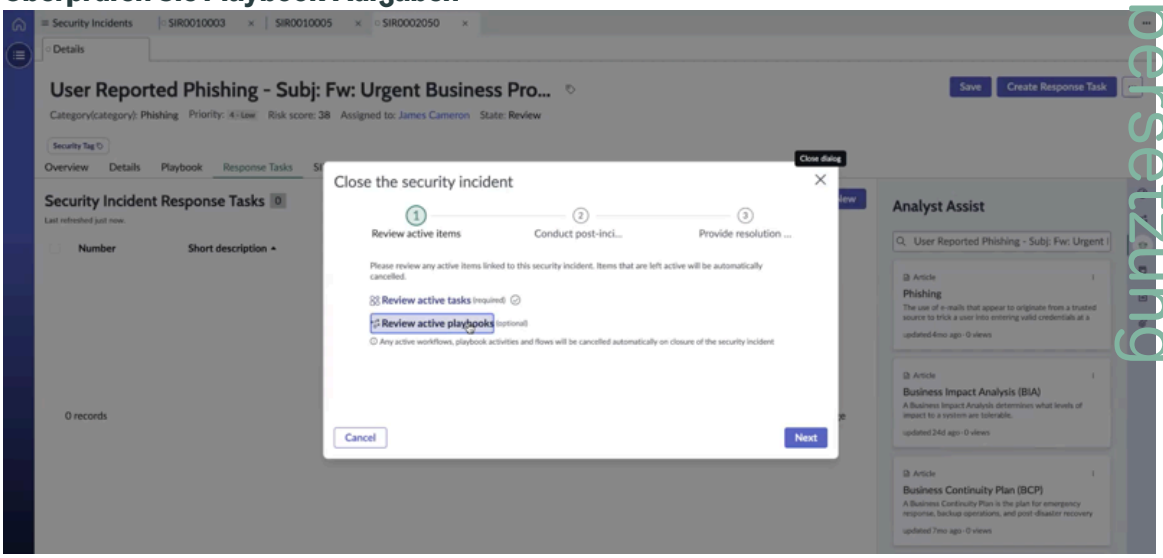
**Abschlussaufgaben werden überprüft**




- Fahren Sie mit dem nächsten Schritt fort, um die aktiven Playbooks für die Überprüfung durch den Analysten zu überprüfen. Dies ist ein optionaler Schritt. Sie können auf den Link klicken, um die aktive Playbook-Aufgabe zu überprüfen und sie nach Bedarf zu schließen.

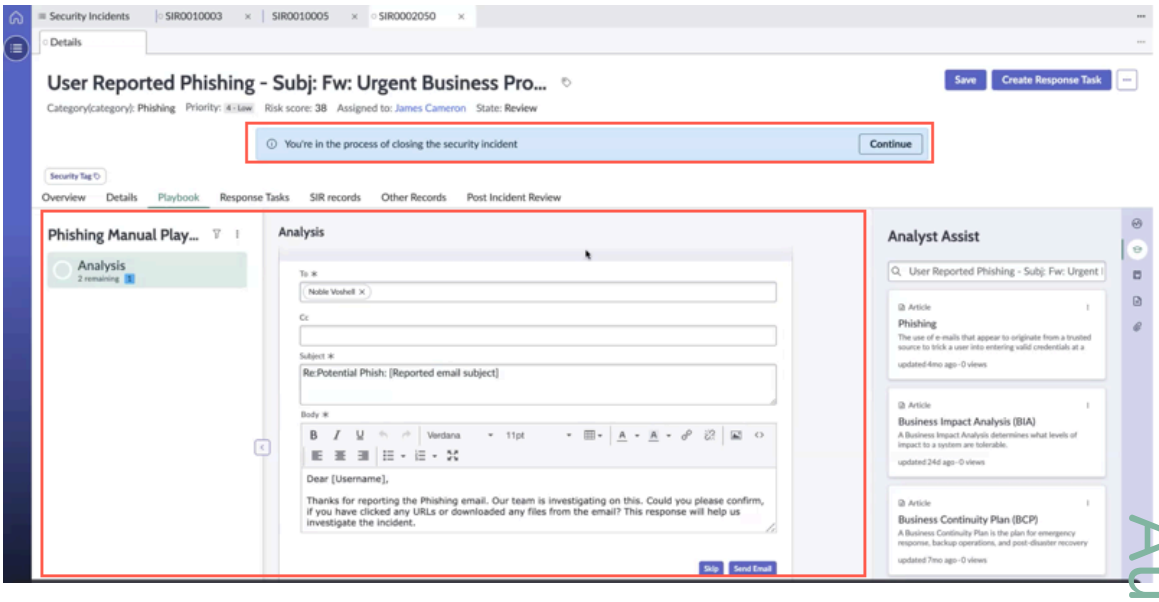
**Hinweis:**
Alle aktiven Workflows, Playbook-Aktivitäten und Flows werden automatisch abgebrochen, wenn der Security Incident geschlossen wird.

**Überprüfen Sie Playbook-Aufgaben**



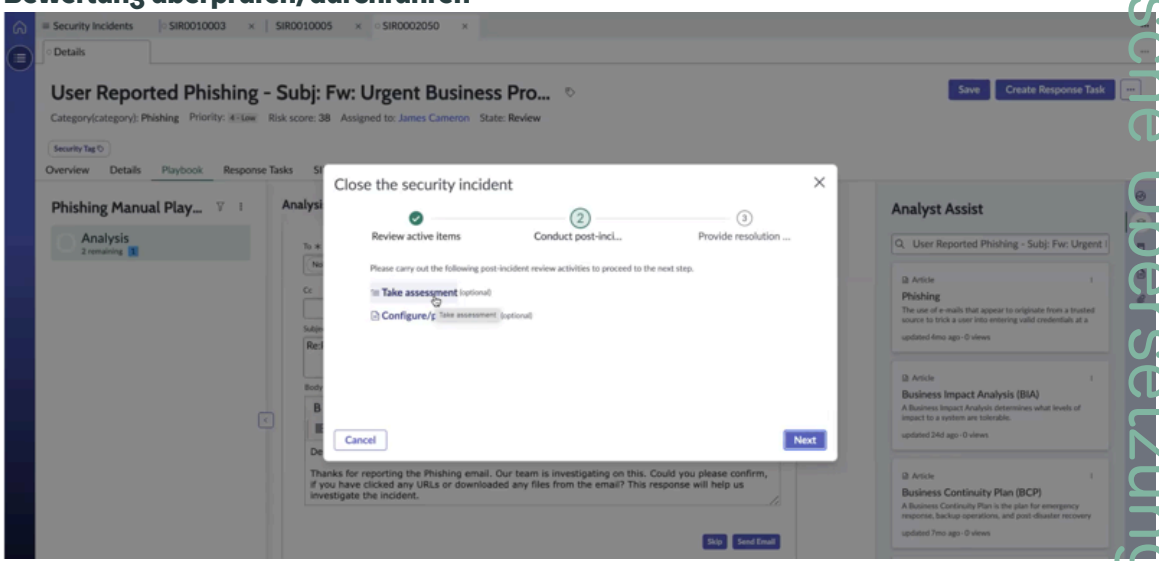

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



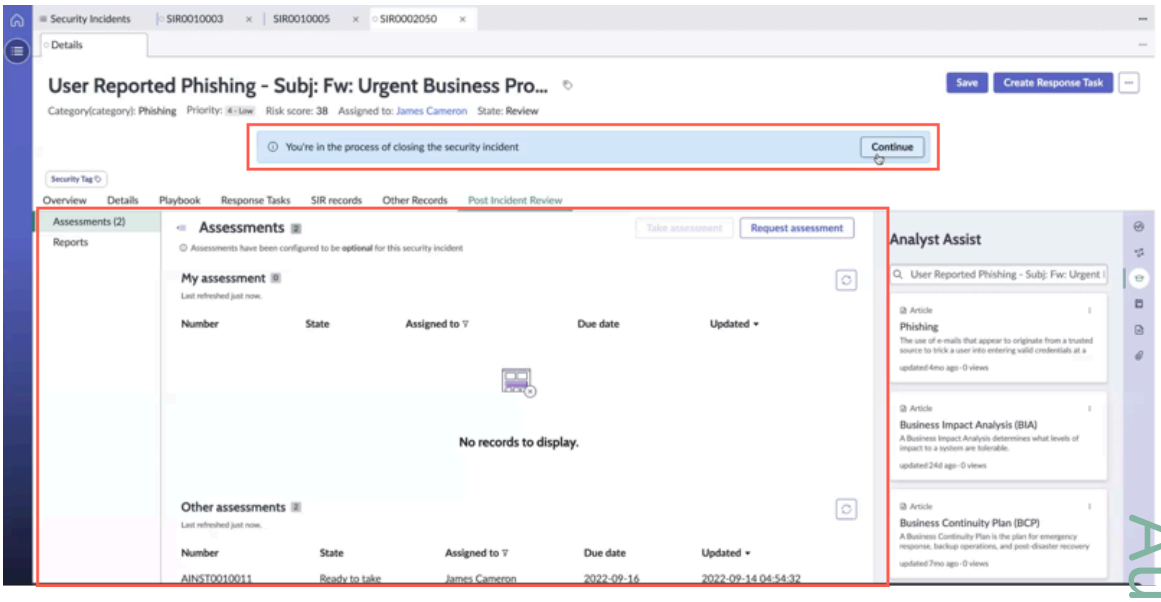

- Überprüfungsbericht nach Incident: Sie werden jetzt zur Überprüfung der Aktivitäten nach Incidents verschoben, um mit dem Abschluss fortzufahren. Wenn die Bewertung optional ist, überspringen Sie den Schritt. Wenn die Bewertung obligatorisch ist, führen Sie die Bewertung durch und schließen Sie sie ab.

### Bewertung überprüfen/durchführen

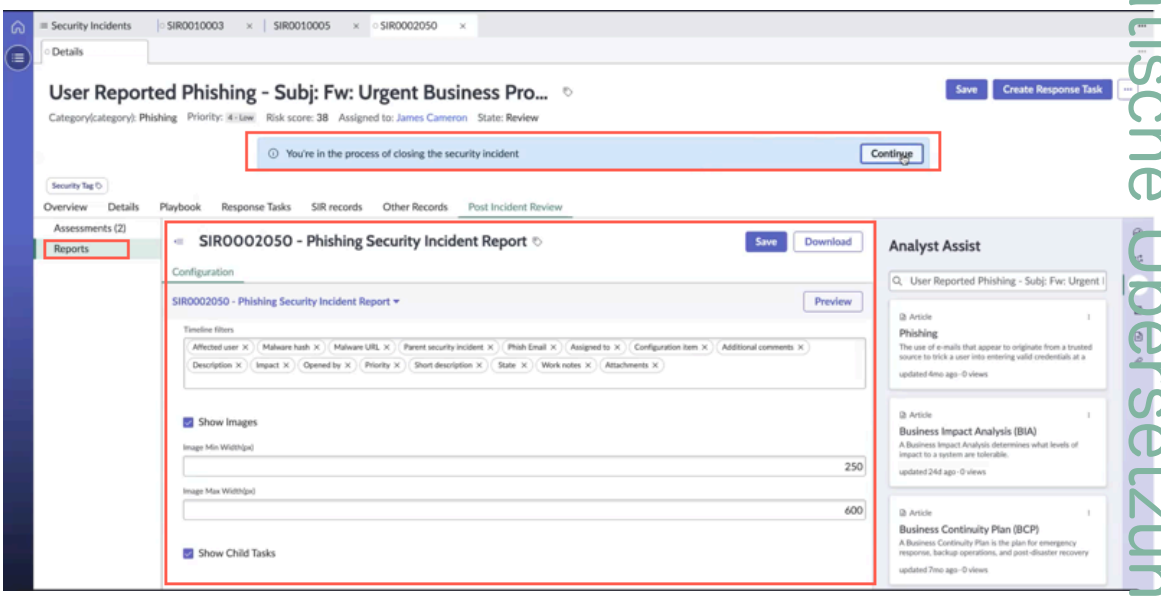



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- Bericht konfigurieren/in der Vorschau anzeigen: Dies ist erneut ein optionaler Schritt. Klicken Sie auf den Link, um den Bericht zu überprüfen, und fahren Sie mit dem **nächsten** Schritt fort.

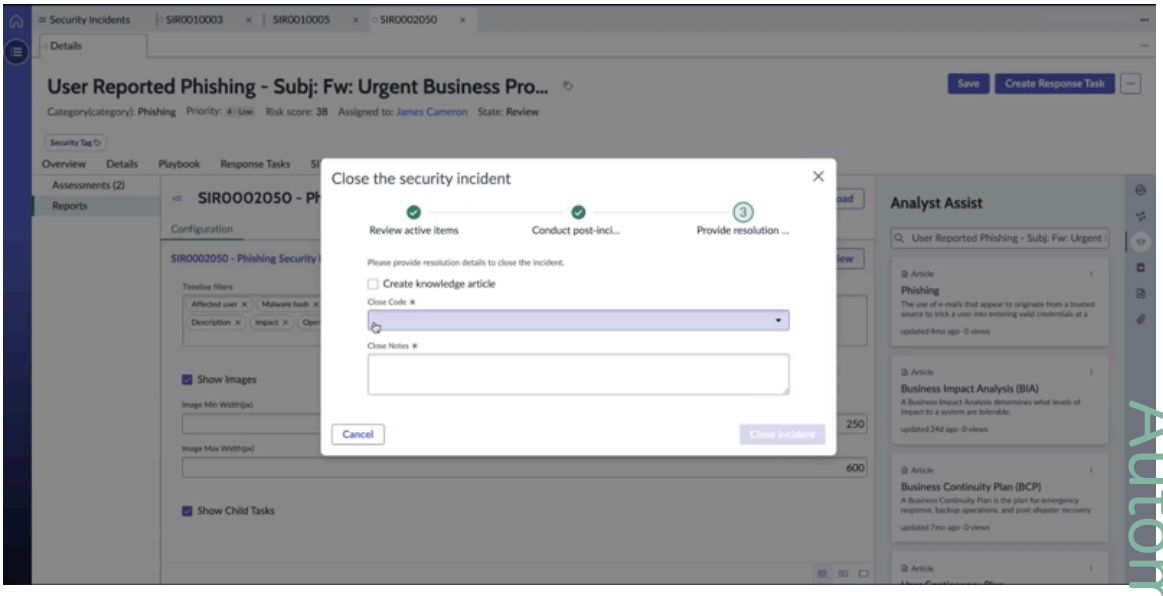



- Lösungsdetails bereitstellen: Der Analyst kann das Kontrollkästchen aktivieren, um Wissensartikel automatisch zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geben Sie den Abschlusscode und die Abschlussnotizen an, und klicken Sie auf **Incident schließen**.




**Hinweis:**
Wenn der Analyst das Dialogfeld **Security Incident schließen** abbricht, kann er zur Registerkarte **Details** navigieren und den Incident-Status in „ **Schließen** “ ändern, um mit dem Abschluss fortzufahren.

## SIR-Arbeitsbereichs-Dashboards anzeigen

In diesem Abschnitt werden die wichtigen Metriken zur Analyse Ihres Security Incident Response -Prozesses vorgestellt, z. B. neue Security Incidents oder das Durchschnittsalter offener Security Incidents.

In der klassischen Benutzeroberfläche sind einige Standard-Dashboards unter der Homepage und Performance Analytics Dashboards verfügbar, wenn das Plugin Performance Analytics für Security Incident Response installiert ist. All dies ist jetzt im neuen Arbeitsbereich im Abschnitt „ **SIR-Dashboards** “ verfügbar.

**Standard-Dashboards unter Homepage**:

- Security Incident Response – Übersicht
  - Analystenübersicht
  - Managerübersicht (in zukünftigen Releases unterstützt)
  - CISO-Übersicht (in zukünftigen Releases unterstützt)
- **Platform Analytics für** *`Security Incident Response`*
  - Security Incident-Explorer
  - CISO-Dashboard (zukünftiges Release)
  - Security Incident-Management
  - KPIs von Security Incident-Management Premium
  - Effizienz von Security Operations
  - Kontextsensible Analysen – SI-Dashboard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Für Security Incident Response-Dashboards wie das CISO-Dashboard kann es zu Wiederholungen von Dashboards in Standard- und Plattformanalysen kommen. Wenn das Plugin installiert ist, wird in diesen Dashboards zusätzlicher Inhalt angezeigt, der nicht als Duplikat verfügbar ist.

Benutzer müssen das Plugin installieren, damit die unter Platform Analytics for Security Incident Response Dashboards aufgeführten Dashboards im Arbeitsbereich vorhanden sind. Andernfalls sind nur die Standard-Dashboards verfügbar.

In der aktuellen Version von SIR Workspacesind die folgenden Dashboards im Abschnitt „ **SIR-Dashboards** “ verfügbar. Die anderen fehlenden Dashboards sind in späteren Releases verfügbar.

### Security Incident Response-Dashboards

| Dashboard | Beschreibung |
|---|---|
| Standard-Dashboard | |
| Sicherheitsanalyst – Übersicht | Mit diesem Dashboard können Sicherheitsanalysten Security Incidents anzeigen, die basierend auf der Arbeit des Analysten mit kritischer Priorität, Arbeit mit hoher Priorität, Security Incidents, die dem Analysten zugewiesen sind, Aufgaben, die den Analysten zugewiesen sind, und Incident-Anzahl zusammengefasst werden. |
| Performance Analytics (PA) für Security Incident Response Dashboards | |
| Security Incident-Explorer | Mit diesem Dashboard können Sicherheitsmanager und Analysten Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen. Mit diesen Ansichten erhalten Manager und Analysten schnell Einblicke in die Häufigkeit, mit der Angriffe auftreten, und darüber, welche Business Services betroffen sind. |
| Security Incident-Management | Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/ Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung einfach nachverfolgen. |
| CISO-Dashboard | Unterstützung in zukünftigem Release vorgeschlagen. |
| Effizienz von Security Operations | Mit diesem Dashboard können Manager und Analysten allgemeine Effizienzmetriken anzeigen und die Leistung des SOC messen. |
| KPIs von Security Incident-Management Premium | Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents nachverfolgen und anzeigen, von der ersten Analyse/Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung. |
| Kontextsensitive Analysen – S | Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter offener Security Incidents, die durchschnittliche Abschlusszeit von Security |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident Response-Dashboards (Fortsetzung)**

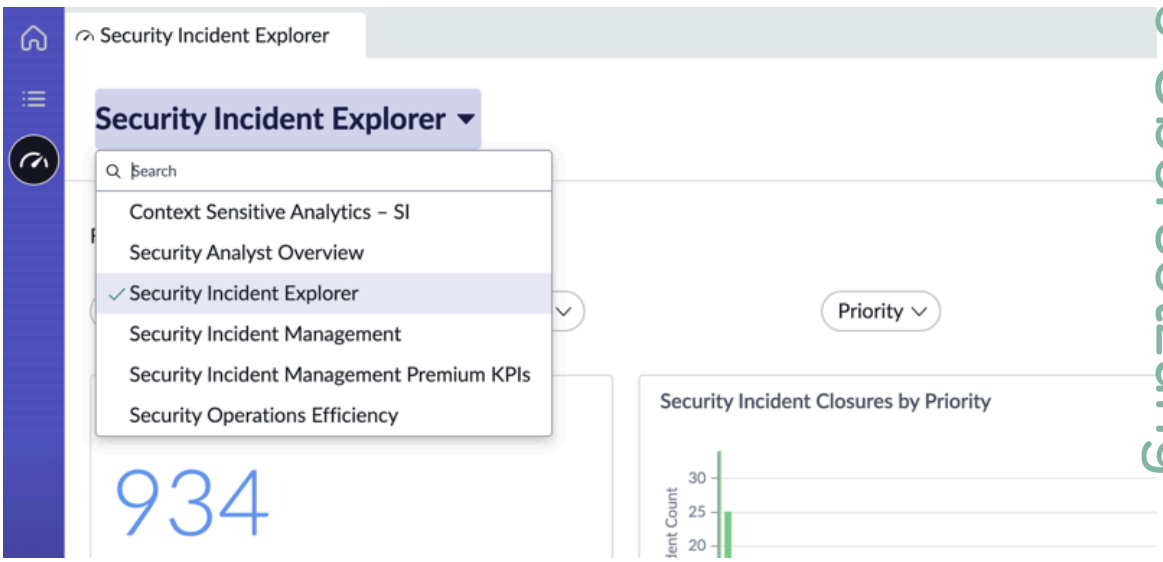
| Dashboard | Beschreibung |
|---|---|
| | Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der anzeigen Incidents, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden. |

## Greifen Sie auf SIR- und PA-Dashboards zu

Das Symbol für **SIR-Dashboards** wird auf der linken Seite der Arbeitsbereichs-Homepage angezeigt.

**Hinweis:**
Benutzer mit sn_si.manager- oder sn_si.admin-Zugriff können die Dashboards bearbeiten. Die Benutzer müssen sich im selben Bereich der Dashboards befinden, die der Benutzer bearbeiten möchte. Wenn beispielsweise das Dashboard für Sicherheitsanalysten im SIR-Arbeitsbereich verfügbar ist, muss sich der Benutzer auch im selben Bereich des SIR-Arbeitsbereichs befinden, um Änderungen am Dashboard vorzunehmen.

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Management Workspace**.
2. Klicken Sie auf das **SIR-Dashboards** .
3. Wählen Sie das gewünschte Dashboard aus der Dropdown-Liste aus.




Sie können die Dashboards bearbeiten, neue Elemente zu den Dashboards hinzufügen und eigene Dashboards erstellen. Weitere Informationen zur Verwendung von Dashboards finden Sie unter Mit interaktiven Dashboards arbeiten

### Zeigen Sie das Dashboard „Sicherheitsanalystenübersicht“ an

Mit diesem Dashboard können Sicherheitsanalysten Security Incidents anzeigen, die basierend auf der Arbeit von Analysten mit kritischer Priorität, Arbeit mit hoher Priorität, Security Incidents, die dem Analysten zugewiesen sind, Aufgaben, die den Analysten zugewiesen sind, und Incident-Anzahl zusammengefasst werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

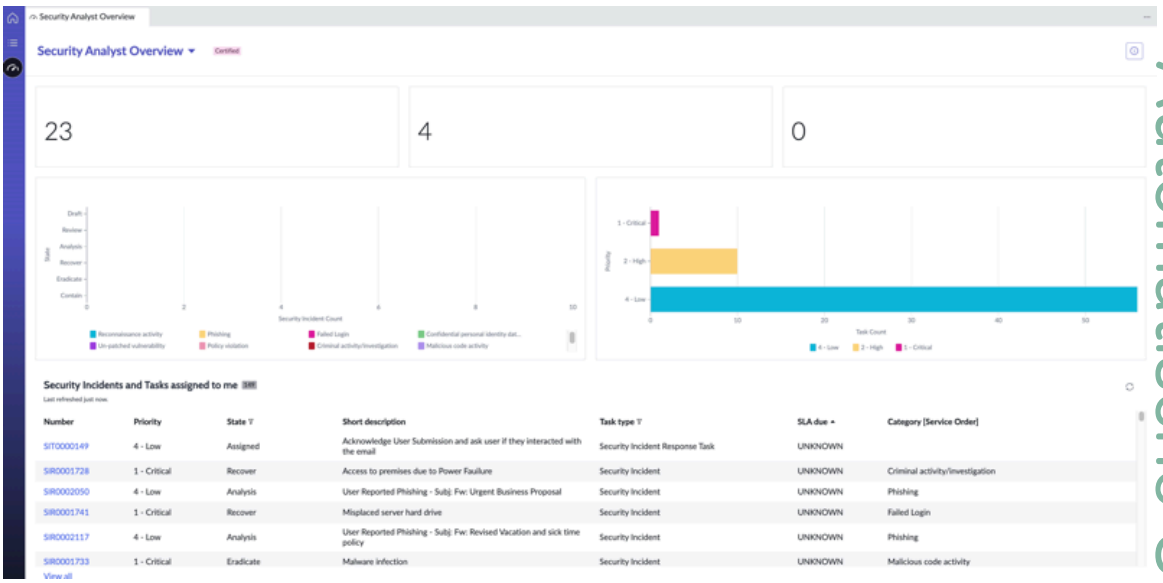
### Vorbereitungen

Standardmäßig wird das Dashboard „Sicherheitsanalystenübersicht“ für Benutzer mit sn_si.analyst-Zugriff angezeigt.

Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (Schreiben)

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Analyst Übersicht** aus.




Weitere Aktionen finden Sie im Dashboard „Security Analyst Overview“ (Sicherheitsanalyst – Übersicht). Ausführliche Informationen zum Dashboard „Security Analyst Overview“ (Sicherheitsanalysten – Übersicht) finden Sie unter Security Incident Response Platform Analytics-Lösungen.

## Zeigen Sie das Security Incident Explorer-Dashboard an

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung gruppiert anzeigen.

### Vorbereitungen

Standardmäßig wird das Security Incident Explorer-Dashboard für Benutzer mit sn_si.manager-Zugriff angezeigt.

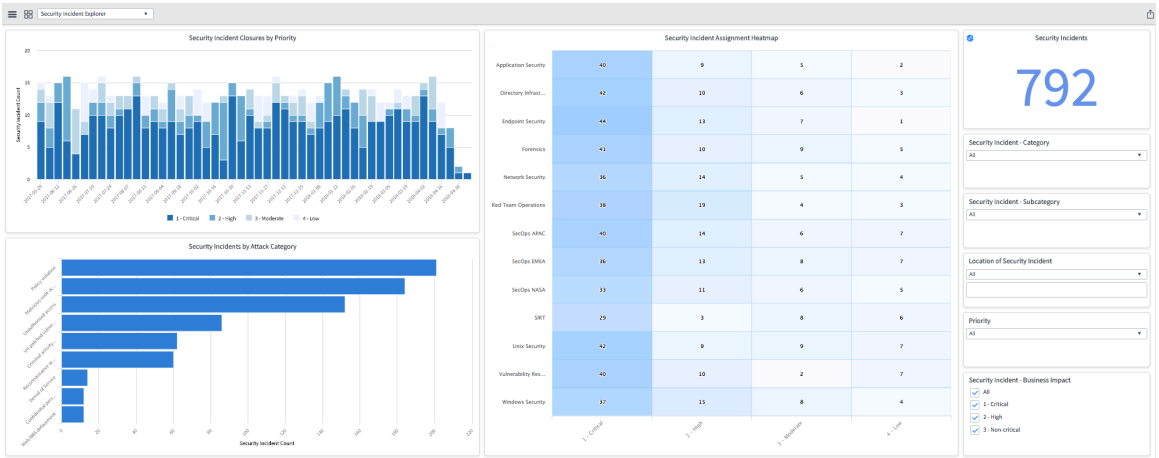
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (Schreiben)

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Incident Explorer** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Zeigen Sie das Security Incident Explorer-Dashboard für weitere Aktionen an. Ausführliche Informationen zum Security Incident Explorer-Dashboard finden Sie unter Security Incident Explorer-Dashboard

Im aktuellen Release wird die folgende Liste von Berichten im Security Incident Explorer-Dashboard nicht unterstützt:

- Security Incident-Zuweisungs-HeatMap: HeatMap-Visualisierung ist nicht verfügbar.
- Security Incident-Übersicht – Zuordnungsvisualisierung ist nicht verfügbar.

### Zeigen Sie das Security Incident Management-Dashboard an

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents von der ersten Analyse/Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung einfach nachverfolgen.

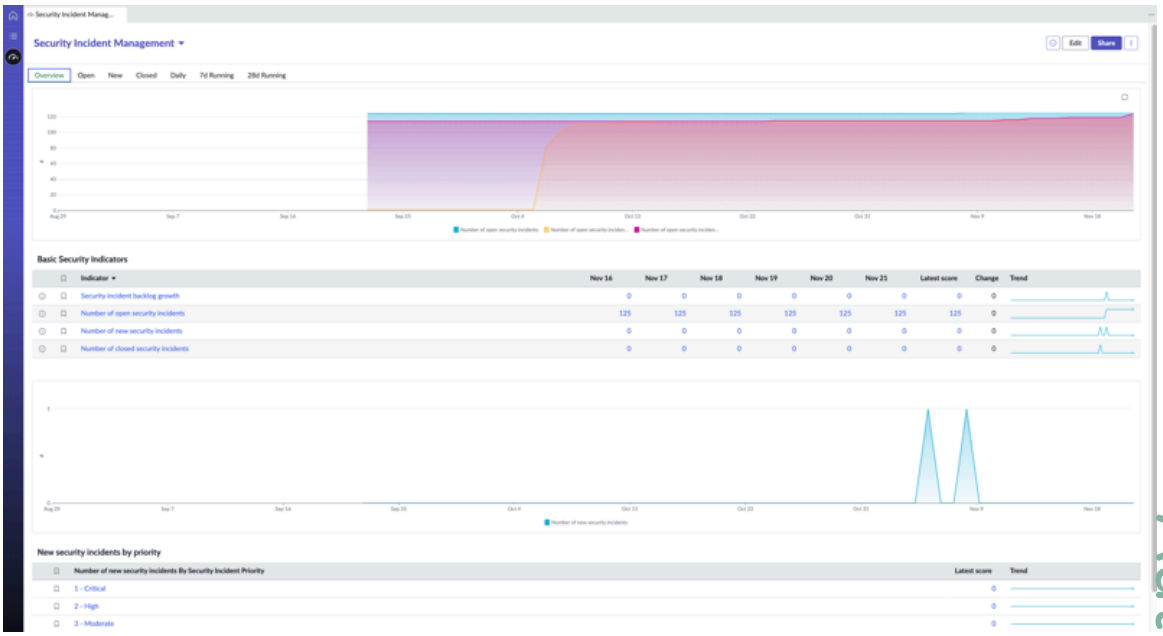
**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie **Security Incident Management** aus der Dropdown-Liste aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Weitere Aktionen finden Sie im Security Incident Management-Dashboard. Ausführliche Informationen zum Security Incident Management-Dashboard finden Sie unter Security Incident Management-Dashboard

### Zeigen Sie das Dashboard „Effizienz von Sicherheitsvorgängen“ an

SOC-Manager (Security Operations Center) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

### Vorbereitungen

Im aktuellen Release wird der folgende Bericht im Dashboard „Effizienz von Sicherheitsvorgängen“ nicht unterstützt:

- Security Incident-Phasenanalyse – Workbench ist nicht verfügbar

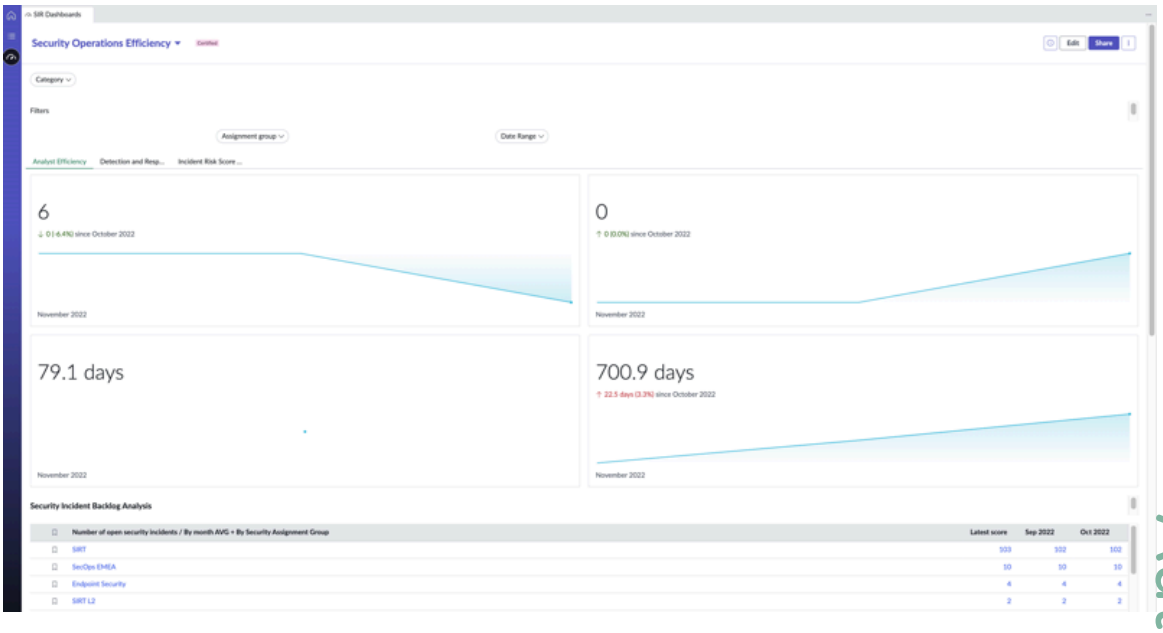
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie in der Dropdown-Liste die Option **Effizienz von Sicherheitsvorgängen** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Weitere Aktionen finden Sie im Dashboard „Effizienz von Sicherheitsvorgängen“. Ausführliche Informationen zum Dashboard „Effizienz von Sicherheitsvorgängen“ finden Sie unter Dashboard „Effizienz von Sicherheitsvorgängen“.

### Zeigen Sie das Dashboard „Security Incident Response Premium-KPIs“ an

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents nachverfolgen und anzeigen, von der ersten Analyse/Erkennung bis hin zu Eindämmung, Beseitigung und Wiederherstellung.

#### Vorbereitungen

Im aktuellen Release wird die folgende Liste von Berichten im KPIs-Dashboard von Security Incident Response Premium nicht unterstützt:

- Nach Status verarbeiten – Workbench ist nicht verfügbar
- Nach Alter verarbeiten – Workbench ist nicht verfügbar
- Security Incidents, die nach Zuweisungsgruppe und Status mehr als 30 Tage offen sind – Heatmap-Visualisierung ist nicht verfügbar.
- Security Incidents, die seit mehr als 30 Tagen nicht nach Zuweisungsgruppe und Status aktualisiert wurden – HeatMap-Visualisierung ist nicht verfügbar.
- Security Incidents mit nicht aktivem Beauftragten – HeatMap-Visualisierung ist nicht verfügbar.

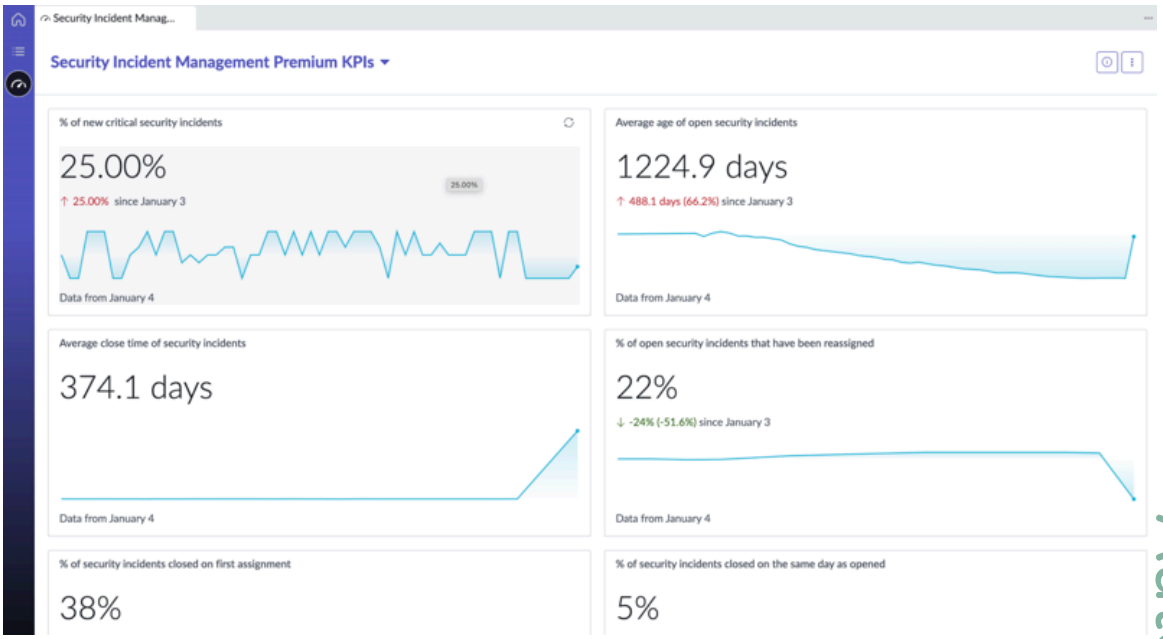
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie in der Dropdown-Liste **Security Incident Response Premium-KPIs** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Weitere Aktionen finden Sie im Dashboard „Security Incident Response Premium-KPIs“.
   Ausführliche Informationen zum KPI-Dashboard von Security Incident Response Premium finden Sie unter Security Incident Management Premium-Dashboard

### Zeigen Sie das Dashboard „Kontextsensitive Analysen – SI“ an

Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter offener Security Incidents, die durchschnittliche Abschlusszeit von Security Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der anzeigen Incidents, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden.

#### Vorbereitungen

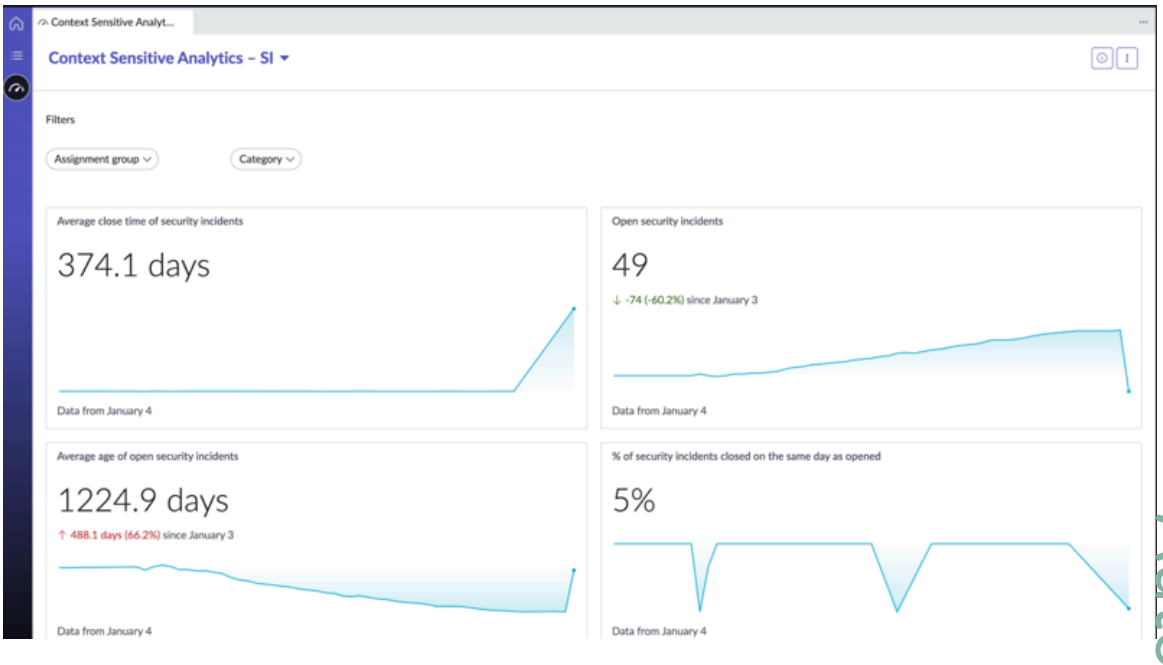
Erforderliche Rolle: sn_si.analyst (Lesen), sn_si.manager oder sn_si.admin (schreiben)

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf das Symbol **SIR-Dashboards**, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie **Context Sensitive Analytics – SI** aus der Dropdown-Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Zeigen Sie das Dashboard „Kontextsensitive Analysen – SI“ an, um weitere Aktionen anzuzeigen.

### Zeigen Sie das CISO-Dashboard an

Dieses Dashboard bietet den Chief Information Security Officers (CISOs) eine allgemeine Übersicht über Security Incidents und wöchentliche Incident-Trends in der Instanz in Form von grafischen Diagrammen. Mit diesen Diagrammen können Sie die Leistung des Security Operations Center (SOC) effektiv anzeigen und analysieren.

### Vorbereitungen

- Erforderliche Rolle: sn_si.admin und sn_si.ciso – Incidents bearbeiten und anzeigen.
- Vergewissern Sie sich, dass Sie die App Performance Analytics for Security Incident Response installiert haben.

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Das CISO-Dashboard und das CISO-Übersichts-Dashboard waren in der klassischen Benutzeroberfläche zwei verschiedene. Aber jetzt wurden die Fähigkeiten der beiden Dashboards unter dem CISO-Dashboard zusammengeführt.

Das CISO-Dashboard bietet wöchentlich wichtige Einblicke in Ihre Security Incidents. Sie können Indikatoren einrichten und Daten-Snapshots der Incidents sammeln, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert.

Sie können die wöchentlichen Trends mithilfe der Widgets im CISO-Dashboard visualisieren. Die Daten oder Statistiken für die Trends Ihrer Security Incidents werden aus den Eigenschaften des wöchentlichen Incident-Indikators erfasst, die von der Organisation definiert werden. Mithilfe der folgenden Diagramme können Sie wichtige Einblicke gewinnen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

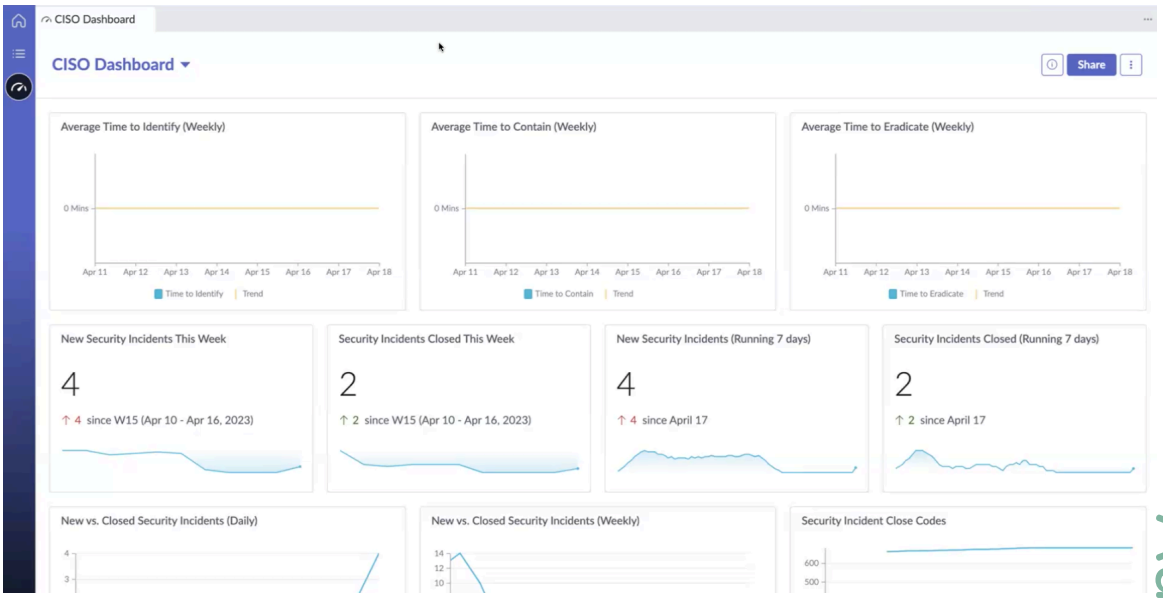
- **Durchschnittliche Zeit bis zur Identifizierung (wöchentlich)**: Dieses Diagramm zeigt die durchschnittliche wöchentliche Zeit, die für die Identifizierung eines Security Incident benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung (wöchentlich)**: Dieses Diagramm zeigt die durchschnittliche wöchentliche Zeit, die für die Eindämmung eines Security Incident benötigt wird.
- **Durchschnittliche Zeit bis zur Beseitigung (wöchentlich)**: Dieses Diagramm zeigt die durchschnittliche wöchentliche Zeit, die für die Beseitigung eines Security Incident benötigt wurde.
- **Neue Security Incidents diese Woche**: Dieses Diagramm zeigt die Anzahl der neuen Security Incidents in dieser Woche.
- **Diese Woche geschlossene Security Incidents**: Dieses Diagramm zeigt die Anzahl der in dieser Woche geschlossenen Security Incidents.
- **Neue Security Incidents (Laufzeit: 7 Tage)**: Dieses Diagramm zeigt die Anzahl der neuen Security Incidents in einer Woche.
- **Geschlossene Security Incidents (Laufzeit: 7 Tage)**: Dieses Diagramm zeigt die Anzahl der neuen Security Incidents, die geschlossen wurden, aber in einer Woche ausgeführt werden.
- **Neue vs. geschlossene Incidents (Täglich)**: Dieses Diagramm zeigt den Vergleich zwischen den täglichen neuen Security Incidents und den täglichen geschlossenen Security Incidents.
- **Neue vs. geschlossene Incidents (wöchentlich)**: Dieses Diagramm zeigt den Vergleich zwischen den wöchentlichen neuen Security Incidents und den wöchentlichen geschlossenen Security Incidents.
- Geschlossencodes für**Security Incidents**: Dieses Diagramm zeigt die geschlossenen Codes der Security Incidents.

### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf der Startseite des Arbeitsbereichs links auf das Symbol **SIR-Dashboards**.
3. Wählen Sie **CISO-Dashboard** aus der Dropdown-Liste aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Zeigen Sie das CISO-Dashboard an, um weitere Aktionen anzuzeigen.

### Zeigen Sie das Dashboard CISO Reporting Übersicht an

Dieses Dashboard bietet den Chief Information Security Officers (CISOs) eine allgemeine Berichtsübersicht über Security Incidents und wöchentliche Incident-Trends in der Instanz in Form von grafischen Diagrammen. Mit diesen Diagrammen können Sie die Leistung des Security Operations Center (SOC) effektiv anzeigen und analysieren.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin und sn_si.ciso – Incidents bearbeiten und anzeigen.

**Warum und wann dieser Vorgang ausgeführt wird**
Das Dashboard „CISO Reporting Overview“ (CISO-Berichterstellungsübersicht) bietet wöchentlich wichtige Einblicke in die Security Incidents. Sie können die wöchentlichen Trends mithilfe von Widgets visualisieren. Anhand der folgenden Diagramme können Sie wichtige Einblicke in die CISO-Berichterstellung gewinnen:

- **Neue Security Incidents diese Woche**: Auf dieser Kachel wird der Bericht über die Anzahl der neuen Security Incidents in dieser Woche angezeigt.
- **Diese Woche geschlossene Security Incidents**: Auf dieser Kachel wird der Bericht zur Anzahl der in dieser Woche geschlossenen Security Incidents angezeigt.
- **Neue Security Incidents (Running 7 days)**: Diese Kachel zeigt den Bericht über die Anzahl der neuen Security Incidents an, die in einer Woche ausgeführt wurden.
- **Geschlossene Security Incidents (Running 7 days)**: Diese Kachel zeigt den Bericht über die Anzahl der neuen Security Incidents an, die in einer Woche geschlossen wurden, aber ausgeführt werden.
- **Durchschnittliche Zeit bis zur Identifizierung**: Auf dieser Kachel wird der Bericht über die durchschnittliche wöchentliche Zeit angezeigt, die für die Identifizierung von Security Incidents benötigt wurde.
- **Durchschnittliche Zeit bis zur Eindämmung**: Diese Kachel zeigt den Bericht über die durchschnittliche wöchentliche Zeit an, die für die Eindämmung von Security Incidents benötigt wurde.

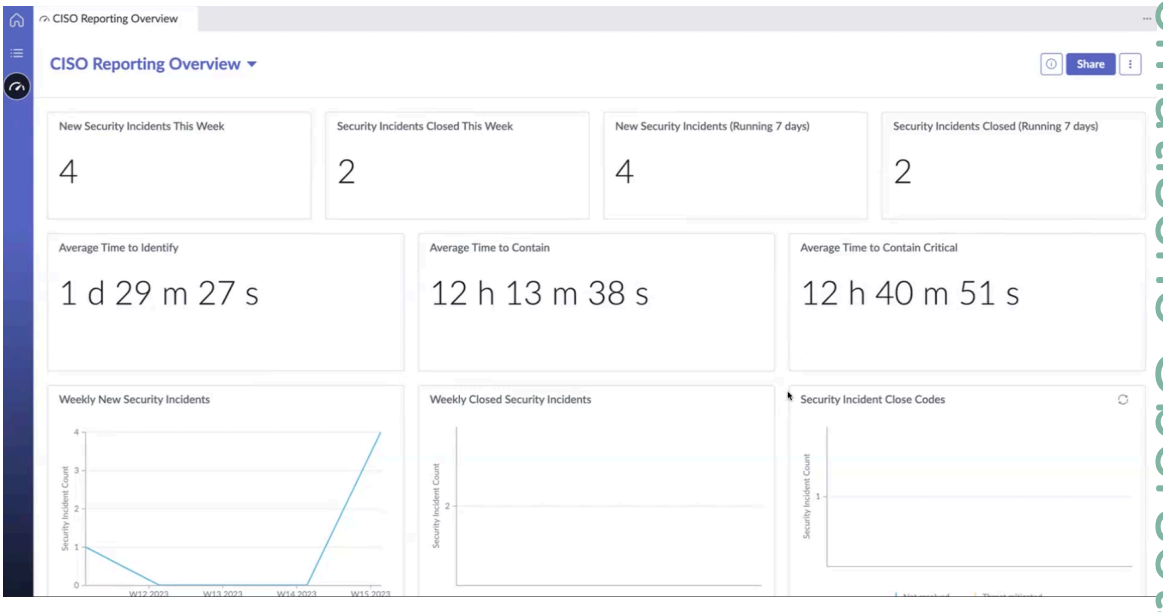


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Durchschnittliche Zeit bis zur Eindämmung**kritischer Security Incidents: Auf dieser Kachel wird der Bericht über die durchschnittliche wöchentliche Zeit angezeigt, die für die Eindämmung kritischer Security Incidents benötigt wurde.
- **Wöchentliche neue Security Incidents**: Dieses Diagramm zeigt den Bericht über die wöchentlichen neuen Security Incidents.
- **Wöchentliche geschlossene Security Incidents**: Dieses Diagramm zeigt den Bericht der wöchentlichen geschlossenen Security Incidents.
- Geschlossencodes für**Security Incident**: Dieses Diagramm zeigt den Bericht der geschlossenen Codes der Security Incidents.

### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf der linken Seite der Arbeitsbereichs-Homepage auf das Symbol **SIR-Dashboards**.
3. Wählen Sie **CISO Reporting Übersicht** aus der Dropdown-Liste aus.




4. Weitere Aktionen finden Sie im Dashboard CISO Reporting.



## Zeigen Sie das Dashboard „Security Incident Manager-Übersicht“ an

Dieses Dashboard bietet Managern einen allgemeinen Überblick über die kritischen Security Incidents oder Security Incidents mit hoher Priorität auf Teamebene, SLAs, die in 24 Stunden ablaufen, und wöchentliche Incident-Trends in der Instanz in Form von Berichten und grafischen Diagrammen.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin – Dashboard bearbeiten und anzeigen.
- sn_si.manager: Dashboard anzeigen.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Security Incidents mit kritischer oder hoher Priorität oder SLAs, die sofortige Aufmerksamkeit erfordern, analysieren. Sie können die wöchentlichen Trends auch mithilfe der Widgets im Dashboard „Security Incident Manager-Übersicht“ anzeigen.

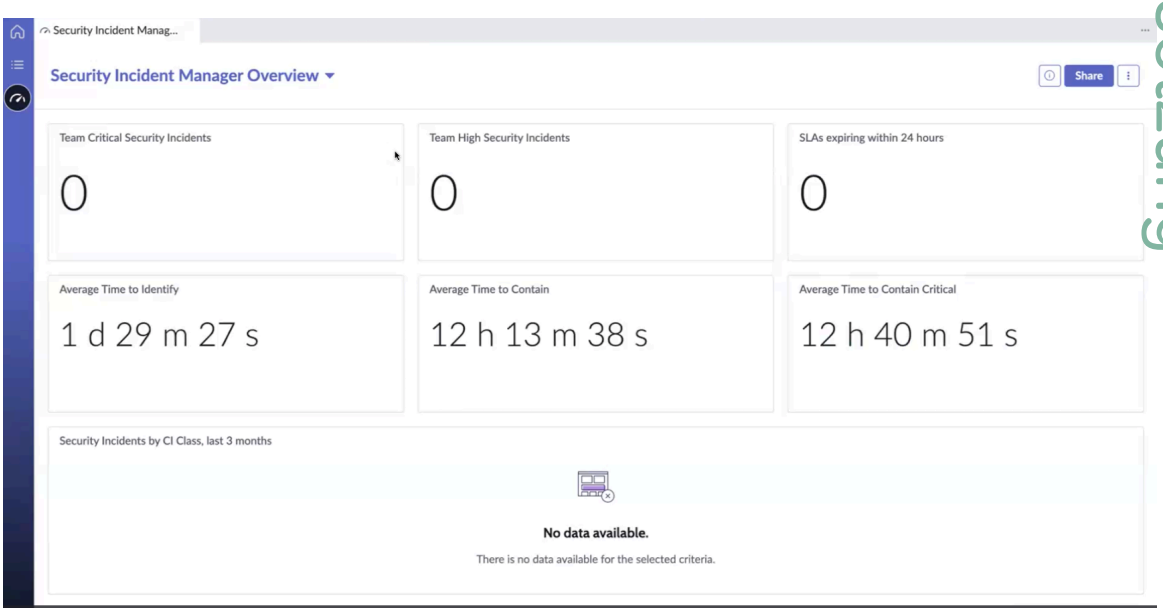
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Daten oder Statistiken für die wöchentlichen oder monatlichen Trends Ihrer Security Incidents werden aus den von der Organisation definierten Incident-Tabellen gesammelt. Mithilfe der folgenden Diagramme können Sie wichtige Einblicke gewinnen:

- **Kritische Security Incidents für Team**: Diese Kachel zeigt die Anzahl der kritischen Security Incidents für das Team in dieser Woche an.
- **Team Incidents mit hoher Sicherheit**: Diese Kachel zeigt die Anzahl der Incidents mit hoher Sicherheit für das Team in dieser Woche an.
- **SLAs, die innerhalb von 24 Stunden ablaufen**: Diese Kachel zeigt die Anzahl der SLAs an, die innerhalb von 24 Stunden ablaufen.
- **Durchschnittliche Zeit bis zur Identifizierung**: Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die für die Identifizierung von Security Incidents benötigt wurde.
- **Durchschnittliche Zeit bis zur Eindämmung**: Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die für die Eindämmung von Security Incidents benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung**kritischer Security Incidents: Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die für die Eindämmung kritischer Security Incidents benötigt wird.
- **Security Incident nach CI-Klasse, letzte 3 Monate**: Dieses Diagramm zeigt die Trends aller Security Incidents basierend auf der CI-Klasse in den letzten drei Monaten.
- **Trend aller Security Incidents nach Kategorie**: Dieses Diagramm zeigt die Trends aller Security Incidents nach Kategorie.
- **Trend aller Security Incidents nach Priorität**: Dieses Diagramm zeigt die Trends aller Security Incidents nach Priorität.

### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**.
2. Klicken Sie auf der linken Seite der Arbeitsbereichs-Homepage auf das Symbol **SIR-Dashboards**.
3. Wählen Sie in der Dropdown-Liste **Security Incident Manager Übersicht** aus.




4. Weitere Informationen finden Sie in der Security Incident Manager-Übersicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Security Incident-Erstellung

Security Incidents können manuell über das Formular oder automatisch über Sicherheits-Events erstellt werden, die von integrierten Warnungsüberwachungstools von Drittanbietern wie Splunk empfangen werden.

Wenn Sie über eine Sicherheitsrolle verfügen, können Sie Security Incidents mit einer der folgenden Methoden manuell erstellen.

**Methoden zum manuellen Erstellen von Security Incidents**

| Methode | Beschreibung |
|---|---|
| Manuell aus der Security Incident-Liste erstellt | Klicken Sie in der Liste „Security Incident“ auf **Neu**, um einen neuen Security Incident zu erstellen. |
| Manuell aus dem Security Incident Catalog erstellt | Sie können Security Incidents erstellen, indem Sie aus den im Security Incident-Katalog definierten Kategorien von Sicherheitsbedrohungen auswählen. |
| Incident-Management | Klicken Sie im Incident-Formular in Incident Management auf Sicherheits-Incident erstellen, um einen neuen **Security Incident** zu erstellen. |
| Manuell aus einer Sicherheitsanforderung konvertiert | Klicken Sie im Formular „Sicherheitsanforderung“ auf In **Security Incident konvertieren, um einen neuen Security Incident** zu erstellen. |
| Manuell aus einer Event Management-Warnung erstellt | Klicken Sie im Formular „Event Management-Warnungen“ auf Security Incident erstellen, um aus einer Warnung einen neuen **Security Incident** zu erstellen. |
| Manuell aus einer Warnung erstellt | Klicken Sie im Event Management-Warnungsformular auf Security Incident erstellen, um einen neuen **Security Incident** zu erstellen. |
| Manuell aus einem Schwachstellendatensatz konvertiert (wenn das Vulnerability Response-Plugin aktiviert ist) | Klicken Sie im Formular „Angreifbare Elemente“ auf Security Incident erstellen, um einen neuen **Security Incident** zu erstellen. |

## Automatische Erstellung von Security Incidents

Im Allgemeinen sind Sicherheitsadministratoren für die Einrichtung von Warnungsregeln verantwortlich, die zur automatischen Generierung von Security Incidents verwendet werden.

**Sicherheitsadministratormethode zum Erstellen von Security Incidents**

| Methode | Beschreibung |
|---|---|
| Automatisch mithilfe von Warnungsregeln erstellt | Security Incidents können basierend auf Warnungsregeln erstellt werden, die in Event Management in Ihrer Rechenzentrumsanwendung definiert sind. |

## Manuelle Erstellung von Security Incidents

Sie können einen Security Incident aus dem Security Incident-Formular sowie aus mehreren anderen Formularen erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Security Incidents basierend auf einem vorhandenen Datensatz aus den folgenden Formularen erstellen:

- Aus einer beliebigen Security Incident-Liste
- Incident-Formular
- Ereignismanagement Warnungsformular
- Formular „Angreifbare Elemente“
- Formular „Sicherheitsanforderung“

### Erstellen Sie einen Security Incident aus der Liste „Security Incident“.

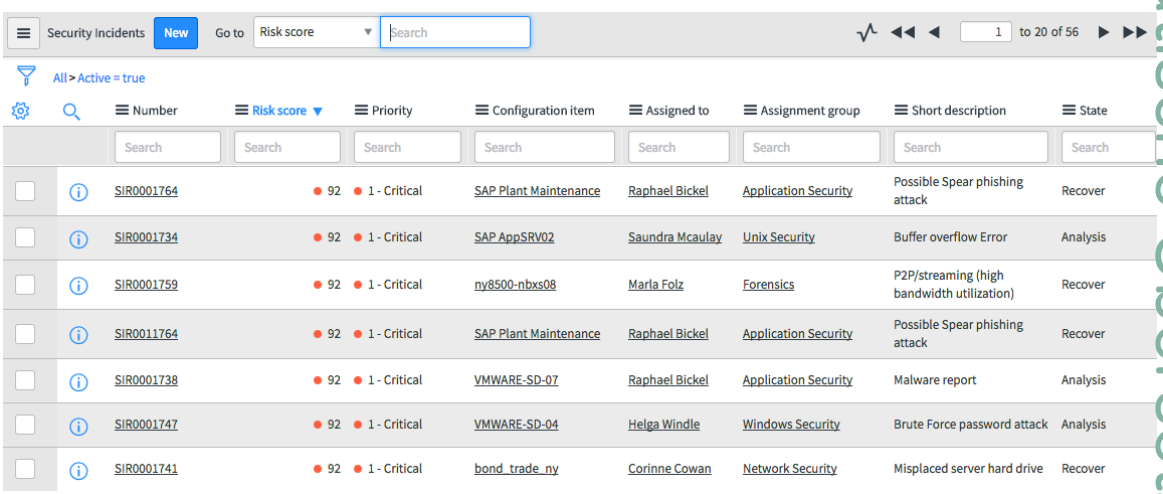
Zusätzlich zu den automatischen Methoden zum Erstellen von Security Incidents können Sie sie bei Bedarf auch manuell erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

#### Prozedur

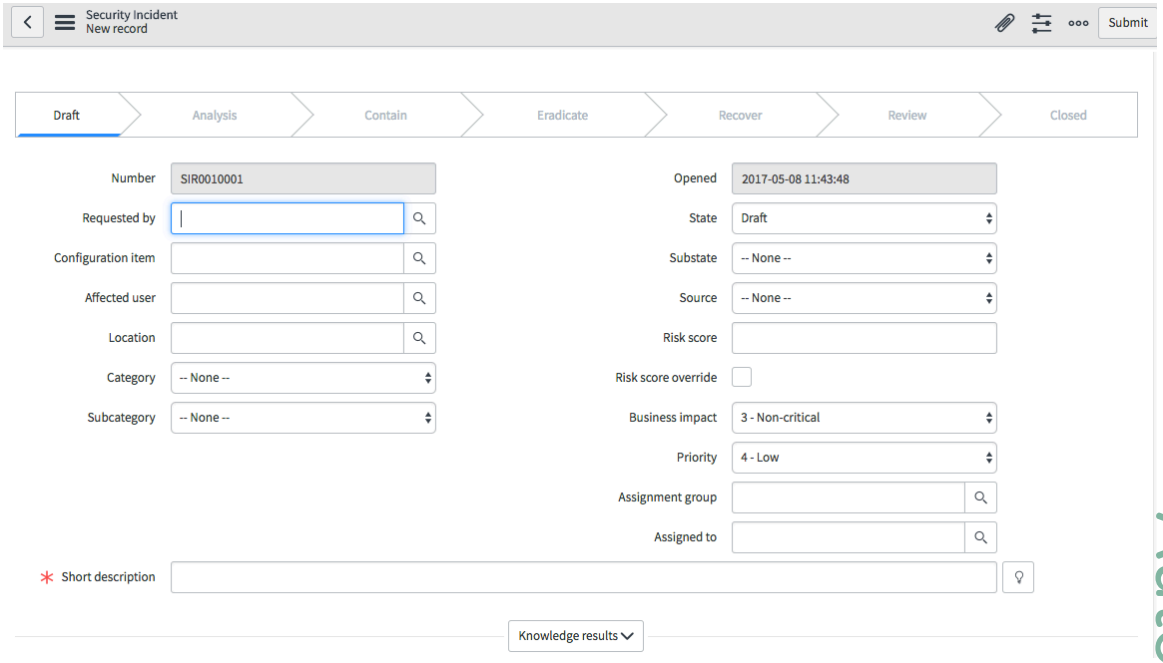
1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.




2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Sicherheits-Tag auswählen | Wählen Sie bei Bedarf ein Sicherheits-Tag aus, um dem Datensatz Metadaten hinzuzufügen, oder geben Sie an, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird nur angezeigt, nachdem der Security Incident gespeichert wurde. |
| Nummer | [Nur Lesen] Die Security Incident-Nummer. |
| Angefordert von | Die Person, die die auszuführende Arbeit anfordert. |
| Konfigurationselement | Der Server, Computer, Router oder ein anderes Konfigurationselement, das vom Sicherheitsproblem betroffen ist. |
| Betroffener Anwender | Die vom Sicherheitsproblem betroffene Person. |
| Standort | Der Standort der anfordernden Person oder Ressource. Wenn kein **Konfigurationselement** ausgewählt ist, wird dieses Feld mit dem Standort der anfordernden Person vorausgefüllt. |
| Kategorie | Die Kategorie, die den Typ des Sicherheitsproblems identifiziert<br><br>Wenn eine Kategorie ausgewählt ist, wird beim Speichern des Datensatzes ein Workflow zur Analyse dieses Problems ausgeführt. Wenn Sie beispielsweise **Denial of Service**auswählen, wird der Workflow Security Incident – Denial of Service – Vorlage ausgeführt.<br><br>Weitere Informationen finden Sie unter Security Incident Response-Workflow-Vorlagen. |
| Unterkategorie | Die Unterkategorie, die das Problem weiter definiert. |
| Geöffnet | [Nur lesen] Zeigt das Datum und die Uhrzeit an, zu der der Incident geöffnet wurde. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Status | Aktueller Status des Security Incident Nach der Erstellung eines Security Incident wird dieses Feld standardmäßig auf **Entwurf**gesetzt. |
| Substatus | Gibt an, ob der Security Incident ein ausstehendes Problem oder einen Change enthält. |
| Quelle | Gibt die Quelle des Security Incident an, z. B. E-Mail, Telefonanruf oder Netzwerküberwachung. |
| Warnungssensor | Sicherheitsintegration, über die Sie die Warnungs- oder Event-Daten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen. |
| Warnungsregel | Die Regel im Sicherheitsprodukt, die die Erstellung dieses Security Incident ausgelöst hat. |
| Risikopunktzahl | Zeigt die für diesen Security Incident berechnete Risikopunktzahl an. Der Wert basiert auf der Priorität des Security Incident, der Art des Security Incident (Denial of Service, Spear Phishing oder böswillige Codeaktivität) und der Anzahl der Quellen, die eine fehlgeschlagene Reputationspunktzahl für einen Indikator ausgelöst haben. Die Risikopunktzahl hilft bei der Priorisierung von Security Incident-Arbeit für Analysten.<br><br>Mit drei Eigenschaften von Security Incidents können Sie einen farbcodierten Punkt festlegen, der neben der Risikopunktzahl in der Listenansicht angezeigt wird, um sie leichter identifizierbar zu machen.<br><br>Wenn Sie Änderungen an bestimmten Feldern im Security Incident vornehmen, z. B. **Geschäftsauswirkung** oder **Priorität**, und den Datensatz speichern, wird die **Risikopunktzahl** automatisch neu berechnet und angezeigt. Die Änderung wird auch in den Arbeitsnotizen und in der zugehörigen Liste „Risikopunktzahl-Audits“ angezeigt.<br><br>**Hinweis:**<br>Die Risikopunktzahl wird auch neu berechnet, wenn betroffene Benutzer einem Security Incident, betroffenen Services oder angreifbaren Elementen zugeordnet werden.<br><br>Sie können auch manuell eine neue **Risikopunktzahl**eingeben. Dies kann nützlich sein, wenn Sie einen bestimmten Security Incident in der Liste der Security Incidents, die Sie analysieren, ganz oben belassen möchten. Wenn Sie eine neue **Risikopunktzahl**eingeben, wird das Kontrollkästchen **Risikopunktzahl überschreiben** automatisch aktiviert. Unabhängig von den im Security Incident vorgenommenen Änderungen wird eine manuell eingegebene Risikopunktzahl nicht automatisch neu berechnet.<br><br>**Hinweis:**<br>Wenn Sie Ihre Instanz von einem früheren Release aktualisiert haben, wurden Risikopunktzahlen für alle offenen Security Incidents berechnet. Weitere Informationen finden Sie unter Security Incident-Rechner verstehen. |
| Überschreibung der Risikopunktzahl | Aktivieren Sie diese Checkbox, um die automatische Aktualisierung der Risikopunktzahl zu überschreiben. Die Überschreibung wird in den Arbeitsnotizen angezeigt. |



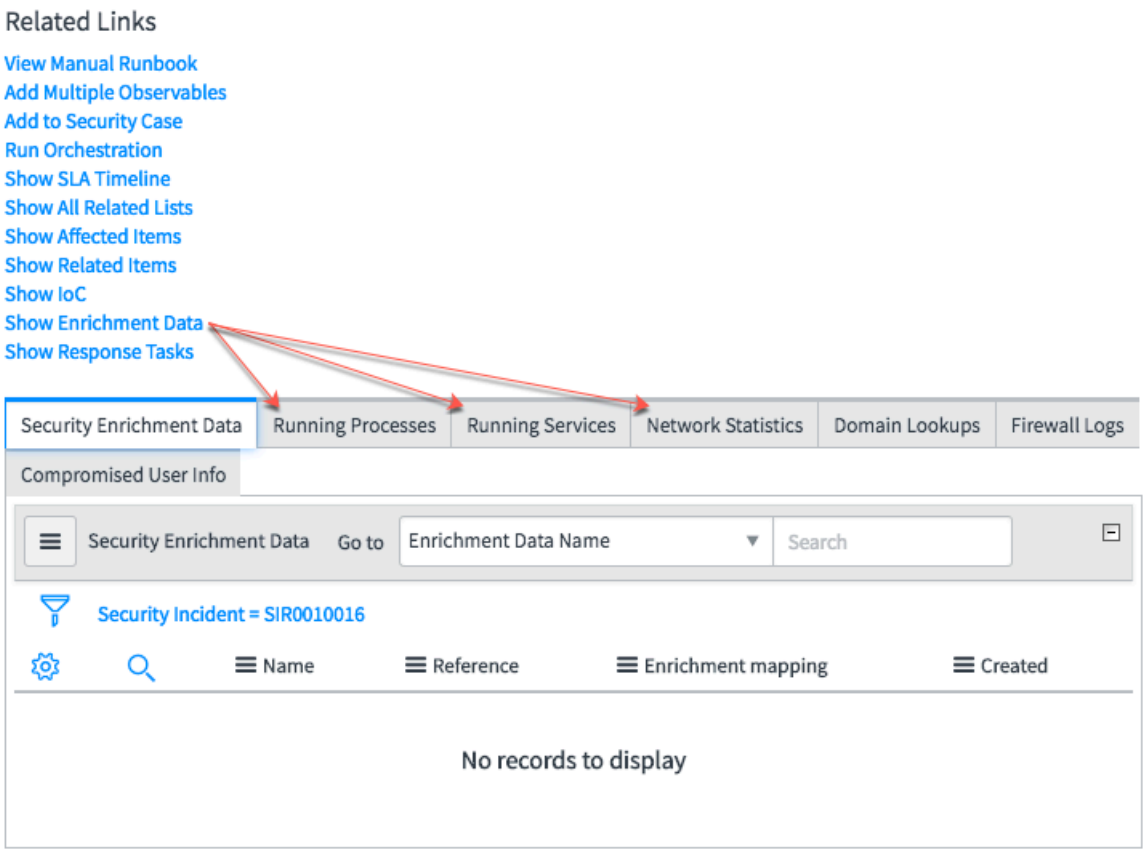
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Geschäftsauswirkung | Wählen Sie die Bedeutung dieses Security Incident für Ihr Unternehmen aus. Der Standardwert ist Nicht kritisch. Wenn Sie nach dem Speichern des Security Incident-Datensatzes den Wert in den Feldern **Priorität** und/oder **Risiko** ändern, wird die **Geschäftsauswirkung** neu berechnet. |
| Priorität | Wählen Sie basierend auf der Dringlichkeit die Reihenfolge aus, in der dieser Security Incident behandelt werden soll. Wenn dieser Wert nach dem Speichern des Datensatzes geändert wird, kann dies Auswirkungen auf die Berechnung der **Geschäftsauswirkung haben**. |
| Zuweisungsgruppe | Die Gruppe, der dieser Security Incident zugewiesen ist. |
| Zugewiesen an | Die Person, der die Analyse dieses Security Incident zugewiesen ist. Zuweisungen können manuell oder automatisch ausgeführt werden. Weitere Informationen finden Sie unter Zuweisen von Sicherheitsanalysten. |
| Kurzbeschreibung | Eine kurze Beschreibung des Security Incident. |
| Wissensergebnisse | Während Sie die Kurzbeschreibung eingeben, werden Links zu zugehörigen Artikeln aus der Knowledge Base angezeigt.<br>Das Scannen der Informationen könnte Ihr Problem lösen. |

4. Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen **Sie Speichern**aus. Wenn Sie dem Security Incident ein neues CI hinzugefügt haben, werden die folgenden Integrations-Workflows automatisch ausgeführt:
   - Workflow „Security Operations – Laufende Prozesse abrufen“.an. Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (CI) von einem Host oder Endpunkt ab.
   - Workflow „Security Incident Response – Laufende Services abrufen“.an. Dieser Workflow ruft eine Liste der ausgeführten Services von Windows-basierten CIs ab.
   - Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“.an. Dieser Workflow ruft eine Liste der aktiven Netzwerkverbindungen von einem Host oder Endpunkt ab.
5. Um die von diesen Workflows abgerufenen Informationen anzuzeigen, **klicken** Sie auf den zugehörigen Link Ergänzungsdaten anzeigen und dann auf eine der angegebenen Registerkarten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Zusätzliche Workflows werden basierend auf den von Ihnen aktivierten Drittanbieterintegrationen wie folgt ausgeführt:

Integration der Tanium-Endpunktplattform: Tanium – Workflow „Laufende Prozesse abrufen“.

**Zugehörige Informationen**

Setup von Security Incident Response

## Erstellen Sie einen Security Incident aus dem Security Incident Catalog

Benutzer in Ihrem Unternehmen können den Security Incident Catalog verwenden, um verschiedene Arten von sicherheitsbezogenen Analysen anzufordern.

### Vorbereitungen

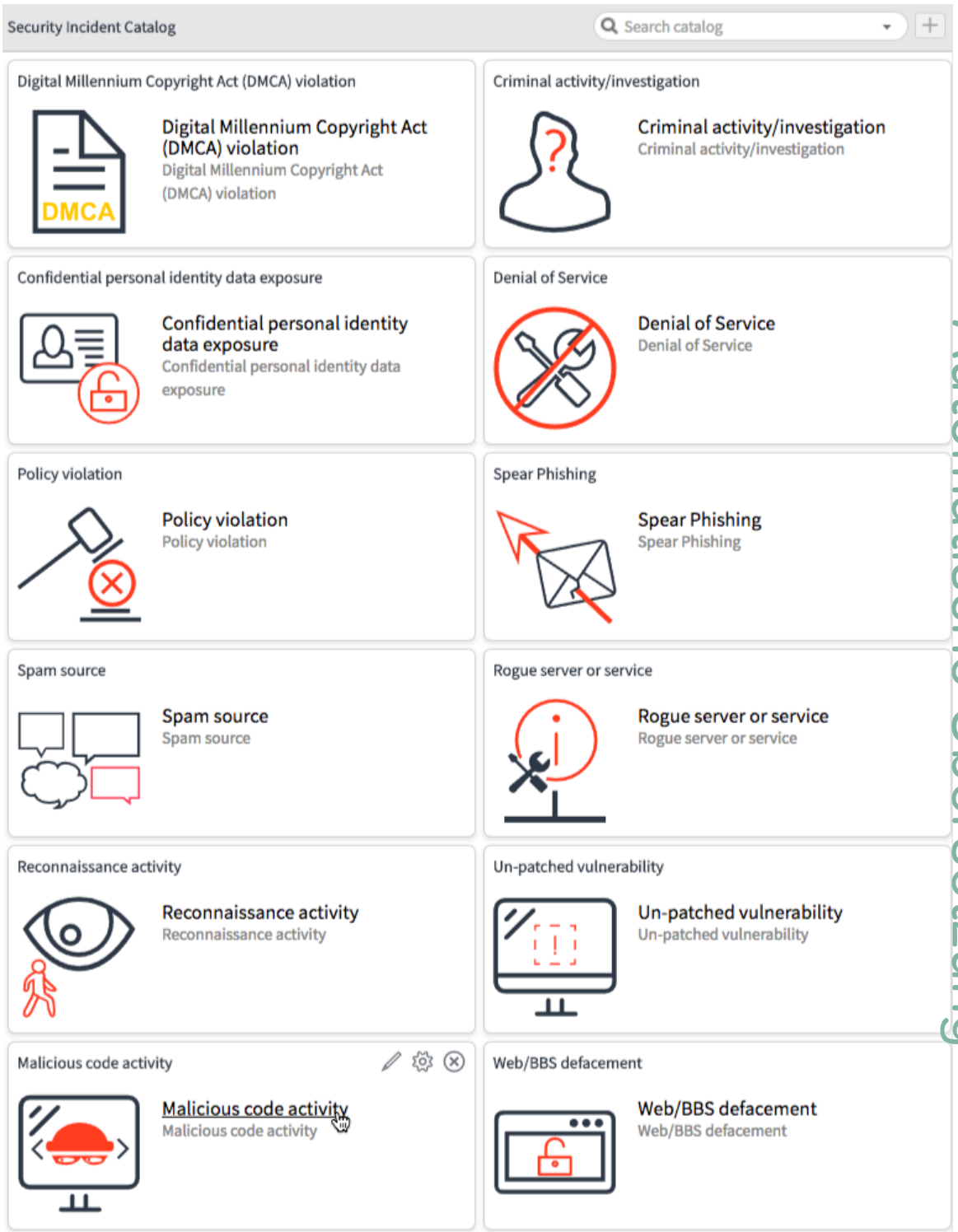
Erforderliche Rolle: keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

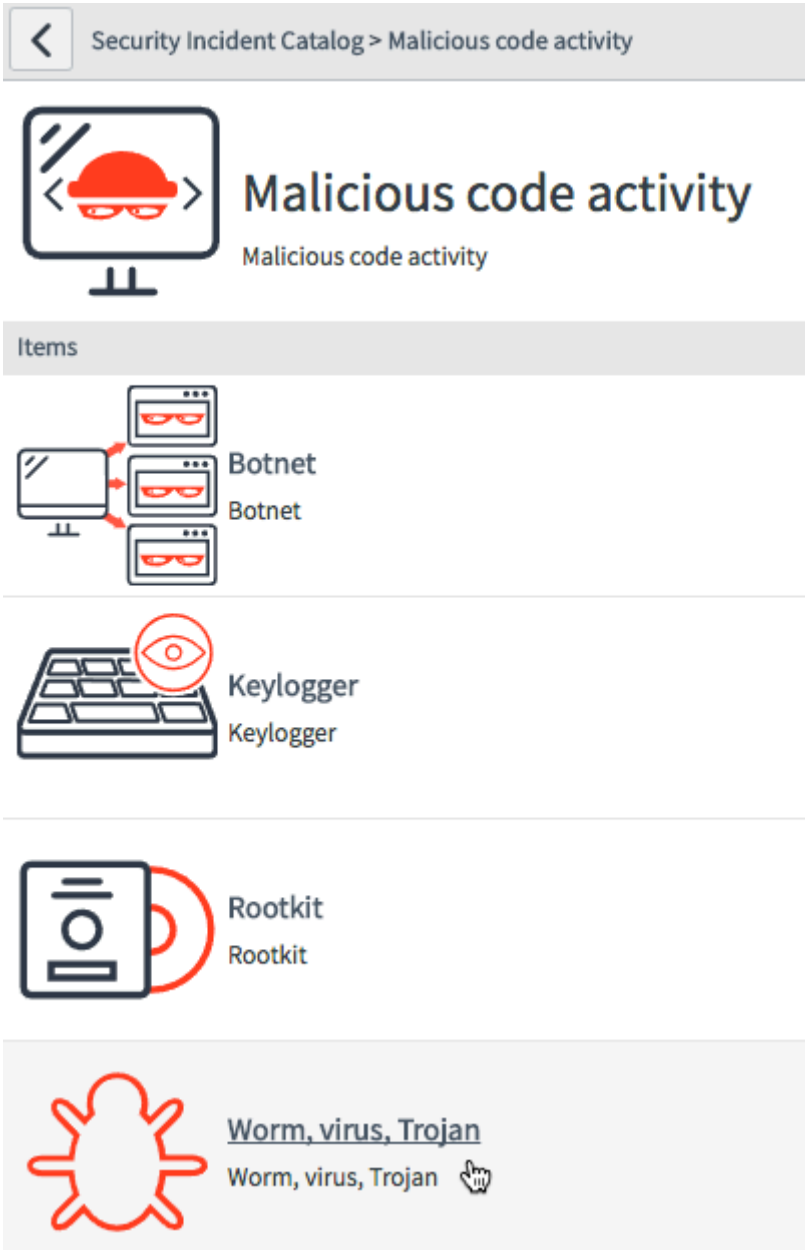
1. Navigieren zu **Alle** > **Selfservice** > **Katalog für Sicherheitsvorfälle**.




2. Klicken Sie auf das Katalogelement, für das Sie eine Anforderung stellen möchten.
   Wenn das Element, das Sie aus dem Hauptkatalog ausgewählt haben, Unterkategorien enthält, wird die Liste angezeigt. Im folgenden Beispiel wurde **die Aktivität „Böswilliger Code** “ ausgewählt.

Automatische Übersetzung

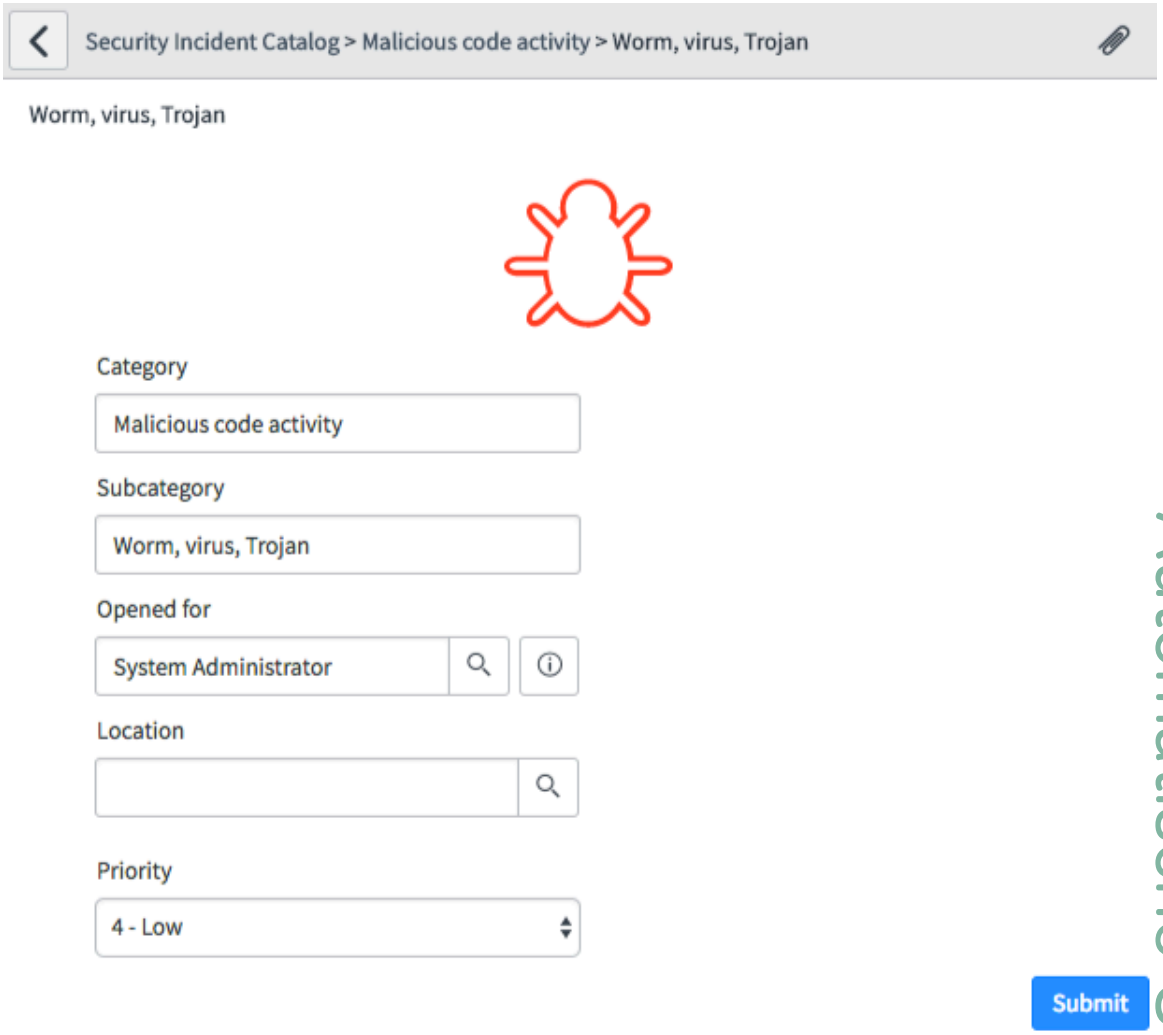
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Klicken Sie auf die Unterkategorie, die der Art der Anforderung entspricht, die Sie stellen möchten. In diesem Beispiel wurde die Unterkategorie **Worm, Virus, Trojan** ausgewählt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie die Informationen für die Anforderung ein, und klicken Sie auf **Absenden**.
   Die Anforderung wird an Ihre Security Incident-Abteilung gesendet.
5. Nachdem Sie die Anforderung übermittelt haben, können Sie den Fortschritt nachverfolgen, indem Sie zu navigieren **Selfservice** > **Meine Anforderungen**, und geben Sie die Anforderungsnummer ein.

### Erstellt einen Security Incident aus einer Event Management-Warnung

Wenn Event Management aktiviert ist, können Sie Security Incidents manuell über das Warnungsformular erstellen.

#### Vorbereitungen

Das Event Management-Plugin erfordert ein separates Abonnement und muss von ServiceNow-Mitarbeitern aktiviert werden. Dieses Plugin enthält Demodaten und aktiviert zugehörige Plugins, wenn sie nicht bereits aktiv sind. Die Serviceanalytik wird automatisch aktiviert, wenn Event Management aktiviert wird.
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

#### Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die **Nummer** der Warnung.
3. Klicken **Sie auf Security Incident erstellen**.
4. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Automatische Erstellung von Security Incidents

Überwachungstools von Drittanbietern wie Splunk können in Security Incident Response integriert werden, sodass aus diesen Tools importierte Sicherheits-Events automatisch Security Incidents generieren. Sie können auch Daten aus Tools von Drittanbietern in Sicherheitswarnungen importieren.

Um Warnungsüberwachungstools in Security Incident Responsezu integrieren, müssen Sie die REST-API verwenden, um in die Tabelle „Security Incident-Import“ [sn_si_incident_import] zu schreiben. Anschließend wird mithilfe der Transformationszuordnungen für **Security Incidents**die Import Set-Quelltabelle Feldern in der Zieltabelle „Security Incident“ [sn_si.incident] zugeordnet.

Wenn Sie versuchen, CI-Datensätze zu importieren, die von der Transformationszuordnung nicht erkannt werden, überprüft das Transformationszuordnungsskript den Datensatz auf Folgendes (in dieser Reihenfolge), um eine Übereinstimmung zu erzielen:

- sys_id
- CI-Name
- vollständig qualifizierter Domänenname
- IP-Adresse

**Hinweis:**
Wenn Sie feststellen, dass die **Security Incident Transform** -Transformationszuordnung für das von Ihnen verwendete Warnungsüberwachungstool einer Drittpartei nicht ausreicht, duplizieren Sie die Transformationszuordnung, erstellen Sie eine neue und bearbeiten Sie die Felder nach Bedarf.

### Aus Events und Warnungen erstellte Security Incidents

Wenn Events aus Warnungsüberwachungstools importiert werden, werden sie zuerst von Ereignismanagement verarbeitet und in Warnungen gruppiert. Diese Warnungen können verwendet werden, um Security Incidents basierend auf anpassbaren Warnungsregeln zu erstellen, oder manuell überprüft werden, um die Warnungen auszuwählen, die als Security Incident untersucht werden sollen.

Eine Beispielwarnungsregel namens **Create security incidents from critical alerts** (Sicherheit Incidents aus kritischen Warnungen erstellen) finden Sie im Modul WarnungsregelnEreignismanagement der Anwendung []. Diese Warnungsregel erstellt automatisch Security Incidents, wenn kritische sicherheitsbezogene Ereignisse von ServiceNow oder von Überwachungsanwendungen von Drittanbietern empfangen werden. Nachdem der Security Incident erstellt wurde, wird er aktualisiert, wenn neue Events eingehen. Sie können die Aufgabenvorlage in der Warnungsregel ändern, um die Anfangswerte für den von dieser Warnungsregel erstellten Security Incident zu ändern. Um die verschiedenen Arten von Security Incidents zu behandeln, die Sie erstellen möchten, können Sie andere Warnungsregeln mit anderen Bedingungen definieren.

Wenn Sie ein Benutzer mit der Rolle „Sicherheitsadministrator“ sind, können Sie einen Security Incident manuell erstellen, indem Sie in einer verdächtigen Warnung auf die Schaltfläche **Security Incident erstellen** klicken.

Es ist wichtig, dass die von externen Tools empfangenen Events die folgenden Informationen enthalten:

- Der Knoten, der auf den Namen, die IP-Adresse oder die sys_id des CI festgelegt ist, das zur betroffenen Ressource wird.
- Die Event-Klassifizierung ist auf Sicherheit festgelegt, um sie von anderen IT-Events zu unterscheiden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Event-Beschreibung, die die Beschreibung des Security Incident ausfüllt.
- Die zusätzlichen Informationen können zusätzliche Informationen enthalten, die nicht in die zuvor aufgeführten Felder oder andere Event-Felder passen, z. B. Kategorie, Angriffsvektoren, Rückgabe-URL oder Korrelations-ID. Das Format ist eine Zeichenfolge, die Feldnamen zusammen mit ihren Werten im folgenden JSON-Format auflistet:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

**Hinweis:**
Wenn für jedes Feld- und Wertepaar das Feld im Security Incident, in dem der Spaltenname mit fieldName übereinstimmt, leer ist, wird es auf fieldValue festgelegt. Wenn das Feld im Security Incident nicht leer ist, wird es nicht geändert. In beiden Fällen werden das Event und alle in den zusätzlichen Informationen codierten Felder und Werte in einem Arbeitsnotizeneintrag aufgezeichnet, der das Event beschreibt. Wenn sich am Security Incident nichts ändert, wird kein Arbeitsnotizeintrag erstellt. Alle Felder in einem Security Incident, einschließlich benutzerdefinierter Felder, die Sie der Tabelle hinzufügen, können festgelegt werden.

### In Sicherheitswarnungen importierte Daten

Wenn ein Event mit mehr JSON-codierten Daten erstellt wird, werden diese Daten in ein beliebiges Feld mit einem Namen importiert, der dem fieldName dieses Werts in den JSON-Daten entspricht.

Wenn Sie Daten in Ihrer Überwachungssoftware einer Drittpartei (z. B. Splunk) haben, die im Basissystem nicht vorhanden sind, können Sie der Warnungstabelle neue Felder hinzufügen, um den Datenimport zu berücksichtigen. Das JSON-Format zum Importieren von Daten in Warnungen ist das gleiche Format, das zum Erstellen von Security Incidents aus Events und Warnungen verwendet wird:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Der einzige Unterschied besteht darin, dass die Daten im Feld immer mit dem Wert fieldValue überschrieben werden.

Wenn die Sicherheitsereignisdaten importiert werden, werden die Felder in der Warnungstabelle mit übereinstimmenden Feldnamen ausgefüllt. Wenn die Warnung später in einen Security Incident umgewandelt wird, werden übereinstimmende Felder im Security Incident mit denselben zusätzlichen Informationsdaten ausgefüllt.

### Erstellen Sie Security Incidents aus von Benutzern gemeldeten Phishing-E-Mails

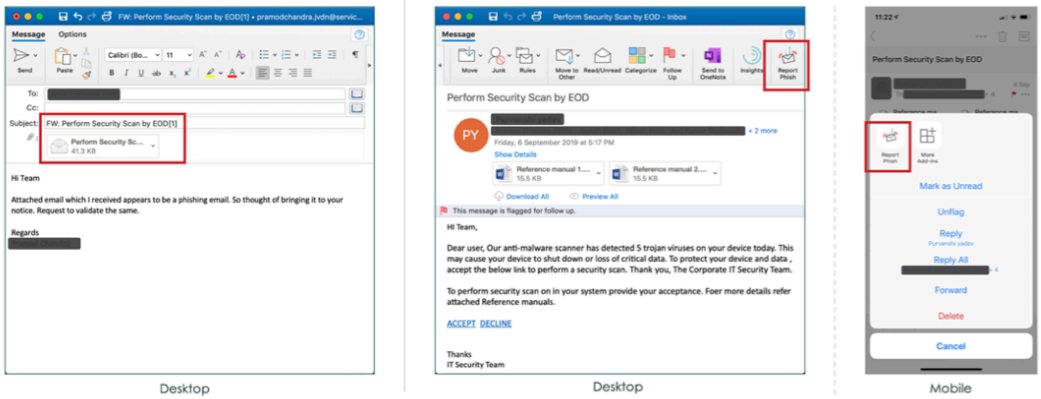
Verwenden Sie diese Funktion, um Security Incidents aus von Benutzern gemeldeten Phishing-E-Mails zu erstellen.

Die erweiterte Funktionalität für von Anwender gemeldetes Phishing umfasst Zusammenfassungsfunktionen, E-Mail-Header-Extraktion und Konfiguration.

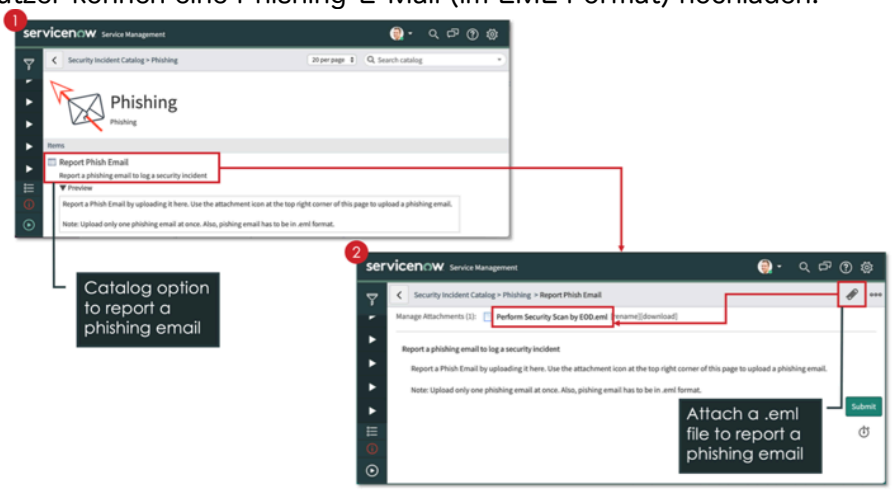
- Benutzer können Phishing-E-Mails auf verschiedene Arten melden:
  - E-Mails können als Anhänge weitergeleitet werden.
  - Wenn das Wombat-Plugin mit dem Microsoft Outlook-Client konfiguriert wurde, können Benutzer:
    - Klicken Sie auf die Schaltfläche **Phishing** melden.
    - Leiten Sie Phishing-E-Mails von einem Mobilgerät mit der Option Phishing **melden weiter**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- Benutzer können eine Phishing-E-Mail (im EML-Format) hochladen.




- Von Benutzern gemeldetes Phishing umfasst eine **Zusammenfassung der Geschäftslogik**, die doppelte Phishing-E-Mails identifiziert, die von Benutzern in einer Organisation gemeldet werden. Benutzer können diese Fähigkeit verwenden, um:
  - Fassen Sie doppelte oder ähnliche, von Benutzern gemeldete Phishing-Incidents (vom Unternehmen initiierte Phishing-Kampagnen) zusammen.
  - Vermeiden Sie die Selektierung doppelter, von Benutzern gemeldeter Phishing-Incidents, und reduzieren Sie den manuellen Aufwand für die Konsolidierung von Incidents.
  - Ermöglichen Sie Sicherheitsanalysten, an einem von einem einzelnen Benutzer gemeldeten Phishing-Incident zu arbeiten.
- Stellt Phishing-E-Mail-Header innerhalb des vom Benutzer gemeldeten Phishing-Incidents bereit.
  - Sicherheitsanalysten können innerhalb des Incident nach wichtigen E-Mail-Header-Informationen suchen.
  - Manueller Aufwand beim Sammeln von Header-Informationen aus anderen Quellen ist nicht mehr erforderlich.
- Die ursprünglich übermittelte Phishing-E-Mail wird als **Phishing-E-Mail-Datensatz** in einer neuen Tabelle gespeichert.
- Sicherheitsanalysten können Details der ursprünglichen Phishing-E-Mail anzeigen, z. B. Phishing-E-Mail-Inhalt, Header, Ursprung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sicherheitsadministratoren können bestimmte Erweiterungen konfigurieren und vornehmen, darunter:
  - Konfigurationen zum Extrahieren von E-Mail-Kopfzeilen aus dem E-Mail-Text (**Phishing** -Einreichungen melden).
  - Filter zum Erfassen ausgewählter Header.
  - Konfigurationen für die Verarbeitung der Zuordnung von übergeordneten und untergeordneten Incidents, wenn doppelte Phishing-E-Mail-Datensätze identifiziert werden.
  - Flow Designer-Konfigurationen zum Ändern der Geschäftslogik der Zusammenfassung basierend auf den Anforderungen.

### Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein

Als Benutzer mit der Rolle „ `sn_si.admin` “ können Sie E-Mail-Abgleichregeln definieren, um von Benutzern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, nach der alle E-Mails, die entweder direkt oder über die Schaltfläche Phishing melden an *`security@acme.com`* gesendet werden, als von Benutzern gemeldete Phishing-E-Mails kategorisiert werden. Weitere Informationen finden Sie unter Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein.

### Definieren Sie Eigenschaften für von Benutzern gemeldetes Phishing

Definieren Sie die Header-Informationen, die aus von Benutzern gemeldeten Phishing-E-Mails erfasst werden müssen. Weitere Informationen finden Sie unter Definieren Sie Eigenschaften für von Benutzern gemeldetes Phishing

### Phishing-E-Mail-Datensätze, die aus von Benutzern gemeldeten Phishing-E-Mails erstellt wurden

Von Benutzern gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Abgleichregeln in Security Incidents konvertiert. Weitere Informationen finden Sie unter Phishing-E-Mail-Datensätze, die aus von Benutzern gemeldeten Phishing-E-Mails erstellt wurden.

### Phishing-E-Mail in Security Incident umwandeln

Der Flow Phishing-E-Mail in Security Incident umwandeln konvertiert Phishing-E-Mail-Datensätze in Security Incidents. Weitere Informationen finden Sie unter Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln.

### Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Zeigen Sie die Details des Security Incident-Datensatzes an, einschließlich zugehöriger Listen, Arbeitsnotizen und anderer wichtiger Informationen. Weitere Informationen finden Sie unter Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden.

#### Erforderliche Komponenten und Plugins

Die in diesem Release verfügbare Funktion für von Benutzern gemeldetes Phishing ist eine erweiterte Version der vorhandenen Funktion für von Benutzern gemeldetes Phishing, die im London-Release verfügbar ist. Weitere Informationen finden Sie im Thema **Regeln zur Validierung von von Benutzern gemeldeten Phishing-Angriffen erstellen** in der London-Dokumentation.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Wichtige Installationsanweisungen**

Diese Erweiterung ersetzt das vorhandene Phishing-Design mit Anwendermeldung. Das neue Design umfasst die folgenden Updates:

- Die vorhandenen eingehenden Aktionen für „Von **Anwender gemeldete Phishing** -E-Mail“ (Typ = Weiterleiten und Typ = Neu) wurden deaktiviert.
- Eine neue eingehende Aktion **Phishing-E-Mail erstellen** ist jetzt verfügbar.
- Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln ist ein neuer Flow, der die Geschäftslogik für die Erstellung und Zusammenfassung von Security Incidents für das neue Design enthält. Sie müssen diesen Flow aktivieren, damit das neue Design wirksam wird.
- Die vorhandenen Phishing-Regeln für Anwenderberichte wurden während des Upgrades beibehalten.

**Hinweis:**
Wenn Sie benutzerdefinierte Aktionen bei eingehender E-Mail und benutzerdefinierte Workflows für von Benutzern gemeldete Phishing-Übermittlungen verwenden, müssen Sie sowohl das alte als auch das neue Design auf in Konflikt stehende oder überlappende Funktionalitäten überprüfen.

Details der Erweiterung**„Anwender gemeldetes Phishing“**: Im Folgenden finden Sie die Details der Erweiterung:

- Phishing-E-Mails auf verschiedene Arten melden: Weitere Informationen finden Sie unter Erstellen Sie Security Incidents aus von Benutzern gemeldeten Phishing-E-Mails. Die Phishing-E-Mail wird dann in die Tabelle `sn_si_phishing_email verschoben`.
- Phishing-E-Mail-Datensätze erstellen: Wenn die E-Mail-Abgleichregeln erfüllt sind (siehe Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein), erstellt die eingehende Aktion Phishing-E-Mail **erstellen** einen Phishing-E-Mail-Datensatz. Die analysierten E-Mail-Kopfzeilen werden in der Tabelle cm`sn_si_phishing_email_header` gespeichert und der Phishing-E-Mail als zugehörige Liste zugeordnet.
- Ähnliche Phishing-Datensätze zu einem einzigen Security Incident zusammenfassen: Der Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln -Flow erstellt Security Incidents aus den Phishing-E-Mail-Datensätzen und fasst ähnliche Datensätze zu einem einzigen Incident zusammen. Die Zusammenfassungsbedingungen können in diesem Flow nach Bedarf geändert werden.

**Hinweis:**

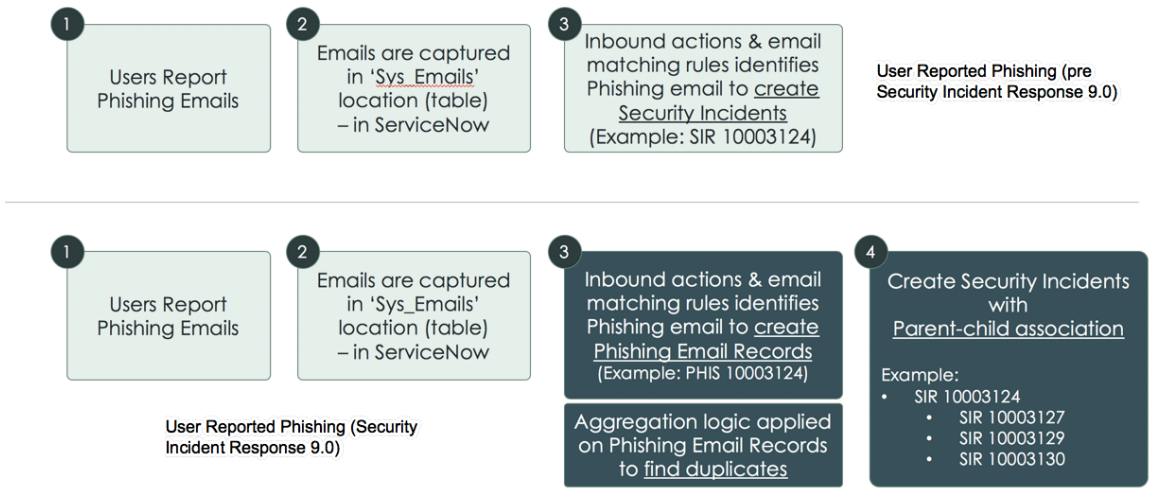
- Die eingehenden Aktionen für **„Vom Anwender gemeldetes Phishing** “, die vor Release Security Incident Response 9.0 verfügbar waren, sind jetzt deaktiviert. Security Incidents werden nicht mehr durch deaktivierte eingehende Aktionen erstellt.
- Die Spoke-Anwendung „Security Operations“ muss installiert sein, damit das neue Design wirksam wird. Dies umfasst den Flow Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln, der standardmäßig in einem inaktiven Status verfügbar ist. Aktivieren Sie diesen Flow, um Security Incidents aus den Phishing-E-Mail-Datensätzen zu erstellen.

Die folgende Abbildung zeigt die Unterschiede zwischen dem alten und dem neuen Design: Von



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## What Happens When User Reports A Phishing Email?




Zur Verwendung der erweiterten Funktion „Von Anwender gemeldetes Phishing“ sind die folgenden Plugins und Komponenten erforderlich:

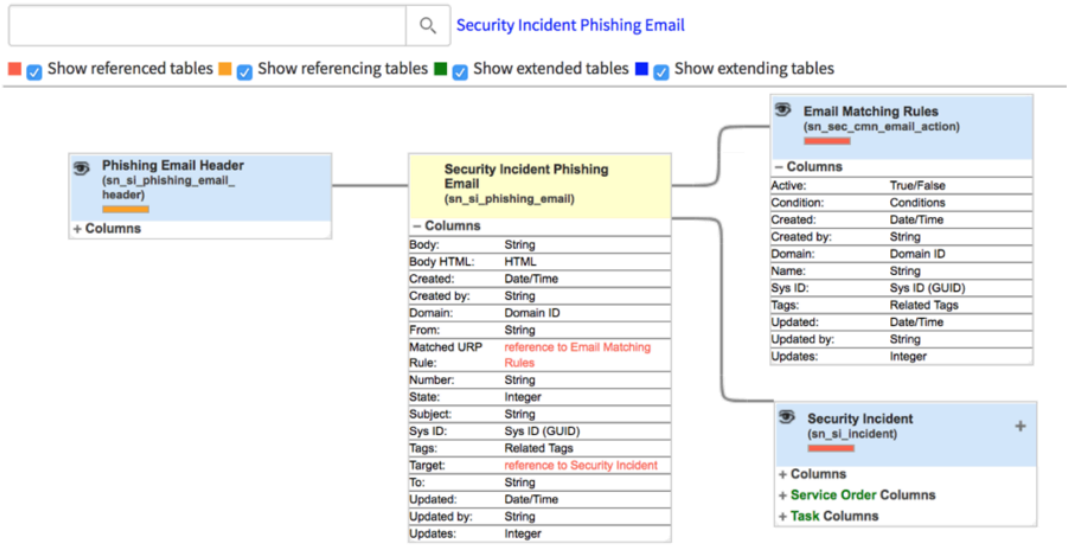
- Security Support Common (*sn_sec_cmn*): Enthält:
  - Eingehende Aktion
  - Neues EmailUserReportedPhishing-Skript
  - Tabelle „Erfassungsregeln“.
- Security Incident Response (sn_si): Umfasst:
  - Security Incident-Tabelle (sn_si_incident)
  - Tabelle „Sicherheits-Phishing-E-Mails“ (sn_si_phishing_email)
  - Tabelle „Sicherheits-Phishing-E-Mail-Header“ (sn_si_phishing_email_header)
  - EML-Upload-Datensatzersteller
- Security Operations Spoke

  Flows und Subflows für die Zusammenfassung von E-Mails und die Umwandlung von Phishing-E-Mails in Security Incidents.

Die folgende Abbildung zeigt die Tabelle „Neue Phishing-E-Mails“ mit Verweisen auf die übereinstimmende URP-Regel und den Zieldatensatz für Security Incidents (sn_si_incident).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein

Als Benutzer mit der Rolle „ `sn_si.admin` “ können Sie E-Mail-Abgleichregeln definieren, um von Benutzern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, nach der alle E-Mails, die entweder direkt oder über die Schaltfläche Phishing melden an *`security@acme.com`* gesendet werden, als von Benutzern gemeldete Phishing-E-Mails kategorisiert werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

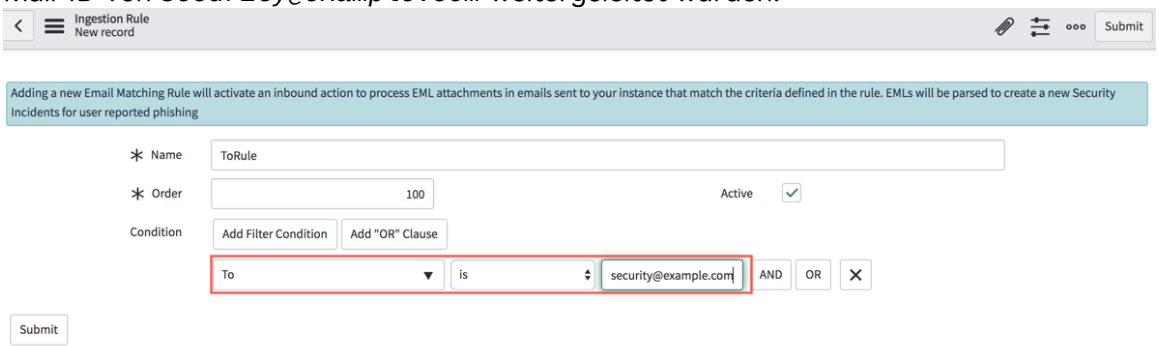
#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften des vom Anwender gemeldeten Phishing**.
2. Klicken Sie auf **Neu**, um eine neue E-Mail-Abgleichregel zu erstellen.
3. Geben Sie einen Namen ein, und definieren Sie eine oder mehrere Bedingungen für die Regel.
4. Klicken Sie auf **Absenden**, um die Regel zu speichern.
   Im Folgenden sind einige Beispielregeln aufgeführt:

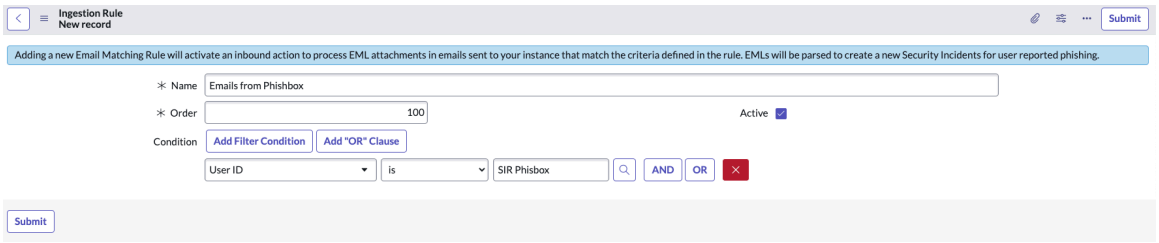


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ToRule**: Filtert E-Mails, die direkt gesendet oder an die E-Mail-ID von *security@example.com* weitergeleitet wurden.




- **Anwender-ID-Regel**: Filtert E-Mails, die von einer bestimmten E-Mail-ID gesendet wurden.




## Definieren Sie Eigenschaften für von Benutzern gemeldetes Phishing

Definieren Sie die Header-Informationen, die aus von Benutzern gemeldeten Phishing-E-Mails erfasst werden müssen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diese Optionen, um die folgenden Einstellungen für von Benutzern gemeldetes Phishing zu konfigurieren.

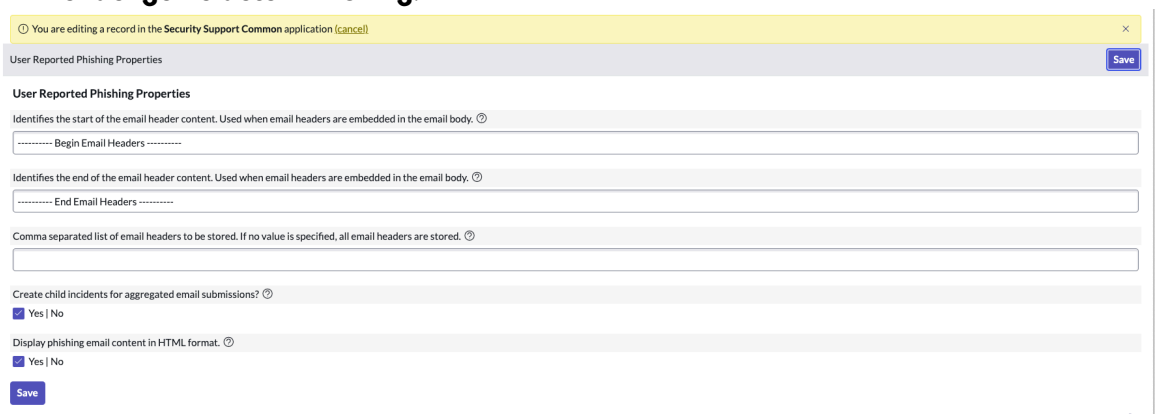
- Konfiguration zum Extrahieren von E-Mail-Kopfzeilen aus dem E-Mail-Text. (**Phishing-Übermittlungen** melden.)
- Filter, um Header auszuwählen.
- Aktivieren oder deaktivieren Sie die Zuordnung zwischen über- und untergeordneten Elementen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften des vom Anwender gemeldeten Phishing**.




2. Geben Sie die Konfiguration zum Extrahieren von E-Mail-Kopfzeilen aus dem E-Mail-Text an:
   - Geben Sie eine Zeichenfolge ein, die den Anfang des E-Mail-Headers identifiziert.
   - Geben Sie eine Zeichenfolge ein, die das Ende des E-Mail-Headers angibt.

   **Hinweis:**
   Wenden Sie diese Einstellungen nur auf Kopfzeilen an, die als Teil des E-Mail-Texts der Phishing-E-Mail erfasst wurden. Wenn beispielsweise das Wombat-Plugin mit dem Microsoft Outlook-Client konfiguriert wurde und der Benutzer auf die Schaltfläche Phishing melden **klickt**, werden die E-Mail-Header gemäß der hier definierten Konfiguration erfasst. Die Header-Informationen werden nicht erfasst, wenn die Phishing-E-Mail als Anhang weitergeleitet wird.

3. Geben Sie Filter an, um Header zu entfernen, die für die Untersuchung des Security Incident nicht erforderlich sind.

   Geben Sie eine durch Kommas getrennte Liste von E-Mail-Kopfzeilen ein, die aus der vom Benutzer gemeldeten Phishing-E-Mail erfasst werden müssen. Wenn Sie hier keinen Wert angeben, werden alle Header-Informationen erfasst.

4. Aktivieren oder deaktivieren Sie die Zuordnung zwischen über- und untergeordneten Elementen. Standardmäßig ist die Option **Ja** aktiviert. Wählen Sie **Ja**, um anzugeben, dass untergeordnete Security Incidents erstellt werden müssen, wenn von Benutzern gemeldete Phishing-E-Mails zusammengefasst werden. Wenn Sie **Nein**auswählen, werden keine untergeordneten Security Incidents erstellt, aber die vom Benutzer gemeldeten Phishing-E-Mails werden dem Security Incident zugeordnet, und der Security Incident-Datensatz wird aktualisiert. Weitere Informationen dazu, wie die untergeordneten Security Incidents erstellt werden, finden Sie unter Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln.
5. Aktivieren oder deaktivieren Sie die Option zum Anzeigen des Phishing-E-Mail-Inhalts im HTML-Format. Standardmäßig ist die Option **Ja** aktiviert. Wählen Sie **Ja**, um den Phishing-E-Mail-Inhalt im HTML-Format anzuzeigen. Wenn Sie **Nein**auswählen, ist der E-Mail-Inhalt im HTML-Format in einem Phishing-Datensatz nicht sichtbar.

### Phishing-E-Mail-Datensätze, die aus von Benutzern gemeldeten Phishing-E-Mails erstellt wurden

Von Benutzern gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Abgleichregeln in Security Incidents konvertiert.

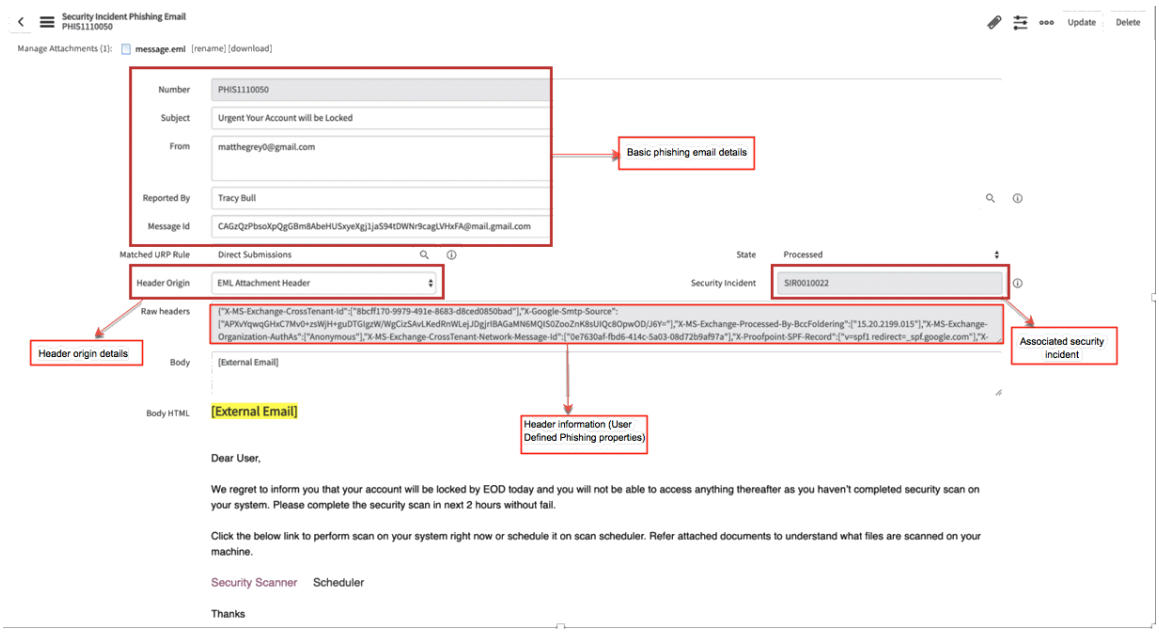
Wenn eine neue Phishing-E-Mail gemeldet wird, werden die folgenden Aktionen ausgeführt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Tabelle *„sys_email“* wird ein E-Mail-Datensatz erstellt.
- Die eingehende Aktion **Phishing-E-Mail erstellen** wird für den E-Mail-Datensatz ausgeführt und verwendet die E-Mail-Abgleichregeln (siehe Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein), um zu bestimmen, ob es sich um eine Phishing-E-Mail handelt.
- Wenn sie als Phishing-E-Mail identifiziert wurde, wird in der Tabelle sn_si_phishing_email ein Phishing-E-Mail-Datensatz erstellt.
- Abschließend wird der Flow Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln angewendet, um den Phishing-E-Mail-Datensatz in einen Security Incident zu konvertieren.

Um die E-Mail-Details anzuzeigen, navigieren Sie zu **Security Incident** > **Alle Phishing-E-Mails anzeigen**. Eine Liste der Phishing-E-Mail-Datensätze wird angezeigt. Klicken Sie auf den Datumslink in der Spalte Erstellt, um den E-Mail-Datensatz anzuzeigen.



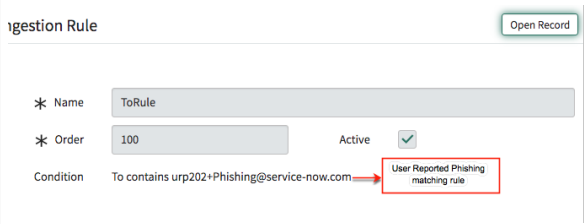

### Phishing-E-Mail-Details für Security Incident

| Feldname | Beschreibung |
|---|---|
| Nummer | Die Nummer, die der vom Benutzer gemeldeten Phishing-E-Mail zugewiesen ist. |
| Betreff | Betreff der E-Mail Die Betreffregel ist in simulierten Phishing-Kampagnen oder -Tests nützlich. In diesem Fall senden Unternehmen betrügerische E-Mails an ihre eigenen Mitarbeiter, um ihre Reaktion auf Phishing und ähnliche E-Mail-Angriffe zu testen.<br><br>Wenn in simulierten Phishing-E-Mail-Tests der Microsoft Outlook-E-Mail-Client mit dem Wombat-Plugin verwendet wird, kann der Benutzer auf die **Schaltfläche** Phishing melden klicken, um die Phishing-E-Mail zu melden. Die E-Mail wird an das Security Operations-Team gesendet, wobei **Simuliertes Phishing** an den Betreff der E-Mail angehängt wird. Dies wird verwendet, um die E-Mail als simulierte Phishing-E-Mail zu identifizieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

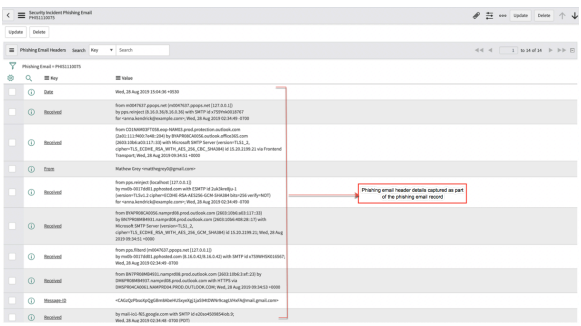
**Phishing-E-Mail-Details für Security Incident (Fortsetzung)**

| Feldname | Beschreibung |
|---|---|
| Von | Die E-Mail-Adresse, von der diese Phishing-E-Mail stammt. Diese Informationen sind verfügbar, wenn die Phishing-E-Mail als EML-Dateianhang weitergeleitet wird oder wenn die ursprünglichen Header in die E-Mail eingebettet sind.<br><br>Wenn der Benutzer die Phishing-E-Mail direkt weitergeleitet hat, ist die Absenderadresse möglicherweise nicht verfügbar. |
| Gemeldet von | Die E-Mail-ID des Benutzers, der diese Phishing-E-Mail gemeldet hat. Klicken Sie auf das **Informationssymbol**, um zusätzliche Details anzuzeigen. |
| Nachrichten-ID | Die der Nachricht zugewiesene ID. |
| Übereinstimmende URP-Regel | Die Regel für vom Anwender gemeldetes Phishing, die auf diese E-Mail angewendet werden soll. Klicken Sie auf das Informationssymbol, um zusätzliche Details anzuzeigen.<br><br>  <br><br><br>Wie Sie in diesem Beispiel sehen können, zeigt das Feld **Bedingung** an, dass die ToRule auf diese E-Mail angewendet wird und ein Security Incident erstellt wird. Weitere Informationen zum Definieren von E-Mail-Abgleichregeln finden Sie unter Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein. |
| Status | Wenn in der Tabelle `sn_si_phishing_email` ein neuer Phishing-E-Mail-Datensatz erstellt wird, wird das Feld Status auf **Neu**festgelegt. Wenn dieser E-Mail-Datensatz in einen Security Incident konvertiert wird (siehe Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln), wird das Feld Status auf **Verarbeitet**aktualisiert. |
| Header-Ursprung | Dieses Feld gibt an, woher die E-Mail-Kopfzeilen stammen oder wie der Benutzer die Phishing-E-Mail gemeldet hat:<br><br>• E-**Mail-Header**: Der Benutzer hat die Phishing-E-Mail an das Sicherheitsbetriebsteam weitergeleitet.<br>• **E-Mail-Text:**<br>  ○ Der Anwender hat auf die Option Phishing melden **geklickt** (wenn das Wombat-Plugin mit dem E-Mail-Client konfiguriert wurde).<br>  ○ Basierend auf der definierten Regel für vom Anwender gemeldetes Phishing wird die Phishing-E-Mail an das Sicherheitsbetriebsteam weitergeleitet.<br>• **EML-Anhang-Header**: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Phishing-E-Mail-Details für Security Incident (Fortsetzung)**

| Feldname | Beschreibung |
|---|---|
| | ○ Anhang: Der Benutzer hat die E-Mail als Anhang (.EML-Datei) weitergeleitet.<br>○ Service Catalog-Übermittlung: Der Benutzer hat die E-Mail als EML-Datei auf den Desktop heruntergeladen und dann an einen angegebenen Speicherort hochgeladen. Der Security Incident wird dann aus der E-Mail erstellt.<br>• **EML-Anhangtext**:<br>○ Der Anwender hat auf die Option Phishing melden **geklickt** (wenn das Wombat-Plugin mit dem E-Mail-Client konfiguriert wurde).<br>○ Basierend auf der definierten Regel für vom Anwender gemeldetes Phishing wird die Phishing-E-Mail als Anhang an das Sicherheitsbetriebsteam weitergeleitet. |
| Security Incident | Dieses Feld ist leer, wenn die vom Benutzer gemeldete Phishing-E-Mail zum ersten Mal gemeldet wird. Wenn der Flow Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln ausgeführt wurde, wird diese E-Mail in einen Security Incident-Datensatz konvertiert und die Nummer dieses Datensatzes wird hier angezeigt. |
| Unformatierte Header | In diesem Feld werden die vollständigen Header-Informationen angezeigt, die aus der E-Mail extrahiert wurden, wie auf der Seite Definieren Sie Eigenschaften für von Benutzern gemeldetes Phishing definiert. Die Header werden in Schlüssel-Wert-Paare analysiert und in der Liste „Phishing-E-Mail-Header“ angezeigt. |
|  | |
| Textkörper | Dies ist der Text der vom Benutzer gemeldeten Phishing-E-Mail. |

### Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln

Der Flow **Phishing-E-Mail in Security Incident** umwandeln ist ein neuer Flow, der Phishing-E-Mail-Datensätze in Security Incidents konvertiert oder umwandelt.

#### Vorbereitungen

**Hinweis:**

Um die Funktion „Vom Anwender gemeldetes Phishing“ zu aktivieren, müssen Sie eine Kopie des Flow erstellen und ihn aktivieren. Wenn Sie benutzerdefinierte eingehende Aktionen und benutzerdefinierte Flows erstellt haben, um von Benutzern gemeldete Phishing-Übermittlungen zu verarbeiten, sind die hier vorgeschlagenen Flow-Änderungen nicht erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erforderliche Rolle: sn_si.admin
- Flow Designer-Spoke muss installiert sein.

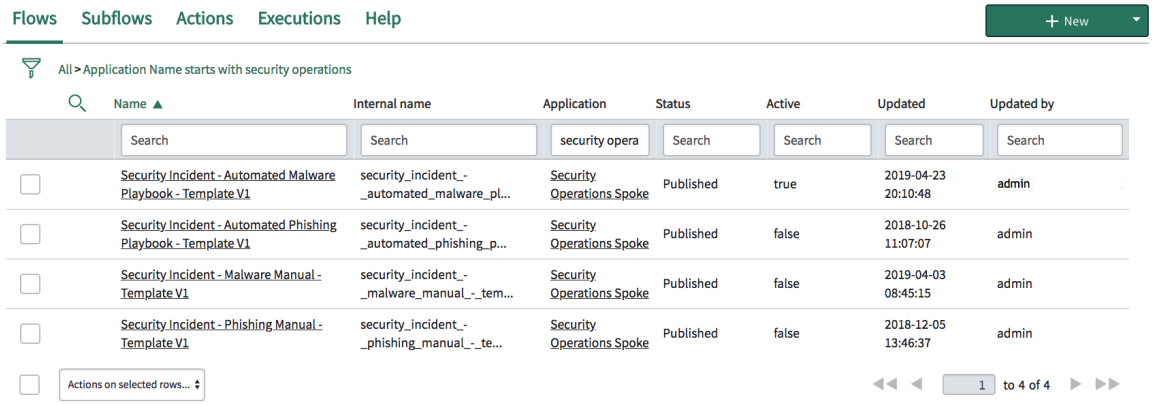
### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird automatisch gestartet, wenn ein von einem Benutzer gemeldeter Phishing-E-Mail-Datensatz mit dem Status **Neu** erstellt wird. Dieser Flow enthält die Logik:

- Sicherheits-Incidents zusammenfassen.
- Aktualisieren Sie Security Incidents mit relevanten Hinweisen.
- Fügen Sie Header-Daten hinzu.
- Erstellen Sie nach Bedarf untergeordnete Incidents.

### Prozedur

- Navigieren zu **Flow Designer** > **Designer** , um die mit der Security Operations-Spoke verfügbaren Flows anzuzeigen.



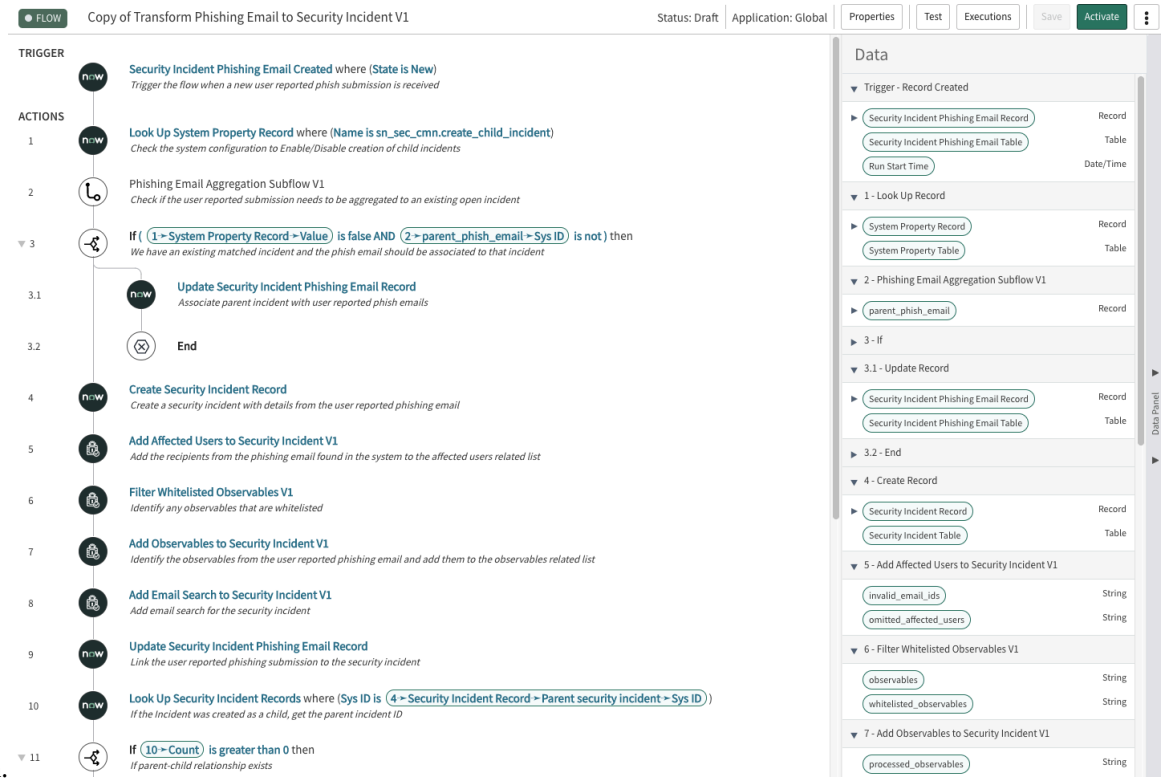

- Klicken Sie auf den Link **Phishing-E-Mail in Security Incidents** umwandeln, um den Flow anzuzeigen.
- Dieser Flow wird mit dem Basissystem bereitgestellt, befindet sich im **schreibgeschützten** Modus und kann nicht verwendet werden.

  Klicken Sie auf das Symbol „ Symbol „Mehr“ , erstellen Sie eine Kopie des Flows, und öffnen Sie sie zur weiteren Verwendung. Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslösebedingungen oder Aktionen ändern oder Aktionen hinzufügen und entfernen. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, müssen Sie den Flow aktivieren



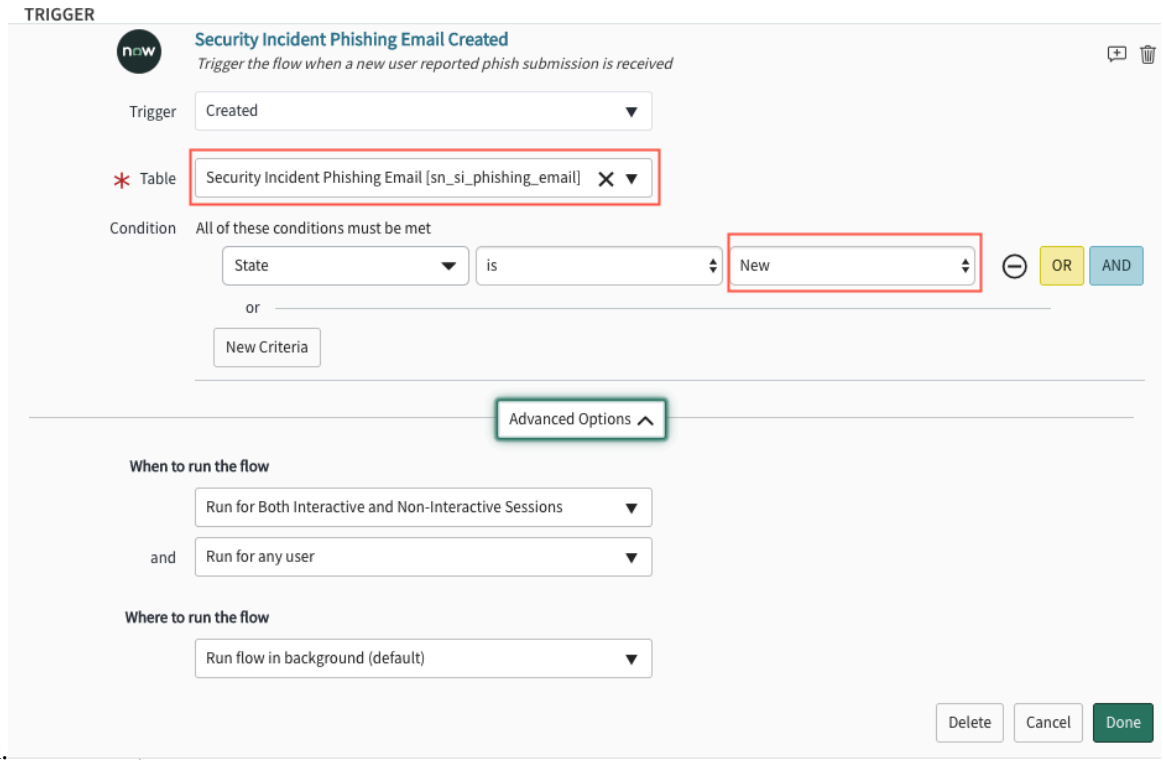
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

( Siehe Aktivieren Sie einen Security Incident Response -Flow), damit er ausgeführt werden kann.




Diese Abbildung zeigt den Auslöser und die mit dem Flow ausgeführten Schritte. Im rechten Bereich wird der Datenfluss angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

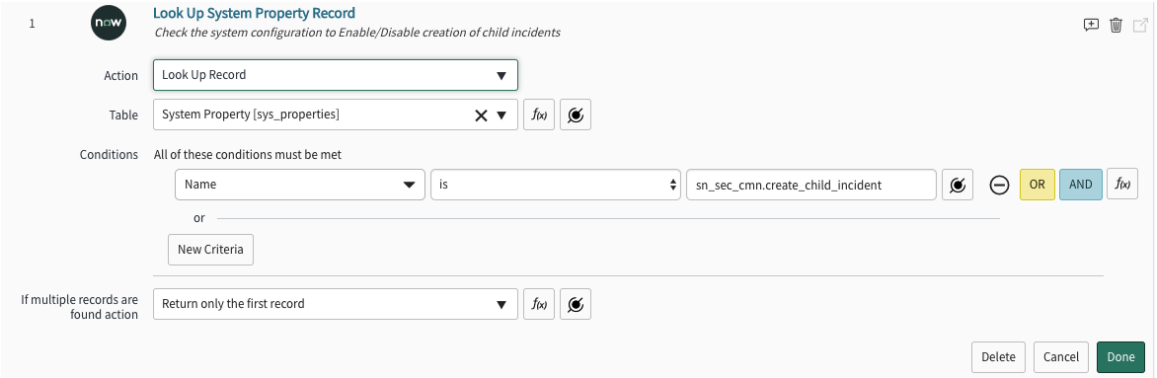
- Klicken Sie auf das **Auslösersymbol**.
  Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind.
  Dieser Flow wird initiiert, wenn ein **neuer** Datensatz in die Tabelle sn_si_phishing_email hochgeladen wird.



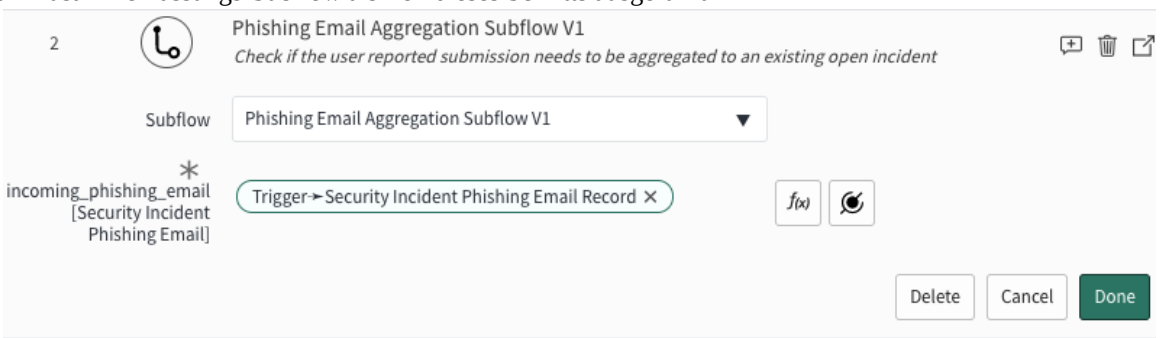

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In Schritt 1 überprüft der Flow, ob die **Option Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** -Kennzeichnung wird auf der Seite Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln aktiviert oder deaktiviert.

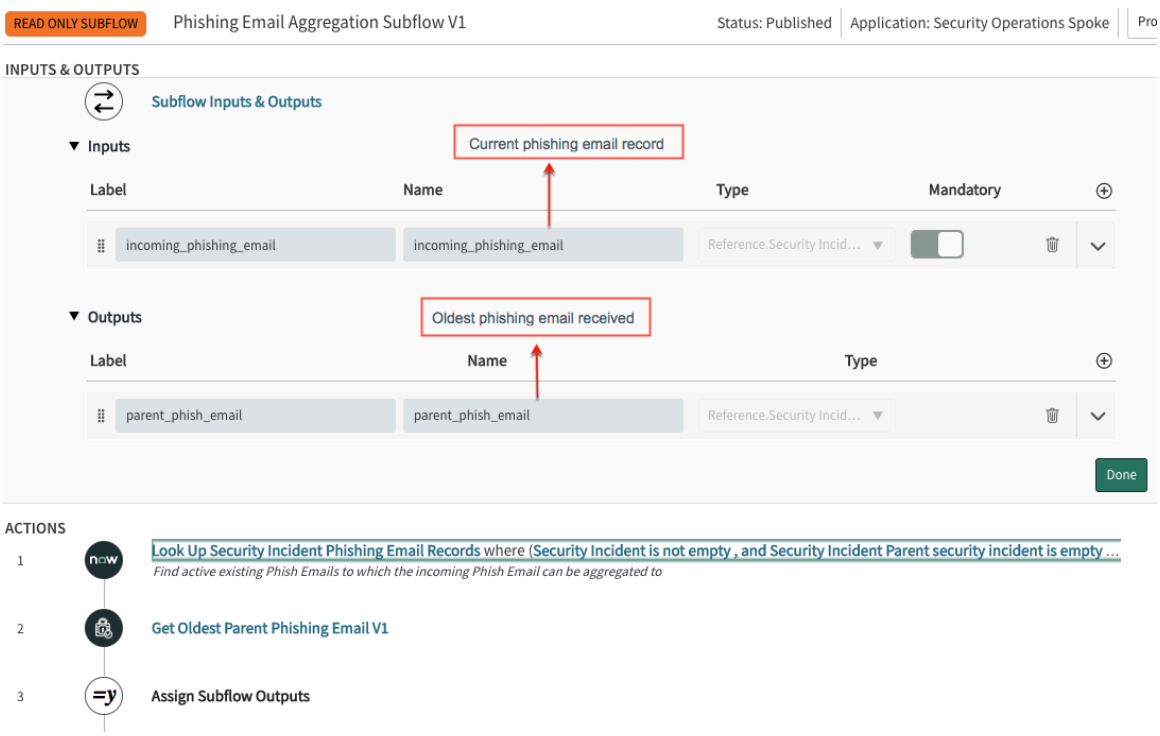



- In Schritt 2 wird der älteste übergeordnete Security Incident identifiziert.
  Beachten Sie das Symbol in Schritt 2. Dies weist darauf hin, dass der Phishing-E-Mail-Zusammenfassungs-Subflow als Teil dieses Schritts ausgeführt




wird.

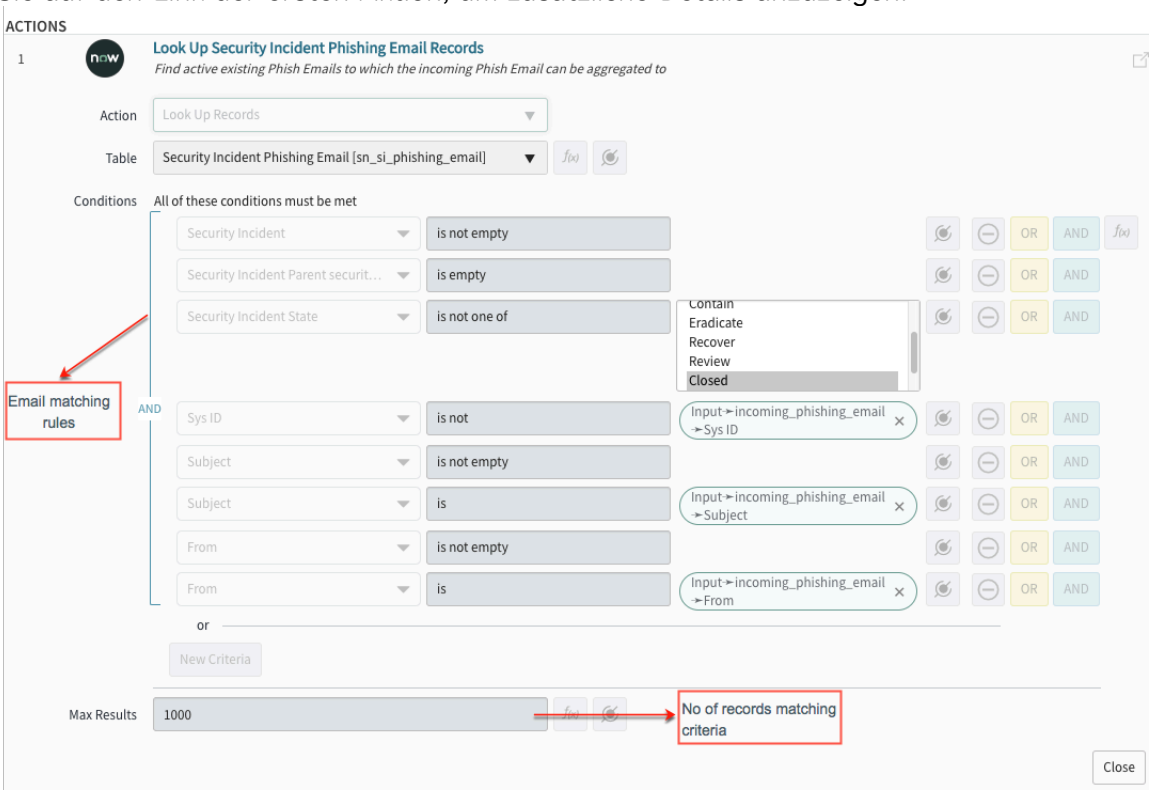
Klicken Sie auf das Aktionsdesigner-Symbol, um eine detaillierte Ansicht der Aktion anzuzeigen. Dieser Subflow überprüft die Phishing-E-Mail und ordnet sie basierend auf den angegebenen Kriterien einem vorhandenen Security Incident zu.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese beiden Aktionen werden ausgeführt, wenn dieser Subflow ausgeführt wird. Klicken Sie auf den Link der ersten Aktion, um zusätzliche Details anzuzeigen.




Mit dieser Aktion werden die E-Mails überprüft, die den Kriterien für die neue eingehende E-Mail entsprechen, basierend auf Bedingungen wie:

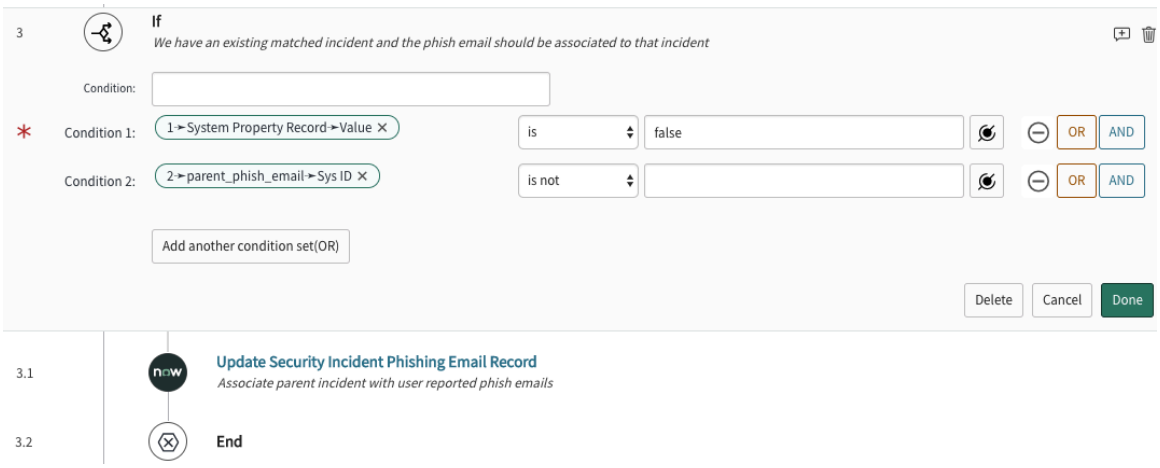
- Status des Security Incidents ist nicht **„Geschlossen“**.
- Betreff oder Von-Wert entsprechen den definierten Bedingungen für die E-Mail-Übereinstimmungsregel (siehe Richten Sie Erfassungsregeln für von Benutzern gemeldetes Phishing ein).

Wenn diese Bedingungen erfüllt sind, können Sie die Anzahl der Datensätze anzeigen, die den Kriterien im Feld Max. Ergebnisse entsprechen. Der älteste oder erste Datensatz in der Liste wird als übergeordneter Datensatz festgelegt, für den die Security Incidents zusammengefasst werden.

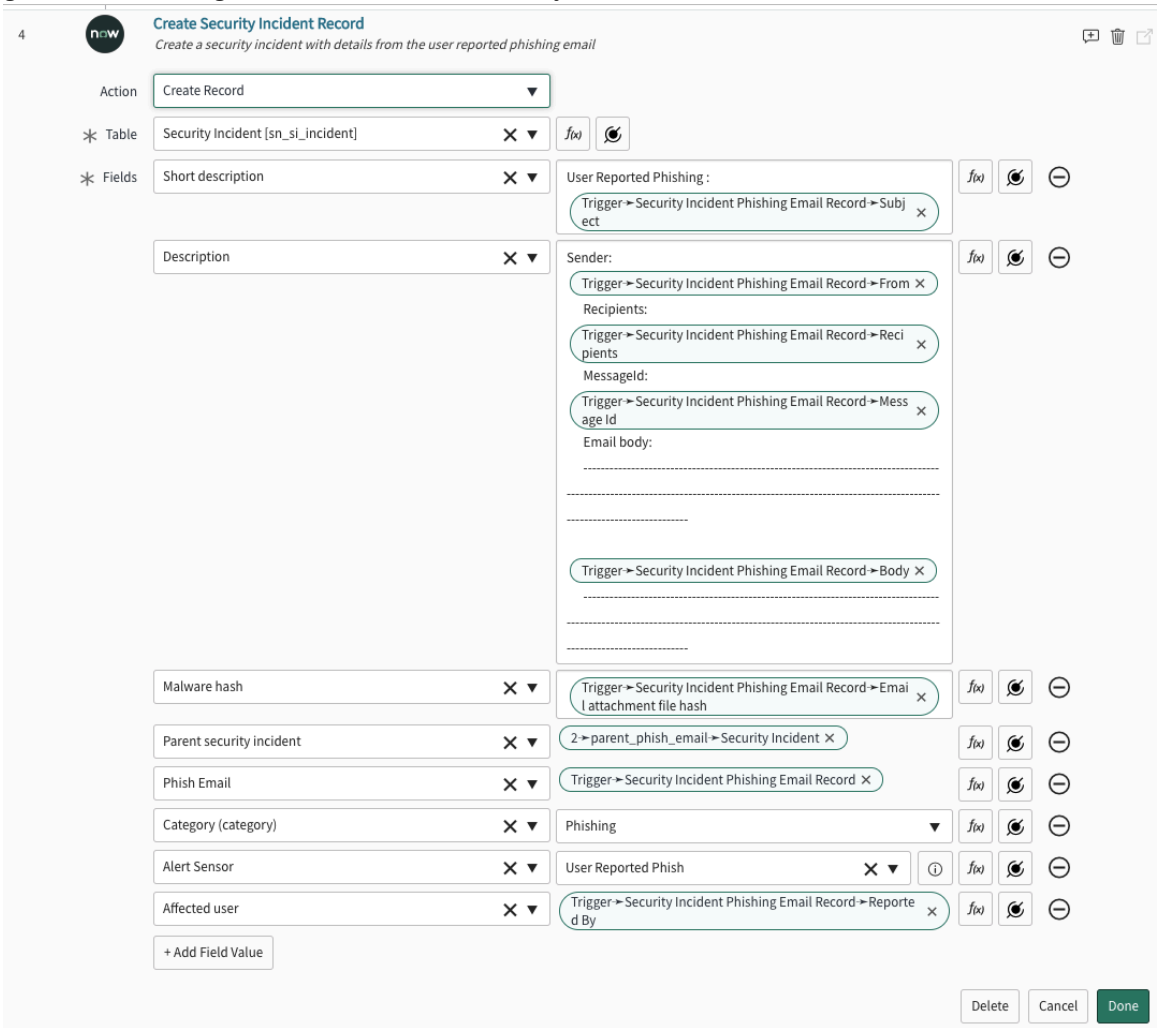
- Schritt 3 ist nur anwendbar, wenn **Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** Kennzeichnung wurde auf der Seite Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln auf „ **Nein** “ festgelegt.
  In diesem Fall wird die Phishing-E-Mail dem Security Incident-Datensatz zugeordnet, und der Flow wird beendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



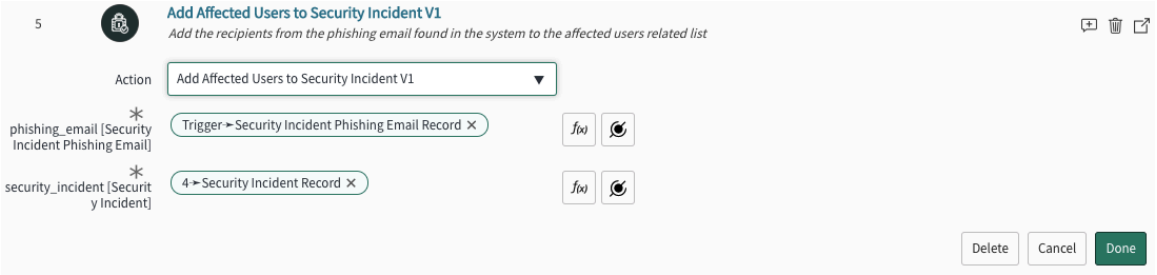

- Wenn die **Option Nachfolge-Incidents für zusammengefasste E-Mail-Übermittlungen erstellen?** auf **Ja**festgelegt wurde, wird der Flow weiterhin ausgeführt, und basierend auf der vom Benutzer gemeldeten Phishing-E-Mail wird ein neuer Security Incident erstellt.



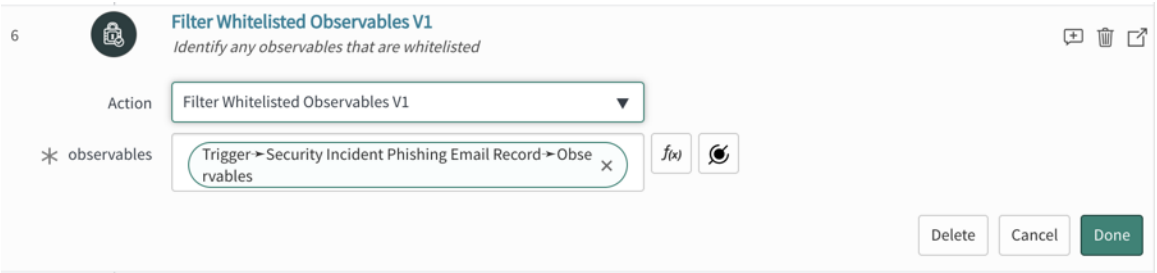

- In Schritt 5 werden Benutzer, die die Phishing-E-Mail erhalten haben (Mitarbeiter in der Liste „An“ und „CC“ der Phishing-E-Mail), der zugehörigen Liste „Betroffene Benutzer“ im Security Incident-Datensatz hinzugefügt.



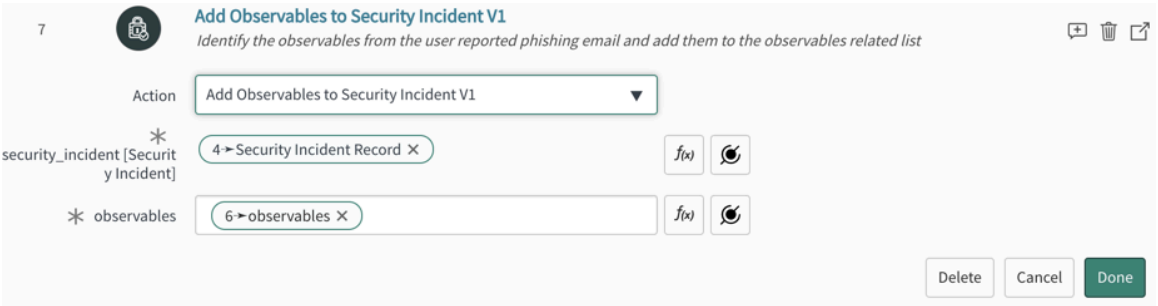
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



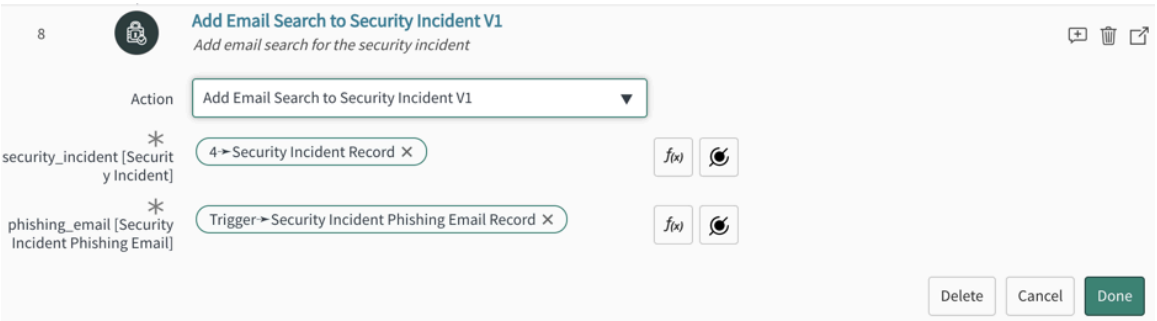

- In Schritt 6 werden die auf der Allow-Liste aufgeführten erkennbaren Elemente aus der Liste der erkennbaren Elemente im Security Incident gefiltert.
  Diese zulässigen aufgelisteten erkennbaren Elemente werden dem Security Incident nicht hinzugefügt.




- In Schritt 7 werden unbekannte erkennbare Elemente aus der vom Benutzer gemeldeten Phishing-E-Mail identifiziert und der zugehörigen Liste „Erkennbare Elemente“ hinzugefügt.



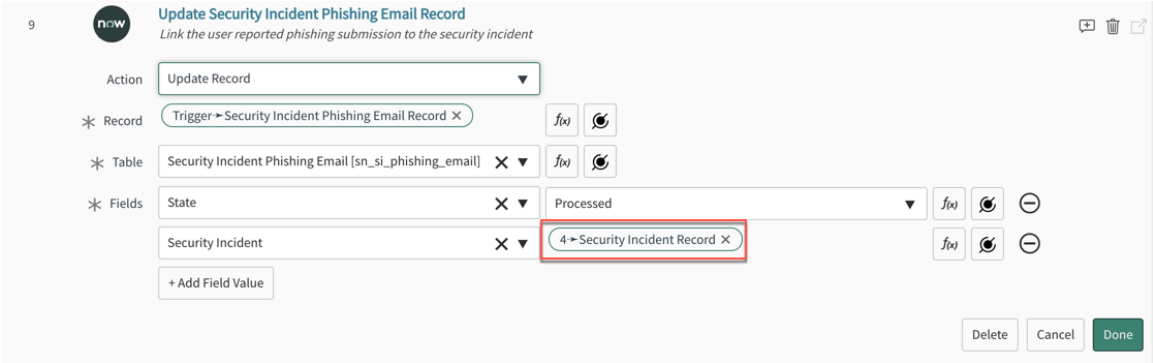

- In Schritt 8 wird eine E-Mail-Suchabfrage generiert, die eine Kombination aus Betreff und Absenderadresse der E-Mail ist.
  Diese Informationen sind nützlich, um die Mitarbeiter in der Organisation zu identifizieren, die Phishing ausgesetzt waren.



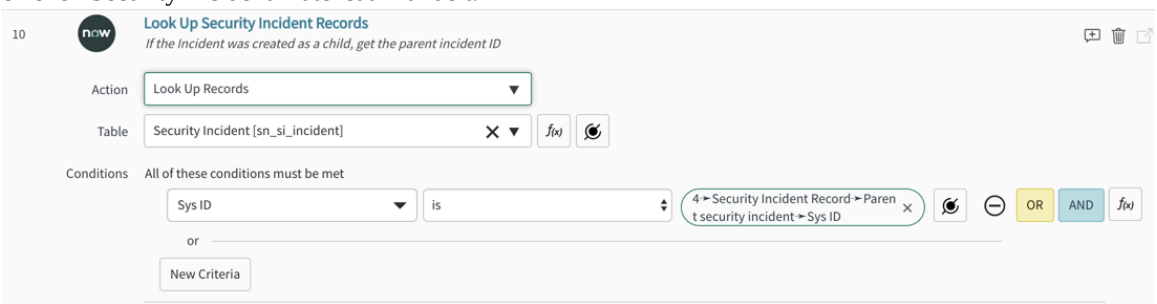

- In Schritt 9 wird die vom Benutzer gemeldete Phishing-E-Mail dem Security Incident zugeordnet, und der Security Incident-Datensatz (in Schritt 4 erstellt) wird aktualisiert.



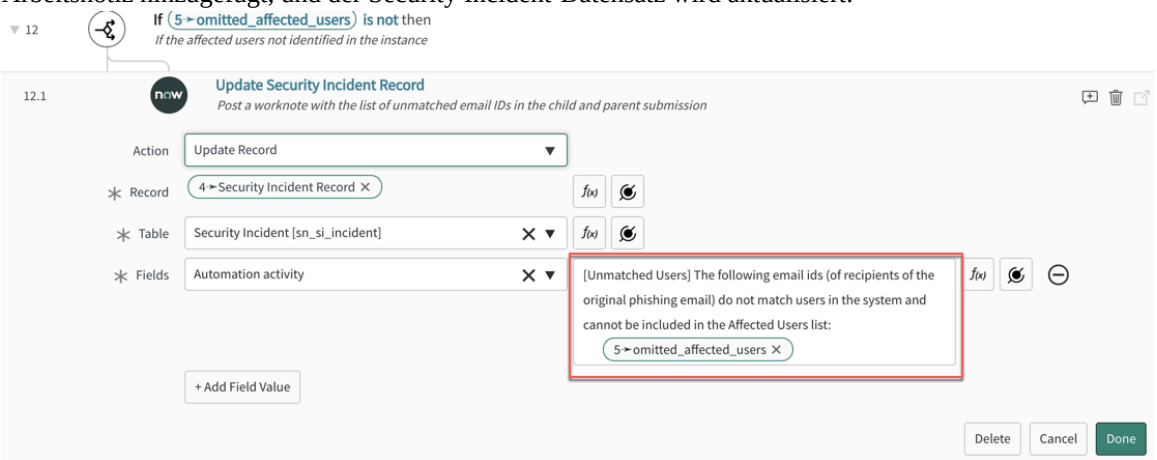
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- In Schritt 10 wird der übergeordnete Security Incident identifiziert und es wird überprüft, ob es sich um einen offenen Security Incident-Datensatz handelt.



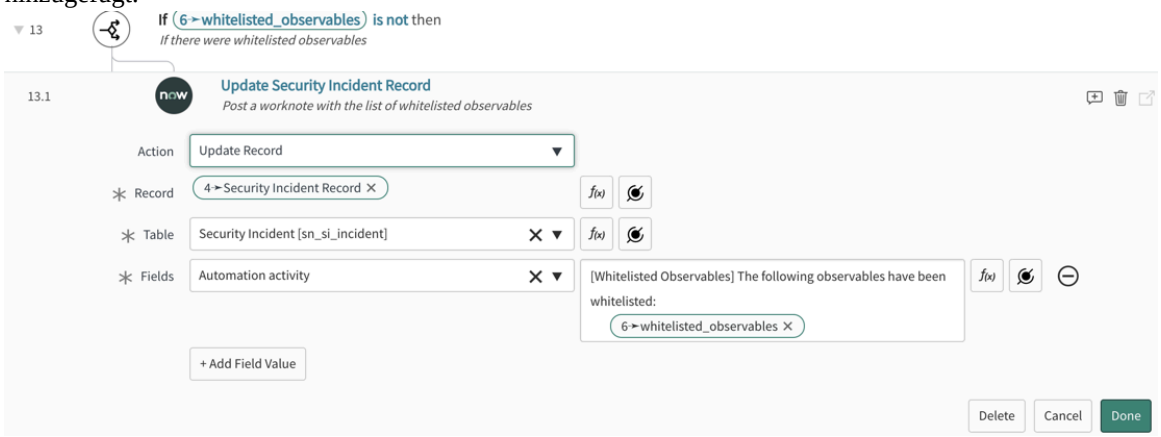

- Wenn die übergeordnete Sicherheit aktiv ist, werden den untergeordneten und übergeordneten Security Incident-Datensätzen Notizen hinzugefügt, die angeben, wie sie einander zugeordnet sind.
- Wenn in Schritt 12 keine betroffenen Benutzer gefunden wurden (in Schritt 5 des Flows), wird eine Arbeitsnotiz hinzugefügt, und der Security Incident-Datensatz wird aktualisiert.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

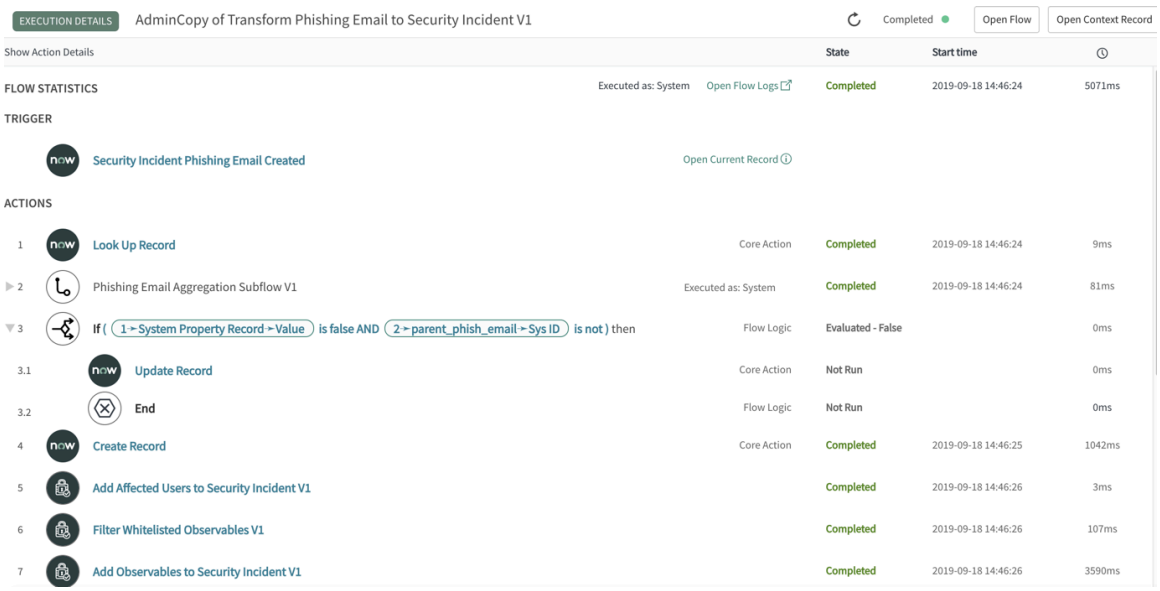
- In Schritt 13 wird eine Arbeitsnotiz mit der Liste der in der Allow-Liste aufgeführten erkennbaren Elemente hinzugefügt.




## Nächste Maßnahme

Sie können auf **Test** klicken, um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flow auf **Aktivieren**, um den Flow zu aktivieren und auszuführen.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.




Wenn der Flow ausgeführt wurde, wird der Phishing-E-Mail-Datensatz in einen Security Incident konvertiert. Siehe Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

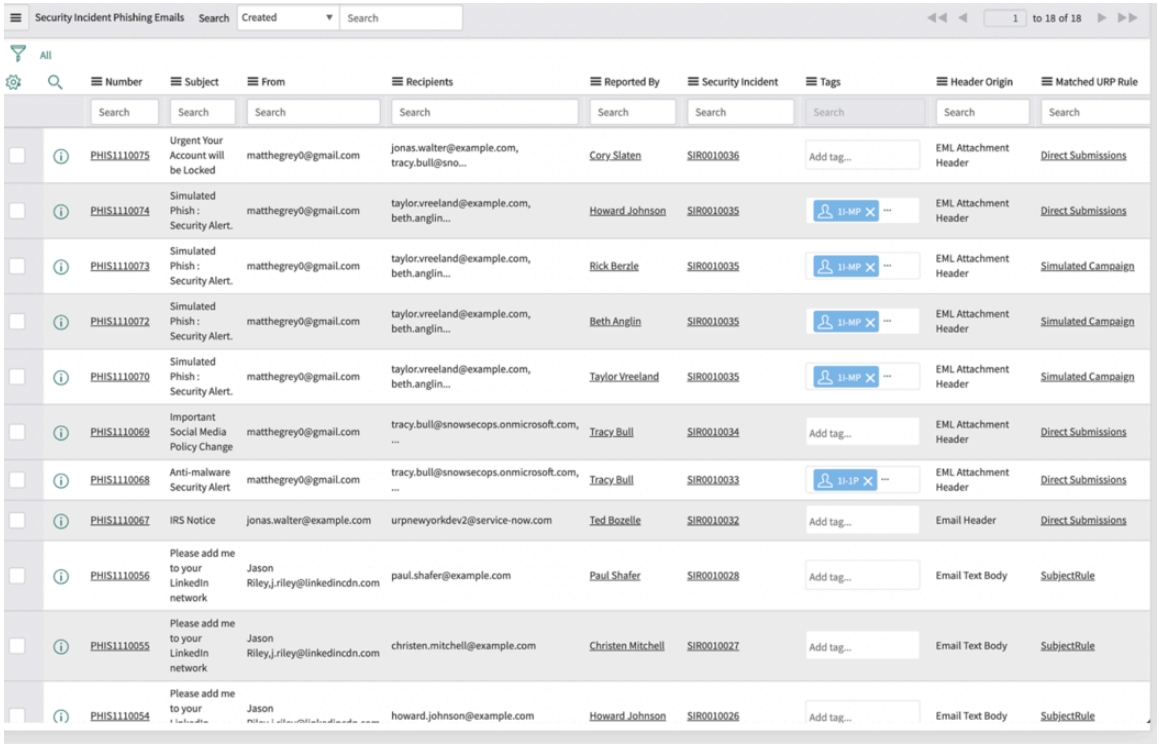
### Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Phishing-E-Mail-Datensätze, die in der Tabelle `sn_si_phishing_email` gespeichert sind, werden in Security Incident-Datensätze konvertiert.

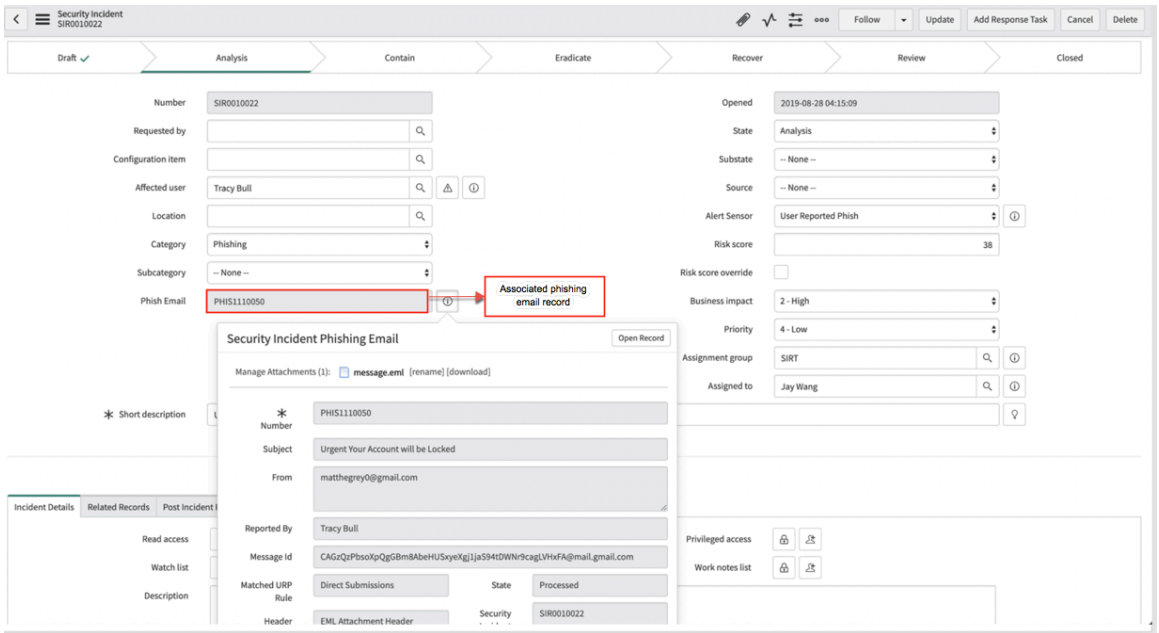
Um den Security Incident anzuzeigen, der dem Phishing-E-Mail-Datensatz zugeordnet ist, klicken Sie auf **Sicherheitsvorfall** > **Phishing-E-Mail** > **Alle Phishing-E-Mails anzeigen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Klicken Sie auf den Link in der Spalte „Security Incident“, der dem Phishing-E-Mail-Datensatz zugeordnet ist. Die Details des Security Incident werden angezeigt.




## Zugehörige Listen

Scrollen Sie nach unten zum Abschnitt „Zugehörige Links“ des Security Incident, und klicken Sie auf **Alle anzeigen zugehörige Liste**. Zeigen Sie Details wie untergeordnete Security Incidents, betroffene Benutzer und zugehörige Phishing-E-Mails an.

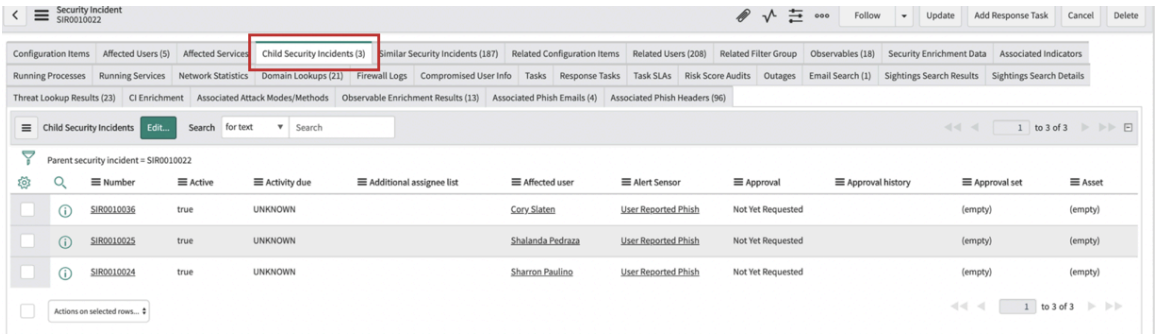
### Untergeordnete Security Incidents

Klicken Sie auf die Registerkarte **Untergeordnete Security Incidents**. Sie können eine Liste der untergeordneten Security Incidents anzeigen, die dem übergeordneten Security Incident basierend auf der angewendeten Zusammenfassungslogik zugeordnet sind. Für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

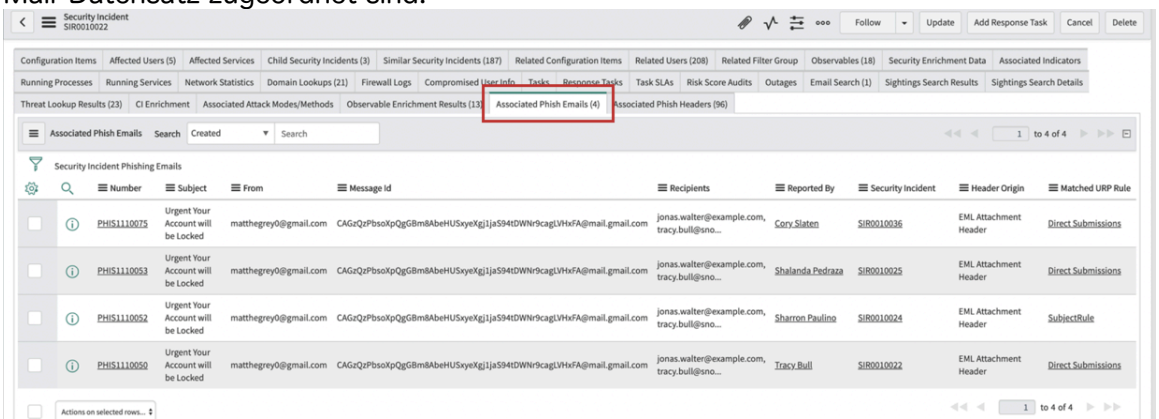
jeden hinzugefügten untergeordneten Datensatz wird dem übergeordneten Datensatz eine automatisierte Systemaktivität (im Abschnitt „Arbeitsnotiz“) hinzugefügt. Dadurch wird der Sicherheitsanalyst über den zusammengefassten untergeordneten Datensatz benachrichtigt.

**Hinweis:**
Sie können die untergeordneten Security Incidents hier nur anzeigen, wenn die Kennzeichnung **Untergeordnete Incidents für zusammengefasste E-Mail-Übermittlungen erstellen** auf der Seite „Anwender gemeldete Phishing-Eigenschaften“ auf **Ja** festgelegt ist. Details siehe Definieren Sie Eigenschaften für von Benutzern gemeldetes Phishing.




### Zugehörige Phishing-E-Mails

Klicken Sie auf die Registerkarte **Zugehörige Phishing-E-Mails**. Sie sehen eine Liste der Phishing-E-Mail-Datensätze (doppelte Datensätze), die dem übergeordneten Phishing-E-Mail-Datensatz zugeordnet sind.

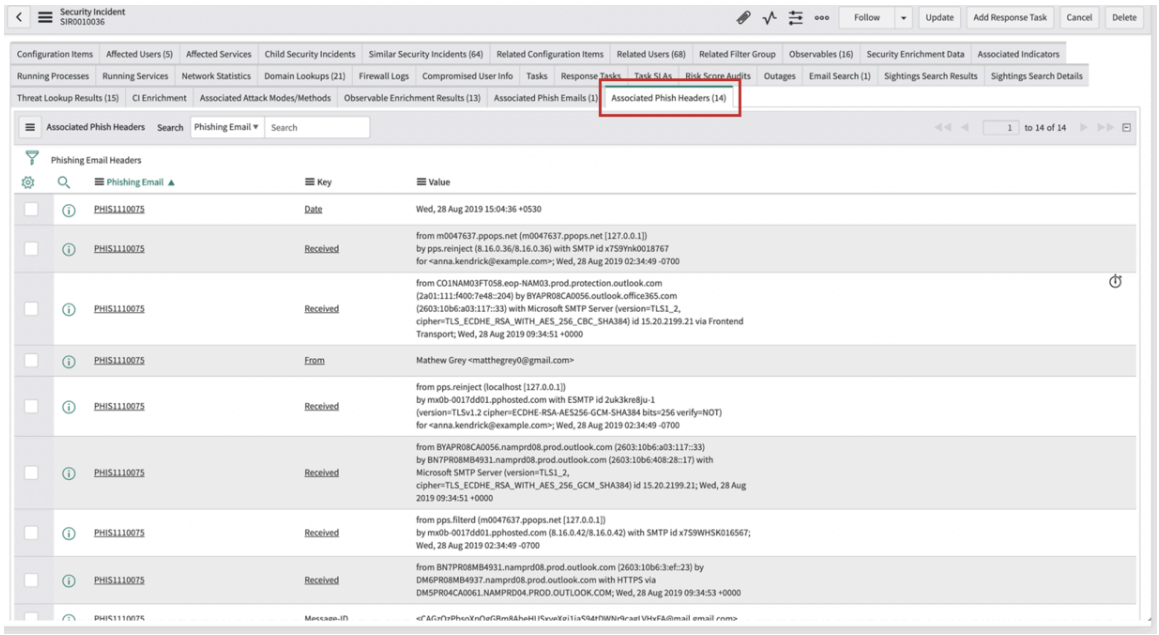



### Zugehörige Phishing-E-Mail-Header

Klicken Sie auf die Registerkarte **Zugehörige Phishing-E-Mails**. Sie sehen die Headerdetails der Phishing-E-Mail, die im Rahmen des Security Incident erfasst wurden. Sie können die zusammengefassten Kopfzeilen aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die für den übergeordneten Security Incident zusammengefasst sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

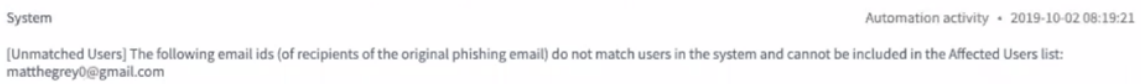



## Zulässige Liste erkennbarer Elemente

Während der Flow Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln ausgeführt wird, können Sie den Status des Security Incidents überwachen. Wenn bestimmte erkennbare Elemente als erkennbare Elemente der zulässigen Liste markiert sind, werden sie nicht der zugehörigen Liste „Erkennbare Elemente“ hinzugefügt. Durch Markieren der erkennbaren Elemente in der Allow-Liste können Sie sicherstellen, dass nur die wichtigen Details angezeigt werden. Beispiel: Wenn www.google.com eine der URLs ist, die als zulässige Liste markiert wurde, wird die folgende Systemmeldung angezeigt. Die Liste der zulässigen erkennbaren Elemente stellt sicher, dass nur die wichtigen erkennbaren Elemente überwacht werden.

## Nicht abgeglichene Benutzer werden erfasst

Einige E-Mail-IDs in der Liste „An“ und „CC“ der Phishing-E-Mail gehören möglicherweise nicht zu Benutzern in der Organisation. Diese E-Mail-IDs werden als nicht abgeglichene Benutzer kategorisiert und sind nicht in der zugehörigen Liste „Betroffene Benutzer“ enthalten. Es wird eine Arbeitsnotiz angezeigt, die angibt, dass es sich um nicht abgeglichene Benutzer handelt.



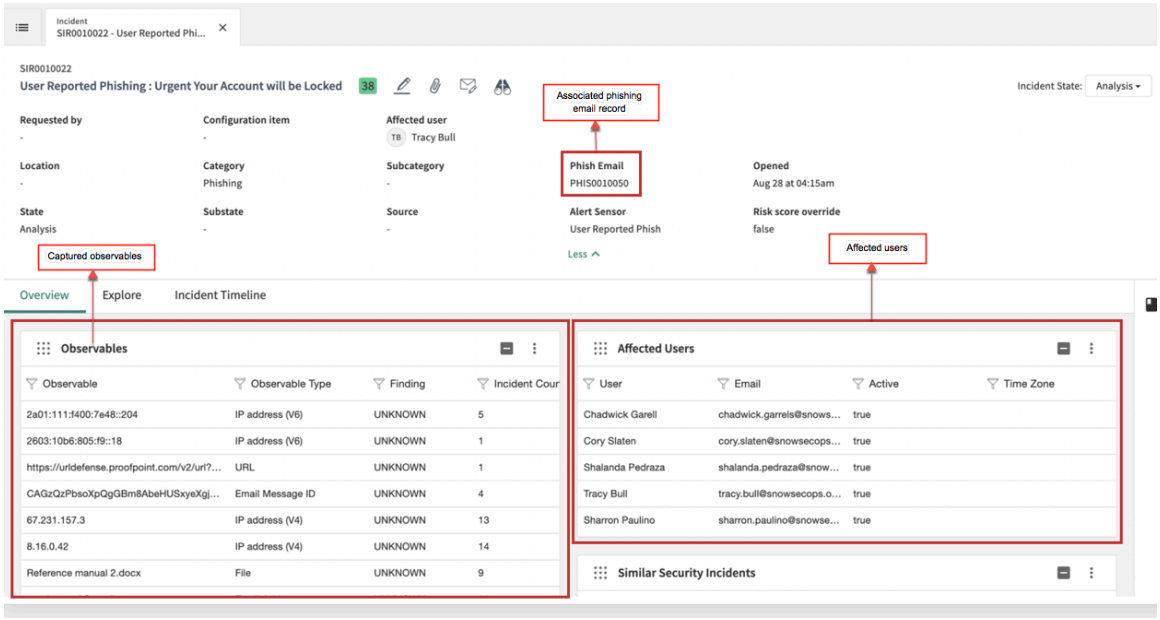

### Benutzer hat Phishing im Security Analyst Workspace gemeldet

Sie können Security Incidents anzeigen, die den Phishing-E-Mail-Datensätzen im Security Analyst Workspace zugeordnet sind.

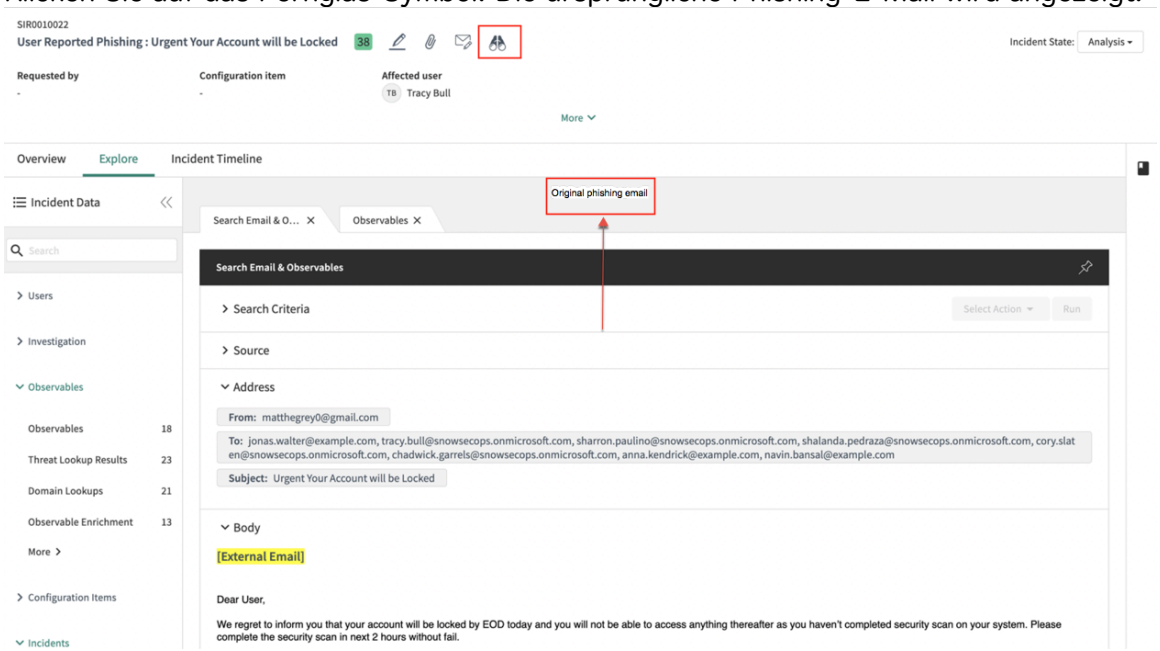
Navigieren zu **Security Incident** > **Neue UI**. Der Arbeitsbereich wird in einer separaten Browserregisterkarte geöffnet. Klicken Sie auf den Security Incident, der dem Phishing-E-Mail-Datensatz zugeordnet ist, um den Security Incident anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



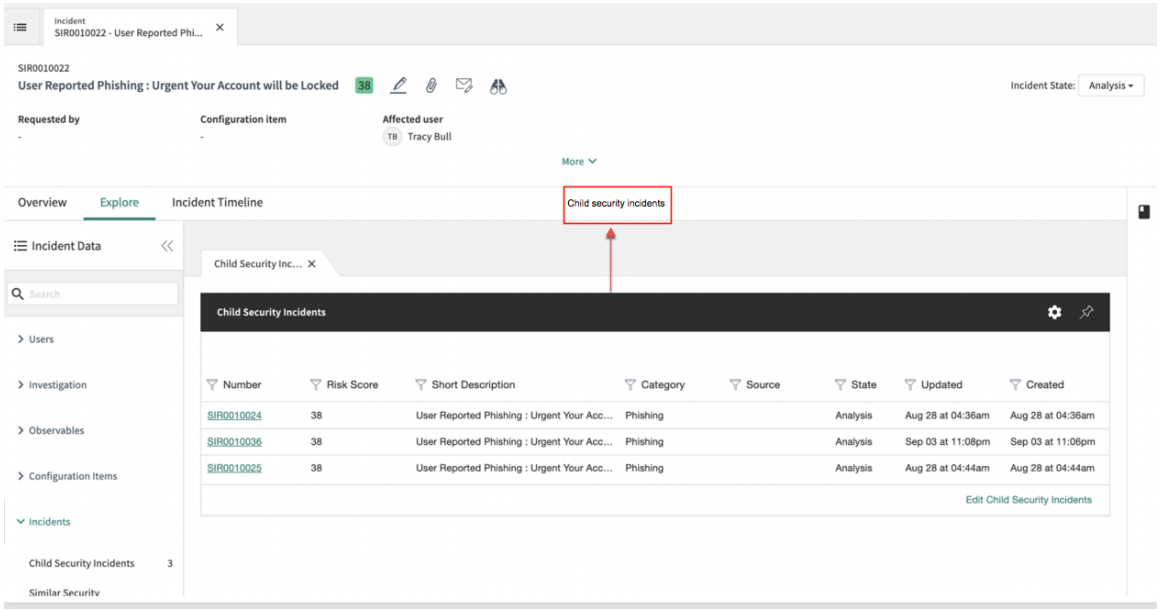

Klicken Sie auf das Fernglas-Symbol. Die ursprüngliche Phishing-E-Mail wird angezeigt.



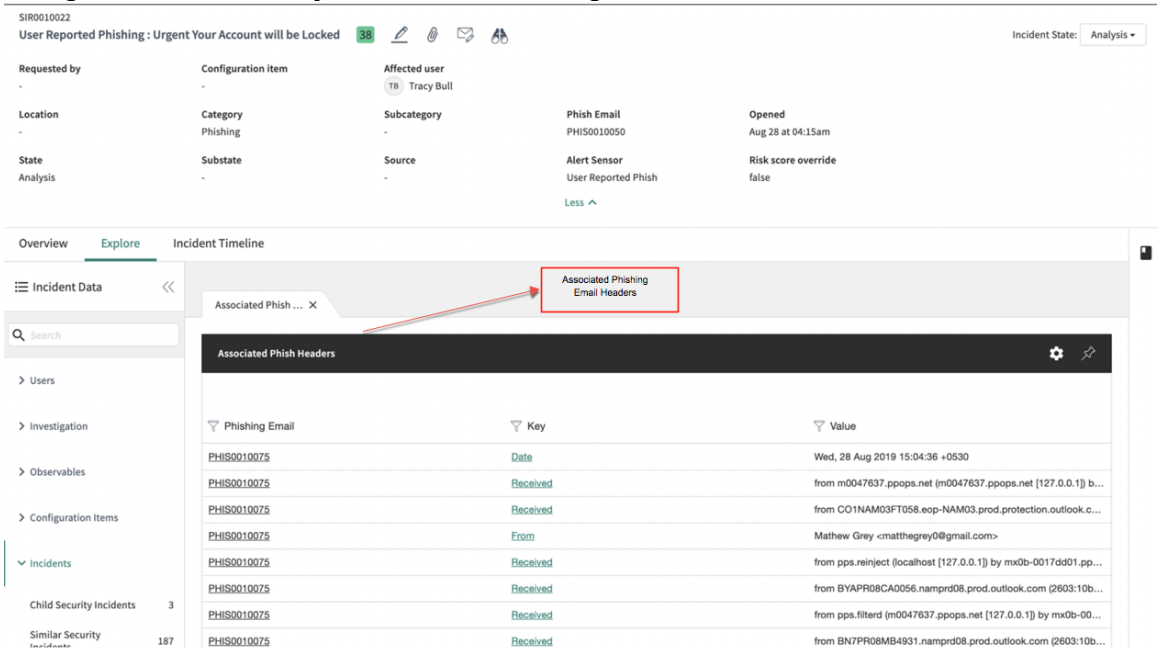

Klicken Sie auf der Registerkarte **Erkunden** auf **Incidents** > **Untergeordnete Security Incidents**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



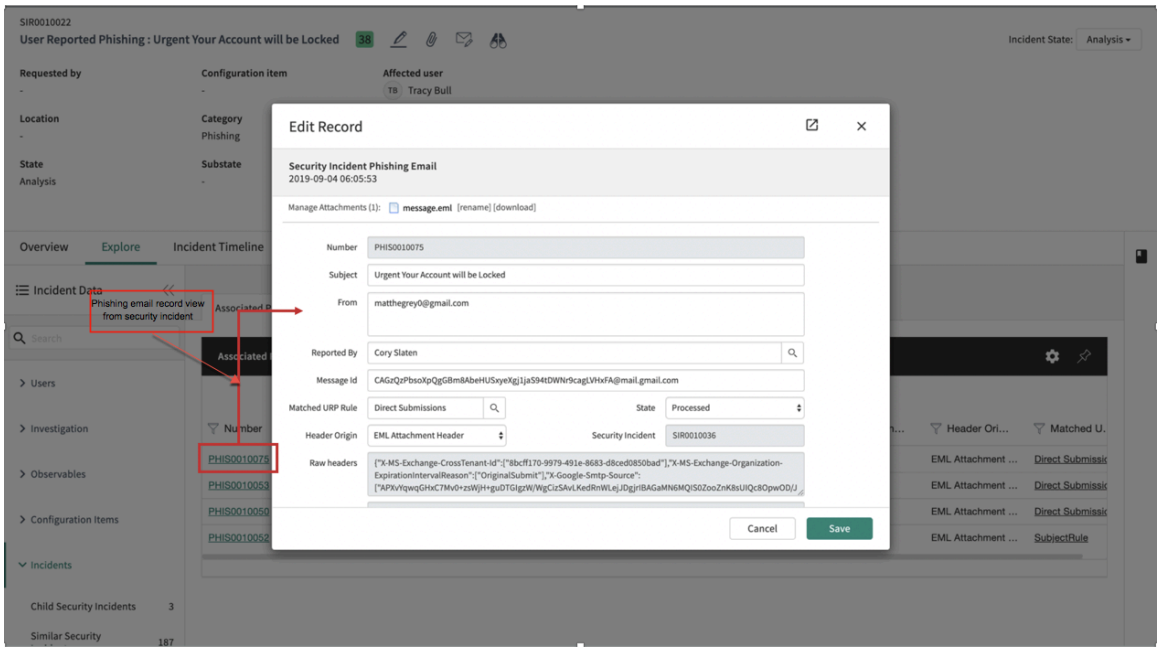

Klicken **Incidents** > **Zugehörige Phishing-Header** > . Sie können die Rollup-Kopfzeilen aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die für den übergeordneten Security Incident zusammengefasst sind.



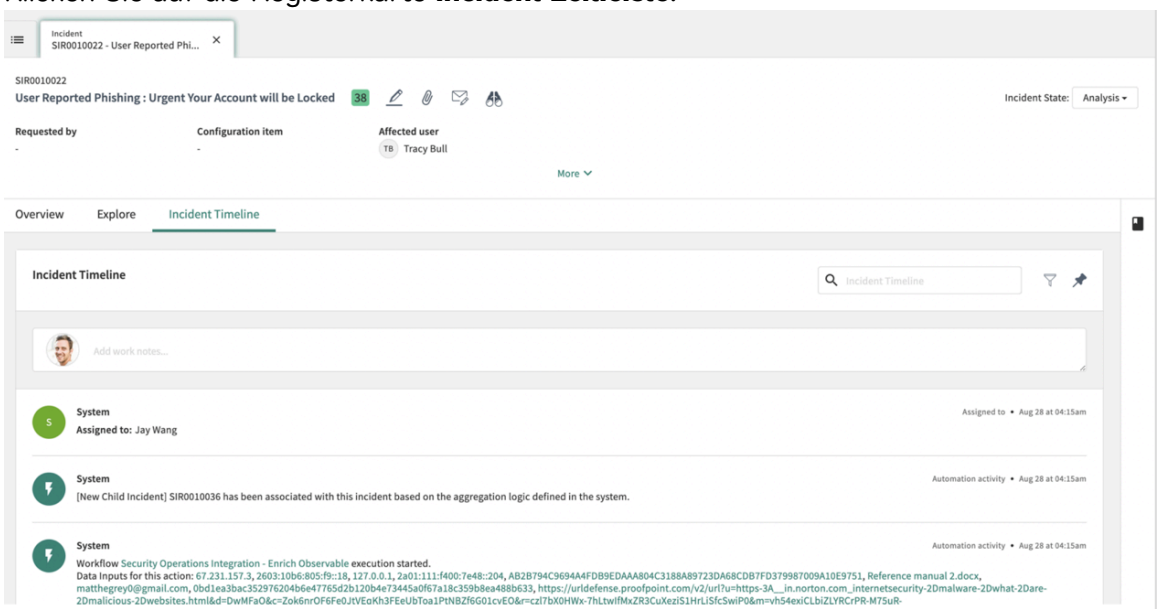

Klicken Sie auf den Phishing-E-Mail-Link, um den Phishing-E-Mail-Datensatz anzuzeigen, der dem Security Incident zugeordnet ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Klicken Sie auf die Registerkarte **Incident-Zeitleiste**.




Sie können die Systemupdates anzeigen, die Folgendes hervorheben:

- Doppelte untergeordnete Datensätze identifiziert.
- Zulässige Liste erkennbarer Elemente.
- Nicht abgeglichene Benutzer, die die Phishing-E-Mail erhalten haben, aber nicht zur Liste der betroffenen Benutzer gehören.

### Häufige Fragen

In diesem Abschnitt werden einige der häufig gestellten Fragen zur erweiterten Funktion für von Benutzern gemeldetes Phishing behandelt.

1. Ich habe die neue Security Incident Response-Spoke installiert, kann jedoch keine von Benutzern gemeldeten Phishing-Incidents anzeigen.

   Standardmäßig wurde die Funktion „Von Anwender gemeldetes Phishing“ deaktiviert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Funktion zu aktivieren, müssen Sie eine Kopie des schreibgeschützten Von Benutzern gemeldete Phishing-E-Mails in Security Incidents umwandeln -Flows erstellen und ihn vor der Verwendung aktivieren.

2. Welche Vorsichtsmaßnahmen werden bei der Erfassung von Phishing-E-Mails und deren Konvertierung in Security Incidents getroffen, um schädliche Links und Anhänge in den Phishing-E-Mails zu behandeln?

   Der Antivirenscanner ServiceNow scannt solche schädlichen Anhänge und Links. Um jedoch sicherzustellen, dass Sicherheitsanalysten die Incidents genau untersuchen können, erfasst die Anwendung Security Incident Response alle Artefakte, die Teil einer Phishing-E-Mail sind. Die Funktion „Von Anwender gemeldetes Phishing“ schaltet jedoch die schädlichen Links in der Phishing-E-Mail stumm, damit Sicherheitsanalysten nicht versehentlich auf diese Links klicken. In Bezug auf schädliche Anhänge müssen Sicherheitsanalysten beim Herunterladen dieser Anhänge vorsichtig sein.

3. Erfassen wir alle schädlichen Dateien, die Teil der Phishing-E-Mails sind, zur Ergänzung von Security Incidents?

   Ja, wir erfassen alle Dateien aus den Phishing-E-Mails. Sie können diese Details anzeigen, die als Teil der erkennbaren Security Incident-Elemente in Form eines Datei-Hashs verfügbar sind.

4. Senden wir schädliche Dateien und Links aus Phishing-E-Mails zur Untersuchung an eine Sandbox-Instanz?

   Derzeit unterstützen wir keine sofort einsatzbereiten Sandbox-Integrationen für die Untersuchung schädlicher Dateien und Links.

5. Gibt es ein Zeitfenster oder einen Auslöser, der die Dauer definiert, in der eingehende doppelte Phishing-E-Mail-Datensätze einem übergeordneten Security Incident zugeordnet werden?

   Doppelte Phishing-E-Mail-Datensätze werden nur für einen aktiven übergeordneten Security Incident zusammengefasst. Wenn der übergeordnete Incident geschlossen oder abgebrochen wird, wird die eingehende neue doppelte Phishing-E-Mail als neuer Security Incident erstellt. In diesem Szenario können Sie jedoch innerhalb des neuen Security Incident den geschlossenen oder abgebrochenen übergeordneten Security Incident in der zugehörigen Liste „ **Ähnliche Security Incidents** “ anzeigen.

   **Hinweis:**
   Dieses Verhalten kann mit dem Flow Designer konfiguriert werden.

6. Unterstützt die Phishing-Funktion für Benutzerberichte die Verwendung nur des Microsoft Outlook Wombat-Plugins zum Erfassen von E-Mail-Header-Details?

   Die Funktion „Anwender gemeldet“ wurde zum Analysieren von E-Mail-Kopfzeilen entwickelt und entspricht den RFC822-Standards. Daher werden ähnlich wie das Wombat-Plugin alle anderen Microsoft Outlook-Plugins unterstützt, die E-Mail-Kopfzeilen basierend auf RFC822-Standards erfassen.

## Datensatzerstellung aus Security Incidents

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG), Incident (INC) oder Problem (PRB)-Datensatz erstellen. Sie können auch aus jedem Security Incident einen Kundenservicefall erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie einen Change, einen Incident oder ein Problem aus einem Security Incident

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG), Incident (INC) oder Problem (PRB)-Datensatz erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn.si_basic oder höher

#### Prozedur

1. Öffnen Sie einen Security Incident mit einer der folgenden Methoden.
   - Öffnen Sie einen vorhandenen Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, und klicken Sie auf einen Security Incident.
   - Erstellen Sie einen Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, klicken Sie auf **Neu**, füllen Sie das Formular aus, und speichern Sie den Datensatz.
2. Klicken Sie mit der rechten Maustaste in die Kopfzeile des Security Incident, und klicken Sie auf eine der folgenden Optionen:
   - **Change erstellen**
   - **Incident erstellen**
   - **Problem erstellen**

   **Hinweis:**
   Diese Auswahl gilt nur, wenn die Popup-Eigenschaft (sn_vul.popup) aktiviert ist. Wenn Sie auf eine dieser Schaltflächen klicken, wird ein Vorschaufenster geöffnet, in dem die Informationen aus dem Security Incident angezeigt werden, die zum Erstellen des Change, Incident oder Problem verwendet wurden. Das heißt, das Konfigurationselement, sein Speicherort, seine Priorität sowie die Kurz- und Langbeschreibung. Wenn Sie eine Change-Anforderung erstellen, können Sie die Felder **Priorität**, **Kurzbeschreibung**und **Beschreibung** bearbeiten. Wenn Sie einen Incident erstellen, können Sie die Felder **Auswirkung**, **Dringlichkeit**, **Kurzbeschreibung** und **Beschreibung** bearbeiten. Die Felder im zugehörigen Security Incident-Bildschirm sind nicht betroffen.
3. Klicken Sie auf **Absenden**, um den Change, den Incident oder das Problem zu erstellen.

### Erstellt einen Customer Service-Fall aus einem Security Incident

Security Incident Response wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem Kundenservice (CS)-Fall zuordnet. Sie können einen CS-Fall aus einem beliebigen Security Incident erstellen, die **Priorität**bearbeiten und **optionale Notizen**hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic und sn_customerservice_agent

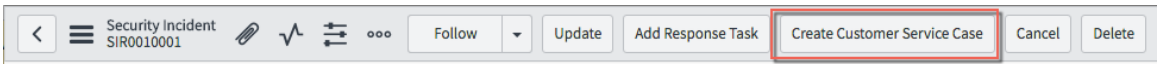
**Hinweis:**
Das Plugin Kundenservice muss aktiviert sein, um diese Aufgabe auszuführen.

#### Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Öffnen Sie den Security Incident, dem Sie einen CS-Fall hinzufügen möchten.
3. Klicken Sie im oberen Header auf **Kundenservicefall erstellen**.



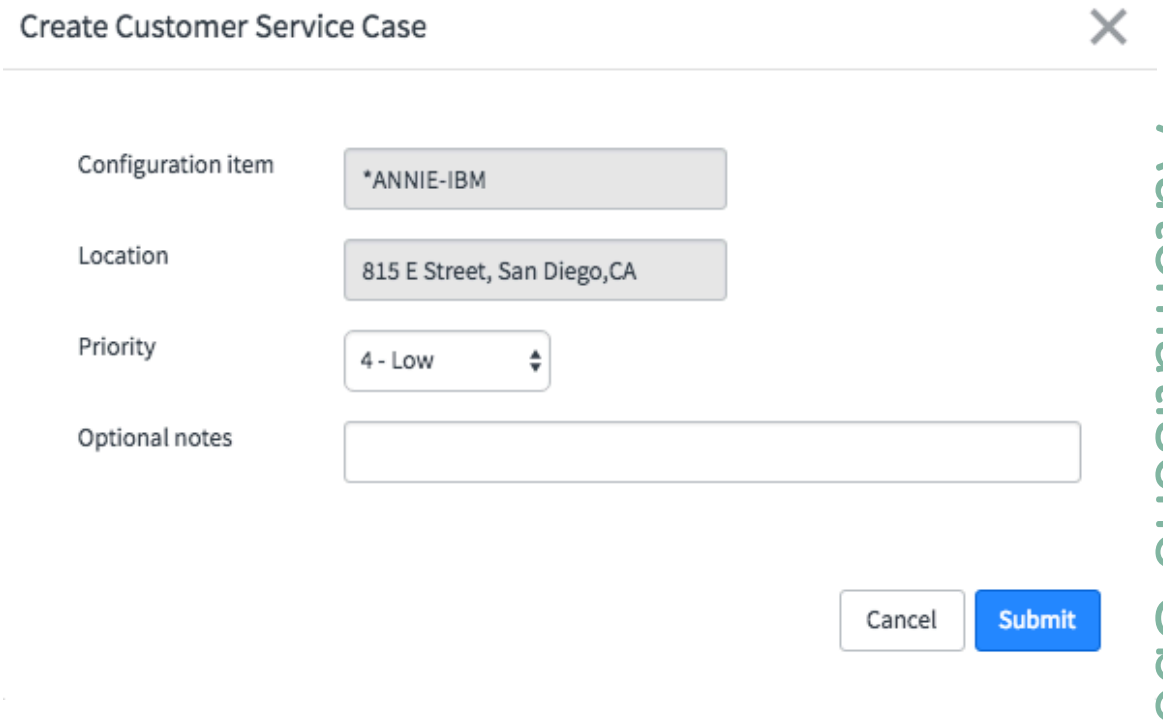
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Popup-Fenster ist basierend auf Ihrer Feldzuordnung vorab mit Informationen aus dem Security Incident ausgefüllt.

4. Sie können eine neue **Priorität** auswählen und **optionale Notizen**hinzufügen.

**Hinweis:**
Das Feld **Priorität** überschreibt die Standardeinstellung. Die **optionalen Notizen** werden an den Incident angehängt.




5. Klicken Sie auf **Absenden**.
Ein CS-Fall wird erstellt und in der zugehörigen Liste „Kundenservicefälle“ im Security Incident angezeigt.
6. Sie können auf den CS-Falllink klicken, um den Fall nachzuverfolgen.

**Zugehörige Informationen**

Kundenservice-Fallverwaltung

## Fügen Sie einem Sicherheitsfall einen Security Incident hinzu

Wenn Sie der Meinung sind, dass ein Security Incident eine höhere Analyseebene erfordert, fügen Sie ihn einem neuen oder vorhandenen Fall hinzu.

### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_si.admin, sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren Sie zu dem Security Incident, der eine Eskalation erfordert, indem Sie auf klicken **Security Incident** > **Incidents** > **Mir zugewiesen**, und öffnen Sie den Security Incident.
2. Klicken Sie auf den zugehörigen Link **Zu Sicherheitsfall hinzufügen**.
   Das Dialogfeld „ **Security Incident(s) zu Sicherheitsfall** hinzufügen“ wird geöffnet.

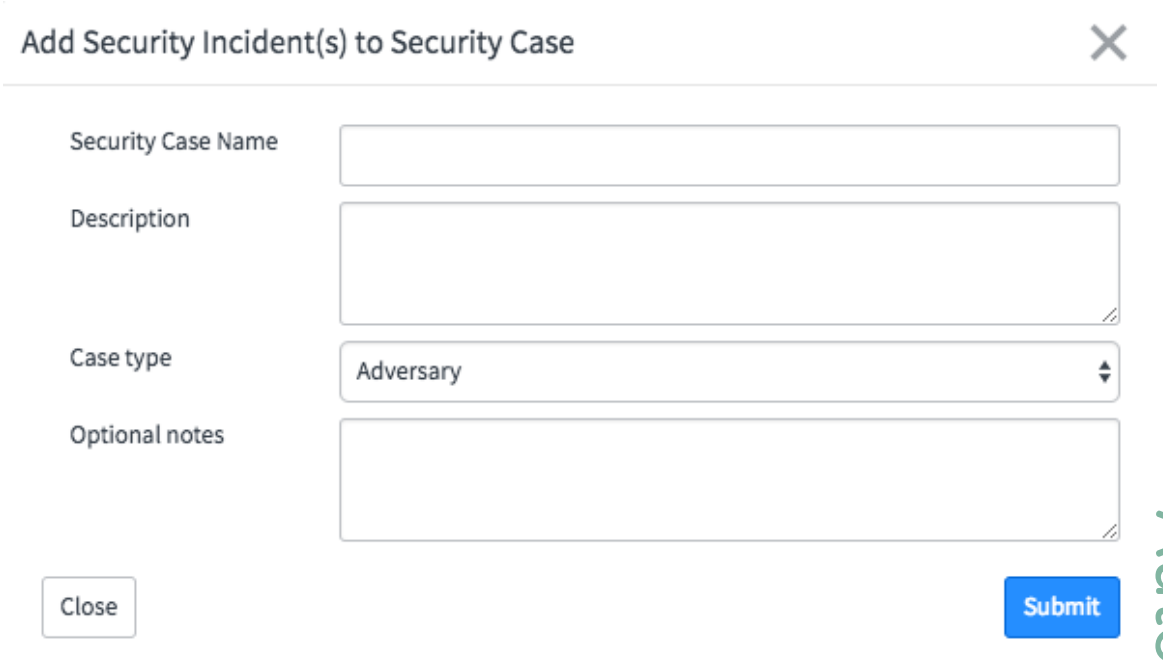
3. Wenn Ihnen ein Fall zugewiesen ist, dem Sie diesen Security Incident hinzufügen möchten, füllen Sie die Felder entsprechend aus, und klicken Sie dann auf **Absenden**.

| Feld | Beschreibung |
|---|---|
| Sicherheitsfall | Wählen Sie den Sicherheitsfall aus. |
| Optionale Notizen | Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert sein könnten. |

4. Wenn Ihnen ein oder mehrere Fälle zugewiesen sind, Sie jedoch einen neuen Fall erstellen und ihm den Security Incident zuweisen möchten, klicken Sie auf **Neuen Fall erstellen**, um zusätzliche Felder anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn Ihnen keine Fälle zugewiesen sind, wird zuerst der obige Bildschirm geöffnet.

5. Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Name des Sicherheitsfalls | Geben Sie den Namen des neuen Sicherheitsfalls ein. |
| Beschreibung | Geben Sie eine Beschreibung für den Fall ein. |
| Falltyp | Wählen Sie die Art des untersuchten Falls aus. |
| Optionale Notizen | Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert sein könnten. |

6. Klicken Sie auf **Absenden**.
Am Anfang des Security Incident wird eine Nachricht zusammen mit einem Link zum neuen Fall angezeigt.

**Zugehörige Informationen**

Security Case Management

## Erstellen Sie Antwortaufgaben

Nachdem ein Security Incident erstellt wurde, können Sie Antwortaufgaben erstellen, um einzelne Aktionen nachzuverfolgen, die als Reaktion auf das Sicherheitsproblem ausgeführt werden sollen.

### Vorbereitungen

Erforderliche Rolle: sn_si.basic

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren Sie zum entsprechenden Speicherort, um den Security Incident zu öffnen, für den Sie Aufgaben erstellen möchten.
   Beispiel:
   - Um eine Antwortaufgabe basierend auf einem Ihnen zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Mir zugewiesen**.
   - Um eine Antwortaufgabe basierend auf einem Ihrem Team zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Dem Team zugewiesen** > **Incidents**.
   - Um eine Antwortaufgabe basierend auf einem nicht zugewiesenen Security Incident zu erstellen, wählen Sie **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**.
2. Öffnen Sie den Security Incident, für den Sie Antwortaufgaben hinzufügen möchten.
3. Klicken Sie im Header des Formulars auf die Schaltfläche **Antwortaufgabe** hinzufügen.

   **Hinweis:**
   Um eine weitere Aufgabe zu erstellen, klicken Sie in der zugehörigen Liste „Incident“ auf die Registerkarte **Aufgaben**. Weitere Informationen zum Erstellen anderer Aufgabentypen finden Sie unter Erstellen Sie eine Aufgabe.

4. Füllen Sie die entsprechenden Felder im Formular aus.

#### Sicherheitsvorfall

| Feld | Beschreibung |
|---|---|
| Sicherheits-Tag auswählen | Wenn Sie Sicherheits-Tagseingerichtet und aktiviert haben, können Sie ein oder mehrere Tags auswählen, um dem Datensatz Metadaten hinzuzufügen, oder den Grad der Vertraulichkeit der Antwortaufgabe angeben.<br>Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt. |
| Nummer | [Schreibgeschützt] Die automatisch generierte Nummer Security Incident Response. |
| Übergeordnet | [Nur Lesen] Die Nummer des zugehörigen Security Incidents. |
| Konfigurationselement | Das vom Sicherheitsproblem betroffene Konfigurationselement (Ressource). |
| Betroffener Anwender | Die vom Sicherheitsproblem betroffene Person. |
| Priorität | Die Priorität, anhand derer bestimmt wird, wann diese Aufgabe ausgeführt wird. |
| Status | Aktueller Status der Sicherheitsreaktionsaufgabe Nach der Aufgabenerstellung wird dieses Feld standardmäßig auf **Entwurf**gesetzt. |
| Kompetenzen | Die zum Ausführen dieser Aufgabe erforderliche Kompetenz. Klicken Sie auf das Sperrsymbol, und wählen Sie die erforderliche Kompetenz aus. Nachdem Sie Ihre Auswahl abgeschlossen haben, klicken Sie erneut auf das Sperrsymbol. |
| Zuweisungsgruppe | Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird. |
| Zugewiesen an | Die Person, der die Aufgabe zugewiesen wurde. |
| Kurzbeschreibung | Eine Beschreibung der Aufgabe Security Incident Response. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beschreibung | Eine Beschreibung für die ausgewählte Aufgabe. |
| Sichere Notizen | Die Arbeitsnotizen, die verschlüsselt und für den Kunden nicht sichtbar sind. |
| Arbeitsnotizen | Die Arbeitsnotizen, die für den Kunden nicht sichtbar sind. |
| Zusätzliche Anmerkungen | Kommentare, die für den Kunden sichtbar sein sollen. |

5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

**Hinweis:**
Nachdem Sie Security Incident Response Aufgaben erstellt haben, können Sie sie mit einer der folgenden Anwendungen im Modul „ **Antwortaufgaben** “ anzeigen:

- **Mir zugewiesen**.
- **Dem Team zugewiesen**.
- **Offene Aufgaben anzeigen**
- **Alle Aufgaben anzeigen**
- **Nicht zugewiesene Aufgaben**.

## Verwalten Sie Predictive Intelligence für von Benutzern gemeldetes Phishing

Die Funktion „Predictive Intelligence for User Reported Phishing“ bietet eine wichtige Lösung für die Selektierung und Priorisierung von von Benutzern gemeldeten Phishing-E-Mails.

In diesem Abschnitt wird Folgendes beschrieben:

- Predictive Intelligence für Phishing-Meldungen von Anwendern
- Erforderliche Komponenten und Plugins
- Generierung des endgültigen Urteils für von Anwender gemeldetes Phishing
- Problembehandlung bei Predictive Intelligence für von Benutzern gemeldetes Phishing

### Predictive Intelligence für Phishing-Meldungen von Anwendern

Diese Funktion unterstützt Sicherheitsanalysten bei der Selektierung und Priorisierung von Phishing-E-Mails, die von Benutzern gemeldet wurden.

Das Predictive Intelligence-Framework bietet Lösungen, mit denen das System trainiert wird, um Datenergebnisse vorherzusagen, zu empfehlen und zu organisieren. Weitere Informationen zu Predictive Intelligence finden Sie unter Predictive Intelligence . Mit diesem Framework können Sie Modelle erstellen, um automatisch vorherzusagen, ob eine von einem Benutzer gemeldete Phishing-E-Mail verdächtig oder legitim ist.

Anhand von Verlaufsdaten zu anwendergemeldeten Phishing-Security-Incidents (E-Mail-Header, E-Mail-Text und Selektierungsergebnisse, die durch die Abschlusscodes für Security Incidents erfasst werden) können Sicherheitsanalysten das System trainieren, um die eingehenden anwendergemeldeten Phishing-Übermittlungen als solche zu klassifizieren, die weiter selektiert werden müssen (wahrscheinlich). verdächtig) und solche, bei denen es sich um zulässige Übermittlungen handelt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die automatische Selektierung eingehender E-Mails können Sicherheitsanalysten die Incident-Warteschlange einfach priorisieren und sich auf Incidents konzentrieren, die wahrscheinlich in erster Linie ein Risiko für die Organisation darstellen, und weniger Aufwand für E-Mails aufwenden, die sehr wahrscheinlich falsch positive Ergebnisse liefern. Das Vorhersageergebnis bietet auch eine Konfidenzpunktzahl für die Klassifizierung, um eine granulare Priorisierung zu ermöglichen.

## Erforderliche Komponenten und Plugins

Um Predictive Intelligence für von Benutzern gemeldetes Phishing zu verwenden, müssen Sie die folgenden Anwendungen installieren

| Plugin-Name | Mindestversion |
|---|---|
| Security Incident Response | 9.0.1 oder 10.0.2 |
| Predictive Intelligence | Orlando-Version |
| Predictive Intelligence für Phishing-Meldungen von Anwendern | 10.0.2 |

**Hinweis:**
Die folgenden neuen Erweiterungen sind mit Security Incident Response 10.4 verfügbar:

- Die Möglichkeit, Abschlusscodes aus benutzerdefinierten Feldern für das Modelltraining auszuwählen.
- Die Möglichkeit, Vorhersagen nach der Modellerstellung explizit zu aktivieren.
- Die Möglichkeit, mithilfe einer Entscheidungstabelle ein endgültiges Urteil über die Übermittlung von Phishing mit Benutzermeldung zu generieren. (erfordert Security Operations Spoke 10.3.0)

Um die neuen Erweiterungen zu verwenden, müssen Sie die folgenden Anwendungen aktualisieren:

| Plugin-Name | Führen Sie ein Upgrade auf durch |
|---|---|
| Security Incident Response | 10.0.4 |
| Predictive Intelligence für Phishing-Meldungen von Anwendern | 10.3.1 |

### Neue und aktualisierte Tabellen

- sn_sir_ml_urp_config (Neu): Enthält die Konfiguration für die URP ML-Anwendung.
- sn_sir_ml_urp_feature (Neu): Datensätze, die aus der E-Mail-Tabelle „sn_si_phishing“ extrahiert wurden.
- sn_sir_ml_urp_feature_import (Neu): Wird verwendet, um historische Phishing-E-Mail-Daten hochzuladen.
- sn_si_incident (aktualisiert): Die folgenden neuen Felder wurden hinzugefügt:
  - Vorhersage akzeptiert
  - Ergebnis der Vorhersage
  - Vertrauensbewertung
- **Skripteinbindungen**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- URPMLUtil: Ruft die Konfiguration ab, führt den Vorhersageauftrag aus und verfolgt den Vorhersageprozess.
- URPMLProcessor: Extrahiert und verarbeitet Daten aus der Tabelle sn_si_phishing_email
- URPMLAction: Führt einen Flow aus, um das Vorhersageergebnis zu akzeptieren.

## Generierung des endgültigen Urteils für von Anwender gemeldetes Phishing

Security Incident Response-Teams können jetzt das endgültige Urteil für einen von einem Benutzer gemeldeten Phishing-Datensatz basierend auf den Ergebnissen von Predictive Intelligence- und Bedrohungsanreicherungsintegrationen steuern.

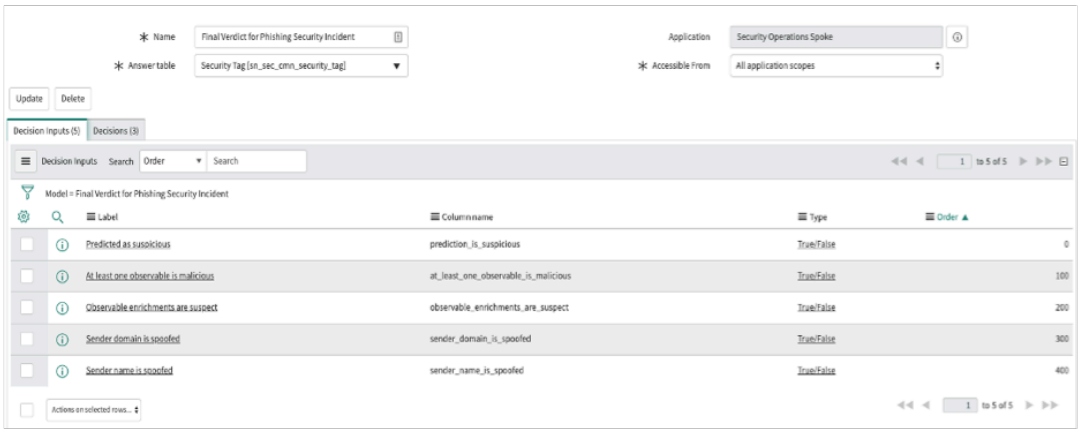
Die Generierung dieses endgültigen Urteils wird durch ein Entscheidungstabellenkonstrukt aktiviert und in einem Flow genutzt.

**Voraussetzungen**

Stellen Sie sicher, dass alle in Erforderliche Komponenten und Plugins aufgeführten Plugins installiert wurden.

Navigieren zu **Predictive Intelligence für Phishing** > **Endgültiges Urteil** > **Endgültiges Urteil für Phishing-Security Incident**.

Die Registerkarte **Entscheidungseingaben** zeigt die verschiedenen Bedingungen, die ausgewertet wurden, um zu dem endgültigen Urteil zu gelangen.




Die folgenden Bedingungen sind mit dem Basissystem verfügbar:

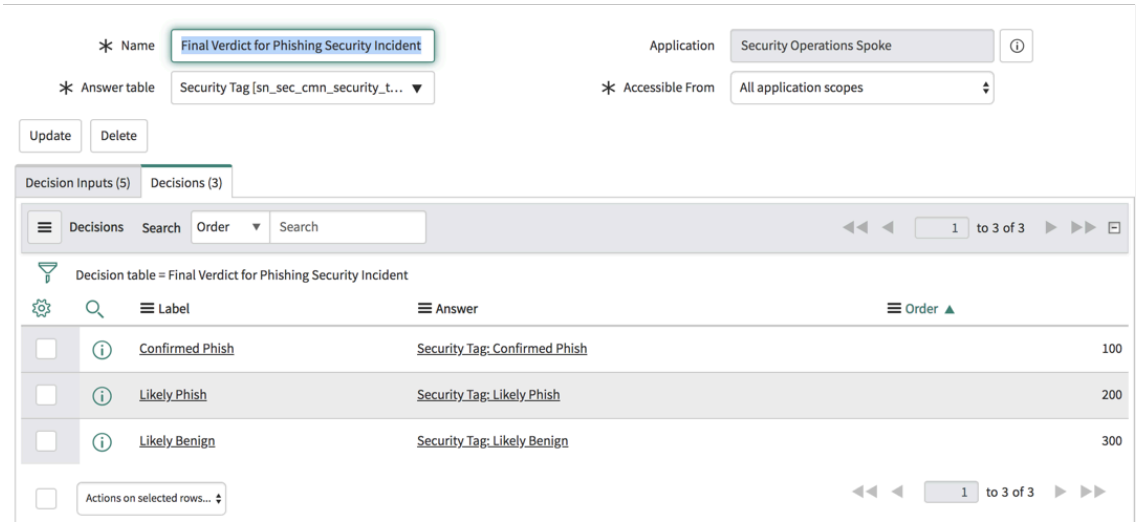
- Als verdächtig vorhergesagt: Wenn Predictive Intelligence die Phishing-E-Mail des Benutzers als **verdächtig**gemeldet hat.
- Mindestens ein erkennbares Element ist böswillig: Wenn ein an dem Security Incident beteiligtes erkennbares Element (z. B. URL, Domäne, IP, Hash) von Threat Intelligence-Quellen als **böswillig** klassifiziert wurde.
- Ergänzung erkennbarer Elemente ist verdächtig: Wenn die Ergänzung erkennbarer Elemente (z. B. Aktualität der Phishing-Domänenregistrierung, Land der Phishing-Domänenregistrierung) als verdächtig eingestuft wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Absenderdomäne ist gefälscht: Wenn der Verdacht besteht, dass die E-Mail-Domäne des Phishers eine vertrauenswürdige Domäne gefälscht hat.
- Absendername ist gefälscht: Wenn die E-Mail-Adresse des Phishers im Verdacht steht, einen vertrauenswürdigen Mitarbeiter einer Organisation gefälscht zu haben.

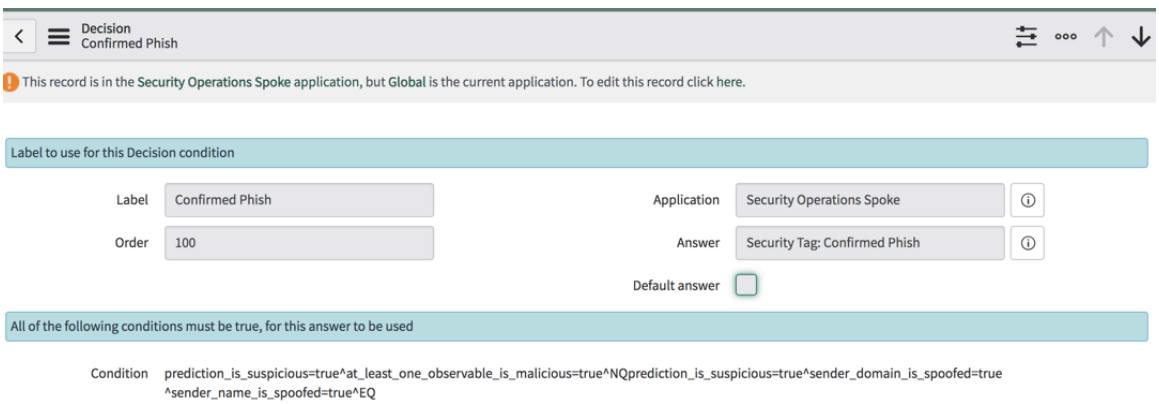
Die Registerkarte **Entscheidungen** zeigt die endgültigen Urteilsoptionen, die für einen bestimmten Security Incident getroffen werden können.




Die folgenden Entscheidungen sind mit dem Basissystem verfügbar:

- Bestätigtes Phishing: Wenn die Bedingungen zum endgültigen Urteil als bestätigte Phishing-E-Mail geführt haben.
- Wahrscheinlich Phishing: Wenn die Bedingungen zum endgültigen Urteil als potenziellen Phishing-Versuch geführt haben.
- Wahrscheinlich gutartig: Wenn die Bedingungen zum endgültigen Urteil als gutartige Übermittlung geführt haben.

Sie können die Bedingungen anzeigen, die für jede der endgültigen Urteilsoptionen ausgewertet wurden. Klicken Sie auf den Link Bezeichnung, um die Bedingungen anzuzeigen.




Sie können die mit dem Basissystem bereitgestellte Entscheidungstabelle anpassen oder eine eigene Entscheidungstabelle erstellen. Diese Entscheidungstabelle kann in Security Incident Response-Playbooks genutzt werden. Der **Subflow „Endgültiges Urteil für Phishing-**



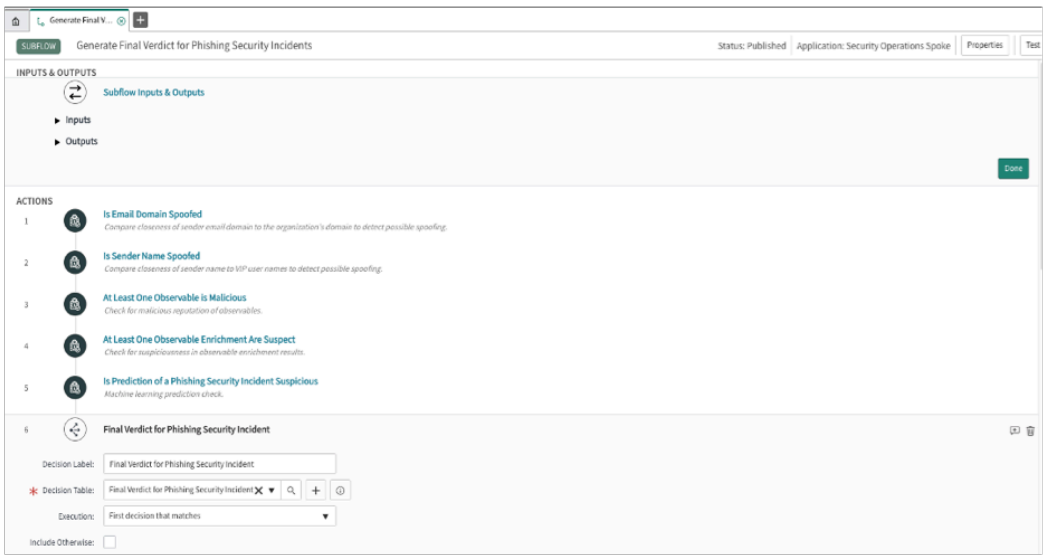
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incidents** generieren“ ist mit dem Basissystem verfügbar. Dieser Subflow generiert automatisch das endgültige Urteil für einen Phishing-Security Incident und wendet ein Sicherheits-Tag basierend auf dieser Entscheidung an. Sie können diesen Subflow als Teil des **Automated Phishing** -Playbooks einbeziehen.

Die Eingaben für diesen Subflow sind:

- incident_id: Die Sys-ID des Phishing-Security Incident
- c_level_names: Kommagetrennte Liste von Namen (z. B. Namen von Führungskräften in der Organisation), die beim Phishing-Angriff wahrscheinlich gefälscht wurden.
- Trusted_domains: Kommagetrennte Liste der vertrauenswürdigen E-Mail-Domänen.
- capability_keywords: Kommagetrennte Liste von Stichwörtern, die die Bösartigkeit des erkennbaren Elements aus den Anreicherungsergebnissen angeben.
- sender_email (optional): Die E-Mail-Adresse des Absenders der Phishing-E-Mail.

Die Ausgabe dieses Flows kann „ **Confirmed Phish**“, „ **Wahrscheinlich Phish**“ oder „ **Wahrscheinlich gutartig**“ sein.




## Problembehandlung bei Predictive Intelligence für von Benutzern gemeldetes Phishing

In diesem Abschnitt werden einige häufige Problemszenarien behandelt.

- Problem: Ich kann die Predictive Intelligence-Konfiguration nicht ändern.

  Lösung: Überprüfen Sie, ob Sie über die entsprechenden Berechtigungen verfügen. Sie müssen sich als Benutzer mit der Rolle ml_admin anmelden, um Schwellenwerte zu ändern. Einige Szenarien erfordern möglicherweise noch höhere Berechtigungen, z. B. müssen Sie das Trainingsdatenlimit ändern. In solchen Szenarien müssen Sie sich an den Kundensupport von wenden.

- Problem: Das Modelltraining ist fehlgeschlagen.

  Lösung: Überprüfen Sie, ob die URLs des ML-Planers eingerichtet wurden. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** und prüfen Sie, ob die Eigenschaft `glide.shared_service_scheduler.url` konfiguriert wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Problem: Vorhersageergebnisse sind für einen Security Incident nicht verfügbar.

  Lösung:

  - Überprüfen Sie, ob die Vorhersage-URL in der *Systemeigenschaft* `glide.prediction_service.url` eingerichtet wurde, und stellen Sie sicher, dass das Rechenzentrum mit der URL übereinstimmt.
  - Überprüfen Sie, ob die geplante Aufgabe „Anwender gemeldete Phishing-E-Mail vorhersagen“ aktiv ist.

## Konfigurieren Sie Predictive Intelligence für von Benutzern gemeldetes Phishing

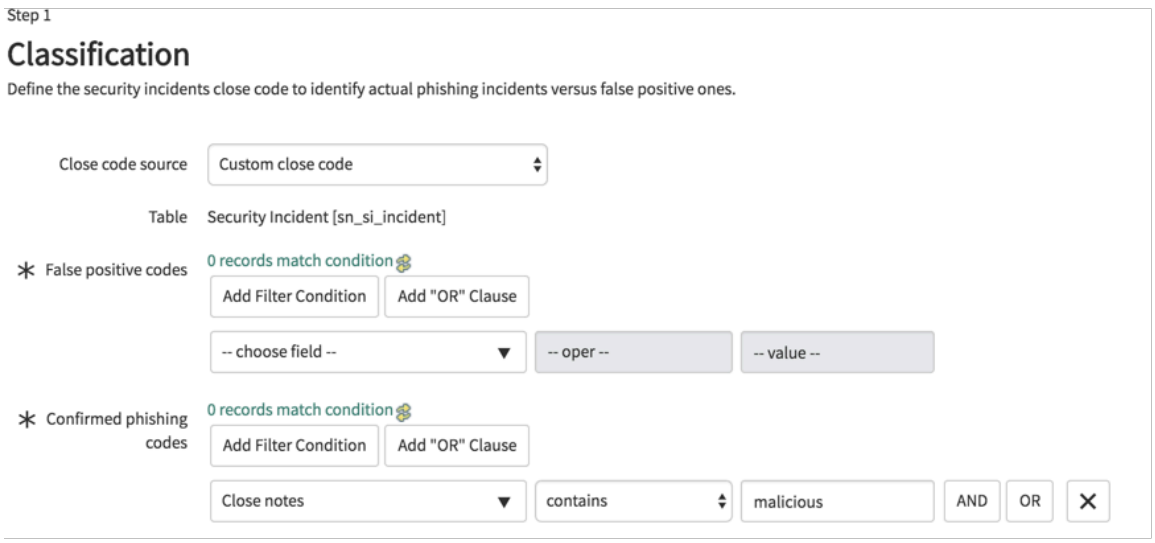
Konfigurieren und bereiten Sie das Modell vor, um von Benutzern gemeldete Phishing-E-Mails zu identifizieren.

### Vorbereitungen

Erforderliche Rolle: ml_admin

### Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence für Phishing** > **Konfiguration**.
2. Wählen Sie in Schritt 1 der Konfiguration eine der folgenden Optionen aus der Liste Abschlusscodequelle aus:
   - Standard-Abschlusscode: Wählen Sie diese Option aus, um die standardmäßigen Abschlusscodes für Security Incidents anzugeben, die vom Trainingsmodell verwendet werden müssen, um schädliche und legitime E-Mails zu identifizieren. Klicken Sie auf das Sperrsymbol, und wählen Sie einen oder mehrere Falsch positive Codes oder Bestätigte Phishing-Codes aus.
   - Benutzerdefinierter Abschlusscode: Wählen Sie die Option Benutzerdefinierter Abschlusscode aus, wenn Sie Abschlusscodes aus benutzerdefinierten Feldern definieren möchten, die als Teil Ihrer vorhandenen Incident-Antwortverfahren verwendet werden können. Um einen Abschlusscode zu definieren, wählen Sie ein Feld aus der Tabelle „Security Incident“ aus, und geben Sie eine oder mehrere Filterbedingungen an.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Importieren Sie in Schritt 2 Verlaufsdaten, die zum Trainieren des Modells verwendet werden können. Wählen Sie die Datenquelle für den Import der Verlaufsdaten aus. Dies kann sein:
   - Tabelle „Von Anwender gemeldete Phishing-E-Mail“: Sie können die Anzahl der Datensätze anzeigen, die als Verlaufsdaten importiert werden können. Wählen Sie diese Option aus, und klicken Sie auf **Importieren**.
   - Benutzerdefinierte Datenquelle: Sie können eine einzelne formatierte CSV-Datei anhängen, die Verlaufsdatensätze enthält. Wählen Sie die Datei aus, und klicken Sie auf **Importieren**.

   **Hinweis:**
   Die CSV-Datei, die Sie importieren, muss die folgenden Kopfzeilen enthalten:
   - Bezeichnung
   - Header
   - Haupttext

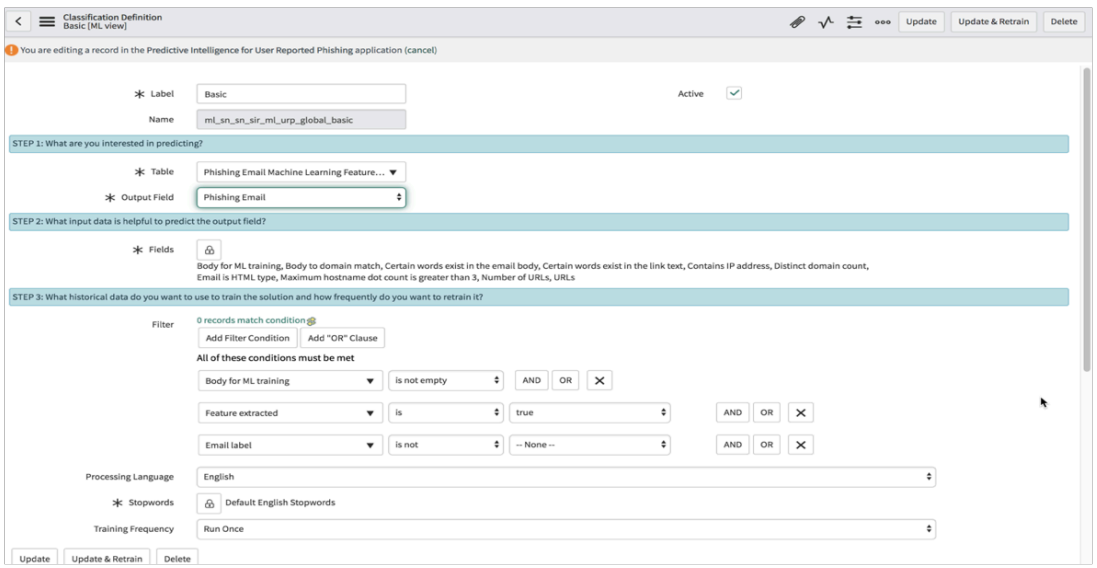
   Jeder Datensatz muss ein Tag „Böswillig“ oder „Legitim“ in der Spalte Bezeichnung in der CSV-Datei enthalten.

   Klicken Sie auf **Import abbrechen**, um den Import der Daten zu beenden. Der Importvorgang wird abgebrochen, und alle bisher importierten Datensätze werden gelöscht.

4. Nachdem Sie die Verlaufsdaten importiert haben, klicken Sie auf den Link, um die Seite zu aktualisieren. Sie können dann entweder weitere Trainingsdaten importieren oder mit dem nächsten Schritt fortfahren.
5. Überprüfen Sie in Schritt 3, ob die Anzahl der für das Training verfügbaren Datensätze die Mindestanforderungen an den Schwellenwert erfüllt.

   **Hinweis:**
   Die Standardwerte für die maximale und minimale Anzahl von Trainingsdatensätzen werden angezeigt. Diese Schwellenwerte können auf der Seite für maschinelles Lernen der Plattform geändert werden. Wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten.

6. Wenn die Trainingsdaten ausreichend sind, klicken Sie auf **Modell**trainieren.
   Sie können die Eingaben für das Training im folgenden Bildschirm aktualisieren.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Zu den Vorhersageeingaben, die Sie ändern können, gehören:
   - Was möchten Sie vorhersagen?
   - Welche Eingabedaten sind hilfreich, um das Ausgabefeld vorherzusagen?
   - Welche Verlaufsdaten möchten Sie zum Trainieren der Lösung verwenden, und wie häufig möchten Sie sie erneut trainieren?

   Die Standardwerte für diese Eingaben werden angezeigt. Sie können sie ändern und auf eine der folgenden Optionen klicken:
   - **Aktualisieren**: Aktualisiert die Definition des Schulungsmodells.
   - **Aktualisieren und neu trainieren**: Aktualisiert die Definition des Trainingsmodells und trainiert das Modell neu (löst die Funktion „ **Modell** trainieren“ aus).
8. Wenn Sie das Training des Modells abgeschlossen haben, klicken Sie auf das Kontrollkästchen **Vorhersage aktivieren**.
   Mit diesem Modell werden jetzt Vorhersagen für jeden von Benutzern gemeldeten Phishing-Datensatz bereitgestellt. Wenn Sie keine Vorhersagen für die von Benutzern gemeldeten Phishing-Datensätze mehr bereitstellen möchten, deaktivieren Sie das Kontrollkästchen **Vorhersage aktivieren**, und klicken Sie auf **Deaktivieren**.

## Zuweisen von Sicherheitsanalysten

Abhängig von Ihren Einstellungen im Bildschirm SIR „ Administrationskonfiguration“ können Sie Sicherheitsanalysten manuell zu Security Incidents zuweisen. automatisch mithilfe eines Workflows; oder automatisch mithilfe der automatischen Zuweisung.

### Manuelle Analystenzuweisung

Sie können den Bildschirm Security Incident Response Administrationskonfiguration so konfigurieren, dass Sicherheitsanalysten manuell zugewiesen werden müssen, wenn jemand oder die Anwendung SIR einen Security Incident erstellt oder eine Sicherheitsreaktionsaufgabe generiert.

Wenn ein Security Incident oder eine Antwortaufgabe nicht automatisch zugewiesen werden kann, können Sie den Bildschirm SIR Administrationskonfiguration so einstellen, dass die manuelle Zuweisung von Sicherheitsanalysten erforderlich ist. Dies ist eine gute Wahl, wenn Sie eine begrenzte Anzahl von Sicherheitsanalysten für die Bearbeitung von Anforderungen haben oder diese einfach nicht automatisch zuweisen möchten.

### Workflow-basierte Zuweisung von Sicherheitsanalysten

Sie können den Bildschirm Security Incident Response Administrationskonfiguration so konfigurieren, dass ein ausgewählter Workflow zur Zuweisung des Sicherheitsanalysten verwendet wird, wenn jemand oder die SIR-Anwendung einen Security Incident oder eine Sicherheitsreaktionsaufgabe erstellt.

Im Konfigurationsbildschirm „Security Incident Administration“ können Sie einen Workflow verwenden, um jedem Security Incident oder jeder Sicherheitsreaktionsaufgabe einen Analysten zuzuweisen. Diese Option ist eine gute Wahl für Organisationen, die einen benutzerdefinierten Prozess zur Lösung von Sicherheitsproblemen verwenden oder anderweitig über einen automatisierbaren Prozess verfügen.

### Automatische Zuweisung von Sicherheitsanalysten

Sie können den Bildschirm Security Incident Response „ Administrationskonfiguration“ so konfigurieren, dass der Sicherheitsanalyst automatisch zugewiesen wird, wenn jemand



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder die Anwendung SIR einen Security Incident oder eine Sicherheitsreaktionsaufgabe erstellt. Mit der automatischen Zuweisung können Sie basierend auf den Anforderungen Ihrer Organisation die Kriterien definieren, nach denen Analysten automatisch Security Incidents zugewiesen werden.

## Automatische Zuweisung von Service Desk-Mitarbeitern basierend auf Service Desk-Mitarbeiter-Bewertungen

Wenn die automatische Zuweisung aktiviert ist und ein Security Incident oder eine Antwortaufgabe erstellt wird, werden die folgenden Aktionen ausgeführt:

- Die verfügbaren Sicherheitsanalysten werden basierend auf den in der Konfiguration definierten Kriterien ausgewertet.
- Ein geeigneter Sicherheitsanalyst wird automatisch der Aufgabe zugewiesen.
- Die Aufgabe wird in den Status **Zugewiesen** versetzt.

Wenn die Konfiguration so eingerichtet ist, dass mehr als ein Satz von Bedingungen berücksichtigt wird, z. B. Kompetenzen, Standort, Zeitzone oder Gruppenabdeckungsbereich, werden die Sicherheitsanalysten basierend auf den Einstellungen der Gewichtungseigenschaft und anderen Kriterien ausgewertet. Diese Konfigurationseinstellungen helfen Ihnen bei der automatischen Zuweisung von Service Desk-Mitarbeitern basierend auf optionalen Eigenschaften. Die berechneten Bewertungen werden verwendet, um den besten Service Desk-Mitarbeiter für den Security Incident oder die Reaktionsaufgabe zu bestimmen. Jede Kombination von bewertungsbasierten Methoden kann im Konfigurationsbildschirm der Anwendung aktiviert werden.

Beim Erstellen einer Aufgabe wird eine Bewertung für jeden Typ der aktivierten Auswahlkriterien für alle verfügbaren Außendienstmitarbeiter berechnet. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die automatische Zuweisung berücksichtigt.

Die Einstellungen für die Gewichtungseigenschaften der automatischen Zuweisung finden Sie in **Security Incident** > **Administration** > **Eigenschaften**, sind in den Bewertungsberechnungen enthalten.

Mit diesen Werten können Sie Prioritäten für die Auswahlkriterien für die automatische Zuweisung festlegen, die für Ihre Organisation wichtiger sind. Legen Sie die Prioritätswerte zwischen 1 (weniger wichtig) und 10 (wichtig) fest.

Ein Beispiel dafür, wie sich die Gewichtungseigenschaften auf die Bewertungen der Außendienstmitarbeiter auswirken, finden Sie unter Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

## Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts

Service Desk-Mitarbeiter können basierend auf dem Heimatstandort in ihrem Benutzerdatensatz und dem Standort der Aufgaben automatisch zugewiesen werden.

Die automatische Zuweisung nach Standort wird durchgeführt, wenn die **Konfigurationsoption Bei der automatischen Auswahl von Agenten wird deren Standort berücksichtigt** aktiviert ist.

Wenn eine Aufgabe (Security Incident oder Reaktionsaufgabe) erstellt wird, wird der Agent, der dem Aufgabenstandort am nächsten ist, für die Aufgabe berücksichtigt. Wenn die Anwendung so konfiguriert ist, dass nur der Standort berücksichtigt wird, wird die Aufgabe automatisch dem nächstgelegenen Service Desk-Mitarbeiter zugewiesen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Aufgabe erstellt wird, werden die Standorte von Service Desk-Mitarbeitern mit den folgenden Bereichen verglichen, um die Bewertungen der einzelnen Standorte von Service Desk-Mitarbeitern zu bestimmen.

**Berechnung der Standortberechnung**

| Entfernung (km) vom Außendienstmitarbeiter zur Aufgabe | Bewertung |
|---|---|
| 0 bis 0,1 | 1 |
| 0,11 bis 0,5 | 0,9 |
| 0,51 bis 5 | 0,7 |
| 5,1 bis 10 | 0,5 |
| 10,1 bis 20 | 0,4 |
| 20,1 bis 30 | 0,3 |
| 30,1 bis 40 | 0,2 |
| 40,1 bis 100 | 0,1 |
| >100 | 0 |

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien konfiguriert ist, z. B. Kompetenzen, Zeitzone oder Zeitplan, werden die Bewertungen aller Auswahlkriterien gewichtet und zusammengefasst. Der Agent mit der höchsten Gesamtbewertung wird automatisch der Aufgabe zugewiesen. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

## Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Kompetenzen

Service Desk-Mitarbeiter können basierend auf ihren Kompetenzen und den für die Ausführung der Aufgabe erforderlichen Kompetenzen automatisch zugewiesen werden. Fähigkeiten ihren Benutzerdatensätzen mit zuweisen **Kompetenzen** > **Anwender**.

Die automatische Zuweisung nach Kompetenzen kann durchgeführt werden, wenn die Konfigurationsoption Bei der **automatischen Auswahl von Agenten für Aufgaben müssen Kompetenzen** vorhanden sein auf **alle** oder **einige**festgelegt ist.

Wenn eine Aufgabe, die Kompetenzen enthält, automatisch zugewiesen wird, werden die Kompetenzen eines Service Desk-Mitarbeiters mit den für die Ausführung der Aufgabe erforderlichen Kompetenzen verglichen. Eine Bewertung wird basierend auf der Konfigurationsoption für Kompetenzen berechnet. Wenn die Option auf **einige** festgelegt ist, wird der Außendienstmitarbeiter mit der besten Übereinstimmung der Fähigkeiten der Aufgabe automatisch zugewiesen. Wenn die Option auf **alle** festgelegt ist, werden nur Außendienstmitarbeiter berücksichtigt, die alle erforderlichen Fähigkeiten besitzen. Wenn keiner der Service Desk-Mitarbeiter alle für die Ausführung der Aufgabe erforderlichen Kompetenzen besitzt, wird niemand automatisch zugewiesen.

Eine Kompetenzbewertung wird wie folgt berechnet:

Skills_agent/Skills_task

Wobei:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Skills_agent die Anzahl der Fähigkeiten des Außendienstmitarbeiters ist, die den für die Aufgabe erforderlichen Fähigkeiten entsprechen.
- Skills_task die Gesamtanzahl der für die Aufgabe erforderlichen Fähigkeiten ist.

Wenn eine Aufgabe beispielsweise vier Fähigkeiten erfordert und Außendienstmitarbeiter A drei davon und Außendienstmitarbeiter B zwei davon besitzt, dann ist die:

- Kompetenzbewertung Agent A = 3/4 oder 0,75
- Kompetenzbewertung von Service Desk-Mitarbeiter B = 2/4 oder 0,5

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien konfiguriert ist, z. B. Standort oder Zeitzone, werden die Bewertungen aller Auswahlkriterien gewichtet und zusammengefasst. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

## Automatische Zuweisung von Service Desk-Mitarbeitern anhand von Zeitzonen

Service Desk-Mitarbeiter können basierend auf der in ihren Benutzerdatensätzen definierten Zeitzone und der Zeitzone der Aufgaben automatisch zugewiesen werden.

Wenn die Option Bei der **automatischen Auswahl von Agenten wird die Zeitzone für die Aufgabenkonfiguration berücksichtigt** aktiviert ist, kann die automatische Zuweisung nach Zeitzone durchgeführt werden.

Wenn eine Aufgabe erstellt wird, werden Mitarbeiter in der Zeitzone, die der Zeitzone der Aufgabe am nächsten liegt, für die Aufgabe berücksichtigt. Wenn die Anwendung so konfiguriert ist, dass nur die Zeitzone berücksichtigt wird, kann nur einem Service Desk-Mitarbeiter in derselben Zeitzone die Aufgabe automatisch zugewiesen werden.

**Hinweis:**
Es ist wichtig, dass die Zeitzonen für den Service Desk-Mitarbeiter und die Aufgabe richtig eingestellt sind.

Wenn eine Aufgabe erstellt wird, werden die Service Desk-Mitarbeiter basierend auf der Zeitzone der Aufgabe und der Zeitzone des Service Desk-Mitarbeiters anhand der folgenden Formel bewertet:

1 - [abs(Task_tz – Agent_tz) ÷ 12]

wobei:

- abs die mathematische Funktion ist, um den absoluten Wert zu berechnen.
- Task_tz der Versatz zwischen der Zeitzone der Aufgabe und GMT ist.
- Agent_tz der Versatz zwischen der Zeitzone des Außendienstmitarbeiters und GMT ist.

Beispielsweise wird eine Aufgabe in New York City (GMT-4) erstellt, und zwei Außendienstmitarbeiter stehen zur Verfügung, um die Aufgabe auszuführen, einer in Los Angeles (GMT-7) und einer in Paris, Frankreich (GMT + 1).

Die Bewertung des Außendienstmitarbeiters in Los Angeles wird wie folgt berechnet:

1 - abs((-4) - (-7)) ÷ 12 oder 0,75

Die Bewertung des Außendienstmitarbeiters in Paris wird wie folgt berechnet:

1 - abs((-4) - (+1)) ÷ 12 oder 0,58



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die automatische Zuweisung der Aufgabe nur auf der Zeitzone basiert, wird sie dem Mitarbeiter aus Los Angeles zugewiesen.

Wenn die Anwendung für die Verwendung anderer Auswahlkriterien konfiguriert ist, z. B. Kompetenzen oder Standort, werden die Bewertungen aller Auswahlkriterien gewichtet und summiert. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

## Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Gruppenabdeckungsgebieten

Service Desk-Mitarbeiter können basierend auf dem in ihren Benutzerdatensätzen definierten Gruppenabdeckungsbereich automatisch zugewiesen werden.

## Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien

Wenn eine Aufgabe erstellt wird, werden die Bewertungen der Service Desk-Mitarbeiter berechnet. Weitere Informationen finden Sie unter:

- Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts
- Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Kompetenzen
- Automatische Zuweisung von Service Desk-Mitarbeitern anhand von Zeitzonen

Die automatische Zuweisung basiert auf der folgenden Berechnung:

(Criteria_1-Bewertung x Criteria_1-Gewichtung) + (Criteria_2-Bewertung x Criteria_2-Gewichtung) + (Criteria_3-Bewertung x Criteria_3-Gewichtung) / Anzahl der verwendeten Kriterientypen, wobei:

Anzahl der verwendeten Kriteriumtypen = 1, 2 oder 3, abhängig von den verwendeten Einstellungen für Standort, Fähigkeiten und Zeitzone.

In diesem Beispiel wird die automatische Zuweisung von Außendienstmitarbeitern basierend auf Standort und Fähigkeiten berechnet. Das Beispiel basiert auf folgenden Annahmen.

- Die Konfigurationsoption **Bei der automatischen Auswahl von Agenten wird deren Standort berücksichtigt** ist für die Anwendung aktiviert.
- Die Konfigurationsoption **Für die automatische Auswahl von Agenten für Aufgaben müssen Fähigkeiten von Agenten vorhanden sein** ist für die Anwendung aktiviert.
- Die Eigenschaft **Gewichtung der Fertigkeit** ist für die Anwendung auf 10 festgelegt.
- Die Eigenschaft **Standortgewichtung** ist für die Anwendung auf 5 festgelegt.
- Außendienstmitarbeiter A und B stehen zur Verfügung, um eine Aufgabe auszuführen, und die Aufgabe erfordert vier spezifische Fähigkeiten.
- Service Desk-Mitarbeiter A befindet sich 5 km vom Standort der Aufgabe entfernt und verfügt über drei der vier erforderlichen Fähigkeiten.
- Der Standort von Service Desk-Mitarbeiter B befindet sich 0,25 km vom Standort entfernt und verfügt über zwei der erforderlichen Fähigkeiten.

Bei der automatischen Zuweisung für die Service Desk-Mitarbeiter wird folgende Berechnung verwendet: [(Standortbewertung x Standortgewichtung) + (Kompetenzbewertung x Kompetenzgewichtung)]/ 2



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Berechnung der automatischen Zuweisung für Service Desk-Mitarbeiter A lautet: [(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55
- Die Berechnung der automatischen Zuweisung für Agent B lautet: [(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475

In diesem Beispiel wird Agent A die Aufgabe automatisch zugewiesen.

## Verwaltung von Security Incidents und eingehenden Anforderungen

Nachdem ein Security Incident erstellt wurde, gibt es zahlreiche Arten von Informationen, die hinzugefügt und angezeigt werden können, während die Analyse des Problems in Richtung einer Lösung voranschreitet.

In diesem Abschnitt wird Folgendes beschrieben:

- Erstellen Sie eine eingehende Anforderung
- Erkennbare Elemente verwalten
- Verwalten Sie Suchen und Scans
- on-Demand-Orchestrationverwalten
- Berechnen Sie den Schweregrad eines Security Incident
- Verwalten von Aktivitäten nach Incidents
- Schließen Sie Security Incidents

### Erstellen Sie eine eingehende Anforderung

Im Gegensatz zu Security Incidents haben eingehende Anforderungen im Allgemeinen eine niedrigere Priorität. Anforderungen für eine Suche, einen Scan oder ein neues Abzeichen sind Beispiele für eingehende Anforderungen.

#### Vorbereitungen

Erforderliche Rollen: Rolle sn_si.basic oder höher

#### Prozedur

1. Navigieren Sie zu einem der Anforderungsformulare.
   Beispiel: **Alle** > **Security Incident** > **Eingehende Anfragen** > **Mir zugewiesen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Sicherheitsanforderung**

| Feld | Beschreibung |
|---|---|
| Nummer | [Nur Lesen] Die automatisch generierte Sicherheitsanforderungsnummer. |
| Unternehmen | Das anfordernde Unternehmen. |
| Standort | Der CI-Speicherort, falls zutreffend. Dieses Feld wird vorausgefüllt, wenn das CI ausgewählt wird. |
| Konfigurationselement | Das von der Anforderung betroffene Konfigurationselement. |
| Priorität | Die Priorität der Anforderung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Geöffnet | [Schreibgeschützt] Datum und Uhrzeit des Öffnens der Anforderung. |
| Status | Aktueller Status der Sicherheitsanforderung. Nach der Erstellung der Sicherheitsanforderung wird dieses Feld standardmäßig auf **Entwurf**gesetzt. |
| Zuweisungsgruppe | Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird. |
| Zugewiesen an | Die Person, der die Arbeit zugewiesen wurde. |
| Kurzbeschreibung | Eine kurze Beschreibung der Sicherheitsanforderung, die für die anfordernde Person sichtbar ist. |
| Beschreibung | Die vollständige Beschreibung der Anforderung, die für die anfordernde Person sichtbar ist. |
| Arbeitsnotizen | Arbeitsnotizen, die für die anfordernde Person sichtbar sind. |

4. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.
5. Wenn Sie die Anforderung zu einem Security Incident eskalieren müssen, klicken Sie **auf In Security Incident konvertieren**.

## Erkennbare Elemente verwalten

Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hinweisen. Typische erkennbare Elemente sind IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. Threat Intelligence Tabellendaten für erkennbare Elemente sind innerhalb eines Security Incidents verfügbar.

Zu den Informationen zu erkennbaren Elementen gehören Wert, Typ, Kontext und Zeitstempel.

Sie können erkennbare Elemente manuell oder automatisch über Suchanforderungen erstellen oder löschen.

Der Registerkarte „ **Ergebnisse der Bedrohungssuche** “ wurde eine neue **Spalte** „Ergebnis“ hinzugefügt. Mögliche Werte sind: Böswillig und Unbekannt.

Wenn eine IoC-Suchanforderung kein erkennbares Element eines Security Incident findet, wird es als Unbekannt gekennzeichnet.

Wenn eine IoC-Suchanforderung ein erkennbares Element eines Security Incident findet, wird es als böswillig gekennzeichnet.

Während eines Upgrades wird die Spalte „Ergebnis“ für vorhandene Elemente auf **Böswillig** festgelegt.

**Hinweis:**
Während die Tabellendaten für erkennbare Elemente Threat Intelligence Teil eines Security Incident sind, ist keine andere Interaktion mit dem Modul Threat Intelligence enthalten. Für die vollständige Bedrohungsfunktionalität ist das Plugin Threat Intelligence im Abonnement verfügbar.

**Zugehörige Informationen**

Erstellen Sie ein erkennbares Security Incident-Element



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie IoC-Informationen für einen Security Incident an

Sie können IoC-Informationen anzeigen, z. B. erkennbare Elemente und Sichtungssuchergebnisse, die einem Security Incident zugeordnet sind.

## Vorbereitungen

Erforderliche Rolle: sn_si.basic

## Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie IoC-bezogene Informationen anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

| Registerkarte | Beschreibung |
|---|---|
| Erkennbare Elemente | Zeigen Sie erkennbare Elemente an, die dem Security Incident zugeordnet sind, oder fügen Sie sie manuell hinzu oder bearbeiten Sie sie. Weitere Informationen finden Sie unter Erkennbare Elemente verwalten. |
| Zugeordnete Indikatoren | Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Indikatoren anzeigen, die denselben Bedrohungsdatensätzen zugeordnet sind. |
| Ergebnisse von Sightings Search | Enthält Sichtungssuchergebnisse. |
| Details einer Sichtungssuche | Enthält Datensatzdetails der Sichtungssuche |
| Bedrohungssuchen | Speichert Ergänzungsdaten aus Malware-Erkennungssystemen. Diese Registerkarte wird nur angezeigt, wenn das Plugin Threat Intelligence installiert ist. |
| Zugehörige Angriffsmodi/-methoden | Wenn Threat Intelligence aktiviert ist, können Sie alle anderen Angriffstypen anzeigen, die denselben Bedrohungsdatensätzen zugeordnet sind. |
| Anforderungen für Sicherheitsprüfung | Wenn Threat Intelligence aktiviert ist, können Sie Scan- und Suchanforderungen anzeigen, die an den Security Incident angehängt sind. |
| Ressourcen mit ähnlichem IoC | Wenn Threat Intelligence aktiviert ist, können Sie andere Ressourcen mit ähnlichen Indikatoren anzeigen. |
| Anwender mit ähnlichem IoC | Wenn Threat Intelligence aktiviert ist, können Sie andere Benutzer mit ähnlichen Indikatoren anzeigen. |

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie ein erkennbares Security Incident-Element

Sie können ein erkennbares Element innerhalb eines Security Incident erstellen und anzeigen und entsprechende Maßnahmen ergreifen. Die Verfügbarkeit von erkennbaren Elementen im Security Incident ist skalierbar und reduziert die Antwortzeit.

#### Vorbereitungen

Erforderliche Rolle:

- sn_ti_observable.write (schreiben)
- sn_ti_observable.read (read)
- sn_ti_observable.admin (löschen)

#### Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf die Registerkarte Erkennbare **Security Incident-Elemente der** zugehörigen Liste.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Klassifizierungs-Tag auswählen | Wenn Sie Sicherheits-Tags eingerichtet und aktiviert haben, um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des erkennbaren Elements anzugeben.<br>Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt. |
| Wert | Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.<br>**Hinweis:**<br>Wenn ein Bedrohungsscan für eine IP-Adresse oder einen Hash, Malware oder einen anderen Fehler zurückgibt, wird die IP-Adresse oder der Hash-Wert automatisch der Tabelle „Erkennbares Element“ [sn_ti_observable] hinzugefügt. Daher kann im Formular „Erkennbare Elemente“ gesucht werden. |
| Erkennbarer Typ | Wählen Sie die Klassifizierung des erkennbaren Elements aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese erkennbaren Typen werden im Modul **„Erkennbare Typen** “ definiert. |
| Incident-Anzahl | Die Häufigkeit, in der der Wert des erkennbaren Elements gefunden wurde. |
| Ist Zusammensetzung | Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde.<br>Wenn der **erkennbare Typ** auf einen anderen **Wert als die Zusammensetzung**des erkennbaren Elements festgelegt ist und dieses neue erkennbare Element eine Zusammensetzung ist, aktivieren Sie dieses Kontrollkästchen.<br>Wenn der **erkennbare Typ** bereits auf **Zusammensetzung**des erkennbaren Elements festgelegt ist, ist das Kontrollkästchen aktiviert und schreibgeschützt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Eine erkennbare Zusammensetzung ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält. |
| Ergebnis | Wählen Sie eine der folgenden Optionen aus:<br>○ **Böswillig**: Gibt an, dass das erkennbare Element für die Organisation schädlich ist.<br>○ **Verdächtig**: Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte.<br>○ **Bereinigen**: Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist.<br>○ **Unbekannt**: Gibt an, dass das Ergebnis des erkennbaren Elements noch nicht bestimmt wurde.<br>○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche.<br>**Hinweis:** Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert. |
| Operator | Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Ist Zusammensetzung** aktiviert ist. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren Elemente und ihre untergeordneten Elemente berücksichtigt, wenn entschieden wird, ob ein zugeordneter Indikator vorhanden ist.<br>Legen Sie dieses Feld auf **UND fest**, wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugeordneter Indikator als vorhanden betrachtet wird.<br>Legen Sie die Option auf **OR fest**, wenn eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugeordneter Indikator als vorhanden betrachtet wird. |
| Muss nicht vorhanden sein | Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde.<br>Wenn diese Option ausgewählt ist, bedeutet dies, dass das Fehlen des erkennbaren Elements das potenzielle Problem ist (z. B. ein fehlender Registrierungsschlüssel). |
| Standort | Mit den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Laden Sie weitere IoC-Daten in dieses Feld laden. |
| Notizen | Geben Sie zusätzliche Notizen zum erkennbaren Element ein. |

6. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**. Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

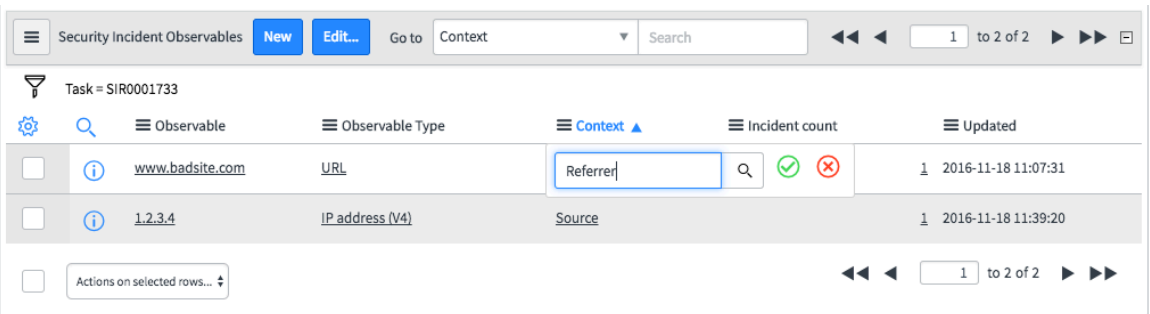


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Liste | Beschreibung |
|---|---|
| Zugehörige Indikatoren | Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden. |
| Zugehörige Aufgaben | Listet Änderungen auf, die dem erkennbaren Element zugeordnet sind. |
| Untergeordnete erkennbare Elemente | Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden. |
| Übereinstimmende Ressourcen für IP | Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen. |
| Quelle erkennbare Elemente | Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf. |
| Sicherheitsanmerkungen | Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden. |

**7.** Kehren wir zum Security Incident zurück: Folgende Informationen sind verfügbar.

**Hinweis:**
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Configuration Items oder Benutzern, die ihm zugeordnet sind. Die Registerkarten **Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert.




| Spalte | Definition |
|---|---|
| Erkennbares Element | Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. |
| Erkennbarer Typ | Spezifischer Typ des erkennbaren Elements. |
| Kontext | Vom Benutzer ausgewählt. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ IP: Quelle oder Ziel<br>**Hinweis:**<br>Wenn Threat Intelligence und Palo Alto Networks – Firewall aktiviert sind, führt das Ändern oder Hinzufügen eines Werts zu diesem Feld dazu, dass der Workflow „ Workflow „Protokolldaten abrufen“. Security Operations Palo Alto Networks - Protokolldaten abrufen“ ausgeführt wird. Der Workflow ruft angereicherte Bedrohungsprotokolldaten von der Firewall ab und hängt sie an den Security Incident an. Die Informationen werden auch analysiert und im Abschnitt „ Firewall-Protokolle “ auf der **Registerkarte** „Ergänzungsdaten“ angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Spalte | Definition |
|---|---|
| | ○ URL: Referrer<br><br>**Hinweis:**<br>Wenn der Benutzer auf einen Link in einer Phishing-E-Mail klickt, ist ein Referrer die URL des letzten Jumps, bevor auf die Malware-URL zugegriffen wird. |
| Incident-Anzahl | Die Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow zu einem anderen Incident hinzugefügt wird. |
| Aktualisiert | Datum und Uhrzeit der letzten Aktualisierung der Liste. |

**Hinweis:**
Wenn das Plugin Threat Intelligence installiert ist, können Sie das erkennbare Element auch in der Liste „Erkennbare Elemente“ im **IoC-Repository**anzeigen.

**Zugehörige Informationen**

Bearbeiten Sie eine Liste erkennbarer Security Incidents

Fügen Sie mehrere erkennbare Security Incident-Elementehinzu

### Erkennbare Dateielemente verwalten

„Erkennbare Dateielemente verwalten“ bietet strenge Sicherheitsmaßnahmen zum Speichern verdächtiger Dateien und aktiviert die erkennbaren Dateitypen für die Sandbox-Integration.

### Vorbereitungen

Erforderliche Rolle: sn_ti_malicious_attachment_access (upload)

Laden Sie die erkennbaren Elemente des Dateityps hoch:

- Automatisch: Wenn die Security Incidents für die Phishing-E-Mails erstellt werden, werden die Anhänge in der Phishing-E-Mail als erkennbare Elemente des Dateityps erstellt.
- Manuell: Ein Sicherheitsanalyst kann die verdächtigen Dateien auch hochladen, um erkennbare Elemente des Dateityps zu erstellen.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können erkennbare Dateitypen für einen Security Incident erstellen und anzeigen. Die verdächtigen Dateien, die Teil der erkennbaren Elemente sind, werden an einem bestimmten Speicherort gespeichert, auf den der Sicherheitsanalyst zugreifen kann, um die Datei nur mit einer bestimmten Rolle herunterzuladen.

### Prozedur

1. Navigieren Sie zu einem Security Incident.
2. **Wählen** Sie auf der Registerkarte **Alle zugehörigen Listen** anzeigen die Option Erkennbare Elemente aus.

   Wenn die Phishing-E-Mail Anhänge enthält, werden diese Anhänge standardmäßig als erkennbare Elemente des Dateityps im entsprechenden Security Incident erstellt. Jeder

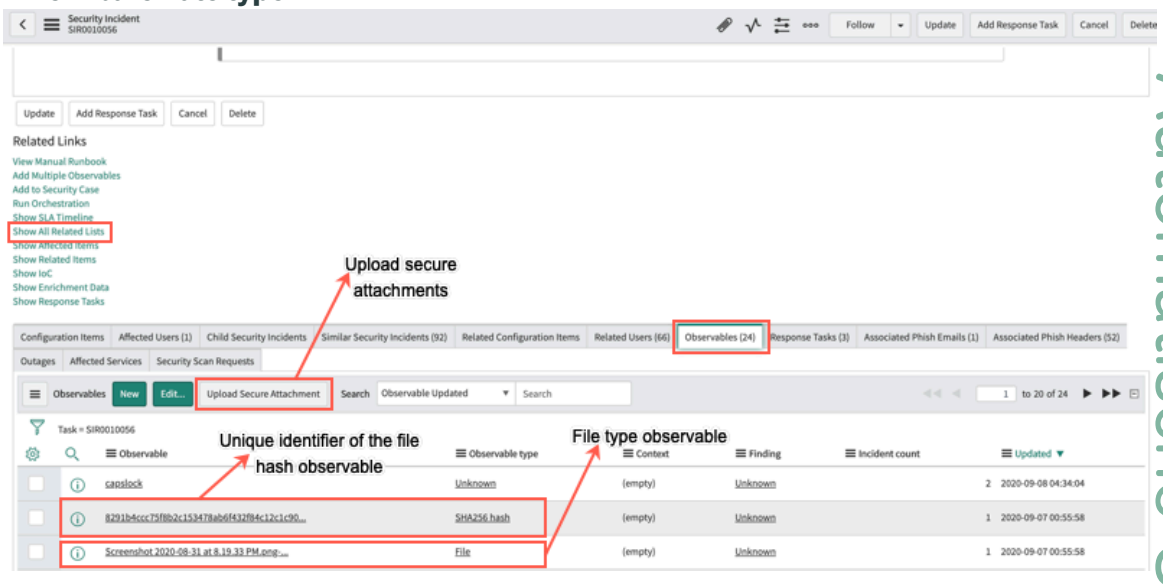


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anhang wird als zwei erkennbare Elemente erstellt, z. B. Dateityp und erkennbares Datei-Hash-Element.

3. So laden Sie die sicheren Anhänge manuell hoch:
   - Klicken Sie **auf Sicheren Anhang hochladen**.
   - Klicken Sie beim Hochladen sicherer Anhänge auf **Datei auswählen**, um eine oder mehrere Dateien hochzuladen. Jede Datei wird als einzelner erkennbarer Datensatz betrachtet.
   - Klicken Sie auf **Erkennbare Dateielemente** erstellen, um die erkennbaren Dateitypen zu erstellen, z. B. den Dateityp und den Datei-Hash, der ein eindeutiger Bezeichner ist.

**Erkennbare Dateitypen**




Wählen Sie den erkennbaren Dateityp aus, der für weitere Integrationen wie Sandbox, Bedrohungssuche verarbeitet werden soll. Darüber hinaus können Sie die Anhänge auch aus dem erkennbaren Dateityp herunterladen.

**Hinweis:**

Die Bedrohungssuche (VirusTotal) ruft die Datei aus den gesicherten Anhängen für die erkennbaren Elemente des neuen Dateityps ab, und die folgenden Systemeigenschaften gelten nicht für die erkennbaren Elemente des neuen Dateityps.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Zur Schnellreferenz: Der erkennbare Dateityp wird dem erkennbaren Hash-Element als untergeordnetes Element zugeordnet, und das erkennbare Hash-Element wird dem erkennbaren Dateielement als untergeordnetes Element zugeordnet.

Wenn die Phishing-E-Mail-Anhänge die definierte Größe überschreiten, werden die erkennbaren Elemente nicht erstellt. Sie müssen die Systemeigenschaften ändern, um die größeren Dateien zu unterstützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Systemeigenschaften der Dateigröße

| Systemeigenschaft | Beschreibung |
|---|---|
| glide.email.inbound.max_total_attachment_size_bytes | Wenn Sie die Phishing-E-Mail direkt weiterleiten, verwenden Sie diesen Systemeigenschaftenwert, um die Dateigröße von 18 MB auf die gewünschte Dateigröße zu erhöhen. |
| com.glide.attachment.max_get_size | Wenn Sie die Phishing-E-Mail als Anhang weiterleiten, verwenden Sie diesen Systemeigenschaftswert, um die folgenden Systemeigenschaften im globalen Bereich zu erstellen und die Dateigröße von 5 MB auf die gewünschte Größe zu erhöhen. |

Sie können auch wie folgt einen neuen erkennbaren Dateityp erstellen:

**a.** Klicken Sie auf **Neu**.

**b.** Wählen Sie als **Typ des erkennbaren Elements Kategorie: Datei aus**

**c.** Klicken Sie auf **Hochladen**, um eine Datei anzuhängen.

### Bearbeiten Sie eine Liste erkennbarer Security Incidents

Sie können bearbeiten, welche erkennbaren Elemente in der Liste einem Security Incident zugeordnet sind und angezeigt werden sollen.

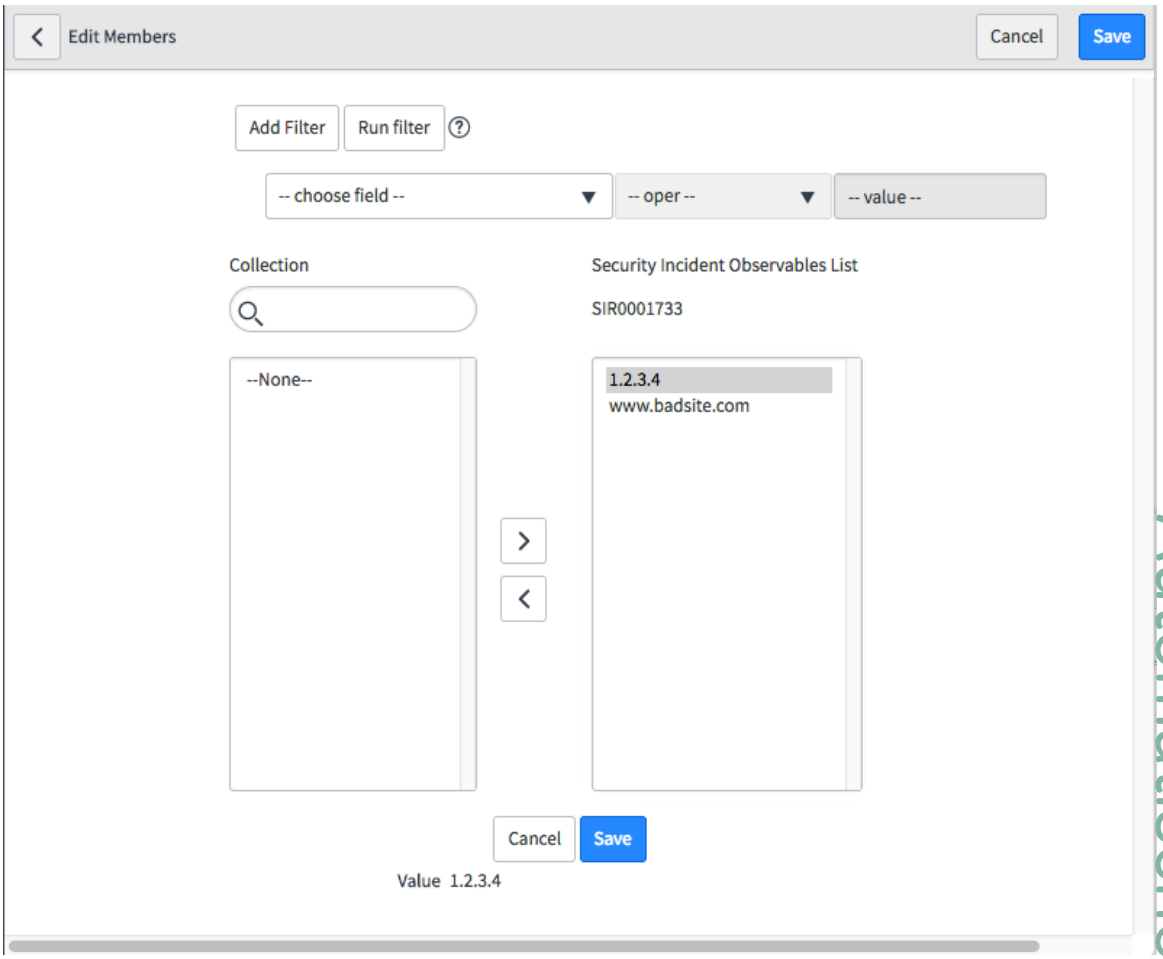
**Vorbereitungen**
Erforderliche Rolle: sn_si.basic

**Prozedur**

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf die Registerkarte Erkennbare **Security Incident-Elemente der** zugehörigen Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Fügen Sie der Liste erkennbare Elemente hinzu, oder entfernen Sie sie.
   Erstellen Sie einen Filter für lange Listen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Speichern**.

> **Hinweis:**
> Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Configuration Items oder Benutzern, die ihm zugeordnet sind. Die Registerkarten **Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert.
> Wenn das Plugin Threat Intelligence aktiviert ist und mindestens eineSecurity Incident Response-Integrationen -Integrationsimplementierung aktiviert ist, führt Security Operations-Integration – Funktion „Bedrohungssuche“. einen oder mehrere Workflows aus, und Bedrohungssicherheitssuchen werden für die hinzugefügten erkennbaren Elemente ausgeführt. Die Ergebnisse werden auf der Registerkarte Ergebnisse der **Bedrohungssuche angezeigt**.

**Zugehörige Informationen**

Fügen Sie mehrere erkennbare Security Incident-Elementehinzu

Erstellen Sie ein erkennbares Security Incident-Element

## Fügen Sie mehrere erkennbare Security Incident-Elementehinzu

Um Zeit zu sparen, können Sie der Liste der erkennbaren Security Incident-Elemente mehrere erkennbare Elemente hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_ti_write

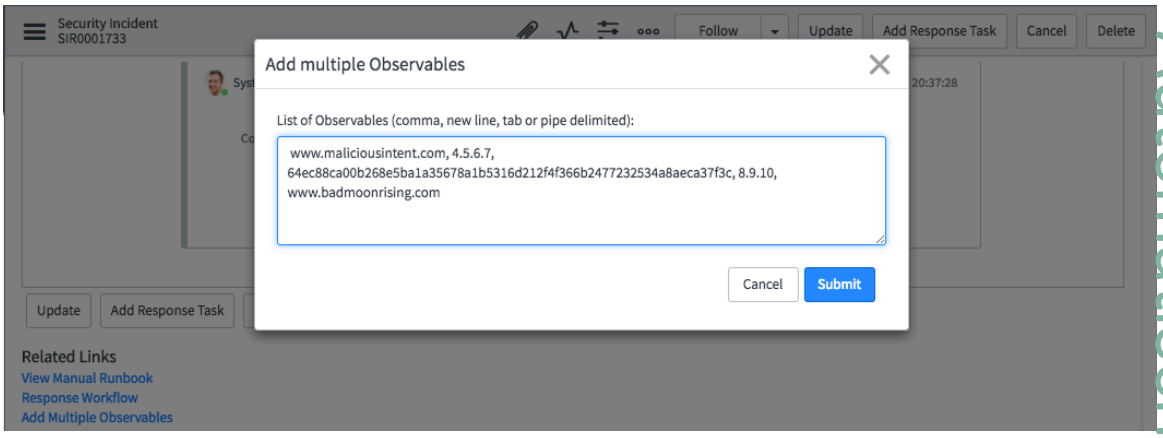
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Beim Hinzufügen mehrerer erkennbarer Security Incident-Elemente werden Duplikate während der Verarbeitung ignoriert.

### Prozedur

1. Navigieren Sie zu **Security Incident**.
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf den zugehörigen Link **Mehrere erkennbare Elemente hinzufügen**.
4. Geben Sie mehrere erkennbare Elemente ein, oder fügen Sie sie ein.
   Einträge können einen beliebigen erkennbaren Typ aufweisen. Akzeptierte Formate sind: Komma, neue Zeile, Registerkarte oder Pipeline-Trennzeichen.




**Hinweis:**
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Configuration Items oder Benutzern, die ihm zugeordnet sind. Die Registerkarten **Zugehörige Konfigurationselemente** und **Zugehörige Benutzer** werden entsprechend aktualisiert.

Hinweis: Erkennbare Werte, die nicht automatisch erkannt werden, werden dem Typ „Unbekannt“ zugewiesen.

5. Klicken Sie auf **Absenden**.

### Automatische Protokolldatenanreicherung erkennbarer Security Incidents

Wenn bestimmte Anwendungen und Integrationen eingerichtet werden, einschließlich Threat Intelligence und der Palo Alto Networks – Firewall -Integration, können Informationen zu erkennbaren Elementen in einem Security Incident automatisch mit Bedrohungsprotokolldaten angereichert werden, wenn die Quell-IP für die erkennbaren Elemente geändert wird.

Wenn eine Änderung erfolgt, initiiert eine Geschäftsregel einen Workflow, der Daten aus Bedrohungsprotokollen auf Ihrer Firewall abruft und die Informationen zu erkennbaren Elementen im Security Incident anreichert.

Bevor erkennbare Elemente angereichert werden können, müssen die folgenden Schritte ausgeführt werden.

- Threat Intelligence muss aktiviert sein.
- Die Palo Alto Networks-Firewall- Integration muss aktiviert und konfiguriert sein. Dies kann auch Richten Sie SSH-Anmeldeinformationen für den MID Server einenthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach Abschluss dieses Setups führt die Änderung der Quell-IP von erkennbaren Elementen, die einem Security Incident zugeordnet sind, dazu, dass eine Geschäftsregel den Workflow „ **Security Operations Palo Alto Networks – Protokolldaten abrufen** “ ausführt. Workflow-Aktivitäten stellen eine Suchabfrage auf der Firewall in die Warteschlange und geben eine Auftrags-ID zurück, die verwendet wird, um Bedrohungsprotokolldaten von der Firewall abzurufen und als XML-Datei an den Security Incident anzuhängen.

**Zugehörige Informationen**

Workflow zum Anreichern von AutoFocus-Sitzungsinformationen abrufen

Security Operations Integration Palo Alto Networks Firewall-Startprogramm-Workflow

Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten

Workflow „Protokolldaten abrufen“.

WildFire-Datenanreicherungs-Workflow abrufen

## Veröffentlichen Sie erkennbare Elemente in einer Drittanbieter-Beobachtungsliste

Sie können ein oder mehrere erkennbare Elemente oder zugeordnete Indikatoren in einer Drittanbieter-Beobachtungsliste veröffentlichen. Derzeit ist CrowdStrike Falcon Host die einzige Implementierung, die diese Funktionalität unterstützt.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

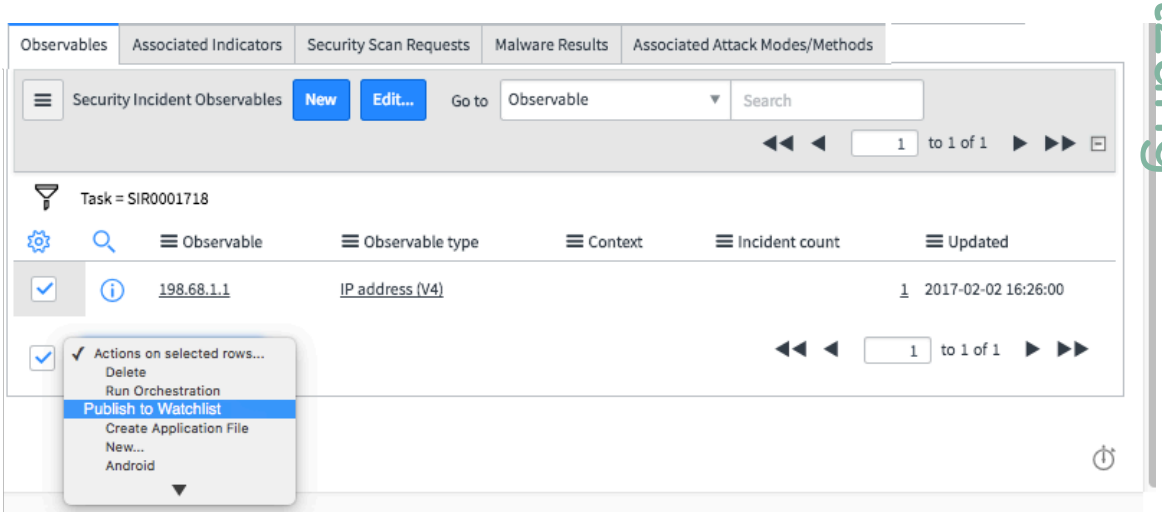
### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**

Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Prozedur

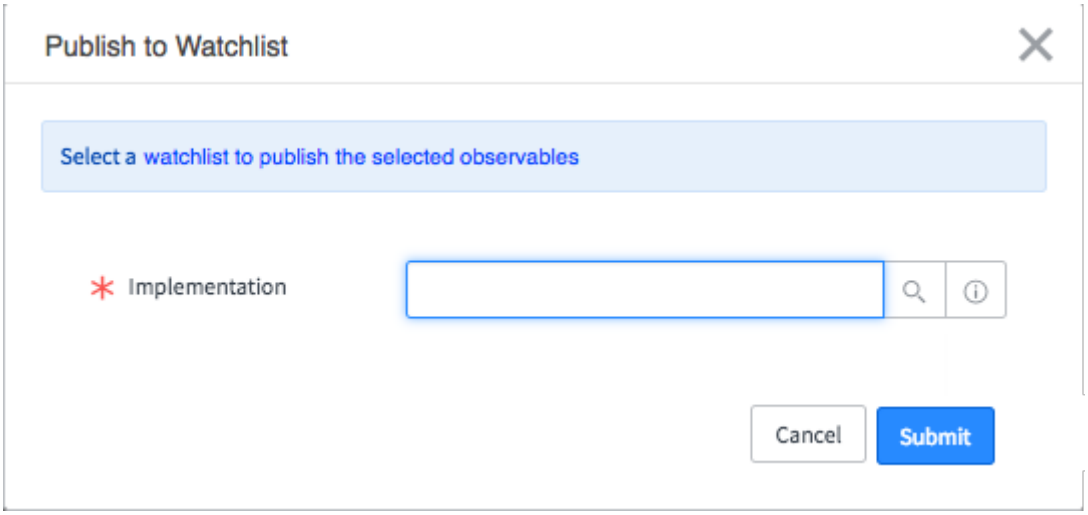
1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie auf der Registerkarte „ **Zugehörige Liste** “ die Option Erkennbare **Elemente** aus.
3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf In **Beobachtungsliste veröffentlichen**.




Das Dialogfeld wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie die Implementierung ein, oder wählen Sie sie aus.

> **Hinweis:**
> Ein Workflow wird von Integration von Sicherheitsvorgängen – Fähigkeit „In Beobachtungsliste veröffentlichen“. ausgelöst, wenn Sie die CrowdStrike Falcon Host-Implementierung auswählen.

5. Klicken Sie auf **Absenden**.

## Verwalten Sie Suchen und Scans

Sie können Suchen und Schwachstellenprüfungen anhand von Security Incidents und aus dem Security Incident-Katalog durchführen, um potenzielle Bedrohungen und Schwachstellen zu identifizieren.

### Senden Sie eine IoC-Suchanforderung aus einem Security Incident

Eine IoC-Suche wird automatisch ausgeführt, wenn einem Security Incident erkennbare Elemente hinzugefügt werden. Wenn Ihr Security Incident Anhänge enthält, können diese per Tastendruck leicht gefunden werden.

#### Vorbereitungen

Für automatische IoC-Suchen muss das Plugin Threat Intelligence aktiviert sein.

Erforderliche Rolle: sn_si.basic

> **Hinweis:**
> Standardmäßig ist der **Suchtyp** für **Datei** inaktiv.

#### Prozedur

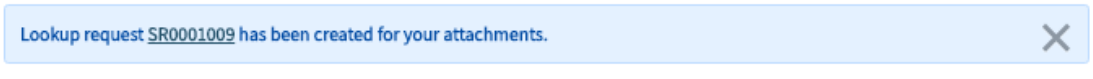
1. Erstellen Sie einen neuen Security Incident, oder öffnen Sie einen vorhandenen, wenn Sie neue Dateien an ihn anhängen möchten.
2. Klicken Sie im Formular-Header auf das Büroklammer-Symbol, und hängen Sie eine oder mehrere Dateien an.
3. Wenn Sie Ihre Eingaben im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und klicken Sie auf **Speichern**.
   Nachdem der Datensatz gespeichert wurde, wird die Schaltfläche **Anhänge** suchen angezeigt.
4. Klicken Sie **auf Anhänge suchen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
In den Arbeitsnotizen unter „ **Incident-Details** “ wird der Fortschritt des Suchvorgangs gemeldet.

5. Sie können auf die Suchnummer am Ende der Nachricht klicken, um den Suchdatensatz anzuzeigen. Sie können auf den Referenzlink Nachschlagen klicken, um detaillierte Ergebnisse anzuzeigen.




### Senden Sie eine IoC-Suchanforderung aus dem Security Incident Catalog

Wenn das Plugin Security Incident Response aktiviert ist, können Sie Bedrohungssuchen für Dateien, Hash-Werte, URLs und IP-Adressen aus dem Security Incident Catalog übermitteln. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse im Modul „ **Meine Anforderungen** “ anzeigen.

#### Vorbereitungen
Erforderliche Rolle: keine

#### Warum und wann dieser Vorgang ausgeführt wird
Suchen werden automatisch für den Standardsuchtyp für jede im Suchdatensatz aufgeführte Suchquelle ausgeführt. Die Ergebnisse der Suchanforderung sind im Modul **„Meine Anforderungen** “ verfügbar.

#### Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Katalog für Sicherheitsvorfälle**.
2. Klicken Sie **auf IoC-Suche**.
3. Klicken Sie **auf Dateien, Hash-Werte, URLs oder IP-Adressen suchen**.
4. Geben Sie eine oder mehrere der folgenden Optionen ein:

**IoC-Suchanforderung**

| Zu suchendes Element | Beschreibung |
|---|---|
| Dateien | Klicken Sie auf das Büroklammersymbol, suchen Sie die zu suchenden Dateien, und hängen Sie sie an.<br>**Hinweis:**<br>Standardmäßig ist der **Suchtyp** für **Datei**inaktiv. Dateien werden konvertiert und als Hash-Wert übermittelt. |
| URLs | Geben Sie im Feld URLs die **URLs** ein, nach denen Sie suchen möchten, getrennt durch Kommas. Beispiel: www.abc.com,www.xyz.net. |
| IP-Adressen | Geben Sie im Feld IP- **Adressen** die IP-Adressen ein, nach denen Sie suchen möchten, getrennt durch Kommas. |
| Hash-Werte | **Geben Sie im Feld Hash-Werte die Hash** -Werte ein, nach denen Sie suchen möchten, getrennt durch Kommas. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zu suchendes Element | Beschreibung |
|---|---|
| | **Hinweis:**<br>Wenn der **Suchtyp** für **Datei** inaktiv ist, ist dieser Wert die Standardaktion für **Datei-** und **Hash-Werte**. |

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Absenden**.
6. Um den Status und/oder die Ergebnisse der Suchen anzuzeigen, navigieren Sie zu **Selfservice** > **Meine Anforderungen**.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   In den Arbeitsnotizen unter **Aktivität** werden die während der Suche ausgeführten Aufgaben aufgelistet, einschließlich der Erstellung einzelner Suchvorgänge für jede Datei, Hash-Wert, URL oder IP-Adresse und der Suchergebnisse.

### Senden Sie eine Anforderung zur Schwachstellenprüfung aus einem Security Incident

Wenn Ihr Security Incident ein oder mehrere Konfigurationselemente (Server, Computer usw.) aufweist, können diese über das Formular Security Incident Response auf Schwachstellen gescannt werden.

#### Vorbereitungen

Das Vulnerability Response-Plugin muss aktiviert sein.

Erforderliche Rolle: sn_si.write

#### Prozedur

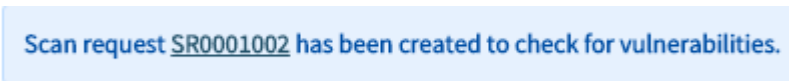
1. Erstellen Sie einen Security Incident, und beziehen Sie mindestens eine Ressource ein.
   Sie können auch einen vorhandenen Incident öffnen, der Konfigurationselemente enthält.
2. Wenn Sie Ihre Eingaben im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und klicken Sie auf **Speichern**.
   Nachdem der Datensatz gespeichert wurde, wird ein zugehöriger Link Nach **Schwachstellen** suchen angezeigt.

   **Hinweis:**
   Wenn die zugehörige Liste Nach **Schwachstellen** suchen nicht angezeigt wird, müssen Sie zu navigieren **Schwachstelle** > **Scanner**, richten Sie mindestens einen Scanner ein, und legen Sie dessen Standard auf **true**fest.

3. Klicken Sie **auf Nach Schwachstellen suchen**.

   **Hinweis:**

   Am oberen Rand des Security Incident-Formulars wird eine Nachricht zusammen mit einem Link zum Scan-Datensatz angezeigt.

4. Sie können auf die Scan-Anforderungsnummer klicken, um den Scan-Datensatz anzuzeigen.
   Die Incident-Details zeigen die Ergebnisse des Scans im Datensatz der Sicherheitsscan-Anforderung an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Senden Sie eine Schwachstellen-Scan-Anforderung aus dem Security Incident Response-Katalog

Sie können Schwachstellenprüfungen für CIs und IP-Adressen aus dem Katalog Security Incident Response übermitteln. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse im Modul „ **Meine Anforderungen** “ anzeigen.

#### Vorbereitungen
Erforderliche Rolle: keine

#### Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Katalog für Sicherheitsvorfälle**.
2. Klicken Sie auf **Schwachstellenprüfung**.
3. Klicken Sie **auf Konfigurationselement und IP-Adressen scannen**.
4. Geben Sie einen oder mehrere der folgenden Punkte ein, die gescannt werden sollen.

**Schwachstellenscanner**

| Zu scannendes Element | Beschreibung |
|---|---|
| Konfigurationselement | Wählen Sie im Feld **Zu scannendes Konfigurationselement das zu scannende** CI aus. |
| IP-Adressen | Geben Sie im Feld **Zu scannende** IP-Adressen die IP-Adressen durch Kommas getrennt ein. |

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Absenden**.
   Wenn ein erkennbares Element gefunden wird, wird gemäß den STIXX-Standards ein Indikator erstellt.
6. Um den Status und/oder die Ergebnisse der Scans anzuzeigen, navigieren Sie zu **Selfservice** > **Meine Anforderungen**.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   In den Arbeitsnotizen unter **Aktivitäten** werden die während des Scans ausgeführten Aufgaben aufgelistet, einschließlich der Erstellung einzelner Scans für jedes CI oder jede IP-Adresse und die Ergebnisse der Scans.

## on-Demand-Orchestrationverwalten

Während der Analyse Security Incident Response möchte ein Sicherheitsanalyst möglicherweise eine Aufgabe ausführen, die von einem Security Incident-Workflow gesteuert wird. Führen Sie beispielsweise eine Prozesssicherung für ein bestimmtes CI aus. Dies kann mit On-Demand-Orchestration erreicht werden.

Jede registrierte Security Operations-Anwendung enthält mehrere On-Demand-Orchestrationen im Basissystem. Sie können nach Bedarf benutzerdefinierte On-Demand-Orchestrationendefinieren.

Die On-Demand-Orchestration kann über eine Auswahlliste am Ende der folgenden Listen und Formulare in Security Incident Responseaufgerufen werden:

- Formular „Security Incident“
- Security Incident-Liste
- Zugehörige Liste „Erkennbare Elemente für Security Incident“.
- Zugehörige Liste Konfigurationselemente



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

- Eine Eigenschaft in Security Support Common namens **sn_sec_cmn.use_on_demand_tbl_as_allowed** definiert, welche Workflows für die Ausführung bei Bedarf verfügbar sind.
- Wenn die Eigenschaft auf **true**festgelegt ist, sind nur Workflows verfügbar, die in der Tabelle „Orchestration bei Bedarf“ [sn_sec_cmn_on_demand_orchestration] angegeben sind.
- Wenn die Eigenschaft auf „ **false** “ (Standard) festgelegt ist, sind alle Workflows für Anwendungen verfügbar, die in der SecOps- Anwendungsregistrierung konfiguriert sind.
- Abhängig von der Einstellung der Eigenschaft ist die Liste der verfügbaren Workflows auf die Art der zu analysierenden Informationen zugeschnitten.

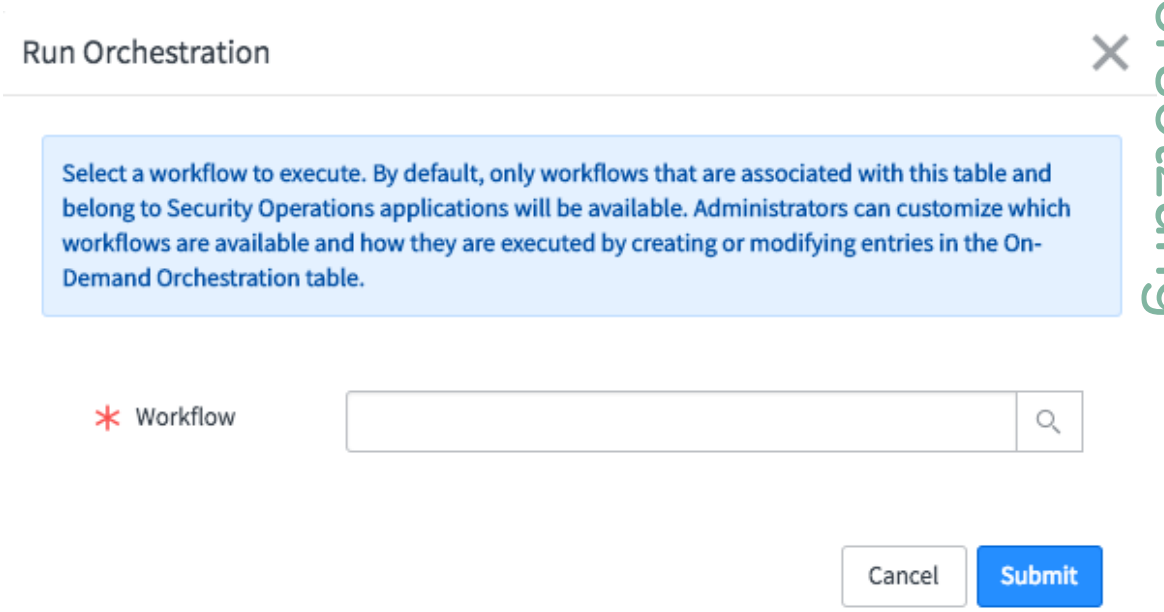
### Führen Sie eine Orchestrierung bei Bedarf über das Security Incident-Formular durch

Die On-Demand-Orchestration kann über eine Auswahlliste am unteren Rand des Security Incident-Formulars aufgerufen werden.

**Vorbereitungen**
Erforderliche Rolle: sn_si.write

**Prozedur**

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
2. Wählen Sie den Datensatz (Security Incident, erkennbares Element oder CI) aus, für den Sie einen Workflow ausführen möchten.
3. Klicken Sie auf den zugehörigen Link **Orchestration** ausführen.
   Das Dialogfeld „ **Orchestration** ausführen“ wird geöffnet. Die Darstellung des Dialogfelds hängt von der Einstellung der Eigenschaft sn_sec_cmn.use_on_demand_tbl_as_whitelist in Security Support Common ab.




4. Klicken Sie auf das Suchsymbol, und wählen Sie den Workflow aus, den Sie ausführen möchten.
   Der ausgewählte Workflow wird ausgeführt. Details finden Sie unter Security Incident Response Orchestration Workflows und Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Führen Sie eine Orchestrierung bei Bedarf über die Liste der Security Incidents durch

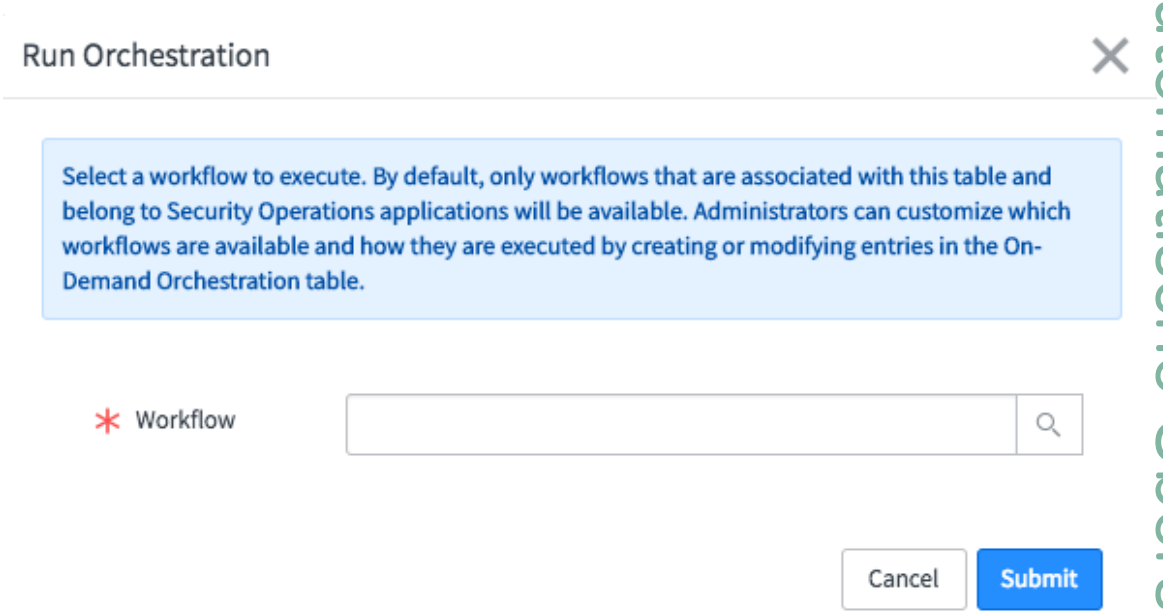
Die On-Demand-Orchestration kann über die Liste „Security Incident“ sowie über zugehörige Listen in Security Incident Responseaufgerufen werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.write

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
2. Aktivieren Sie die Checkbox neben dem Security Incident, für den Sie einen Workflow ausführen möchten.
3. Klicken Sie unten auf dem Bildschirm auf die Auswahlliste **Aktionen für ausgewählte Zeilen** und dann auf **Orchestration ausführen**.
   Das Dialogfeld „ **Orchestration** ausführen“ wird geöffnet. Die Darstellung des Dialogfelds hängt von der Einstellung der Eigenschaft sn_sec_cmn.use_on_demand_tbl_as_whitelist in Security Support Common ab.




4. Klicken Sie auf das Suchsymbol, und wählen Sie den Workflow aus, den Sie ausführen möchten.
   Der ausgewählte Workflow wird ausgeführt. Details finden Sie unter Security Incident Response Orchestration Workflows und Aktivitäten.

### Definieren Sie neue On-Demand-Orchestrationen

Im Basissystem können Sie On-Demand-Orchestrationen auswählen, die vordefinierte Workflows ausführen. Sie können neue On-Demand-Orchestrationen definieren, um anzupassen, wie Workflows aus den **Auswahllisten Orchestration** ausführen aufgerufen werden.

#### Vorbereitungen

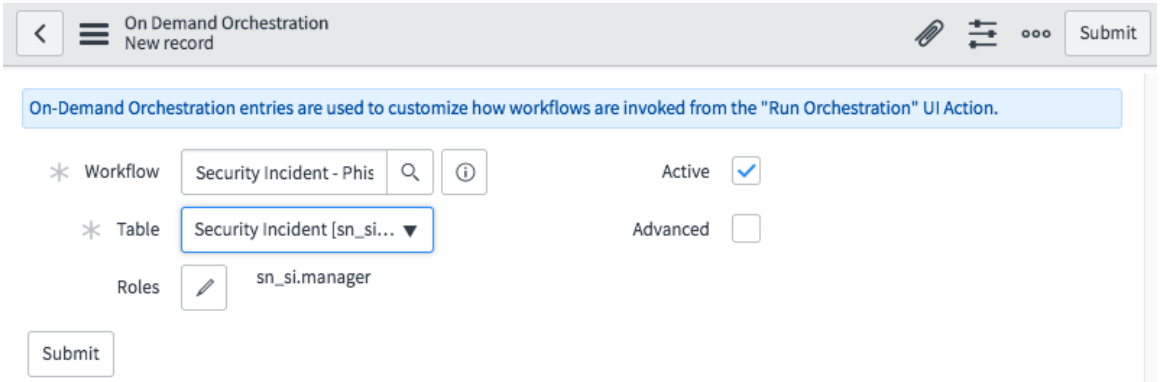
Erforderliche Rolle: sn_si.write

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Orchestration bei Bedarf**
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Füllen Sie die Felder entsprechend aus.

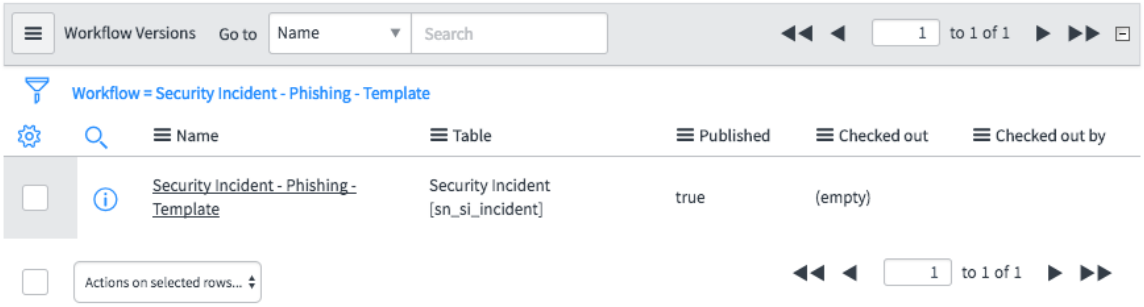
**Orchestration bei Bedarf**

| Feld | Beschreibung |
|---|---|
| Workflow | Wählen Sie den Workflow aus, der in die Auswahlliste **Orchestration** ausführen aufgenommen werden soll. |
| Tabelle | Wählen Sie die Tabelle aus, für die der ausgewählte Workflow ausgeführt wird. Wenn die Tabelle nicht mit der für den ausgewählten Workflow konfigurierten Tabelle übereinstimmt, müssen Sie das Kontrollkästchen **Erweitert** aktivieren und das Ausführungsskript so ändern, dass bei der **Ausführung** der korrekte Datensatz an den Workflow übergeben wird. |
| Rollen | Wählen Sie nach Bedarf zusätzliche Rollen aus, um einzuschränken, wer diesen Workflow in der **Auswahlliste Orchestration** ausführen sehen kann. |
| Aktiv | Aktivieren Sie dieses Kontrollkästchen, um diesen On-Demand-Orchestration-Datensatz zu aktivieren. |
| Erweitert | Aktivieren Sie diese Checkbox, um das Ausführungsskript so zu ändern, dass es den richtigen Datensatz an die ausgewählte Tabelle für diesen Workflow übergibt. |
| Ausführungsskript | Ändern Sie das Ausführungsskript so, dass der richtige Datensatz an die ausgewählte Tabelle für diesen Workflow übergeben wird.<br><br>Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Erweitert** aktiviert ist. |

**4.** Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen **Sie Speichern**aus.
Die zugehörige Liste **Workflow-Versionen** wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Wenn Sie weitere Änderungen am Workflow vornehmen müssen, müssen Sie ihn auschecken.

**Zugehörige Informationen**

Arbeiten Sie mit Workflow-Versionen

## Registrieren Sie neue Security Operations-Anwendungen für die On-Demand-Orchestration

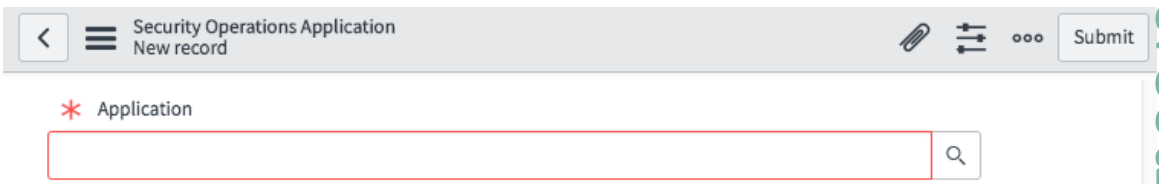
Im Basissystem werden Security Operations-Anwendungen automatisch registriert, wenn sie aktiviert werden. Durch die Registrierung können die mit den Anwendungen verknüpften Workflows für On-Demand-Orchestration-Anforderungen verfügbar gemacht werden. Bei Bedarf können Sie neue Anwendungen definieren und ihnen Workflows für die On-Demand-Orchestration zuordnen.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Prozedur

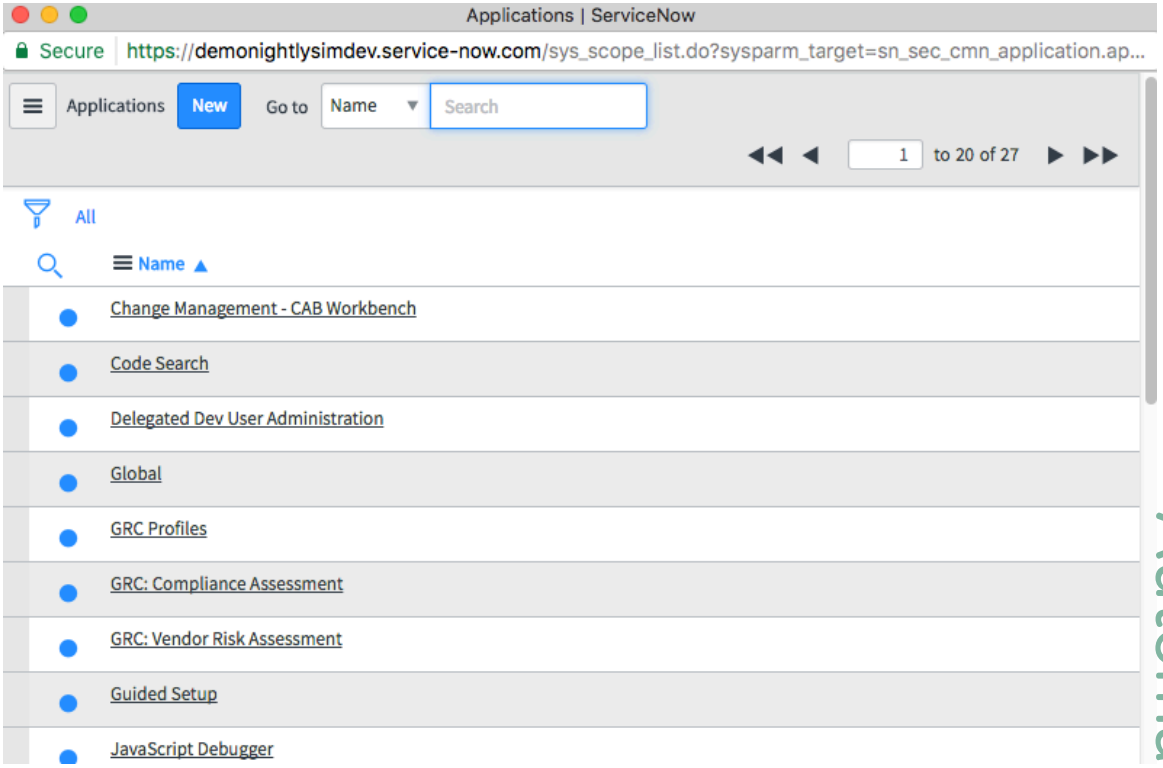
1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **SecOps-Applikationsregistrierung**und klicken Sie auf **Anwendung registrieren**.
   Der Bildschirm „Security Operations-Anwendung“ wird angezeigt.



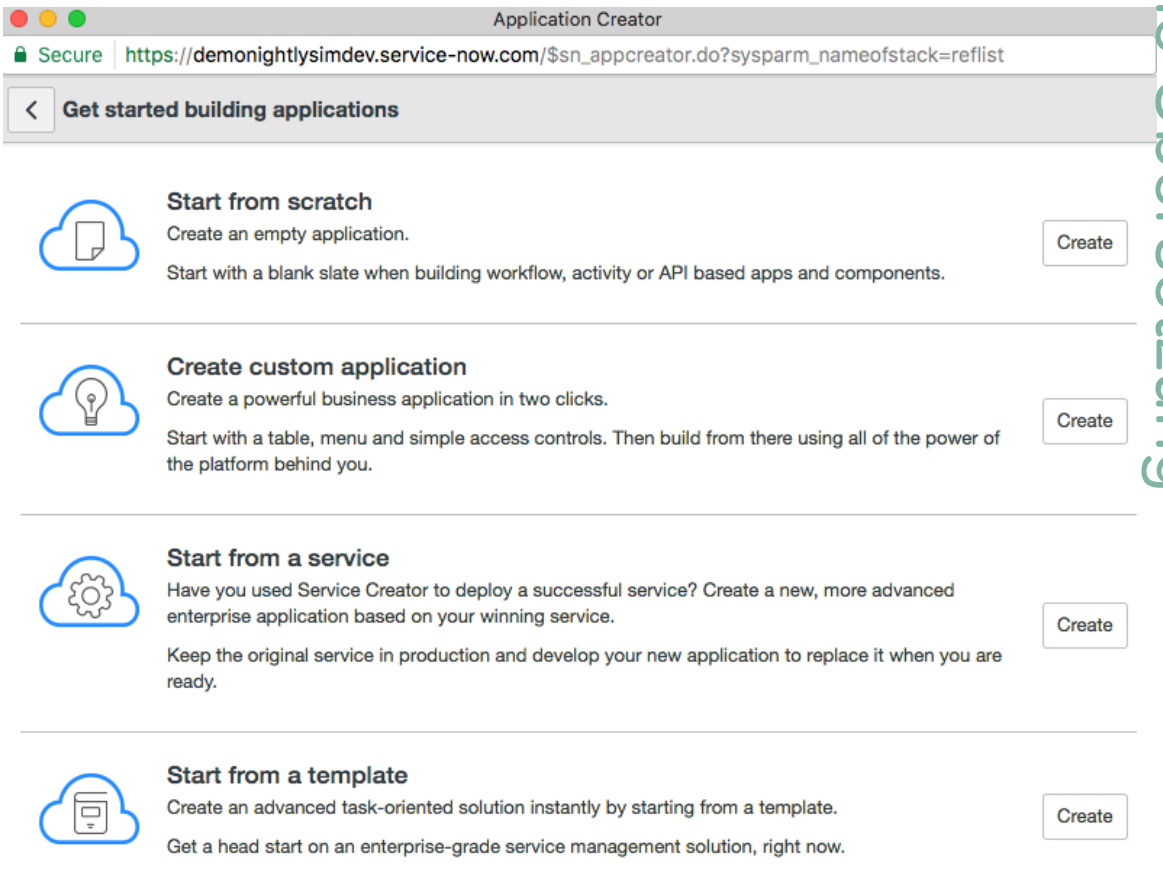

2. Klicken Sie im Feld **Anwendung** auf das Suchsymbol (Lupe).
   Der Bildschirm Anwendungen wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Klicken Sie auf **Neu**.
Der Bildschirm „Application Creator“ wird angezeigt.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die angezeigten Optionen hängen von den Anwendungen ab, die Sie aktiviert haben. Ausführliche Informationen zum Erstellen neuer Anwendungen finden Sie unter Building applications .

4. Nachdem die Anwendung generiert wurde, können Sie Skripts zum Einrichten der On-Demand-Orchestration erstellen.

**Hinweis:**
Das Einrichten der On-Demand-Orchestrierung für neue Anwendungen erfordert fortgeschrittene technische Kenntnisse in Bezug auf Skripterstellung und Erstellung von Auslösern für die Skripts (Business Rules, UI-Aktion, Workflows usw.). Weitere Informationen erhalten Sie von ServiceNow Professional Services.

## Fügen Sie Informationen zu einem Security Incident hinzu

Nachdem ein Security Incident erstellt wurde, können Sie weitere Details zur Unterstützung der Analyse hinzufügen, z. B. Zugriffsrollen und verschiedene Arten von Notizen.

### Vorbereitungen
Erforderliche Rolle: sn_si.basic

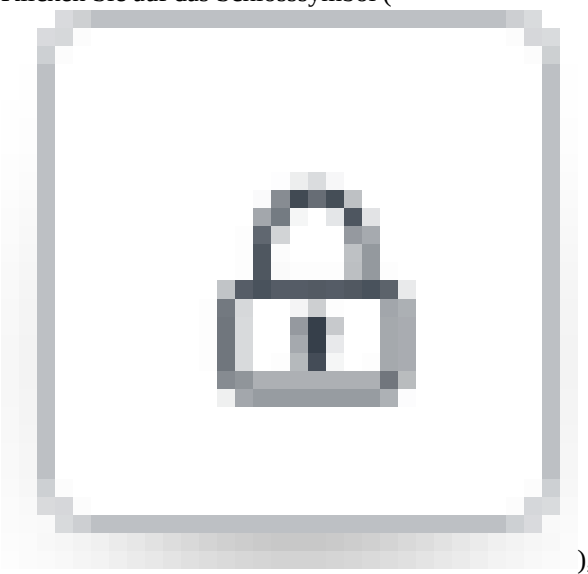
### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Incident-Details**.
3. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Lesezugriff | Gewährt einem Benutzer mit der **speziellen Zugriffsrolle** Lesezugriff auf den Security Incident Der Benutzer kann Arbeitsnotizen lesen und schreiben.<br>**Hinweis:**<br>○ Wenn ein Benutzer sowohl der Liste „ **Lesezugriff** “ als auch der Liste „ **Privilegierter Zugriff** “ hinzugefügt wird, bleiben nur die Berechtigungen für **privilegierten Zugriff** erhalten.<br>○ Benutzer mit nur der Rolle „sn_si.admin“ können sowohl den Lesezugriff als auch den privilegierten Zugriff ändern. |
| Beobachtungsliste | Klicken Sie auf das Sperrsymbol, um Benutzer hinzuzufügen, die benachrichtigt werden, wenn Änderungen am Security Incident auftreten. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer oder zur Eingabe von Benutzer-E-Mail-Adressen verfügbar. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Sperrsymbol, um das Feld zu sperren. |
| Privilegierter Zugriff | Erteilt einem Benutzer mit der **speziellen Zugriffsrolle** Lese- und Schreibzugriff auf alle Felder des Security Incident mit Ausnahme von **Zugewiesen an**. Benutzern mit speziellen Zugriffsrollen wird ein eigenes Modul mit allen Security Incidents zugewiesen. Ihnen stehen keine anderen Module zur Verfügung. Niemand sonst kann das Modul „Für **mich sichtbar“** sehen. |

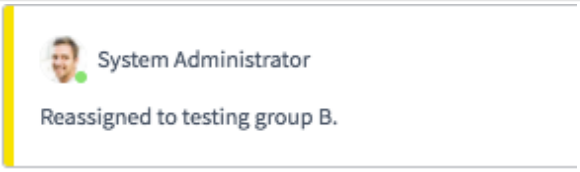
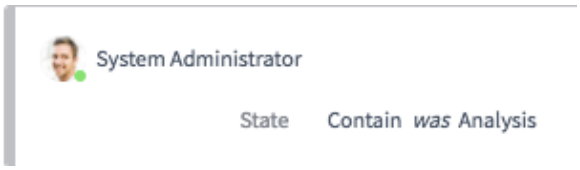


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

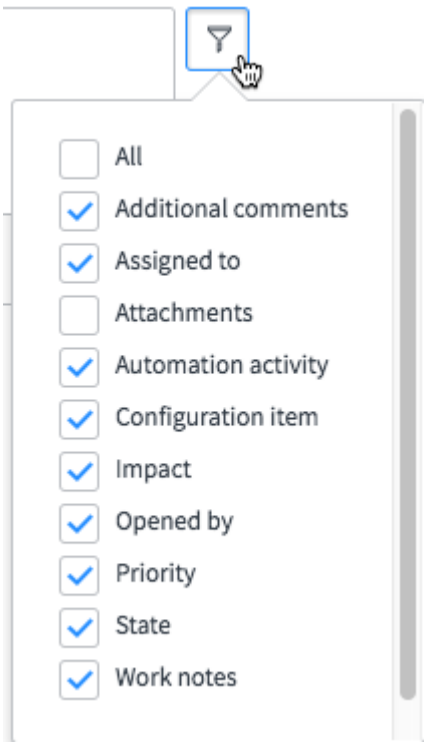
| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br><br>Nur ein zugewiesener Benutzer oder eine Person mit einer Sicherheitsrolle (z. B. sn_si_analyst oder sn_si.admin) kann das Feld **Zugewiesen an** ändern.<br><br>Wenn ein Benutzer sowohl der Liste „ **Lesezugriff** “ als auch der Liste „ **Privilegierter Zugriff** “ hinzugefügt wird, bleiben nur die Berechtigungen für **privilegierten Zugriff** erhalten.<br><br>Wenn ein Benutzer sowohl der Liste „ **Lesezugriff** “ als auch der Liste „ **Privilegierter Zugriff** “ hinzugefügt wird, bleiben nur die Berechtigungen für **privilegierten Zugriff** erhalten. |
| Arbeitsnotizenliste | Klicken Sie auf das Schlosssymbol (  ), um Benutzer hinzuzufügen, die benachrichtigt werden, wenn neue Arbeitsnotizen hinzugefügt werden. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer oder zur Eingabe von Benutzer-E-Mail-Adressen verfügbar. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Sperrsymbol, um das Feld zu sperren. |
| Beschreibung | Geben Sie eine vollständige Beschreibung des Security Incident ein, zusammen mit allen Informationen, die helfen können, die Ursache zu finden oder das Problem zu beheben. |
| Sichere Notizen | Nur Benutzerrollen mit sn_si.admin und sn_si.analyst können die sicheren Notizen anzeigen oder bearbeiten. |
| Arbeitsnotizen | Geben Sie Arbeitsnotizen ein, die für den Kunden nicht sichtbar sind. Arbeitsnotizen werden im **Aktivitätsbereich** angezeigt. |
| Aktivität | Zeigt Informationen an, die manuell in Arbeitsnotizen eingegeben wurden, und alle dynamisch aktualisierten Aufgabenaktivitäten (Aktionen, Kommentare, Arbeitsnotizen usw.) in zugehörigen Datensätzen für diesen Security Incident.<br><br>Arbeitsnotizen werden mit einem gelben Farbband angezeigt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| |  <br>Automatisch generierte Notizen werden mit einem grauen Farbband angezeigt.<br>  |

4. Sie können die Arten der im Feld **Aktivität** angezeigten Informationen einschränken, indem Sie auf das Filtersymbol ( ) klicken.




**Hinweis:**
Mit dem Kontrollkästchen **Automatisierungsaktivität** können Sie alle von diesem Security Incident durchgeführten Ergänzungen einbeziehen, einschließlich Workflow-Aktivitäten, Aktualisierungen der Risikopunktzahl usw.

5. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugehörige Datensätze
- Überprüfung nach Incident
- Abschlussinformationen

6. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

### Fügen Sie einem Security Incident zugehörige Probleme, Changes und Incidents hinzu

Sie können zugehörige Datensätze wie Probleme, Changes und Incidents zu vorhandenen Security Incidents hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Zugehörige Datensätze**.
3. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Problem | Wählen Sie einen Problem-Datensatz (PRB) aus, der das zugrunde liegende Problem löst, das zur Erstellung dieses Security Incident geführt hat. Die PRBs für diesen Incident werden normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars klicken und **Problem erstellen**auswählen. |
| Übergeordnet | Wählen Sie einen Aufgabendatensatz aus, der sich auf das zugrunde liegende Problem bezieht, das zur Erstellung dieses Security Incident geführt hat. |
| Übergeordneter Security Incident | Wählen Sie einen Security Incident-Datensatz aus, der sich auf das zugrunde liegende Problem bezieht, das zur Erstellung dieses Security Incident geführt hat. Weitere Informationen finden Sie unter Übergeordnete und untergeordnete Security Incident-Beziehungen. |
| Incident | Wählen Sie einen Incident-Datensatz (INC) aus, der das zugrunde liegende Problem löst, das zur Erstellung dieses Security Incident geführt hat.<br><br>Der Incident wird normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars klicken und **Incident erstellen**auswählen. |
| Change Request | Wählen Sie einen Change Request (CHG)-Datensatz aus, der das zugrunde liegende Problem löst, das zur Erstellung dieses Security Incident geführt hat. Die Change-Anforderung wird normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars klicken und **Change erstellen**auswählen. |

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Incident Details
   - Überprüfung nach Incident
   - Abschlussinformationen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Rufen Sie eine Prozesssicherung für einen erweiterten Prozess in Windows auf

Ein Sicherheitsanalyst kann eine Prozesssicherung für einen bestimmten Prozess ausführen, ihn in eine Datei speichern und an einer freigegebenen Site in einem internen Netzwerk veröffentlichen. Ein Analyst kann dann einen Deny-Listen-Prozess anzeigen, der in einem Security Incident rot hervorgehoben ist, und zusätzliche Analysen durchführen.

### Vorbereitungen

Folgendes ist erforderlich:

- Ein Client mit Windows Vista oder höher oder ein Server mit Windows Server 2008 oder höher.
- Das installierte Befehlszeilendienstprogramm ProcDump mit einer Systemumgebungsvariablen, die auf den Pfad der ausführbaren Datei procdump verweist. Der Name der Variablen muss PROCDUMP lauten. Dieser Name wird in einem PowerShell-Skript verwendet.

Erforderliche Rolle: sn_si.analyst

### Prozedur

1. Navigieren Sie zu dem Security Incident mit dem erweiterten Prozess, für den Sie einen Produktdump aufrufen möchten, indem Sie auf klicken **Alle** > **Security Incident** > **Offene Incidents anzeigen**, und öffnen Sie einen Security Incident.
2. **Klicken** Sie auf die Registerkarte Ergänzungsdaten.
3. Klicken Sie auf den **Ergänzungsdatensatz Laufende Prozesse** abrufen.
4. Aktivieren Sie die Checkboxen für die laufenden Prozesse, für die Sie einen Procdump ausführen möchten, klicken Sie auf die Dropdown-Liste Aktionen für ausgewählte Zeilen am Ende der Liste, und klicken **Sie auf Procdump ausführen**.
   Die Nachricht **Prodump-Workflow für ausgewählten Prozess initiiert wird** oben in der Liste angezeigt, und der Workflow **„Security Incident Response – Prodump** ausführen“ wird ausgeführt.

## Zeigen Sie Informationen in einem Security Incident an

Sie können über die zugehörigen Links mehrere andere Aktionen für einen vorhandenen Security Incident ausführen.

### Vorbereitungen

Erforderliche Rolle: sn_si.basic

### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Innerhalb von **Zugehörige Links**können Sie die folgenden Aufgaben ausführen:

| Option | Bezeichnung |
|---|---|
| **Manuelles Runbook anzeigen** | Zeigen Sie eine Liste der für diesen Security Incident verfügbaren Runbooks an. |
| **Antwort-Workflow** | Zeigen Sie alle mit diesem Incident verknüpften Workflows an. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| **Mehrere erkennbare Elemente hinzufügen** | Fügt eine Liste von erkennbaren Elementen in durch Kommas, neuen Zeilen, Registerkarten oder Pipelines getrennten Formaten hinzu. |
| **Dem Sicherheitsfall hinzufügen** | Fügt den Security Incident einem oder mehreren Sicherheitsfällen hinzu. Sie können auch einen neuen Sicherheitsfall erstellen und diesen Security Incident hinzufügen. |
| **Ruft QRadar-IP-Zusammenfassungen ab** | Wenn eine QRadar-Integration verfügbar ist und gültige CIs, Quell- und Ziel-IP-Adressen enthält, werden die QRadar-Workflows ausgelöst und die Ergebnisse in Arbeitsnotizen angezeigt. |
| **Orchestration ausführen** | Wählen Sie einen Security Operations-Workflow aus, und führen Sie ihn aus. |
| **View SLA timeline** | Sie können eine SLA-Zeitleiste aus einem Aufgaben-SLA-Datensatz oder aus einer SLA-Definition anzeigen. |
| **Alle zugehörigen Listen anzeigen** | Zeigt alle standardmäßigen zugehörigen Listen und alle manuell hinzugefügten Listen an.<br>**Hinweis:**<br>Manuell hinzugefügte Elemente sind nur in dieser Ansicht verfügbar. |
| **Betroffene Elemente anzeigen** | Zeigt die Listen der CIs, Benutzer und Services an, die direkt von diesem Incident betroffen sind |
| **Zugehörige Elemente anzeigen** | Zeigt die Listen der zugehörigen Incidents, CIs, Benutzer und Gruppen an, die von diesem Incident betroffen sind. |
| **IoC anzeigen** | Zeigt die Listen der erkennbaren Elemente, Indikatoren, Malware, Modi und Methoden sowie Sicherheitsscananforderungen an, die diesem Incident zugeordnet sind. |
| **Ergänzungsdaten anzeigen** | Zeigt die Listen der Ergänzungsdaten, Prozesse, Services, Statistiken, Suchvorgänge, Firewall-Protokolle und gefährdeten Benutzerinformationen an, die diesem Incident zugeordnet sind. |
| **Antwortaufgaben anzeigen** | Zeigt die Listen der Aufgaben, SLAs, Risikopunktzahl-Audits, Ausfälle und Exchange-Suchen an, die diesem Incident zugeordnet sind. |
| **Zeigen Sie Details im externen System an** | Wenn dieser Security Incident aus einer externen Anwendung direkt oder durch Events generiert wurde und ein Link zu den Ursprungsdaten bereitgestellt wurde, wird die URL durch die Aktion **Details in externem System** anzeigen geöffnet. Sie können die Protokolle anzeigen und durchsuchen, die diesen Incident generiert haben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

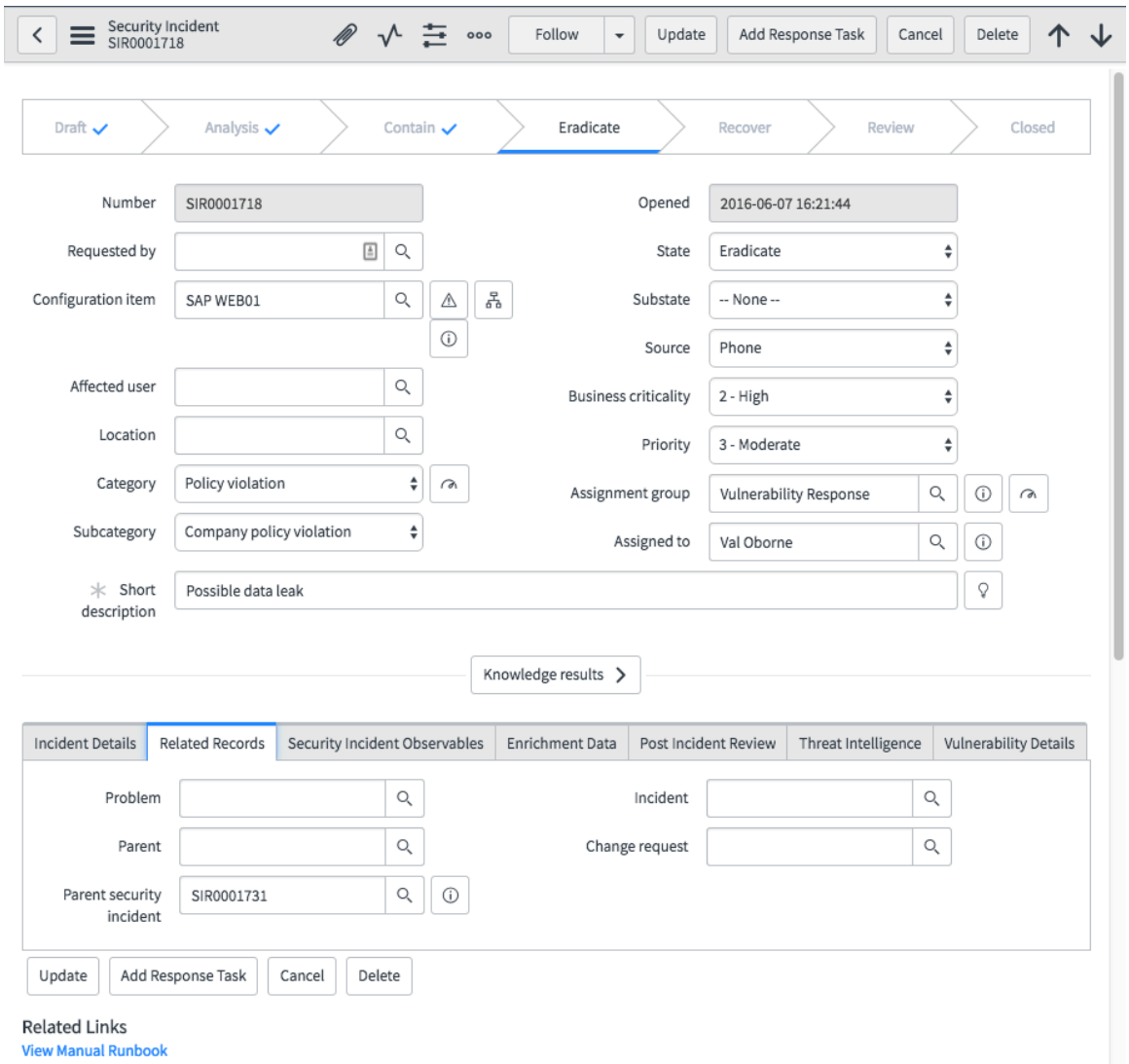
| Option | Bezeichnung |
| --- | --- |
| Suchen Sie nach Schwachstellen | Wenn Vulnerability Response aktiviert ist und Sie mindestens ein betroffenes CI für den Security Incident ausgewählt haben, können Sie eine Scan-Anforderung senden, um zu bestimmen, welche Schwachstellen im CI vorhanden sind. |

### Übergeordnete und untergeordnete Security Incident-Beziehungen

Sie können die Auswirkungen eines bestimmten Problems mithilfe von über- und untergeordneten Security Incident-Beziehungen in Security Incident Responsezuordnen und nachverfolgen.

Auf der Registerkarte „ **Zugehörige Datensätze** “ können Sie jedem Security Incident Response -Formular ein **übergeordnetes Security Incident-** Problem hinzufügen. Diese Funktion macht den Incident automatisch zu einem untergeordneten Incident, der auf der Registerkarte **Zugehörige Listen – Untergeordnete Security Incidents** des übergeordneten Problems angezeigt wird.

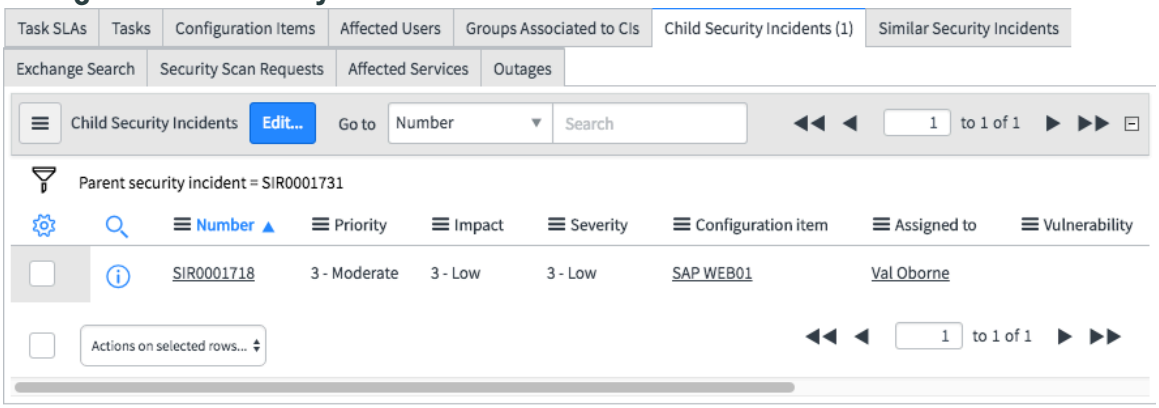
**Hinweis:**
Sie können einen vorhandenen übergeordneten Security Incident nicht zu seinem eigenen untergeordneten Element machen, indem Sie für beide Incidents dieselbe Nummer verwenden.





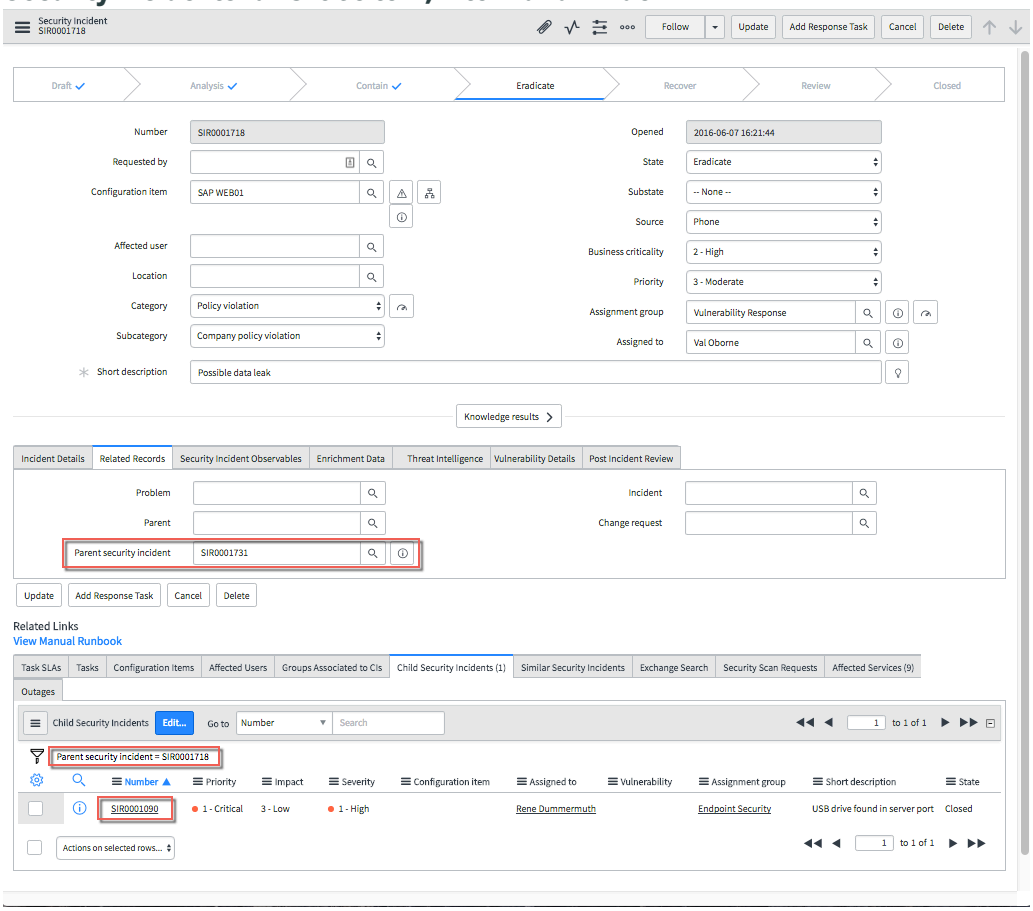

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Untergeordneter Security Incident




Sie können jedem Security Incident-Datensatz auch einen oder mehrere **untergeordnete Security Incidents** hinzufügen, indem Sie auf der Registerkarte **„Untergeordnete Security Incidents** “ auf die Schaltfläche **Bearbeiten** klicken. Im folgenden Beispiel sind alle drei Datensätze verbunden.

### Security Incidents für Großeltern, Eltern und Kinder




Hinweis: Alle im übergeordneten Element aufgezeichneten Arbeitsnotizen werden an alle aktiven untergeordneten Elemente in **Aktivitäten** auf der Registerkarte „ **Incident-Details** “ weitergegeben.

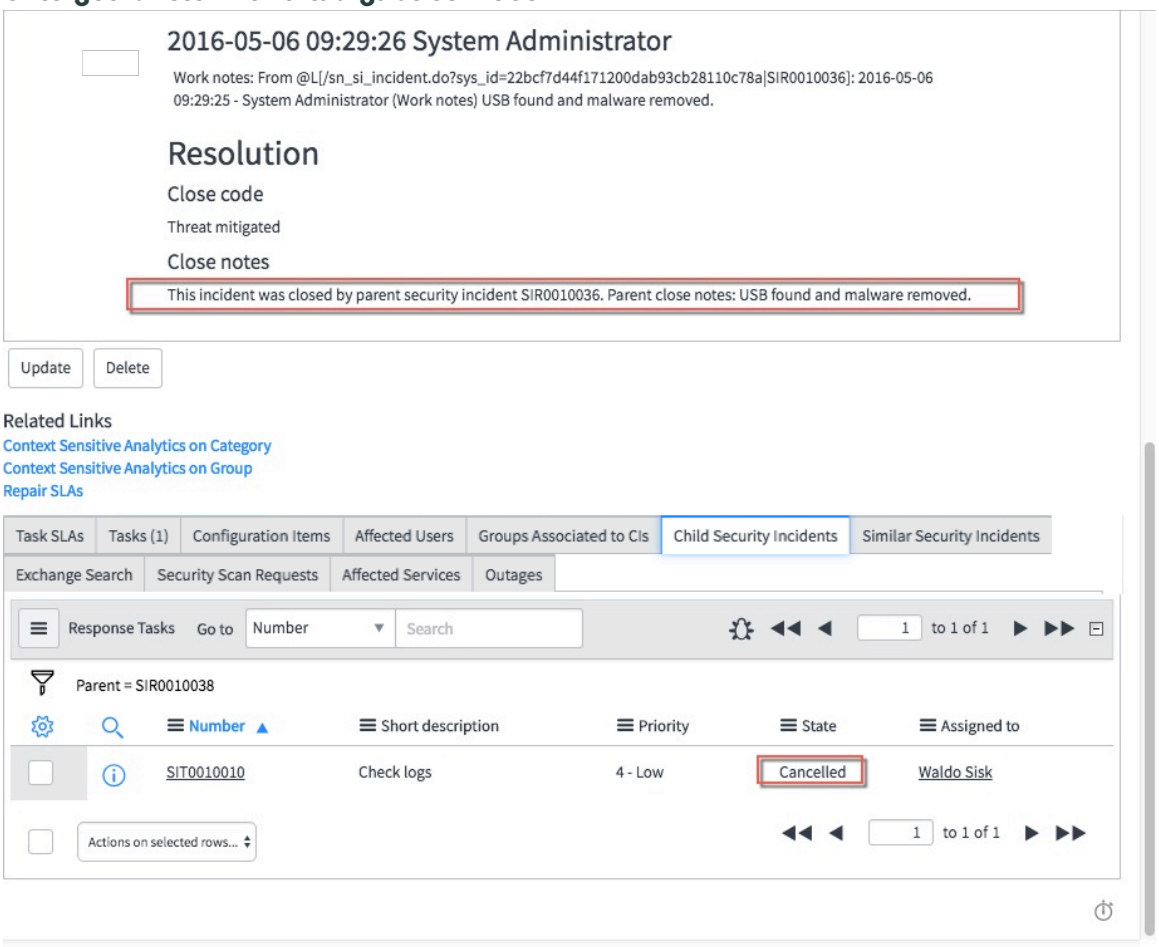
Wenn ein übergeordnetes Element geschlossen oder abgebrochen wird, werden alle aktiven untergeordneten Elemente ebenfalls geschlossen oder abgebrochen. Alle aktiven **Antwortaufgaben** für die untergeordneten Incidents werden abgebrochen. Wenn keine weiteren offenen **Aufgaben**vorhanden sind, wird der untergeordnete Incident geschlossen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beim Schließen wird der Abschluss im **Post Incident Interview** aufgezeichnet, und die Informationen auf der Registerkarte „Abschlussinformationen“ werden vom übergeordneten Element an die **untergeordneten** Elemente weitergegeben.

### Untergeordnete Antwortaufgabe schließen




### Zeigen Sie betroffene Elemente für einen Security Incident an

Sie können betroffene Elemente anzeigen, z. B. CIs, betroffene Benutzer und betroffene Services, die einem Security Incident zugeordnet sind.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie betroffene Elemente anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Betroffene Elemente** anzeigen.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

| Registerkarte | Beschreibung |
|---|---|
| Configuration Items | Betroffene Konfigurationselemente (CI). Nachdem die betroffenen CIs identifiziert wurden, können Sie betroffene Ressourcen manuell aus dieser zugehörigen Liste hinzufügen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Registerkarte | Beschreibung |
|---|---|
| Betroffene Benutzer | Nachdem betroffene Benutzer identifiziert wurden, können Sie betroffene Benutzer manuell aus dieser zugehörigen Liste hinzufügen. |
| Betroffene Services | Zeigen Sie Business Services an, die dem Security Incident zugeordnet sind, oder fügen Sie sie hinzu.<br>**Hinweis:**<br>Wenn ein betroffenes CI hinzugefügt wird, nachdem der Security Incident geöffnet wurde, empfiehlt es sich, mit der rechten Maustaste in den Formularheader zu klicken und **Betroffene Services aktualisieren**auszuwählen. |

**Hinweis:**
Wenn die Integrationsfunktion „ Security Operations Integration - Get Running Processes “ aktiv ist und Sie einem Security Incident ein CI hinzufügen, wird der Workflow „ Laufende Prozesse abrufen“ ausgeführt und eine Liste der laufenden Prozesse für das CI abgerufen.

Wenn die Integrationsfunktion „ Security Operations Integration - Isolate Host “ aktiv ist, können Sie ein oder mehrere CIs auswählen und deren Systemverbindungen zu anderen Geräten einschränken. Aktivieren Sie dazu die Kontrollkästchen für die CIs, und klicken Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen aufHost isolieren**.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

### Zeigen Sie zugehörige Elemente für einen Security Incident an

Sie können zugehörige Elemente anzeigen, z. B. ähnliche und untergeordnete Security Incidents, zugehörige Benutzer, Schwachstellengruppen und angreifbare Elemente, die einem Security Incident zugeordnet sind.

#### Vorbereitungen
Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie zugehörige Elemente anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Zugehörige Elemente** anzeigen.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

| Registerkarte | Beschreibung |
|---|---|
| Untergeordnete Security Incidents | Wählen Sie einen Aufgabendatensatz aus, der sich auf das Problem bezieht, das zur Erstellung dieses Security Incident geführt hat. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Registerkarte | Beschreibung |
|---|---|
| Ähnliche Security Incidents | Zeigen Sie alle anderen Security Incidents an, die mit einem dieser Datensätze für erkennbare Elemente verknüpft sind. |
| Zugehörige Configuration Items | Zeigt eine Liste von Security Incidents an, die Konfigurationselemente mit demselben erkennbaren Element wie dieser Security Incident enthalten. Diese Liste kann mithilfe der Filtergruppe „ **CI-Ausschlüsse** “ gefiltert werden. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp Ziel ausgeschlossen. |
| Zugehörige Benutzer | Zeigt eine Liste von Security Incidents an, die Benutzer mit denselben erkennbaren Elementen wie dieser Security Incident enthalten. Diese Liste kann mithilfe der Filtergruppe „ **Benutzerausschluss** “ gefiltert werden. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp Ziel ausgeschlossen. |
| Zugehörige Filtergruppe | Nachdem Konfigurationselemente identifiziert wurden, werden übereinstimmende CIs oder Filtergruppen automatisch hinzugefügt. |
| Schwachstellengruppen | Wenn Vulnerability Response aktiviert ist, können Sie die mit diesem Security Incident verknüpften Schwachstellengruppen anzeigen. |
| Angreifbare Elemente | Wenn Vulnerability Response aktiviert ist, können Sie angreifbare Elemente anzeigen, die diesem Security Incident zugeordnet sind. |
| Risiken | Wenn eines der wichtigsten Risikomanagement-Plugins (Policy and Compliance Management, Audit, Management oder Risk Management) aktiviert ist, können Sie mit dem Security Incident verbundene Risiken anzeigen oder hinzufügen.<br><br>Sie können diese zugehörige Liste aus dem Kontextmenü der Formularkopfzeile unter hinzufügen **Konfigurieren** > **Zugehörige Listen**. |
| Konfigurationselement-Ereignisse | Wenn Ereignismanagement aktiviert ist, können Sie Events anzeigen. |
| Konfigurationselementwarnungen | Wenn Ereignismanagement aktiviert ist, können Sie Warnungen anzeigen. |
| Kundenservicefälle | Wenn Kundenservice aktiviert ist, können Sie Fallinformationen von Kundenservice anzeigen. |

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie Ergänzungsdaten für einen Security Incident an

Sie können Ergänzungsdaten anzeigen, z. B. laufende Prozesse, laufende Services und Netzwerkstatistiken, die einem Security Incident zugeordnet sind.

## Vorbereitungen

Erforderliche Rolle: sn_si.basic

## Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Ergänzungsdaten anzeigen möchten.
2. **Klicken** Sie auf den zugehörigen Link Ergänzungsdaten anzeigen.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

**Hinweis:**
Rohdatendetails werden in einem Anhang zum Ergänzungsdatensatz gespeichert. Wenn sie die Feldgrenze überschreiten, werden die angezeigten Details abgeschnitten.

| Registerkarte | Beschreibung |
|---|---|
| Laufende Prozesse | Speichert die vom Workflow Security Incident Response **„Laufende Prozesse** abrufen“ erstellten Datensätze. |
| Laufende Services | Speichert die vom Workflow Security Incident Response **„Laufende Services** abrufen“ erstellten Datensätze. |
| Netzwerkstatistiken | Speichert die vom Workflow Security Incident Response **„Netzwerkstatistiken** abrufen“ erstellten Datensätze. |
| Domänensuchen | Wenn das Plugin WhoisXML-API-Integration aktiviert ist, speichert die Datensätze, die durch eine Whois-Suche erstellt wurden. |
| Firewall-Protokolle | Speichert Ergänzungsdaten aus Firewall-Protokollen, z. B. Palo Alto Network-Firewall-Protokolle |
| Informationen zum gefährdeten Benutzer | Speichert Accounts, die durch eine „Have I Been Pwned?“-Anfrage als gefährdet identifiziert wurden Suche. |

Hinweis: Auf der Registerkarte **Sicherheitsanreicherungsdaten** werden Rohdaten aus Security Incident Response -Workflows angezeigt, z. B. Abrufen von Netzwerkstatistiken oder Ausführen von Prozessen. Diese Registerkarte kann angezeigt werden, indem Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen klicken.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie Informationen zu Antwortaufgaben für einen Security Incident an

Sie können Informationen zu Antwortaufgaben anzeigen, z. B. Aufgaben-SLAs, Risikopunktzahl-Audits. und Ausfälle, die einem Security Incident zugeordnet sind.

#### Vorbereitungen
Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Antwortaufgaben anzeigen möchten.
2. Klicken Sie auf den zugehörigen Link **Antwortaufgaben anzeigen**.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

| Registerkarte | Beschreibung |
|---|---|
| Aufgaben | Zeigt Aufgaben an, die bereits für den Security Incident definiert wurden. Sie können eine Antwortaufgabe manuell erstellen oder Erstellen Sie einen anderen Aufgabentyp aus dieser zugehörigen Liste. |
| Antwortaufgaben | Zeigt Aktionen an, die als Reaktion auf den Security Incident ausgeführt werden sollen. |
| Aufgaben-SLAs | Zeigen Sie aktive Aufgaben-SLAs an, die für den Security Incident definiert wurden, oder fügen Sie sie hinzu. |
| Risikopunktzahl-Audits | Ein Audit-Datensatz für jede Instanz einer Risikopunktzahl, die geändert wird. |
| Ausfälle | Zeigen Sie neue Ausfalldatensätze an, die dem Security Incident zugeordnet sind, oder fügen Sie sie manuell hinzu. |
| E-Mail-Suche | Eine Liste von Datensätzen, die Suchkriterien zum Ausführen von Abfragen auf einem E-Mail-Server enthält, z. B. Microsoft® Exchange Server (basierend auf der installierten Implementierung), und die erhaltenen Ergebnisse speichert.<br>**Hinweis:**<br>Wenn Security Operations-Integration – E-Mail-Such- und Löschfunktion nicht aktiv ist, wird der zugehörige Link **E-Mail-Suche** nicht angezeigt. |

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

### Zeigen Sie zugehörige Events und Warnungen in Security Incidents an

Während an einem Security Incident gearbeitet wird, können Sie die Details der Events anzeigen. Für -Warnungen können Sie diese Warnungen anzeigen und bestätigen und bei Bedarf Incidents oder Security Incidents aus ihnen erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Das Support-Plugin „Security Incident Response Event Management“ muss aktiviert sein.

Erforderliche Rolle: si.sn_agent

### Prozedur

1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**) an.
2. Wenn die vom angezeigten Security Incident betroffenen Ressourcen in den letzten 24 Stunden Warnungen oder Events erhalten haben, wird eine oder beide der folgenden zugehörigen Listen angezeigt.
   - Security Incident-CI-Warnungen
   - Security Incident CI-Ereignisse
3. Klicken Sie auf die zugehörige Liste, die Sie anzeigen möchten.

| Zugehörige Liste | Beschreibung |
|---|---|
| Security Incident-CI-Warnungen | Sie können Details für Warnungen anzeigen, die in den letzten 24 Stunden eingegangen sind. Sie haben die Möglichkeit, auf **Bestätigen** zu klicken, um anzugeben, dass Sie über die Warnung Bescheid wissen und sie bearbeitet wird. Verwenden Sie **Schließen**, um anzugeben, dass die Warnung nicht wichtig ist. |
| Security Incident CI-Ereignisse | Sie können Details für Events anzeigen, die in den letzten 24 Stunden eingegangen sind. |

## Zeigen Sie die Zuordnung von Security Incidents zu Kundenservicefällen an

Security Incident Response wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem Kundenservice -Fall zuordnet. Sie können den Security Incident für die CS-Fall-Standardzuordnung anzeigen.

### Vorbereitungen

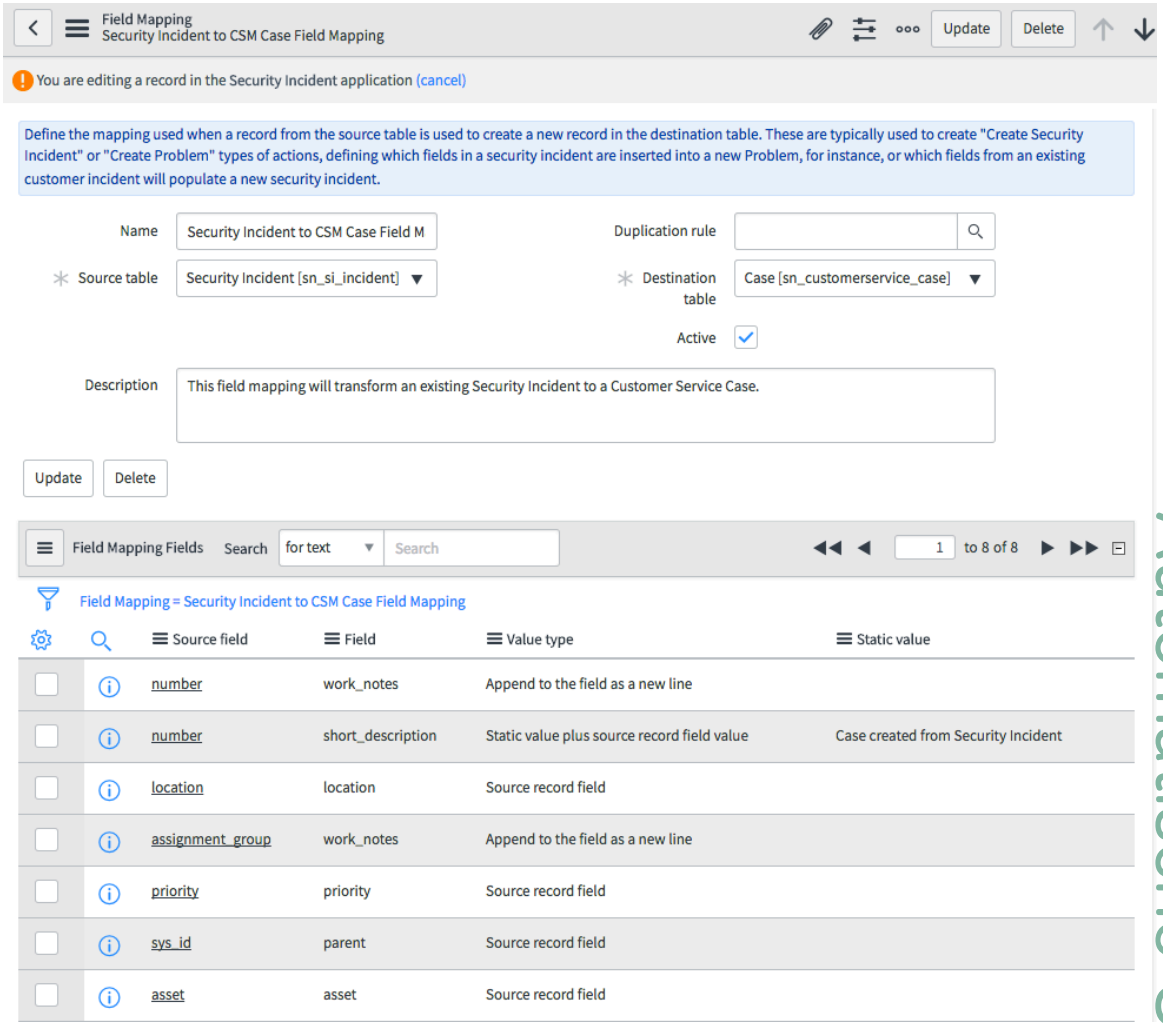
Erforderliche Rolle:sec_cmn.read

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**.
2. Klicken Sie **auf Zuordnung Security Incident zu CSM-Fallfeld**, um die Standardzuordnung anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Sie können die Zuordnung nach Bedarf bearbeiten.
4. Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren**.

### Zeigen Sie ein Security Incident Response-Runbook an

Runbooks geben Ihnen Zugriff auf Verfahren im Zusammenhang mit Aufgaben, an denen Sie arbeiten.

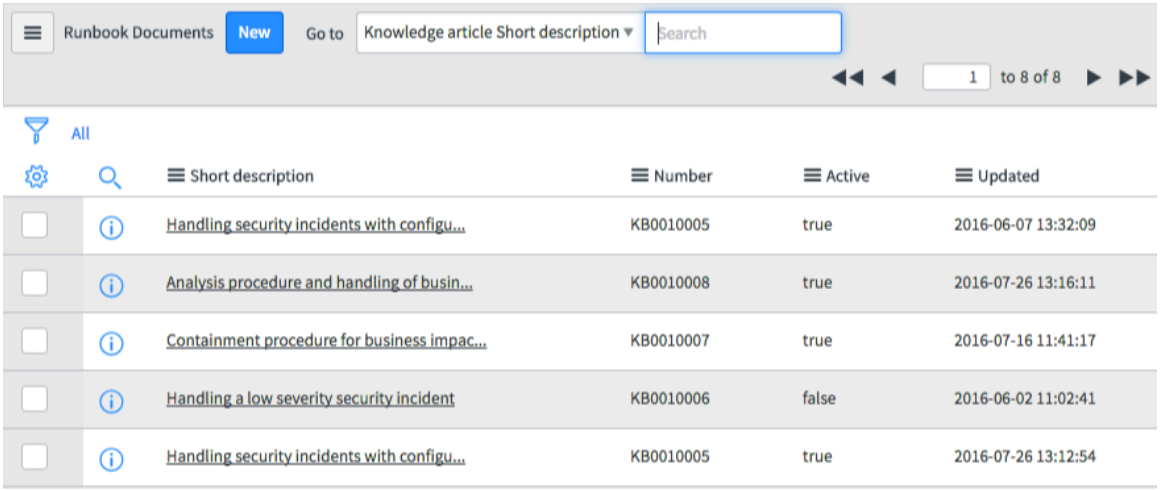
**Vorbereitungen**
Erforderliche Rolle: sn.si.knowledge_admin

**Prozedur**

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Zeigen Sie Runbook-Dokumente an**.
2. Wählen Sie ein Runbook aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Um ein Runbook zu erstellen, klicken Sie auf **Neu**.
   Weitere Informationen finden Sie unter Runbook erstellen.

### Identifizieren Sie alle Konfigurationselemente, die von einem Security Incident betroffen sind

Wenn Sie wissen, welche Ressource (Server, Desktop oder anderes Konfigurationselement) hinter einem Security Incident steht, und zugehörige Ressourcen und Geschäftsservices identifizieren möchten, die betroffen sein können, können Sie die Business Service Management-Zuordnung (BSM) verwenden.

#### Vorbereitungen

Erforderliche Rolle: admin oder sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Die BSM-Zuordnung zeigt die vorgelagerten und nachgelagerten Abhängigkeiten für ein ausgewähltes Stamm-CI an.

Es gibt zwei Methoden, mit denen Sie die BSM-Zuordnung für ein CI anzeigen können:

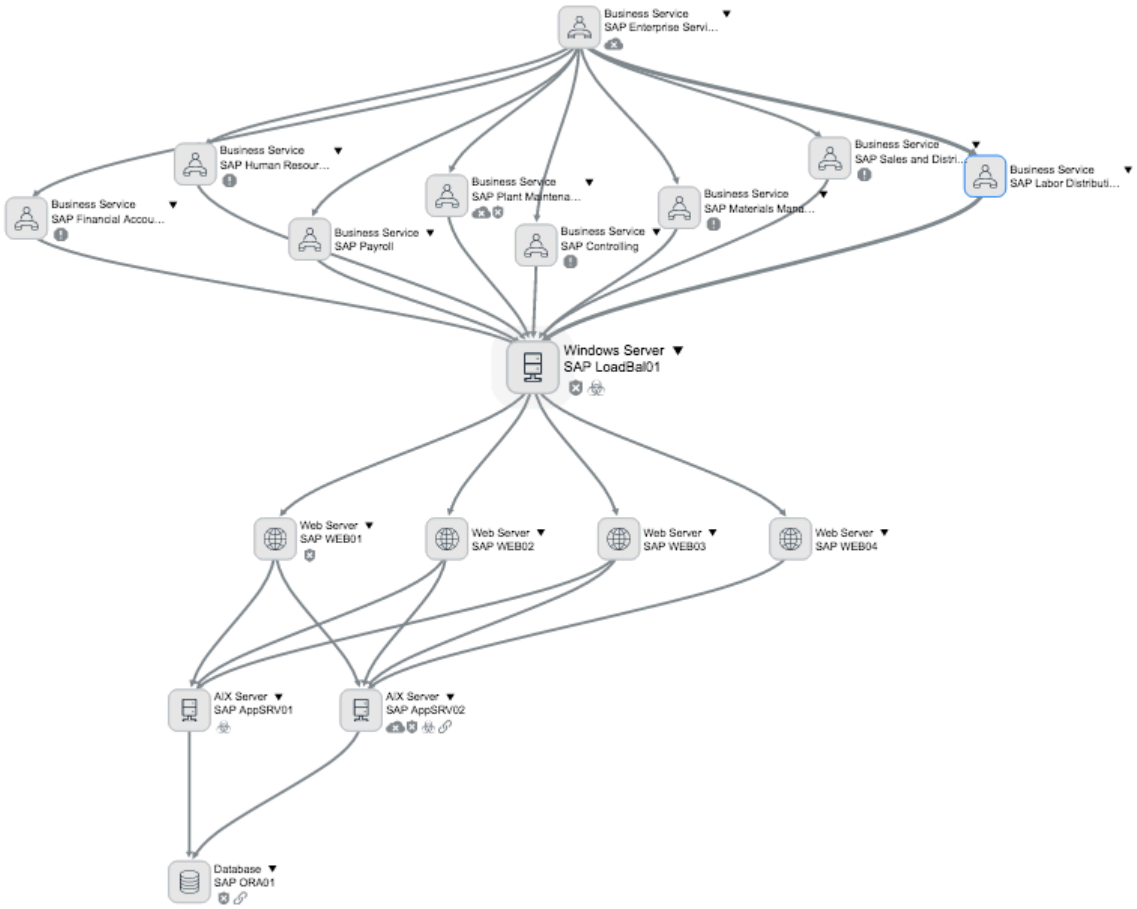
- Wenn Sie CIs aus dem Kontext einer Aufgabe anzeigen möchten, zeigen Sie sie im Security Incident-Formular an.
- Wenn Sie CIs nicht aus der Aufgabenansicht anzeigen möchten, zeigen Sie sie in der Navigationsleiste an.

#### Prozedur

1. Füllen Sie im Security Incident-Formular das Feld **Konfigurationselement** aus, und klicken Sie auf das BSM-Zuordnungssymbol ( ).
   Der Bildschirm „BSM-Zuordnung“ zeigt die Zuordnung für den letzten Incident, auf den Sie in Incident Management zugegriffen haben, oder den letzten Security Incident, auf den Sie in Security Incident Management zugegriffen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




2. Klicken Sie auf die Symbole neben einem Konfigurationselement, um verschiedene Arten von Details zur Ressource (Server, Desktop oder anderes CI) anzuzeigen.

   Klicken Sie beispielsweise auf das Warnungssymbol ( ⚠ ), um die mit dem CI verknüpften Warnungen anzuzeigen.

   **Hinweis:**
   Um eine Liste aller verfügbaren Symbole anzuzeigen, klicken Sie über der BSM-Zuordnung auf **Filter**, und erweitern Sie **Filteraufgabentypen**.

3. Um die Zuordnung in verschiedenen Konfigurationen anzuordnen, wählen Sie eines der über der Zuordnung aufgeführten Formate aus (**Vertikal**, **Horizontal**, **Radius**), oder klicken Sie auf **Filter**, um die Zuordnung zur einfacheren Anzeige zu filtern.

4. Wenn Sie die BSM-Zuordnung über das Security Incident-Formular geöffnet haben, können Sie dem Security Incident ein abhängiges CI hinzufügen, indem Sie mit der rechten Maustaste auf das CI klicken und **Betroffene CIs**hinzufügen auswählen.
   Sie können auch mehrere CIs gleichzeitig hinzufügen. Ziehen Sie ein Kästchen um die CIs, die Sie hinzufügen möchten, klicken Sie mit der rechten Maustaste in das Kästchen, und wählen **Sie Betroffene CIs**hinzufügen aus.
   Die CIs werden der zugehörigen Liste „Betroffene CIs“ des Security Incident hinzugefügt.

## Berechnen Sie den Schweregrad eines Security Incident

Sie können den Schweregrad eines Security Incident mit vordefinierten Rechnern berechnen.

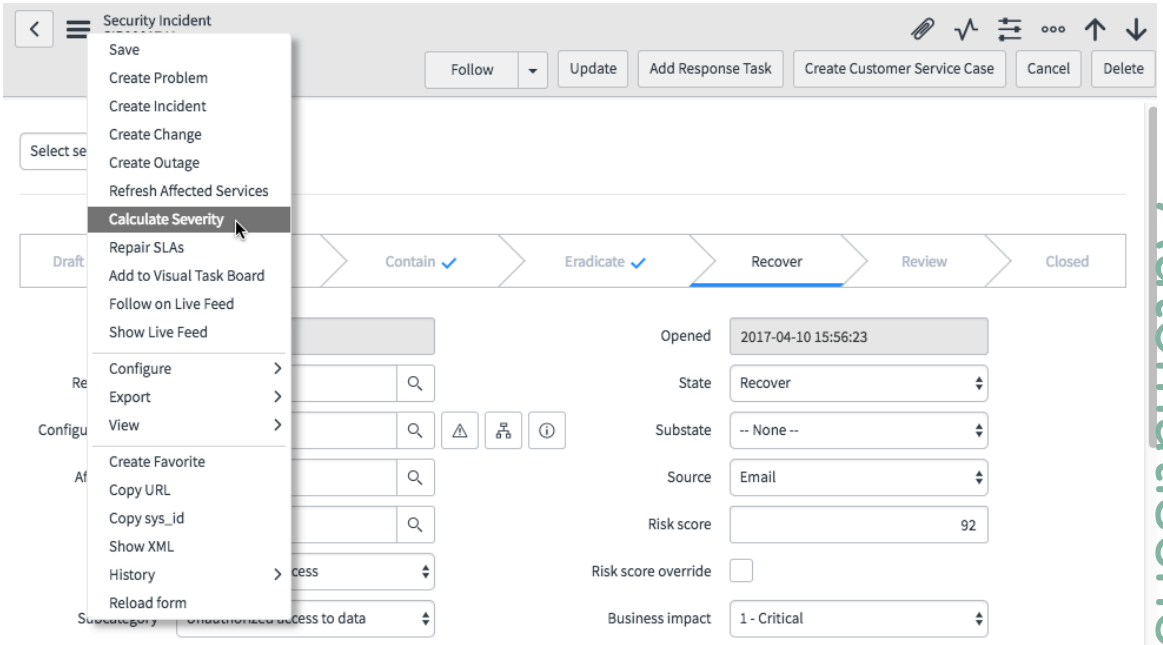
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.basic

### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie den Schweregrad berechnen möchten.
2. Klicken Sie auf das Kontextmenü der Formularkopfzeile, und wählen Sie **Schweregrad berechnen**aus:




Der Schweregrad wird basierend auf den vordefinierten Regeln für Basisrechner berechnet. Weitere Informationen finden Sie unter Security Incident-Rechner verstehen.

## Suchen und löschen Sie Phishing-E-Mails

Das Löschen von Phishing-E-Mails kann dazu beitragen, das Risiko eines bestimmten Angriffs in einer Organisation zu reduzieren. Sie können Phishing-E-Mails auf Ihrem E-Mail-Server verwalten, indem Sie sie suchen, Genehmigungen erteilen und löschen.

### Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.cap_email_read

Sie können ermitteln, wie viele Benutzer Ziel eines Phishing-Angriffs waren, indem Sie einen E-Mail-Datensatz abfragen, der einem Security Incident zugeordnet ist.

Unterstützte Software:

- Microsoft® Exchange Server 2010

Einschränkung: Wenn Sie den E-Mail-Text durchsuchen, können Sie maximal 1.500 Postfächer durchsuchen.

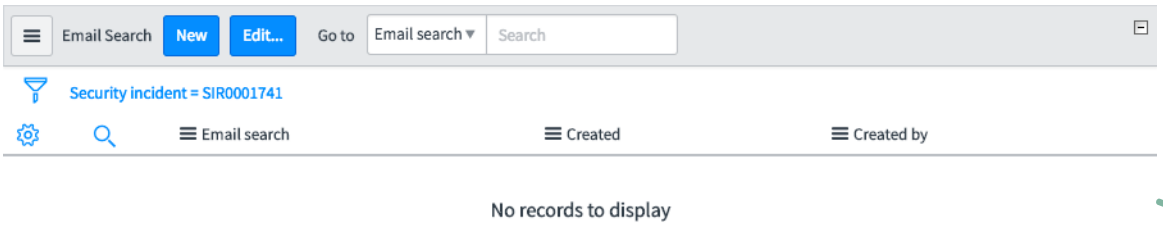
### Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird von Integration von Sicherheitsvorgängen – Workflow „E-Mails suchen und löschen“. verwendet, um eine Abfrage für Ihren E-Mail-Server auszuführen. Abhängig von den von Ihnen ausgewählten Suchkriterien identifiziert die Suche alle E-Mails innerhalb eines Phishing-Angriffs und gibt die Gesamtzahl der betroffenen E-Mails oder Details aus den betroffenen E-Mails zurück.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

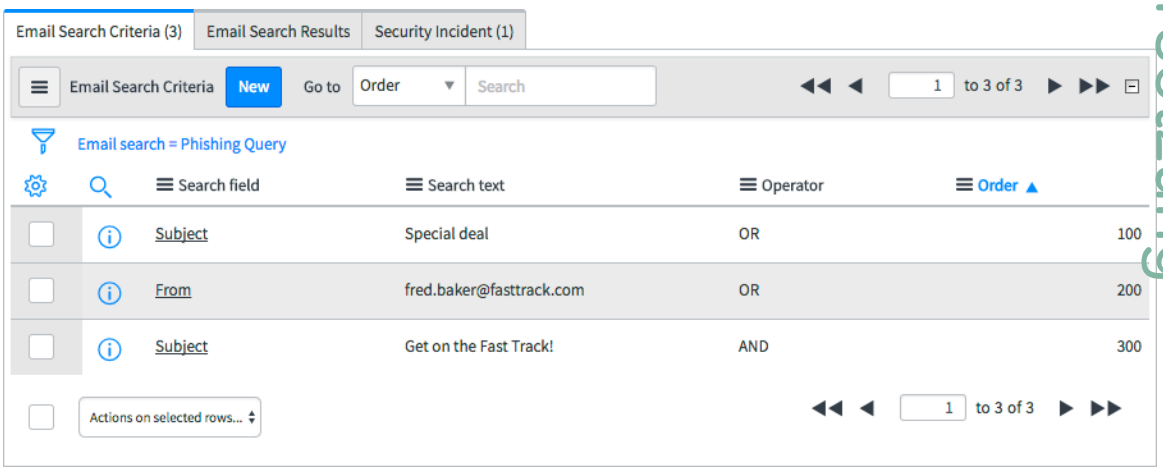
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Wählen Sie einen Security Incident aus.
3. Wenn die zugehörige Liste **E-Mail-Suche** nicht sichtbar ist, klicken Sie auf den zugehörigen Link **Alle zugehörigen Links** anzeigen.
4. Klicken Sie auf die zugehörige Liste E- **Mail-Suche**.




5. Klicken Sie auf **Neu**.
6. Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Suchabfrage |
| Abfrage von Kriterium | Eine Vorschau der Abfrage, die auf dem E-Mail-Server ausgeführt wird. Wird aus allen zugeordneten aktiven Suchkriteriendatensätzen generiert. |
| Beschreibung | Beschreiben Sie, wonach die Suchabfrage sucht. |

7. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.




8. Klicken Sie auf die Registerkarte E- **Mail** -Suchkriterien und dann auf **Neu**.
9. Füllen Sie die Felder aus, oder bearbeiten Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| E-Mail-Suche | Zeigt den Namen der E-Mail-Suche an. Sie können sie bei Bedarf ändern. |
| Suchfeld | Feld, nach dem auf dem E-Mail-Server gesucht werden soll.<br><br>Das Suchfeld bietet die folgenden Auswahlmöglichkeiten:<br><br>**Betreff**<br><br>Dieses Kriterium sucht nach E-Mails, die den im Feld **Suchtext** angegebenen Betreffzeilentext enthalten. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail zurückgegeben, einschließlich Empfangsdatum der E-Mail, E-Mail-Lesestatus, Empfänger und Nachrichten-ID.<br><br>**Von**<br><br>Dieses Kriterium sucht nach E-Mails, die die vollständige E-Mail-Adresse des Absenders enthalten (z. B. jane.doe@abc.com), die im Feld **Suchtext** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail zurückgegeben, einschließlich Empfangsdatum der E-Mail, E-Mail-Lesestatus, Empfänger und Nachrichten-ID.<br><br>**Hinweis:**<br>Sie können die Felder „ **Von** “ und **„Empfänger** “ nicht in derselben Abfrage verwenden.<br><br>**Empfänger**<br><br>Dieses Kriterium sucht nach E-Mails, die die vollständige E-Mail-Adresse des Empfängers enthalten (z. B. john.doe@abc.com), die im Feld **Suchtext** angegeben ist. Außerdem wird nach E-Mails in den Feldern „An“, „Cc“ und „Bcc“ gesucht. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail zurückgegeben, |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

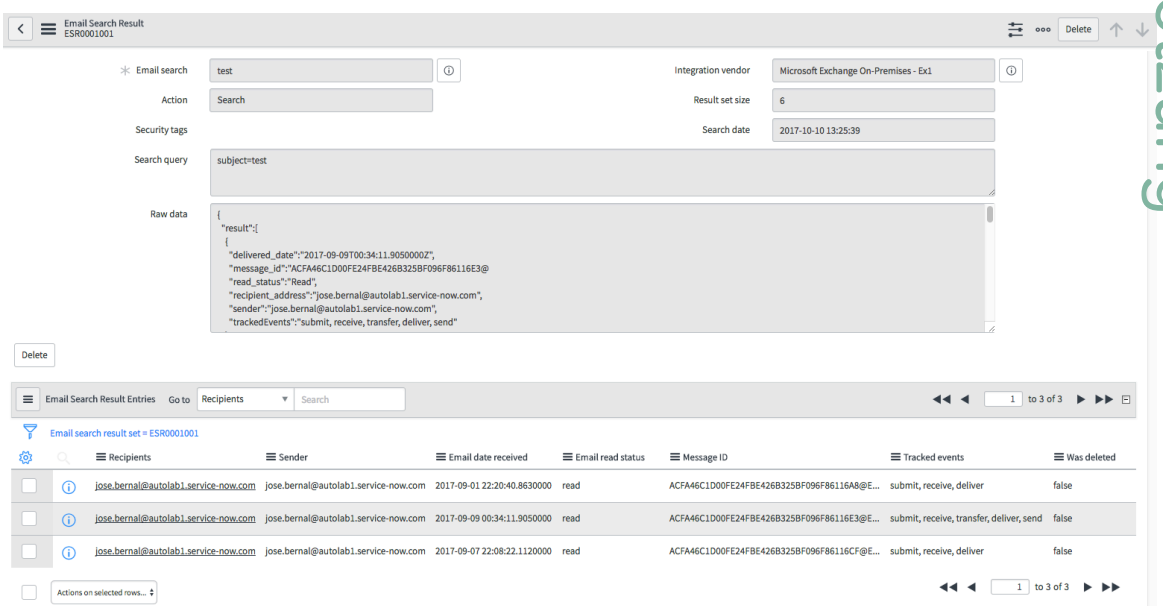
| Feld | Beschreibung |
| --- | --- |
| | einschließlich Empfangsdatum der E-Mail, E-Mail-Lesestatus, Empfänger und Nachrichten-ID.<br><br>**Hinweis:**<br>Sie können die Felder „ **Von** “ und **„Empfänger** “ nicht in derselben Abfrage verwenden.<br><br>**Textkörper**<br><br>Dieses Kriterium sucht nach E-Mails, die den im Feld Suchtext angegebenen **Text** enthalten. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.<br><br>**Hinweis:**<br>Wenn Sie den E-Mail-Text durchsuchen, können Sie maximal 1.500 Postfächer durchsuchen.<br><br>**Cc:**<br><br>Dieses Kriterium sucht nach E-Mails, die die vollständige Cc-E-Mail-Adresse (z. B. jane.doe@abc.com) enthalten, die im Feld **Suchtext** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.<br><br>**Bcc:**<br><br>Dieses Kriterium sucht nach E-Mails, die die vollständige BCC-E-Mail-Adresse (z. B. jane.doe@abc.com) enthalten, die im Feld **Suchtext** angegeben ist. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.<br><br>**Anhang**<br><br>Dieses Kriterium sucht nach E-Mails, die entweder den Namen der **Anhangdatei** oder den im Feld Suchtext angegebenen Inhalt des Anhangs enthalten. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Für die Suche im Inhalt von Anhängen werden nur Nur-Text-Anhänge unterstützt.<br><br>**Aufbewahrungsrichtlinie**<br><br>Dieses Kriterium sucht nach E-Mails, die Aufbewahrungsrichtliniennummern enthalten, die im Feld **Suchtext** angegeben sind. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. |
| Aktiv | Aktivieren Sie diese Checkbox, um diese E-Mail-Suchabfrage zu aktivieren. |
| Operator | Mögliche Werte sind AND und OR. Sie können definieren, wie Suchkriterien kombiniert werden, um auf dem E-Mail-Server ausgeführt zu werden. |
| Bestellung | Die Reihenfolge, in der die Suchabfrage anhand der Suchkriterien erstellt wird. |
| Suchtext | Der zu suchende Text. Einfache Anführungszeichen, doppelte Anführungszeichen und Doppelpunkte werden nicht unterstützt. |

10. Klicken Sie auf **Absenden**.
11. Wiederholen Sie diese Schritte nach Bedarf, um zusätzliche Suchkriterien zu definieren.
12. Sie können die Ergebnisse der Suche anzeigen, indem Sie auf die Registerkarte E- **Mail-Suchergebnisse** klicken.

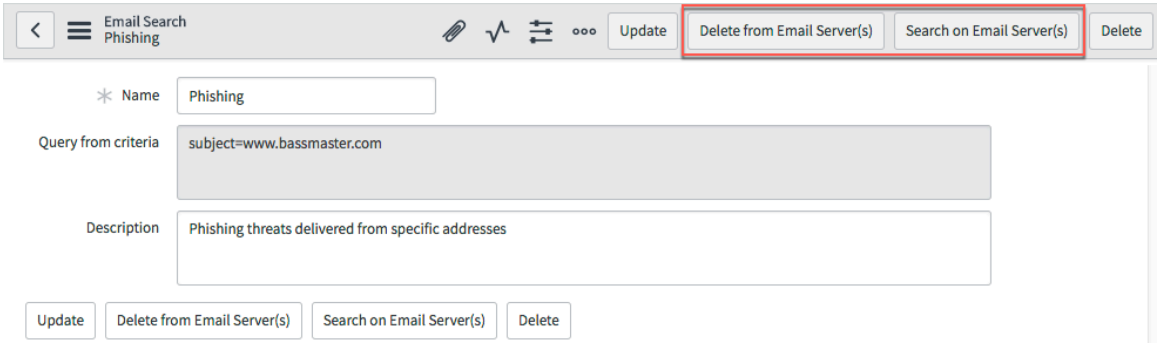



Jede Zeile im Formular „E-Mail-Suchergebniseinträge“ stellt eine separate E-Mail dar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Nachdem Sie einen Suchkriteriendatensatz erstellt haben, werden im Formular „E-Mail-Suche“ zwei Schaltflächen angezeigt: **„Von E-Mail-Servern löschen“** und „ **Auf E-Mail-Servern suchen“**.




14. Um auf dem ausgewählten Server nach E-Mails zu suchen, die den von Ihnen definierten Suchkriterien entsprechen, klicken Sie **auf E-Mail-Server**durchsuchen.

## Erstellen Sie einen Wissensartikel zu Security Incidents

Während Sie mit Security Incidents und Reaktionsaufgaben arbeiten, werden Wissensartikel automatisch angezeigt, um relevante Informationen zur Aufgabe bereitzustellen, die Sie ausführen. Ihre Organisation kann Artikel in der Knowledge Base für Security Incidents erstellen und verwalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.knowledge_admin

### Warum und wann dieser Vorgang ausgeführt wird

Wissensartikel enthalten Sicherheitsinformationen, dokumentieren die Arten von Cyberbedrohungen, denen Ihr Unternehmen ausgesetzt ist, und bieten Antworten und Antworten auf diese Bedrohungen.
Bei Bedarf können Sie Wissensartikel in Runbooks organisieren, die Zuordnungen zwischen den Artikeln und bestimmten Aufgaben erstellen. Sie können beispielsweise ein Runbook mit Bedingungen konfigurieren, die bewirken, dass ein Knowledge Base-Artikel über Phishing angezeigt wird, wenn Sie einen Security Incident für einen Phishing-Angriff erstellen. Weitere Informationen finden Sie unter Erstellen Sie ein Security Incident Response-Runbook.

Wissensartikel in Runbooks können auch bestimmten Aufgaben in einem Playbook zugeordnet werden. Weitere Informationen finden Sie unter Verknüpfen Sie einen Wissensartikel mit einer Playbook-Aufgabe.

Wissensartikel haben unter anderem folgende Vorteile.

- Mitarbeiter haben eine Informationsquelle, die sich leicht durchsuchen lässt.
- Informationen können auf dem neuesten Stand gehalten werden, da Wissensartikel einen definierten Lebenszyklus haben: Erstellen, Überprüfen und Aktualisieren, Veröffentlichen und Außerkraftsetzen.
- Wenn Sie eine Sicherheitsanforderung, einen Incident oder eine Antwortaufgabe manuell erstellen, wird während der Eingabe der Kurzbeschreibung eine Liste der relevanten Artikel angezeigt.

**Hinweis:**
Es ist wichtig, jeder Knowledge Base für Security Incidents einen Knowledge Manager zuzuweisen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**.
2. Klicken Sie auf das Symbol Artikel erstellen ( ).
3. Füllen Sie die entsprechenden Felder im Formular aus.

### Wissensformular

| Feld | Beschreibung |
|---|---|
| Nummer | Die automatisch generierte KB-Nummer. |
| Wissensdatenbank | Die für diesen Artikel ausgewählte Knowledge Base. |
| Kategorie | Die Kategorie für diesen Artikel. |
| Veröffentlicht | Wann dieser Wissensartikel veröffentlicht wurde. Dieser Wert wird festgelegt, wenn der Artikel erstellt wird, und aktualisiert, wenn der Artikel veröffentlicht wird. |
| Gültig bis | Wann dieser Wissensartikel abläuft. Dieser Artikel wird nach diesem Datum nicht in Suchergebnissen angezeigt, oder wenn kein Datum ausgewählt ist. |
| Bild | Ein Bild, das bei der Suche im veralteten Wissensportal neben dem Artikel angezeigt wird. |
| Workflow | [Schreibgeschützt] Der Veröffentlichungsstatus des Artikels, z. B. Entwurf oder Veröffentlicht. Wenn Beim Einfügen eines neuen Artikels aus einem vorhandenen Artikel wird der Status des neuen Artikels auf **Entwurf**zurückgesetzt. |
| Quelle | Die Aufgabe, für die dieser Knowledge Base-Artikel erstellt wurde, als Reaktion darauf, falls vorhanden. Dieses Feld wird automatisch festgelegt, wenn Sie den Knowledge Base-Artikel aus einem Aufgabendatensatz erstellen. |
| Link zu Anhang | Kontrollkästchen zum automatischen Herunterladen einer angehängten Datei, wenn ein Benutzer auf den Artikel zugreift, anstatt die Artikelansicht zu öffnen. Fügen Sie dem Artikel einen Anhang hinzu, um diese Option zu verwenden. |
| Anhänge anzeigen | Kontrollkästchen zum Anzeigen von Anlagen für Benutzer, die diesen Knowledge Base-Artikel anzeigen. Anhänge werden unter dem Artikeltext angezeigt. Fügen Sie dem Artikel einen oder mehrere Anhänge hinzu, um diese Option zu verwenden. |
| Kurzbeschreibung | Der Titel des Artikels. Dieser Titel erscheint beim Durchsuchen der Knowledge Base-Artikel oben im Artikel. |
| Text | Inhalt für den Artikel. Verwenden Sie den WYSIWYG-HTML-Editor, um Inhalte zu erstellen. Beim Durchsuchen von Knowledge Base-Artikeln wird eine Vorschau des Inhalts angezeigt. |

**Hinweis:**
Wenn Sie einen Wissensartikel erstellen, der einer Playbook-Aufgabe zugeordnetwerden soll, legen Sie das Feld **Knowledge Base** auf **Security Incident Response Runbook fest**.

4. Klicken **einreichen** um den Artikel zu erstellen.

## Nächste Maßnahme

Alle zusätzlichen Schritte, die zum Veröffentlichen des Artikels erforderlich sind, z. B. Genehmigungen, hängen vom ab Veröffentlichungs-Workflow für die Knowledge Base.

### Zugehörige Informationen

Erstellen Sie ein Security Incident Response-Runbook

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eskalieren Sie einen Security Incident

Wenn für einen Security Incident ein Eskalationspfad vorhanden ist, ist die Schaltfläche Eskalieren im Header des Security Incident verfügbar.

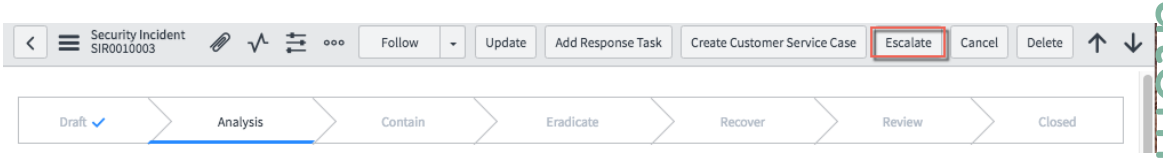
### Vorbereitungen

Erforderliche Rolle: sn_si.admin

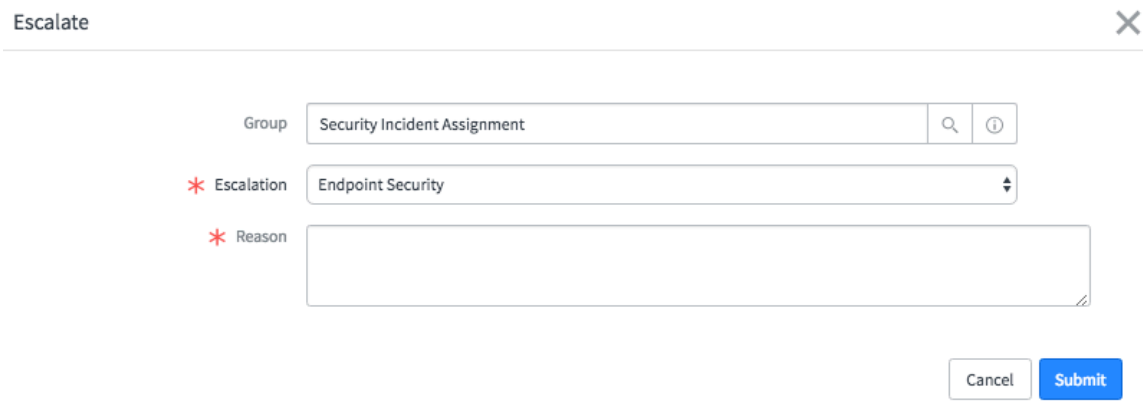
Sie müssen eine Eskalationsgruppe erstellt haben, damit diese Schaltfläche angezeigt wird. Weitere Informationen finden Sie unter Erstellen Sie eine Security Operations benutzerdefinierte Eskalationsgruppe.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Öffnen Sie den Incident, den Sie eskalieren möchten.
3. Klicken Sie auf die Schaltfläche **Eskalieren**.




4. Wählen Sie eine Eskalationsgruppe aus.
5. Geben Sie einen Grund für die Eskalation ein.




6. Klicken Sie auf **Absenden**.
   Aktualisiert **„Zuweisungsgruppe“** und „ **Zugewiesen an** “ für den Security Incident

## Verwalten von Aktivitäten nach Incidents

Basierend auf den Anforderungen Ihres Unternehmens ist häufig eine Überprüfung der Herkunft und Behandlung von Security Incidents erforderlich.

Die Überprüfung nach Incident -Funktionalität in ServiceNow bietet viele Tools zum Automatisieren, Nachverfolgen, Überwachen und Vereinfachen dieses Prozesses.

In diesem Abschnitt wird Folgendes beschrieben:

- Weisen Sie Rollen für die Überprüfung nach Incidents zu
- Konfigurieren Sie eine Bewertungsauslöserbedingung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie eine fragebogenbasierte Überprüfung nach Incidents durch
- Erstellen Sie PIR-Zuweisungsregeln
- Überprüfungsbericht nach Incident

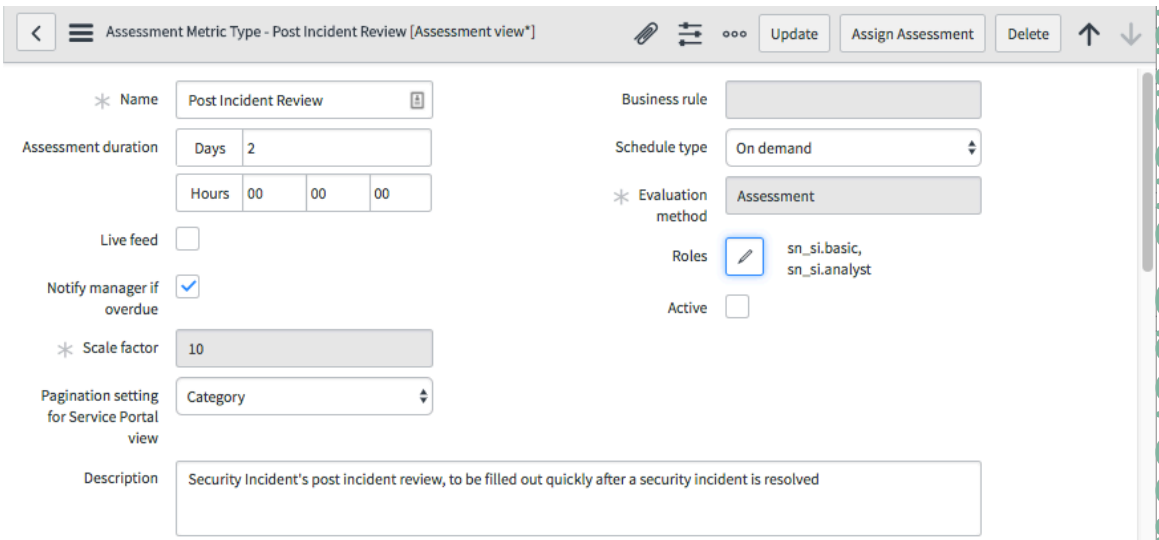
### Weisen Sie Rollen für die Überprüfung nach Incidents zu

Sie können Fragen an bestimmte vordefinierte Gruppen richten, indem Sie Rollen den PIR-Kategorien (Post Incident Review) zuweisen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren zu **Alle** > **Bewertungen** > **Metrikdefinition** > **Typen**.
2. Suchen Sie in der Spalte **Typen** nach einem Datensatz **Überprüfung nach Incident**.
3. Öffnen Sie den Datensatz.
4. Weisen Sie eine oder mehrere Rollen für diese Fragenkategorie zu.




5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Benutzeradministration** > **Anwender**.
7. Wählen Sie einen Benutzer aus
8. Fügen Sie dem Benutzerdatensatz eine oder mehrere Metriktyprollen hinzu.

> **Hinweis:**
> Die Rollen müssen den Rollen entsprechen, die in der Kategorie „Überprüfung nach Incident“ zugewiesen sind.

### Überprüfungsbericht nach Incident

Mit der Funktion „Post Incident Review“ (PIR) können Sie die Überprüfungsberichte nach Incidents über die Registerkarte „Post Incident Review“ einrichten und herunterladen.

Der Sicherheitsadministrator kann die Berichtsvorlagen erstellen und konfigurieren und diese Vorlagen mithilfe der Berichtskonfiguration dem Security Incident zuordnen. Ein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsanalyst kann den Bericht anzeigen oder herunterladen, nachdem der Security Incident gelöst und der Status auf den Status Überprüfen aktualisiert wurde.

Ein PDF-Bericht wird generiert und an den Security Incident angehängt, wenn der Incident nach erfolgreicher Konfiguration in den Status „Geschlossen“ verschoben wird.

**Hinweis:**
Die Berichtsfunktion ist ab Orlando Patch9 anwendbar und wird unterstützt.

Um Ihre Überprüfungsberichte nach Incidents anzupassen, müssen Sie die folgende Konfiguration vornehmen.

1. **Berichtsvorlagen**: Passen Sie die folgenden Berichtsvorlagenfunktionen an und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen:
   a. Zeitleiste
   b. Branding
   c. Vorlagenskripts
2. **Berichtkonfiguration**

In diesem Abschnitt wird das Konfigurationsverfahren beschrieben:

## Berichtsvorlagen

Verwenden Sie den Abschnitt „Berichtsvorlagen“, um primäre und zusätzliche Berichtsvorlagen zu erstellen, die auf die Security Incidents angewendet werden, um den Bericht zur Überprüfung nach Incidents zu generieren. Sie können den Bericht entsprechend Ihren Anforderungen formatieren und konfigurieren. Die Vorlagen helfen Ihnen auch, die Bewertungsdetails in die Vorlage aufzunehmen.

Im Folgenden sind einige optionale Schritte aufgeführt, die beim Erstellen der Vorlage ausgeführt werden können:

1. Branding-Informationen konfigurieren
2. Seitengröße und Seitenrand einrichten.
3. Hinzufügen von Security Incident-bezogenen Feldern (sowohl benutzerdefiniert als auch standardmäßig).
4. Verwendung der folgenden vordefinierten benutzerdefinierten Token:
   a. *$sessionUser*: gibt den angemeldeten Benutzernamen zurück
   b. *$date*: Gibt das aktuelle Datum zurück
   c. *$if_not_null_start#&#$if_not_null_end*Wenn diese Tags für Felder verwendet werden, werden die Tags nur angezeigt, wenn der Wert vorhanden ist. Beispiel:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Einschließlich der zugehörigen Listendaten mithilfe der Vorlagenskripts. Weitere Informationen finden Sie im folgenden Abschnitt über **Vorlagenskripts**.
6. Einschließlich der Zeitleisteninformationen mithilfe der Zeitleistenfilter. Weitere Informationen finden Sie im folgenden Abschnitt zur **Zeitleiste**.
7. Verwalten und Formatieren des Vorlageninhalts wie Anhänge, Tabellen und Bilder.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die erweiterten Funktionen der Symbolleiste für Berichtsvorlagen sind erst ab Release Paris verfügbar.

Wichtige Punkte für Berichtsvorlagen:

1. Die an die Berichtsvorlage angehängten Bilder werden im Bericht „Überprüfung nach Incident“ nur angezeigt, wenn sie in der Tabelle „sys_attachment“ enthalten sind.

   **Hinweis:**
   Bilder, die aus der Tabelle „db_image“ ausgewählt wurden, werden nicht im Überprüfungsbericht nach Incident angezeigt.

2. Videos werden im Überprüfungsbericht nach Incident nicht unterstützt.
3. Die URLs in der PDF-Datei können nicht angeklickt werden. Zum Aktivieren der nicht anklickbaren URLs (.) wird als (Punkt) bezeichnet.
4. Der Bericht wird nicht generiert, wenn die Größe der Berichtsvorlage 50 MB überschreitet.
5. Die für den Inhalt der Berichtsvorlage ausgewählte Schriftartfamilie wird nicht auf die PDF-Datei angewendet, wenn sie nicht vom PDF-Generator unterstützt wird.

   **Hinweis:**
   Wenn die entsprechende Schriftart nicht vorhanden ist, identifiziert der PDF-Generator die nächstliegende Schriftart und generiert dann die PDF-Datei.

6. Wenn Sie höhere Seitenrandwerte angeben, ist das Generieren eines Überprüfungsberichts nach Incidents fehlgeschlagen. Beispiel: Oberer und unterer Rand > 450 und linker und rechter Rand > 450.
7. Wenn ein großer Text in der Berichtsvorlage ohne Leerzeichen enthalten ist, wird der Text möglicherweise abgeschnitten. Zeigen Sie eine Vorschau des Texts an, und ändern Sie ihn entsprechend.

Der Sicherheitsadministrator kann eine Vorschau des Berichts mithilfe der Schaltfläche **Vorschaubericht anzeigen**, die auf der Seite „Berichtsvorlage“ verfügbar ist.

**Hinweis:**

**Wählen Sie einen Security Incident aus, um eine Vorschau eines Berichts mit dieser Vorlagenoption** anzuzeigen, und klicken Sie auf **Berichtvorschau**.

## Branding

Sie können den Namen der Branding-Vorlage, das Kopf- und Fußzeilenbild, den Kopf- und Fußzeilentext hinzufügen, Seitenzahlen generieren und den Branding-Datensatz nach der Erstellung in die Berichtsvorlage einfügen.

Es folgt ein Beispiel für ein Branding-Berichtsformat:

Wichtige Punkte für das Branding von Berichtsvorlagen:

1. Die maximal zulässige Größe für Kopf- und Fußzeilenbilder beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
2. Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wenn sich der Text des Fußzeilenbilds und der Berichtsinhalt während der Vorschau überschneiden, müssen Sie Änderungen am Branding-Datensatz vornehmen.

**b.** Wenn der Fußzeilentext einen URL-Link enthält, kann er sich mit dem Fußzeilenbild überschneiden. Zeigen Sie eine Vorschau an, und korrigieren Sie sie nach Bedarf.

### Zeitleiste

Mit der Zeitleistenkonfiguration können Sie die Zeitleistenfilter nach Bedarf erstellen und ändern. Sie können die Aktivitätstypen filtern, die in den Bericht aufgenommen werden sollen, konfigurieren, ob die untergeordneten Aufgaben in den Bericht aufgenommen oder ausgeschlossen werden sollen, und konfigurieren, ob die Bilder in den Bericht aufgenommen oder ausgeschlossen werden sollen.

Wenn Sie eine Zeitleistenkonfiguration verwenden und ausfüllen möchten, müssen Sie das Tag wie unten beschrieben hinzufügen: `${timeline:timeline name}`. Im Setup werden zwei Beispiel-Zeitleistenkonfigurationen bereitgestellt, die in der Phishing-Berichtsvorlage und der Standardberichtsvorlage verwendet werden. Sie können die Konfigurationen ändern und wiederverwenden.

### Vorlagenskripts

Verwenden Sie die Vorlagenskripts, um die zugehörigen Listendaten, den Datums- und Zeitstempel und alle anderen Daten einzubeziehen, die nicht direkt Dot-Walk-fähig sind. Nachfolgend sehen Sie ein Beispiel:

**Erstellen Sie ein Vorlagenskript, um die zugehörige Liste in der Berichtsvorlage anzuzeigen**:

1. Um die zugehörigen Listendaten vorzubereiten, rufen Sie die Methode PostIncidentReportUtils.fetchRelatedListDataForReport auf.
2. Um die Schritt-1-Daten im Tabellenformat und -stil darzustellen, rufen Sie die Methode ReportTemplateUtil.construTablefunction auf.

Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag als `${template_script:script name}`hinzufügen.

Im Folgenden finden Sie einige Beispielvorlagenskripts zum Konfigurieren und Ändern Ihrer Nachfolgeberichte zu Incidents.
Berichtsvorlagenskripts – wichtige Punkte:

1. Wenn eine zugehörige Liste mit mehr als 5 Spalten hinzugefügt wird, werden die Tabellendaten während der PDF-Erstellung abgeschnitten. Die Mindestbreite jeder Spalte ist auf 124 Pixel festgelegt.
2. Wenn ein Vorlagenskript den Inhalt in der Berichtsvorlage aufgrund technischer Probleme nicht laden kann, wird im Bericht die Fehlermeldung „Fehler beim Auswerten des Vorlagenskripts“ angezeigt, und der Sicherheitsadministrator muss die Richtigkeit des Skripts bewerten, um das Problem zu beheben Problem.
3. si_assessments: Standardmäßig werden dem Bericht alle Bewertungskategorien hinzugefügt. Der Sicherheitsadministrator kann die Daten filtern, indem er das Vorlagenskript nach Bedarf ändert. Fügen Sie den Parameter `categories: sys_id1, # sys_id2;` hinzu, um die Daten zu filtern.
4. Zeit bis zur Lösung und Zeit bis zum Identifizieren von Skripts: Verwenden Sie die Definitionsdatensätze, die Teil der zugehörigen Metrikliste sind. Wenn die Definitionsdatensätze für den Security Incident nicht verfügbar sind, erstellen oder fügen Sie diese Definitionsdatensätze hinzu, um die Werte für die beiden Felder auszufüllen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Standardmäßig hat der Sicherheitsadministrator keinen Zugriff zum Anzeigen der Versionsdatensätze einer Tabelle. Sie müssen die Administratorrolle hinzufügen, um auf die Versionsdatensätze zuzugreifen und die vorherige Version wiederherzustellen.

### Berichtkonfiguration

Verwenden Sie den Abschnitt „Berichtskonfiguration“, um die Bedingungen einzurichten und die Berichtsvorlagen auf die Security Incidents anzuwenden. Sie können derselben Bedingung einen primären Bericht und eine oder mehrere zusätzliche Berichtsvorlagen hinzufügen.

Im Folgenden finden Sie eine Beispielbedingung, die bereitgestellt wird, um die Phishing-Berichtsvorlage auf die Incidents der Phishing-Kategorie anzuwenden, und die andere, um die Standardberichtsvorlage auf alle Security Incidents anzuwenden. Die Standardberichtsvorlage wird auf die Security Incidents angewendet, wenn die Bedingungen nicht erfüllt sind.

### Verfahren zum Deaktivieren der neuen Implementierung

1. Deaktivieren Sie die folgenden Geschäftsregeln:
   a. PIR-PDF generieren
   b. Wissen bei Abschluss neu erstellen
2. Aktivieren Sie die folgenden Geschäftsregeln:
   a. Generiert PIR beim Überprüfen und Schließen
   b. Wissen beim Abschluss erstellen
   c. [PIR bei Abschluss/Stornierung/Löschen erneut generieren]
3. Aktivieren Sie die UI-Regel *`Hide PIR field when empty`*.
4. Wechseln Sie zum Formularlayout im Security Incident-Formular. Im Abschnitt „ **Überprüfung nach Incident** “:
   a. Entfernen Sie die PIR-Berichtsauswahl aus dem PIR-Abschnitt
   b. Fügen Sie dem PIR-Abschnitt das Feld „Nachfolgebericht zum Incident“ hinzu

### Konfigurieren Sie die Eigenschaften des PIR-Berichts (Post Incident Review) für untergeordnete Security Incidents

Sie haben die Möglichkeit, die folgenden beiden PIR-Berichtseigenschaften für untergeordnete Security Incidents zu konfigurieren:

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

**Hinweis:**

Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie PIR-Berichtseigenschaften für untergeordnete Security Incidents

| Eigenschaft | Verwendung |
|---|---|
| sn_si.generate_pir_report_for_child_si | Option zum Aktivieren der Generierung von PIR-Berichten (Post Incident Review) für untergeordnete Security Incidents.<br>• **Typ**: true \| false<br>• **Standardwert**: false<br>• **Speicherort**: Navigieren Sie zu Alle > Systemeigenschaften > Alle Eigenschaften. |
| sn_si.include_child_si_timeline_in_pir | Option, um die Zeitleiste der untergeordneten Security Incidents in den PIR-Bericht des übergeordneten Security Incidents aufzunehmen.<br>• **Typ**: true \| false<br>• **Standardwert**: false<br>• **Speicherort**: Navigieren Sie zu Alle > Systemeigenschaften > Alle Eigenschaften. |

### Verwalten Sie den Bericht zur Überprüfung nach Incidents

Der Bericht zur Überprüfung nach Incidents verwalten enthält die Informationen, die vom Sicherheitsadministrator konfiguriert und angewendet wurden. Sicherheitsanalysten können die Zeitleistenfilter zur Laufzeit ändern und herunterladen.

#### Vorbereitungen
Erforderliche Rolle: sn.si_analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Der Sicherheitsanalyst kann eine der verfügbaren primären oder zusätzlichen Berichtsvorlagen auswählen und die Zeitleistenfilter konfigurieren, eine Vorschau anzeigen und den Bericht herunterladen. Der Sicherheitsanalyst kann den Bericht auch direkt mit der zuletzt angewendeten Zeitleistenkonfiguration herunterladen.

Sicherheitsanalysten können über die Registerkarte „Überprüfung nach Incident“ auf die Berichte zugreifen.

#### Prozedur

1. Navigieren Sie zu dem Security Incident im Überprüfungsstatus.
2. Klicken Sie auf die Registerkarte **Überprüfung nach Incident**.
3. Wenn sich der Security Incident im **Überprüfungsstatus** befindet:
   **Berichtsvorlage:**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standardmäßig wird die primäre Berichtsvorlage, die auf der Setup-Seite konfiguriert wurde, auf den Security Incident angewendet und steht zum Download zur Verfügung.

- Der Analyst kann andere Berichte aus der Dropdown-Liste auswählen, um den Bericht zu konfigurieren und herunterzuladen.

4. **Konfigurieren/Vorschau:**

   Ein Sicherheitsanalyst kann eine Vorschau der Berichtsvorlagenkonfiguration anzeigen und sie ändern. In der aktuellen Konfiguration kann der Sicherheitsanalyst nur die Zeitleistenfilter ändern.

   Wenn die Konfiguration für den primären Bericht geändert wird, bevor der Security Incident geschlossen wird, wird der Bericht zur Überprüfung nach Incidents, der an den Security Incident angehängt ist, gemäß den vom Sicherheitsanalysten vorgenommenen Änderungen aktualisiert. Nach dem Abschluss kann der Analyst die Konfiguration ändern und den Bericht unterwegs herunterladen. Der angehängte Bericht würde jedoch der letzten Konfiguration vor dem Abschluss folgen.

   Führen Sie die folgenden Schritte aus, um den Bericht zu konfigurieren bzw. eine Vorschau anzuzeigen:

   a. Wählen Sie die gewünschte Berichtsvorlage aus der Dropdown-Liste „ **Berichtsvorlage** “ auf der Registerkarte „ **Überprüfung nach Incident** “ aus.

   b. Klicken Sie auf die Registerkarte **Konfigurieren/Vorschau**.

   c. **Aktualisieren** oder konfigurieren Sie die Zeitleistenfilter nach Bedarf.

   d. Verwenden Sie das Kontrollkästchen **Bilder** anzeigen, um die Bilder in die Zeitleiste ein- oder auszuschließen. Wenn diese Option deaktiviert ist, werden nur die Namen der Bilder in den Zeitleistenabschnitt aufgenommen.

   e. Verwenden Sie das Kontrollkästchen **Untergeordnete Aufgaben** anzeigen, um alle untergeordneten Aufgaben aufzulisten, die dem Security Incident zugeordnet sind.

5. **Speichern Sie** die Konfiguration, und klicken Sie auf die Registerkarte **Vorschau**, um eine Vorschau des Berichts anzuzeigen und ihn herunterzuladen.

6. Klicken Sie auf **Herunterladen**, um den Bericht direkt herunterzuladen.

### Konfigurieren Sie eine Bewertungsauslöserbedingung

Definieren Sie Regelbedingungen, und generieren Sie erforderliche und optionale Bewertungen für bestimmte Security Incidents.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Hinweis:**
Um die Funktion „Auslöserbedingungen für Bewertung nach Incident“ zu verwenden, müssen Sie ein Upgrade auf Security Incident Response 11.0 durchführen. Vor dem Upgrade müssen Sie alle Anpassungen rückgängig machen, die am Metriktyp „Überprüfung nach Incident“ und an den Auslöserbedingungen vorgenommen wurden. Darüber hinaus müssen Sie möglicherweise auch die Anpassungen rückgängig machen, die an den Business Rules vorgenommen wurden, die für die Überprüfung nach Incidents spezifisch sind.

- Bewertungen anfordern, um abgeschlossen zu sein
- Store-Beauftragter



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Setup für Bewertungen**.
2. Klicken Sie im Abschnitt „Auslösebedingungen für **Bewertung konfigurieren** “ auf **Konfigurieren**.

**Hinweis:**
Im Formular „Bewertungskonfigurationen“ und im Abschnitt „Bewertungskonfigurationen“ ist das Kontrollkästchen **Bewertungen generieren** standardmäßig aktiviert.

- Wenn Sie das Kontrollkästchen aktivieren, wird für jeden Security Incident eine optionale Bewertung erstellt.
- Wenn Sie das Kontrollkästchen deaktivieren, werden keine Bewertungen generiert. Die Bewertungsregeln werden nicht angezeigt, und Sie können keine Bedingungen für die Security Incidents konfigurieren.

3. Geben Sie im Formular „Bewertungskonfigurationen“ im Abschnitt „Bedingungen“ die erforderlichen Informationen an.

   a. Geben Sie im Feld **Name** den Regelnamen an.

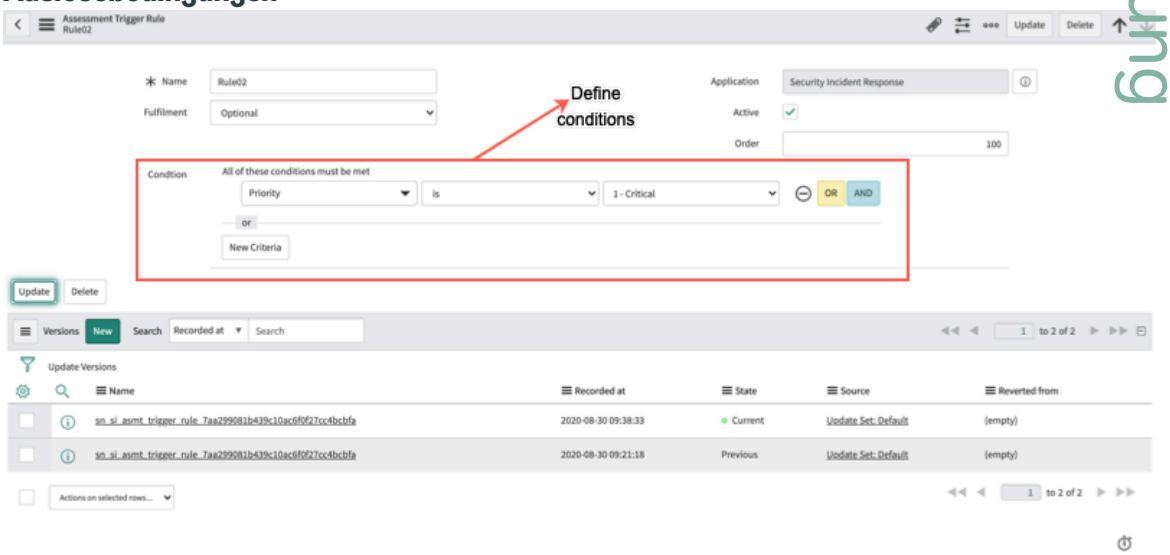
   b. **Geben Sie** im Feld Erfüllung den Erfüllungstyp an.

   c. Um eine Bedingung zu konfigurieren, klicken Sie auf den Regeldatensatz, und definieren Sie Bedingungen im Feld **Bedingung**.

**Hinweis:**

- Wenn Sie eine Regel erstellen, ohne eine Bedingung im Feld **Bedingung** zu definieren, wird die Bedingung als „wahr“ ausgewertet, und die Regel gilt für alle Security Incidents.
- Sie können eine bestimmte Regel definieren, um die Bewertungen entweder obligatorisch oder optional zu machen. Für die verbleibenden Security Incidents, die nicht den definierten Regeln entsprechen, werden keine Bewertungen generiert.

**Auslösebedingungen**




Automatische Übersetzung

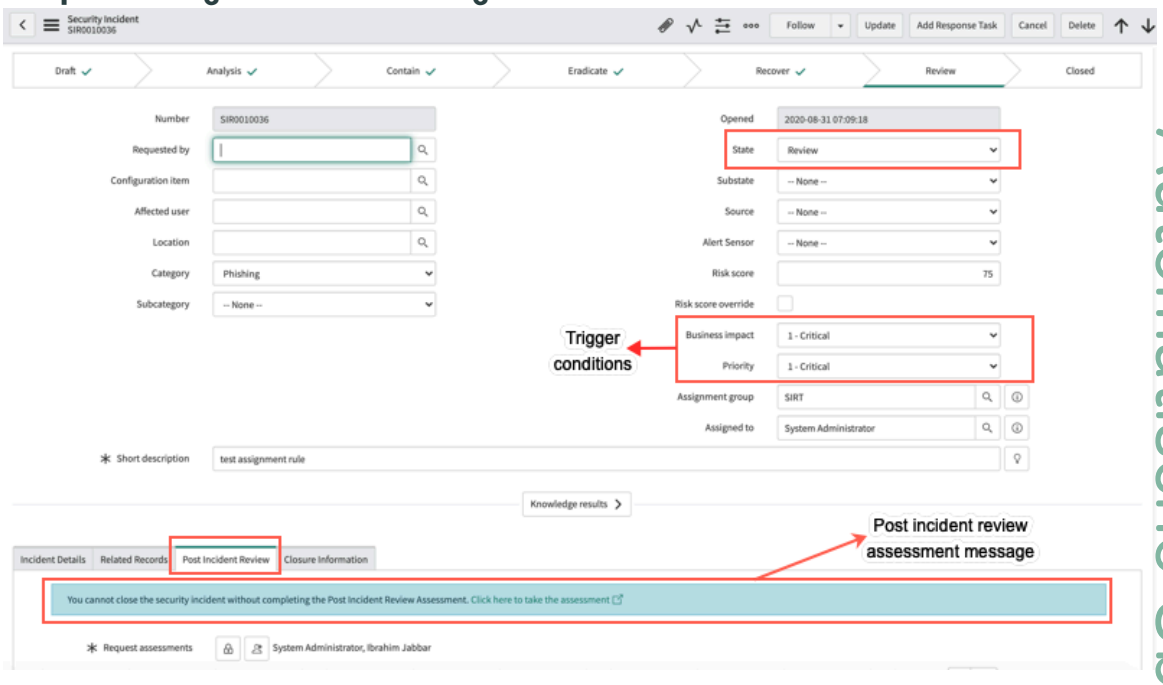
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Beispiele für Auslöserbedingungen für Bewertungen

Die folgenden Beispiele zeigen verschiedene Szenarien, wie obligatorische und optionale Auslöserbedingungen für Bewertungen generiert werden.

- Generieren Sie im Formular „Bewertungsauslöserbedingung“ obligatorische Bewertungen, wenn die **Priorität** und die **Geschäftsauswirkung** für einen Security Incident auf der Seite „ **Bewertungsauslöserregel** “ auf „ **Kritisch** “ festgelegt werden. In einem solchen Szenario können die Sicherheitsanalysten den Incident erst schließen, wenn die obligatorischen Bewertungen abgeschlossen sind.

**Beispiel für obligatorische Bewertung**




- Wie Sie in diesem Beispiel sehen können, können Sicherheitsanalysten den Security Incident nicht schließen, wenn sich ein Security Incident im **Überprüfungsstatus** befindet, ohne die **Bewertung nach dem Incident Review**abzuschließen. Ein Bewertungslink ist verfügbar, um die Bewertung an die Sicherheitsanalysten zu übermitteln, die dem Incident zugewiesen sind (oder die Bewertung angefordert haben).
- Generieren Sie im Formular „Bewertungsauslöserbedingung“ optionale Bewertungen, wenn die **Priorität** und die **Geschäftsauswirkung** für einen Security Incident auf **Hoch**festgelegt sind. In diesem Beispiel werden die Bewertungen automatisch abgebrochen, wenn die Sicherheitsanalysten die Bewertungen nicht abschließen und den Security Incident nicht schließen.
- Falls die obligatorischen oder optionalen Bewertungen nicht mit dem Security Incident übereinstimmen, werden für solche Security Incidents keine Bewertungen generiert. Ein Sicherheitsanalyst kann den Security Incident schließen, ohne die Bewertung nach dem Incident Review abzuschließen.

### Führen Sie eine fragebogenbasierte Überprüfung nach Incidents durch

Sie können entscheiden, dass eine Überprüfung des Security Incidents nach einem Incident gerechtfertigt ist. Eine Überprüfung nach Incidents beschreibt, was passiert ist, hilft zu bestimmen, warum der Incident aufgetreten ist, und zeigt, wie er in Zukunft vermieden oder behandelt werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.manager, sn_si.analyst

**Hinweis:**
Jeder Benutzer kann unabhängig von seiner Rolle an einem Fragebogen zur Überprüfung nach Incidents teilnehmen. Rollen können einer Überprüfung zugewiesen werden.

### Warum und wann dieser Vorgang ausgeführt wird

Die Anwendung ServiceNow Security Incident Response kann die Erfassung von Informationen zur Überprüfung nach Incidents von allen an einem Security Incident beteiligten Personen mithilfe von Fragebögen automatisieren. Wenn Sie sich für die Verwendung eines Fragebogens als Teil einer Überprüfung nach einem Incident entscheiden, wird eine Liste mit Fragen, die für den Security Incident relevant sind, an die benutzerdefinierte Teilnehmerliste gesendet. Wenn jeder Benutzer den Fragebogen ausfüllt, wird automatisch der Nachfolgebericht zum Incident generiert. Der Bericht fasst alle Informationen im Zusammenhang mit dem Security Incident sowie alle Antworten auf die Überprüfung nach Incidents zusammen.

Zwar wird mit dem Basissystem eine anfängliche Liste von Fragen bereitgestellt, diese sind jedoch anpassbar. Sie können Kategorien erstellen und ihnen neue Fragen hinzufügen oder einzelne Fragen innerhalb vorhandener Kategorien ändern. Sie können Fragen basierend auf Rollen stellen. Sie können festlegen, wann bestimmte Fragen gestellt werden. Es kann Fragen geben, die Sie beispielsweise nur für Ihre UNIX-Server oder nur bei kriminellen Aktivitäten stellen. Sie können Fragen definieren, die abhängig von der Antwort auf eine andere Frage oder dem Wert in einem Feld im Formular gestellt werden. Es kann sogar Fragen geben, die vollständig durch Abfragen der Datenbank ausgefüllt werden.

Nachdem der Security Incident gelöst und in den Status „ **Überprüfung** “ versetzt wurde, werden Bewertungen für alle zugewiesenen Benutzer und Benutzer generiert, die direkt aus der Liste **„Bewertungen anfordern“** hinzugefügt werden.

Der Fragebogen kann ein hilfreiches Tool sein, um Informationen über die Behandlung des Security Incident aus verschiedenen Quellen zu sammeln.

Während der Überprüfung können Sie der Liste weitere Benutzer hinzufügen oder vorhandene Benutzer aus der Liste entfernen, es sei denn, sie haben bereits mit dem Ausfüllen des Fragebogens begonnen. Wenn Sie der Liste neue Benutzer hinzufügen, erhalten diese die Fragen, wenn der Datensatz gespeichert wird. Der Security Incident kann erst geschlossen werden, wenn alle Fragebögen ausgefüllt wurden. Wenn Fragebögen von jedem Benutzer ausgefüllt werden, wird der Nachfolgebericht zum Incident automatisch generiert (und erneut generiert) und auf der Registerkarte „Nachprüfung nach **Incident** “ angezeigt.

So starten Sie eine Überprüfung nach Incidents:

### Prozedur

1. Erstellen Sie einen Security Incident, oder öffnen Sie einen vorhandenen, indem Sie zu navigieren **Security Incident** > **Incidents** > **Mir zugewiesen (oder „Dem Team zugewiesen“ oder „Nicht zugewiesene Incidents“)**.
2. Klicken Sie auf die Registerkarte **Überprüfung nach Incident**.
3. Das Feld **Bewertungen anfordern** ist standardmäßig auf die Person im Feld **Zugewiesen an** festgelegt. Klicken Sie auf das Sperrsymbol, um weitere Benutzer zur Überprüfungsliste hinzuzufügen. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer, Rollen oder zur Eingabe von Benutzer-E-Mail-Adressen verfügbar.
4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf das Sperrsymbol, um das Feld zu sperren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können auch Bedingungen definieren, die bei Erfüllung in einem Security Incident dazu führen können, dass bestimmte Benutzer automatisch dem Feld **Bewertungen anfordern** für diesen Security Incident hinzugefügt werden. Wenn beispielsweise die **Kategorie** eines Security Incident in **Phishing**geändert wird, können bestimmte Personen, die über Erfahrung mit Phishing-Bedrohungen verfügen, der Überprüfungsliste nach Incident hinzugefügt werden. Weitere Informationen finden Sie unter Erstellen Sie PIR-Zuweisungsregeln.

5. Klicken Sie auf **Aktualisieren**.
Wenn der Incident in den **Überprüfungsstatus** versetzt wird (oder sofort, wenn er sich bereits im **Überprüfungsstatus** befindet), erhält jeder der Benutzer in der Überprüfungsliste eine erste E- Mail-Benachrichtigung . Erinnerungen werden gesendet, wenn das Fälligkeitsdatum näher rückt. Wenn jeder Benutzer über den E-Mail-Link oder über zu auf den Fragebogen zugreift **Überprüfung nach Incident** > **Meine ausstehenden Überprüfungen**, stammen die angezeigten Fragen aus allen Kategorien, die zu diesem Security Incident passen. Wenn der Überprüfungsliste vor Erreichen des Fälligkeitsdatums neue Benutzer hinzugefügt werden, erhalten sie beim Speichern des Security Incident Benachrichtigungen.

Wenn Benutzer ihre Fragebögen ausfüllen, werden die Daten im Nachfolgebericht zum Incident zusammengestellt und der Bericht wird auf der Registerkarte „ **Überprüfung nach Incident** “ angezeigt. Die Fragebogendaten werden auf der Registerkarte „ **Ergebnisse** “ angezeigt.

### Erstellen Sie Fragebogenkategorien für die Überprüfung nach Incidents

Sie können die Fragebogenkategorien verwenden, die mit dem Basissystem geliefert werden, oder eigene Kategorien erstellen.

#### Vorbereitungen
Erforderliche Rolle: sn.si_admin

#### Warum und wann dieser Vorgang ausgeführt wird
So erstellen Sie eine neue Kategorie von Fragen:

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**.
2. Klicken Sie **auf Fragen überprüfen**.
Eine Liste der Kategorien wird angezeigt, zusammen mit deren Reihenfolge und Filtern, die definieren, unter welchen Bedingungen die Fragen gestellt werden (z. B. nur, wenn die Security Incident-Kategorie „ *`Kriminelle Aktivität`*“ lautet). Jede Kategorie ist ein Abschnitt im Fragebogen zur Überprüfung nach Incidents, und die Fragen in jeder Kategorie werden nur einbezogen, wenn der Security Incident mit dem Bedingungsfilter übereinstimmt. Zum Beispiel würden Sie für eine Kategorie von Fragen, die nur für Linux-Server gilt, einen Filter einrichten, der Security Incidents auswählt, bei denen der betroffene Ressourcentyp Linux-Server ist. In dieser Kategorie erstellen Sie alle Fragen, die erforderlich sind, wenn ein Security Incident auf einem Linux-Server aufgetreten ist. Sie verwenden eine der im Basissystem bereitgestellten Kategorien oder erstellen eine neue Kategorie. Bei diesem Verfahren wird davon ausgegangen, dass Sie eine neue Kategorie erstellen möchten, bevor Sie Fragen definieren.
3. Klicken Sie in der Liste der Kategorien auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

**Sicherheitsvorfall**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Kategorie, die im Security Incident-Fragebogen angezeigt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Typ | Überprüfung nach Incident ist die Standardeinstellung. |
| Stakeholder ergänzen | Nicht verwendet von Security Incident Response. |
| Tabelle | Dieses Feld wird automatisch zugewiesen, sobald das Formular übermittelt wurde. |
| Filter | Geben Sie die Bedingung ein, die bestimmt, wann Fragen in dieser Kategorie verwendet werden.<br><br>Wenn ein Security Incident-Datensatz diesem Filter entspricht, werden die Fragen in eine Überprüfung nach Incidents für diesen Security Incident aufgenommen. Filter können beliebige Daten im Datensatz oder in anderen mit diesem Datensatz verknüpften Datensätzen verwenden. Zum Beispiel die Abteilung des Vorgesetzten des anfordernden Benutzers. |
| Anwendung | Anwendungsbereich für den Incident. |
| Gewichtung | Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10. |
| Gesamtmetriken | Anzahl der von der Kategorie verwendeten Metriken. |
| Beschreibung | Beschreibung des Fragebogens. |

5. Klicken Sie auf **Absenden**, um die Kategorie zu speichern.

### Verfassen Sie Fragen zur Überprüfung nach Incidents

Sie können die Fragen verwenden, die mit dem Basissystem bereitgestellt werden, oder eigene Fragen erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Die Methoden zum Sammeln von Informationen zur Überprüfung nach Incidents können in Form von Fragen oder als Daten vorliegen, die mithilfe von Skripts automatisch erfasst werden.

Fragen können von den Antworten auf andere Fragen abhängen. Sie können beispielsweise fragen, ob alle erforderlichen Protokolle verfügbar waren. Wenn die Antwort Nein lautet, stellen Sie eine Folgefrage, um festzustellen, welche der erforderlichen Protokolle nicht aktiviert wurden.

Bei der skriptbasierten Datenerfassung, auch als Skriptmetriken bezeichnet, werden Daten im Zusammenhang mit dem Security Incident über von Ihnen geschriebene Skripts erfasst. Diese Aktion kann weit über die Daten im Security Incident-Datensatz selbst hinausgehen. Beispielsweise kann eine Skriptmetrik die aktuelle Ausfallzeit für einen von diesem Security Incident betroffenen Server erfassen.

Schließlich können Sie die beiden Typen mischen. Für Fragen können Standardwerte aus einem Skript oder einfach aus einem Feld im Security Incident-Datensatz übernommen werden. Wenn Sie den Fragetyp Standardantwort von··· verwenden, können Sie auswählen, ob der Benutzer die Frage immer beantworten soll – wobei der Standardwert einen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anfangswert liefert – oder ob dem Benutzer die Frage nur gestellt werden soll Skript oder Feld ist leer.

So erstellen Sie eine neue Frage:

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**.
2. Klicken Sie auf die Kategorie, für die Sie eine neue Frage erstellen möchten.
3. Klicken Sie auf die Registerkarte **Bewertungsmetriken**.
4. Klicken Sie auf **Neu**.
   Sie können auch auf eine vorhandene Frage klicken, um sie zu ändern.
5. Füllen Sie die entsprechenden Felder im Formular aus.

**Formular „Metrik“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Metrik (Frage oder Skript). Wenn die Metrik eine geskriptete Datensammlung ist, wird dieser Name im Nachfolgebericht zum Incident angezeigt. |
| Kategorie | Die Kategorie, zu der die Metrik gehört. Das System füllt diese Kategorie automatisch aus, wenn Sie eine neue Metrik aus dem Formular „Metrikkategorie“ erstellen.<br>**Hinweis:**<br>Sie können die Kategorie nicht ändern, wenn das Feld **Abhängig von** gesetzt ist oder eine andere Metrik von dieser Metrik abhängt. |
| Methode | Gibt den Typ der Metrik wie folgt an:<br>○ *Assessment*: Eine Frage ohne Standardwert. Es gibt mehrere Datentypen, die im **Feld** Datentyp auf der Registerkarte **Feldtyp** definiert werden können, z. B. Kontrollkästchen, Auswahllisten, Texteingabe.<br>○ *Script*: Geskriptete Metrik. Erhält Werte durch Schreiben eines benutzerdefinierten Skripts. Die Methode *Script* ist mit den Datentypen **Duration**, **Number**und **Percentage** kompatibel.<br>○ *Default answer from field*: Eine Frage, bei der die Standardantwort aus einem ausgewählten Feld im Security Incident stammt. Wenn Sie diese Option auswählen, werden der Registerkarte **Allgemein** zwei Felder hinzugefügt:<br>▪ *Default answer*: Wählen Sie das Feld im Security Incident aus, das die Standardantwort für die Frage enthält. Zum Beispiel wäre für die Frage „Wer hat diesen Incident ursprünglich gemeldet?“ das Feld **Angefordert von** eine wahrscheinliche Auswahl.<br>▪ *Ask question*: Gibt an, wann die Frage gestellt werden soll: immer oder nur, wenn das Feld **Standardantwort** leer ist. Im obigen Beispiel würde die Frage gestellt, wenn das Feld „ **Angefordert von** “ leer ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ *`Default answer from script`*: Eine Frage, bei der die Standardantwort aus einem Skript stammt. Die Antwort kann eine Zahl, eine Zeichenfolge oder ein Prozentsatz sein. Die Registerkarte **Allgemein** fügt ein Feld hinzu:<br><br>*`Ask question`*: als Gibt an, wann die Frage gestellt werden soll: immer oder nur, wenn das Skript keine Standardantwort bereitstellt. Das Skript wird in der Registerkarte **Feldtyp** definiert.<br><br>**Hinweis:**<br>Wenn Sie einen **Datentyp** auswählen, der mit der ausgewählten **Methode**nicht kompatibel ist, ändert das System die **Methode** automatisch in einen kompatiblen Wert. |
| Gewichtung | [Erforderlich]<br><br>Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10.<br><br>Dieses Feld ist sichtbar und erforderlich, es sein denn der **Datentyp** ist **Datum**, **Datum/Zeit** oder **Zeichenfolge**. Diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen. |
| Bestellung | [Erforderlich]<br><br>Numerischer Wert, der die Reihenfolge der Metrikfrage in Bewertungsfragebögen in Relation zu anderen Metrikfragen in derselben Kategorie bestimmt. Die Metrik mit dem kleinsten Wert für die Reihenfolge erscheint als erste Frage im Kategoriebereich. Standardmäßig ist die Reihenfolge 100.<br><br>**Hinweis:**<br>Es spielt keine Rolle, welchen Wert für die Reihenfolge Sie für Metriken mit der Skriptmethode verwenden, da sie nicht in Fragebögen angezeigt werden. |
| Aktiv | Kontrollkästchen, das bestimmt, ob diese Metrik verwendet wird. Wenn das Kontrollkästchen nicht aktiviert ist, ist der Metrikdatensatz nicht vorhanden. |
| Obligatorisch | Checkbox, die die Metrikfrage für Bewertungsfragebogen obligatorisch (ausgewählt) oder optional (deaktiviert) macht. Benutzer können Fragebögen erst einreichen, wenn sie gültige Antworten auf alle obligatorischen Fragen geben, die durch eine rote Feldstatusanzeige gekennzeichnet sind.<br><br>Dieses Feld ist nur sichtbar, wenn das Feld **Abhängig von** leer ist und der Datentyp nicht **Checkbox**ist. |

**6.** Klicken Sie auf die Registerkarte **Allgemein**, und füllen Sie die Felder entsprechend aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Allgemein“

| Feld | Beschreibung |
|---|---|
| Frage | Text, der als Frage in Fragebögen zur Überprüfung von Security Incidents verwendet werden soll. Geben Sie eine klare, unkomplizierte Frage ein, die leicht zu beantworten ist, z. B. **Wie haben wir den Incident eingedämmt?** |
| Beschreibung | Informationen zur Metrik und deren Auswertung. Wenn *Method*`Assessment`lautet, fügen Sie Details hinzu, die Benutzern helfen, die Frage zu beantworten. Dieser Text wird als Hinweis angezeigt, wenn ein Benutzer auf den Fragentext im Fragebogen zeigt. |
| Abhängig von und Angezeigt wenn | Wählen Sie eine Frage im **Feld** Abhängig von aus, von der die aktuelle Frage abhängt. Beispiel: Die Frage „Welche zusätzlichen Protokolle wurden benötigt?“ hängt von der Frage „Waren alle benötigten Protokolle verfügbar?“ ab.<br><br>Verwenden Sie als Nächstes das Feld **Angezeigt wenn**, um anzugeben, wann die abhängige Frage in Fragebögen angezeigt werden soll. Beispiel: Wenn die abhängige Frage nur gestellt werden soll, wenn der Benutzer die Frage „Waren alle benötigten Protokolle verfügbar?“ mit **Nein** beantwortet hat. Frage wählen Sie **Nein** im Feld **Angezeigt wenn**.<br><br>**Hinweis:**<br>Das System verhindert die Erstellung rekursiver Abhängigkeiten zwischen Metriken. Wenn beispielsweise Metrik A von Metrik B abhängt, kann Metrik B nicht von Metrik A abhängen. |

7. Klicken Sie auf die Registerkarte **Feldtyp**, und füllen Sie die Felder entsprechend aus.

### Registerkarte Feldtyp

| Feld | Beschreibung |
|---|---|
| Datentyp | Der Datentyp der erwarteten Antwort, von dem die Liste der verfügbaren Typen für die ausgewählte Methode abhängt. Wenn die Methode **Bewertung** ist, bestimmt der Datentyp, wie Benutzer die entsprechende Frage in Fragebögen beantworten. Wenn die Methode **Skript** ist, bestimmt der Datentyp, wie das System die Bewertungsergebnisse berechnet.<br><br>**Hinweis:**<br>Wenn eine andere Metrik von dieser Metrik abhängt, kann der Datentyp nicht geändert werden. |
| Antworten zufällig | Checkbox, die bestimmt, ob die Antwortoptionen für diese Metrikfrage jedes Mal in zufälliger Reihenfolge angezeigt werden sollen, wenn ein Benutzer einen Bewertungsfragebogen öffnet, der die Frage enthält. Die Antworteinstellung kann durch die Reihenfolge beeinflusst werden, in der die Antwortoptionen angezeigt werden. Dies kann zu verzerrten Ergebnissen führen. Durch Randomisieren von Antwortmöglichkeiten kann diese Verzerrung vermieden werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Dieses Feld ist nur sichtbar, wenn Sie im Feld **Datentyp** die Option **Likert-Skala** oder **Auswahl** auswählen. |
| Abhängiges Plugin | [Erforderlich, wenn *Method* **Skript** ist.]<br><br>Plugin, das die im Skript abgefragten Tabellen enthält. Das System führt das Metrikskript nur dann aus, wenn das Plugin aktiv ist. Die standardmäßig verfügbaren Werte sind **Asset Management**, **CMDB**, **Kern**, **Cost Management**, **Procurement** und **Software Asset Management**.<br><br>Dieses Feld ist nur sichtbar, wenn *Method* **gleich Skript** ist.<br><br>**Hinweis:**<br>○ Wenn der Standardwert Core verwendet wird, wird das Skript immer ausgeführt.<br>○ Wenn Sie Administrator sind, können Sie dem Feld weitere Auswahlmöglichkeiten für Plugins hinzufügen. |
| Skaladefinition | Eine Einstellung, die bestimmt, ob bei den Berechnungen von Bewertungsergebnissen kleinere oder größere numerische Werte einer guten Bewertung entsprechen. Wählen Sie **Niedrig** aus, wenn geringere numerische Werte besser sind, z. B. für eine Metrik, die die Anzahl der Fehler für einen Lieferanten misst. Wählen Sie **Hoch**, wenn größere numerische Werte besser sind, z. B. für eine Metrik, die die Benutzerzufriedenheit auf einer Skala von eins bis fünf misst. Der Standardwert ist **Hoch**.<br><br>Dieses Feld ist sichtbar und erforderlich, es sei denn, *Data type* ist **Datum**, **Datum/Uhrzeit** oder **Zeichenfolge**. Die Ergebnisse für diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen. |
| Min. | Niedrigster numerischer Wert, der als Antwortoption bei Assessments oder als skalierter Wert in einer Skriptmetrik verwendet werden soll.<br><br>Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp **Auswahl** oder **Likert-Skala** ist, ist dieses Feld schreibgeschützt und wird automatisch basierend auf der kleinsten Metrikdefinition *Value* festgelegt. |
| Max. | Höchster numerischer Wert, der als Antwortoption oder skalierter Wert verwendet werden soll.<br><br>Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp **Auswahl** oder **Likert-Skala** ist, ist dieses Feld schreibgeschützt und wird automatisch basierend auf der größten Metrikdefinition *Value* festgelegt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Skript | Skript, das die gewünschten Systeminformationen abruft. Das Skript verfügt über eine Eingabevariable, die mit der ID des Security Incident (primär) festgelegt wird, und drei mögliche Ausgabevariablen, die vom Skript festgelegt werden: „string_result“, „scaled_result“ und „actual_result“. Wenn der Datentyp Zeichenfolge ist, ist nur string_result erforderlich.<br><br>Dieses Feld ist sichtbar und erforderlich, wenn *Method* **Skript** ist oder der Standardwert aus einem Skript stammt. |
| Vorlage | Ein vordefinierter Satz allgemeiner Antworten, die für die Frage verwendet werden sollen. Beispielsweise beginnt eine Häufigkeitsvorlage wahrscheinlich mit dem Wert „Nie“ und geht bis zum obersten Wert „Immer“.<br><br>Dieses Feld ist sichtbar und nur erforderlich, wenn *Data type* **Vorlage** ist.<br><br>**Hinweis:**<br>Wenn eine andere Metrik von dieser Metrik abhängt, kann die Vorlage nicht geändert werden. |

8. **Wahlweise:** Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf **Aktualisieren**.

### Erstellen Sie PIR-Zuweisungsregeln

Zusätzlich zum manuellen Hinzufügen von Benutzern zur Bewertungsliste für die Überprüfung nach Incidents für einen Security Incident können Sie Zuweisungsregeln für das automatische Hinzufügen von Benutzern zur Liste definieren.

#### Vorbereitungen

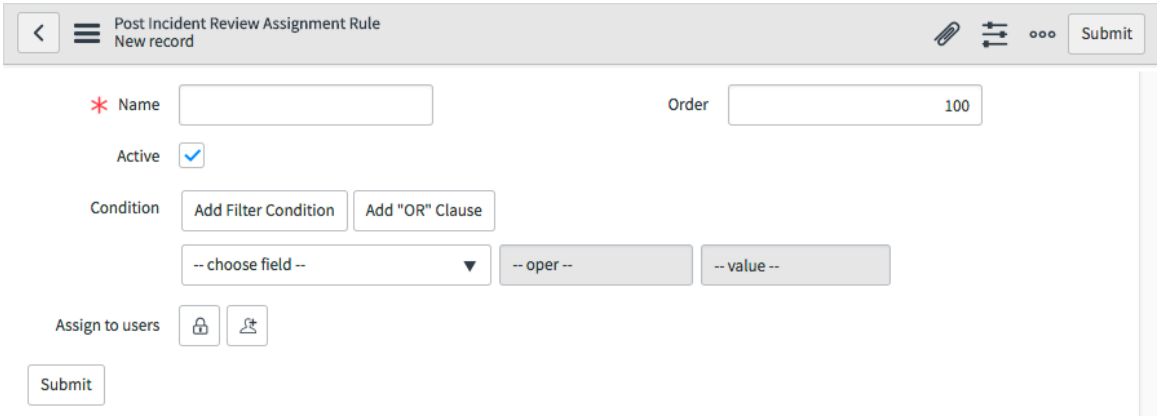
Erforderliche Rolle: sn_si.admin, sn_si.manager, sn_si.analyst

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Setup für Bewertungen**.
2. Führen Sie einen **Drilldown zum Abschnitt „Benutzerzuweisungsregeln** “ durch.
3. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**5.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Zuweisungsregel. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Regel zu aktivieren. |
| Bestellen | Geben Sie einen numerischen Wert ein, um anzugeben, an welcher Stelle in der Liste der Zuweisungsregeln diese Regel angezeigt werden soll. Niedrigere Zahlen erscheinen oben in der Liste.<br>**Hinweis:**<br>Nur die erste übereinstimmende Zuweisungsregel wird ausgeführt, und nur die in dieser Regel definierten Benutzer werden der Bewertungsliste hinzugefügt. |
| Bedingung | Verwenden Sie den Bedingungsgenerator, um die Bedingungen zu definieren, die im Security Incident erfüllt sein müssen, damit diese Regel ausgeführt wird. Weitere Informationen finden Sie im folgenden Beispiel. |
| Benutzern zuweisen | Klicken Sie auf das Schlosssymbol, um Benutzer zur Überprüfungsliste hinzuzufügen. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Benutzer, Rollen oder zur Eingabe von Benutzer-E-Mail-Adressen verfügbar. |

**6.** Klicken Sie auf **Absenden**.

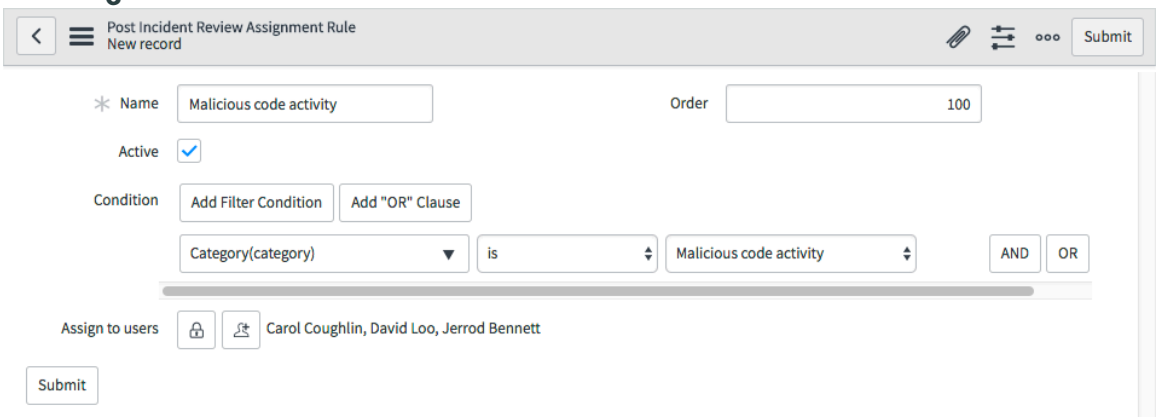
## Example: Böswillige Code-Aktivität

In der hier gezeigten Zuweisungsregel für die Überprüfung nach Incidents werden die drei identifizierten Benutzer (die zufällig Experten im Umgang mit Aktivitäten mit böswilligem Code sind) hinzugefügt, wenn ein Security Incident, bei dem das Feld **Kategorie** auf **Aktivität** böswilliger Code festgelegt ist, in den Status **Überprüfung** übergeht Liste der Benutzer, die den Fragebogen zur Überprüfung nach Incidents für diesen Security Incident erhalten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Böswillige Code-Aktivität**




## Schließen Sie Security Incidents

Wenn ein Security Incident in den Überprüfungsstatus übergegangen ist, ist es möglich, ihn zu schließen und einen entsprechenden Abschlusscode einzugeben. Abschlusscodes können später zur leichteren Lokalisierung durchsucht werden.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
In früheren Versionen von Security Incident Responsekonnten Benutzer Security Incidents oder Anforderungen als Spam schließen. Im Release Istanbul ist die Spam-Option nicht mehr verfügbar. Spam-Security Incidents oder Anforderungen können nach Bedarf abgebrochen oder gelöscht werden.

### Prozedur

1. Wenn der Security Incident, den Sie schließen möchten, noch nicht geöffnet ist, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, und suchen Sie den Security Incident, den Sie schließen möchten.

   **Hinweis:**
   Wenn Bewertungen für die Überprüfung nach Incidents vorhanden sind, die für diesen Security Incident nicht abgeschlossen wurden, kann der Security Incident nicht geschlossen werden. Zurück zu **Security Incident** > **Überprüfung nach Incident** > **Alle unvollständigen Überprüfungen**, suchen Sie die unvollständigen Überprüfungen und bitten Sie die Prüfer, ihre Überprüfungen abzuschließen, oder stornieren Sie die verbleibenden Bewertungen.

2. **Klicken** Sie auf die Registerkarte Abschlussinformationen, und füllen Sie die Felder entsprechend aus.

**Sicherheitsvorfall**

| Feld | Beschreibung |
|---|---|
| Wissensartikel erstellen | Wählen Sie dieses Feld aus, um automatisch einen Knowledge Base-Artikelentwurf zu erstellen, der den Inhalt der Überprüfung nach Incidents enthält. |
| Lösungscode | Wählen Sie den Abschlusscode aus, der den Grund für das Schließen dieses Security Incidents am besten beschreibt.<br>○ Untersuchung abgeschlossen<br>○ Bedrohung verringert |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Gepatchte Schwachstelle<br>○ Ungültige Schwachstelle<br>○ Nicht behandelt<br>○ Falsch positiv |
| Geschlossen von | Zeigt den Benutzer an, der den Security Incident geschlossen hat, nachdem der Datensatz aktualisiert wurde. |
| Geschlossen | Zeigt das Datum und die Uhrzeit des Abschlusses an, nachdem der Datensatz aktualisiert wurde. |
| Abschlussnotizen | Geben Sie zusätzliche Notizen ein, die das Ergebnis des Schließens dieses Security Incident beschreiben. |

3. Klicken Sie auf **Aktualisieren**.
4. Der zugewiesene Benutzer kann den Status **manuell** in **Geschlossen**ändern.
   Wenn ein übergeordneter Incident geschlossen wird, werden alle zum untergeordneten Incident gehörenden Antwortaufgaben abgebrochen. Wenn keine anderen Aufgabentypen vorhanden sind, wird der untergeordnete Incident ebenfalls geschlossen.

### Fügen Sie einem Security Incident Abschlussinformationen hinzu

Wenn sich ein Security Incident im Status Überprüfen oder Geschlossen befindet, können Sie Abschlussinformationen eingeben.

#### Vorbereitungen

Erforderliche Rolle: sn_si.basic

#### Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf die Registerkarte **Zugehörige Datensätze**.
3. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Wissensartikel erstellen | Aktivieren Sie diese Checkbox, um einen Wissensartikel mit dem Inhalt des Nachfolgeberichts zum Incident zu generieren. |
| Lösungscode | Wählen Sie den Abschlusscode aus, der den Grund für das Schließen des Security Incident am besten beschreibt. |
| Geschlossen von | [Nur Lesen] Zeigt den Benutzer an, der den Security Incident geschlossen hat. |
| Geschlossen | [Nur Lesen] Zeigt das Datum und die Uhrzeit an, zu der der Security Incident geschlossen wurde. |
| Abschlussnotizen | Wie der Security Incident geschlossen wurde, einschließlich gelernter Lektionen, Lösung usw. |

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Incident Details
- Überprüfung nach Incident

5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

## Beschränken Sie den Zugriff auf Security Incidents

Verwalten Sie den Zugriff auf Security Incidents, die vertrauliche Informationen enthalten. Sie können Einschränkungen für Security Incidents erzwingen, um zu bestimmen, wer auf einen bestimmten Incident zugreifen kann, und den Zugriff auf bestimmte Benutzer oder Gruppen beschränken.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

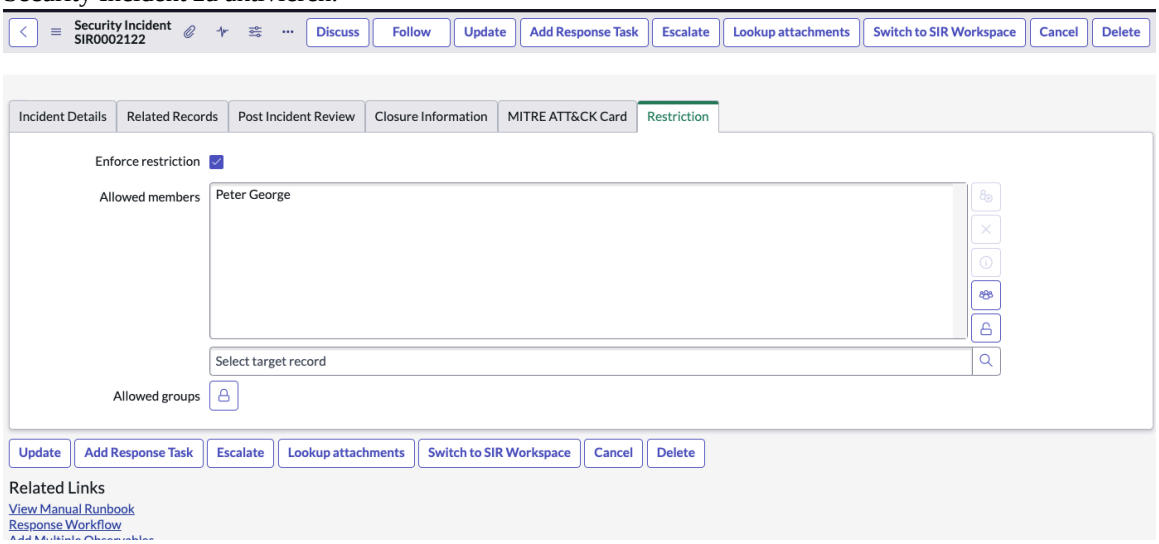
### Warum und wann dieser Vorgang ausgeführt wird

Mit Einschränkungen für Security Incidents können Sie kritische Security Incidents vor dem Zugriff durch andere Benutzer in einer bestimmten Organisation verbergen. Mit diesen Einschränkungen können Sie die Security Incidents, auf die ein Benutzer zugreifen kann, detaillierter steuern. Sie können eine Einschränkung für Security Incidents erzwingen, indem Sie das **Kontrollkästchen Einschränkung** erzwingen aktivieren und dann die Benutzer oder Gruppen auswählen, die auf den jeweiligen Security Incident zugreifen dürfen.

Nachdem Sie die Einschränkung für bestimmte Security Incidents erzwungen und den Zugriff auf bestimmte Benutzer oder Gruppen beschränkt haben, können alle anderen verbleibenden Benutzer in Ihrer Organisation nicht mehr auf diese Security Incidents zugreifen, auch wenn sie nach einem bestimmten eingeschränkten Security Incident suchen.

### Prozedur

1. Öffnen Sie einen Security Incident, den Sie einschränken möchten.
2. Wenn Sie die klassische Benutzeroberfläche verwenden, gehen Sie wie folgt vor:
   a. Klicken Sie auf die Registerkarte **Einschränkung**.
   b. Aktivieren Sie das **Kontrollkästchen Einschränkung erzwingen**, um die Einschränkung des Security Incident zu aktivieren.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**c.** Sie im Feld Zulässige Mitglieder auf das Schlosssymbol, um die Benutzer auszuwählen, die auf den Security Incident zugreifen können.

**d.** Wählen Sie das hinzufügen“ aus, um sich selbst als zulässigen Benutzer hinzuzufügen.

**e.** Klicken Sie auf das Symbol hinzufügen und entfernen, um Benutzer hinzuzufügen oder zu entfernen.

**f.** Sie im Feld Zulässige Gruppen auf das Schlosssymbol, um die Gruppen auszuwählen, die auf den Security Incident zugreifen können.

**g.** Klicken Sie auf das Symbol hinzufügen und entfernen, um Gruppen hinzuzufügen oder zu entfernen.

**Hinweis:**
Nachdem das **Kontrollkästchen Einschränkung erzwingen** für den Security Incident aktiviert wurde, haben nur sn_si.admin und zulässige Mitglieder oder Gruppen Zugriff auf den Security Incident.

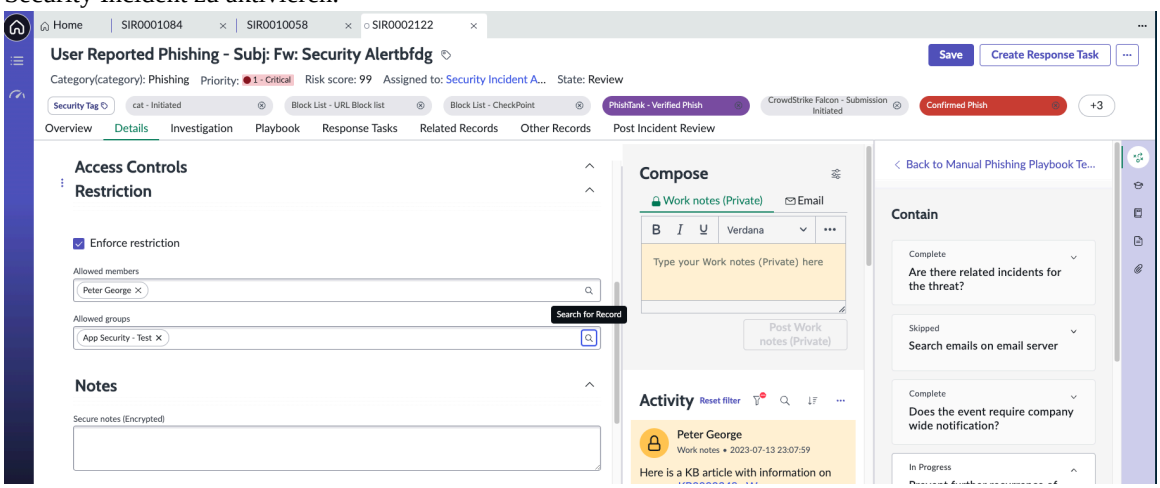
**h.** Klicken Sie auf **Aktualisieren**.

**3.** Wenn Sie SIR Workspace verwenden, gehen Sie wie folgt vor:

**a.** Klicken Sie im Security Incident auf die Registerkarte **Details**.

**b.** Scrollen Sie nach unten, und klicken Sie auf den Abschnitt **Einschränkung**.

**c.** Aktivieren Sie das **Kontrollkästchen Einschränkung erzwingen**, um die Einschränkung des Security Incident zu aktivieren.




**d.** Wählen Sie im Feld Zulässige Mitglieder die Benutzer aus, die über die Suchoption auf den Security Incident zugreifen können.

**e.** Wählen Sie im Feld Zulässige Gruppen die Gruppen aus, die über die Suchoption auf den Security Incident zugreifen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Nachdem das **Kontrollkästchen Einschränkung erzwingen** für den Security Incident aktiviert wurde, haben nur sn_si.admin und zulässige Mitglieder oder Gruppen Zugriff auf den Security Incident.

**f.** Klicken Sie auf **Speichern**.

## Verwalten Sie Sicherheitsbedrohungen mit Security Analyst Workspace

Security Incident Response enthält eine neue Benutzeroberfläche mit der Bezeichnung Security Analyst Workspace, die leistungsstarke Tools zur Unterstützung der Analyse enthält, darunter das Playbook, die Vorschauansicht und Registerkarten für die Bearbeitung mehrerer Security Incidents.

Die leistungsstarken Tools in Security Analyst Workspace wurden speziell für Sicherheitsanalysten entwickelt und ermöglichen die Analyse des ständig wachsenden Datenvolumens im Zusammenhang mit Security Incidents. Und automatisierte Aktionen reduzieren die Untersuchungszeit für Security Incidents erheblich, was den Unterschied zwischen dem Stoppen eines Angriffs und einem Verstoß ausmachen kann.

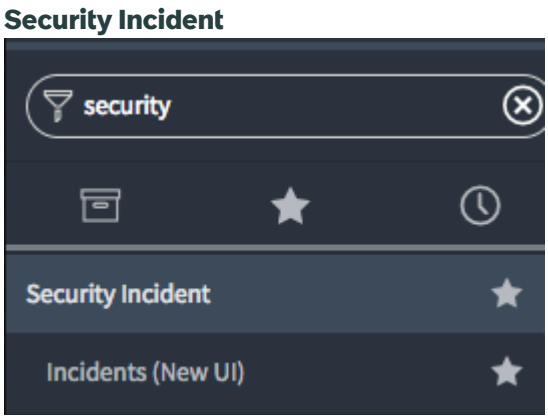
### Vor der Verwendung von Security Analyst Workspace

Bevor Sie Security Analyst Workspaceverwenden können, müssen Sie sicherstellen, dass in Ihrer Instanz mindestens London Patch 3 installiert ist und Sie die richtigen Rollen definiert haben hat die Anwendung Security Incident Response UI aus dem heruntergeladen ServiceNow Store.

**Hinweis:**
Wenn Ihre Instanz eine Version vor London Patch 3 ausführt, müssen Sie das Security Incident Response UI-Plugin über das HI Customer Service-System anfordern.

### Auf Security Analyst Workspace zugreifen

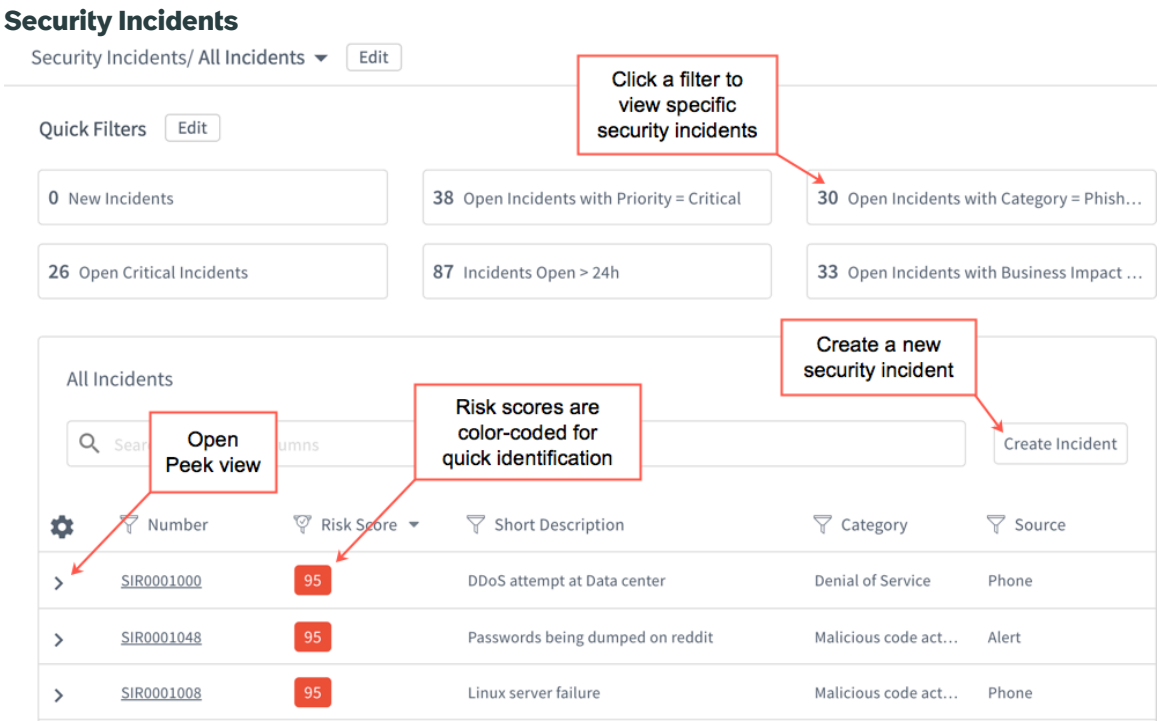
Um auf diesen neuen Arbeitsbereich zuzugreifen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.




Der Arbeitsbereich wird in einer separaten Browserregisterkarte geöffnet.

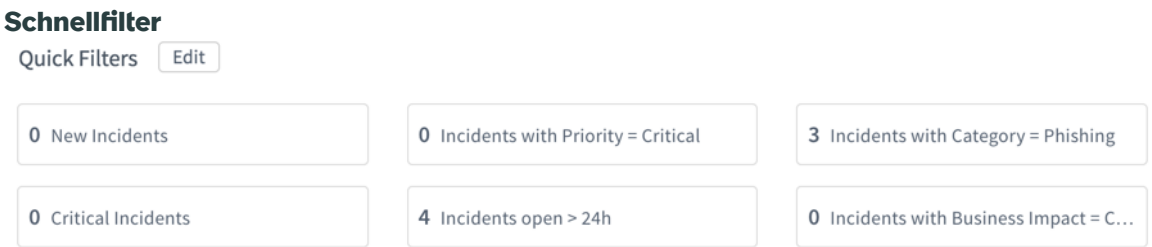


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Suchen Sie die Security Incidents, die Sie mit Schnellfiltern analysieren möchten

Security Analyst Workspace bietet mehrere Tools zum Filtern der Liste der Security Incidents, sodass Sie die Security Incidents, die Sie analysieren möchten, schnell finden können. Mit den Schnellfiltern können Sie eine Teilmenge der Security Incidents basierend auf den Kriterien im Filter auswählen.




Klicken Sie einfach auf den Schnellfilter, den Sie verwenden möchten.

**Hinweis:**
Sie können auf eine Schaltfläche **Bearbeiten** klicken, um anzugeben, welche Schnellfilter auf dem Listenbildschirm angezeigt werden sollen. Es muss mindestens ein Filter ausgewählt werden, maximal sechs.

Sie können zusätzliche Schnellfilter sowie primäre Filter für Security Analyst Workspacein der klassischen Umgebung definieren. Weitere Informationen finden Sie unter Richten Sie primäre und sekundäre Filter für ein Security Analyst Workspace.

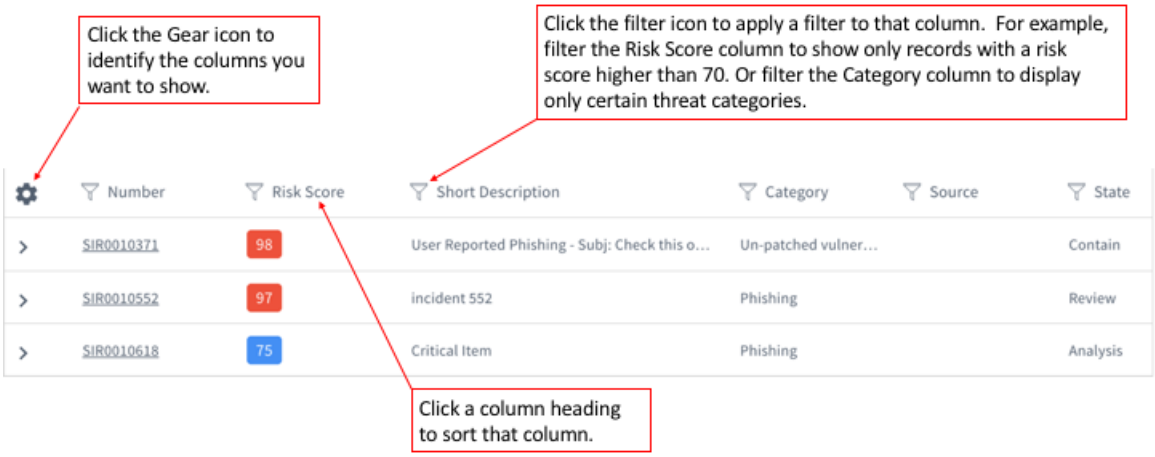
## Personalisieren Sie die Security Incident-Liste

Wie bei allen Listen in Ihrer Instanz bietet Security Analyst Workspace Tools zum Personalisieren der Liste und zum Sortieren der angezeigten Informationen, um Ihre Analyseanforderungen zu erfüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

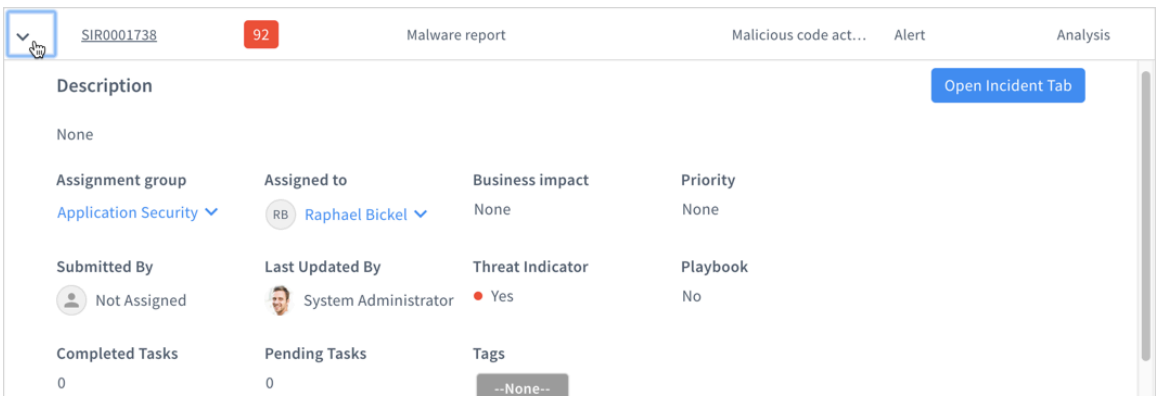
### Personalisieren Sie die Security Incident-Liste




## Sparen Sie Zeit mit der Vorschau

Bevor Sie einen Security Incident-Datensatz öffnen, können Sie in der Vorschauansicht Zeit sparen. Mit dieser Funktion können Sie wichtige Sicherheitsartefakte schnell finden, ohne die gesamte Seite neu laden zu müssen. Klicken Sie einfach auf das Symbol **>** links neben einer Security Incident-Nummer, um einen Überblick zu erhalten.

### Vorschau

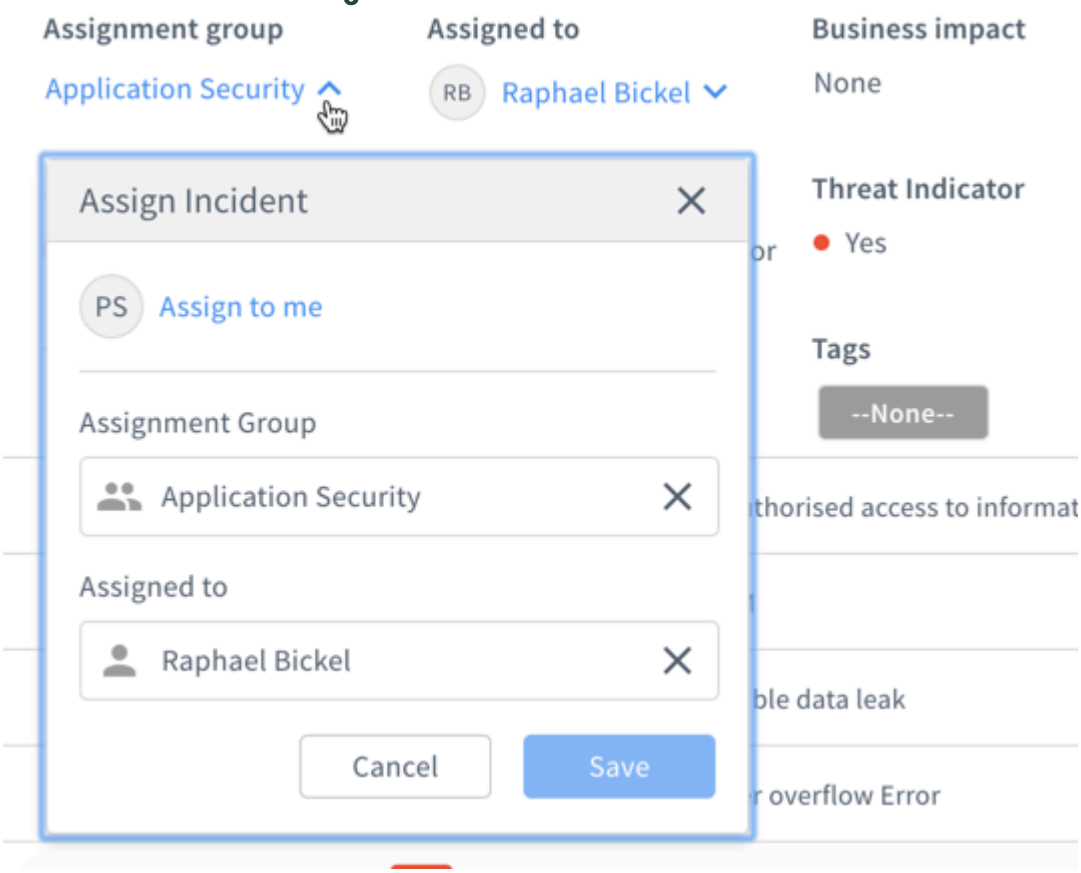



Die Vorschauansicht bietet einen Snapshot wichtiger Informationen in einer einzigen Ansicht. Diese Ansicht kann wertvolle Zeit sparen, wenn Sie mit mehreren Incidents arbeiten. Sie können auf die Abwärtspfeile in bestimmten Feldern klicken, um On-the-fly-Aktualisierungen vorzunehmen, z. B. die Zuweisung einer Zuweisungsgruppe oder eines bestimmten Analysten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Details der Vorschau anzeigen**




## Schnellaktionen für einen Security Incident ausführen

Nachdem Sie einen bestimmten Security Incident ausgewählt und geöffnet haben, können Sie zeitsparende Aktionen für den Datensatz ausführen.

- Wenn der Security Incident geöffnet ist, klicken Sie auf das Symbol **Datensatz bearbeiten**, um schnell Änderungen an einem der zugehörigen Felder vorzunehmen. Wenn der Datensatz geschlossen ist, können Sie nur sein Tag ändern.
- Klicken Sie auf **Anhänge verwalten**, um Dateien an den Security Incident anzuhängen. Sie können angehängte Dateien auch herunterladen oder entfernen und die auf die Anhänge angewendete Verschlüsselung bearbeiten.
- Klicken Sie auf E-Mail **erstellen**, um eine schnelle E-Mail an einen Kollegen zu senden. E-Mails können Freiform sein, oder Sie können vordefinierte E-Mails senden, die aus einer Liste von Vorlagen ausgewählt werden. Gesendete E-Mails und empfangene Antworten werden in der Incident-Zeitleiste erfasst.

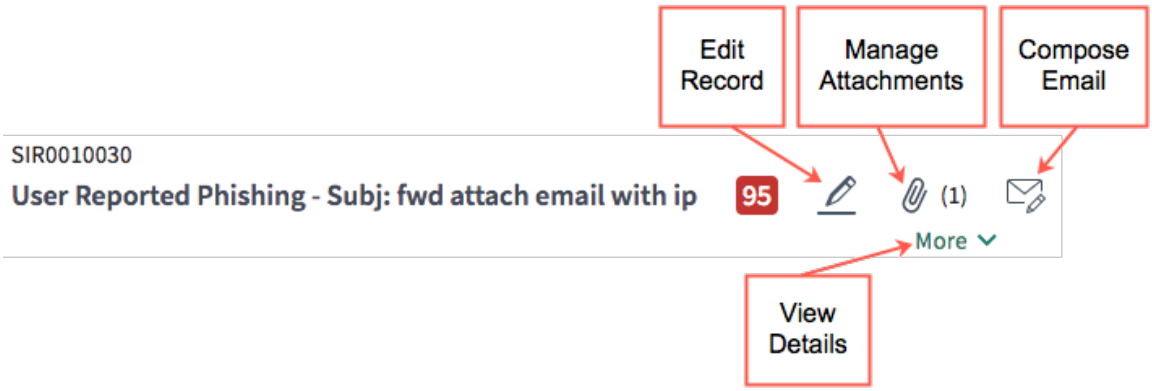
  **Hinweis:**
  Sie können benutzerdefinierte Vorlagen erstellen, die wiederverwendbare Inhalte für E-Mails und E-Mail-Benachrichtigungen enthalten. Variablen können zum Einfügen von Informationen verwendet werden, die für den Security Incident oder die Warnung spezifisch sind, z. B. Betreffzeile, Priorität oder Bedrohungskategorie. Verwenden Sie die Tabelle „Security Incident“ [sn_si_incident] für E-Mails und E-Mail-Benachrichtigungen im Zusammenhang mit Security Incident Response. Weitere Informationen finden Sie unter E-Mail-Vorlagen

- Klicken Sie auf **Mehr**, um einen schnellen Snapshot des Security Incident anzuzeigen, z. B. Beschreibung, Geschäftsauswirkung und Priorität. Sie können auch auf den Abwärtspfeil in den Feldern **Zuweisungsgruppe** und **Zugewiesen an** klicken, um Änderungen an diesen Feldern vorzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

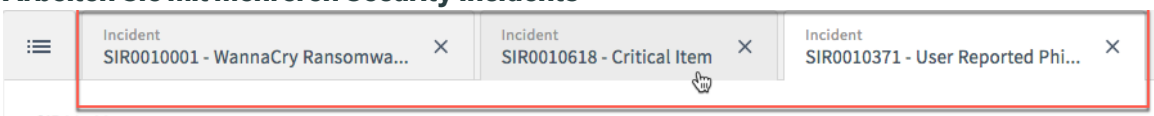
**Zuweisungsgruppe**




## Arbeiten Sie mit mehreren Security Incidents

Über die mit Registerkarten versehene Benutzeroberfläche können Sie mehrere Security Incidents gleichzeitig geöffnet lassen, sodass Sie mit einem einzigen Klick zwischen ihnen wechseln können. Dies kann Zeit sparen und ermöglicht es Ihnen, das Gesamtbild zu sehen, wenn Bedrohungen aus mehreren Quellen erkannt werden.

**Arbeiten Sie mit mehreren Security Incidents**




## Zeigen Sie Analyseinformationen auf den Registerkarten für Security Incidents an

Wenn Sie einen Security Incident-Datensatz öffnen, werden drei Registerkarten angezeigt:

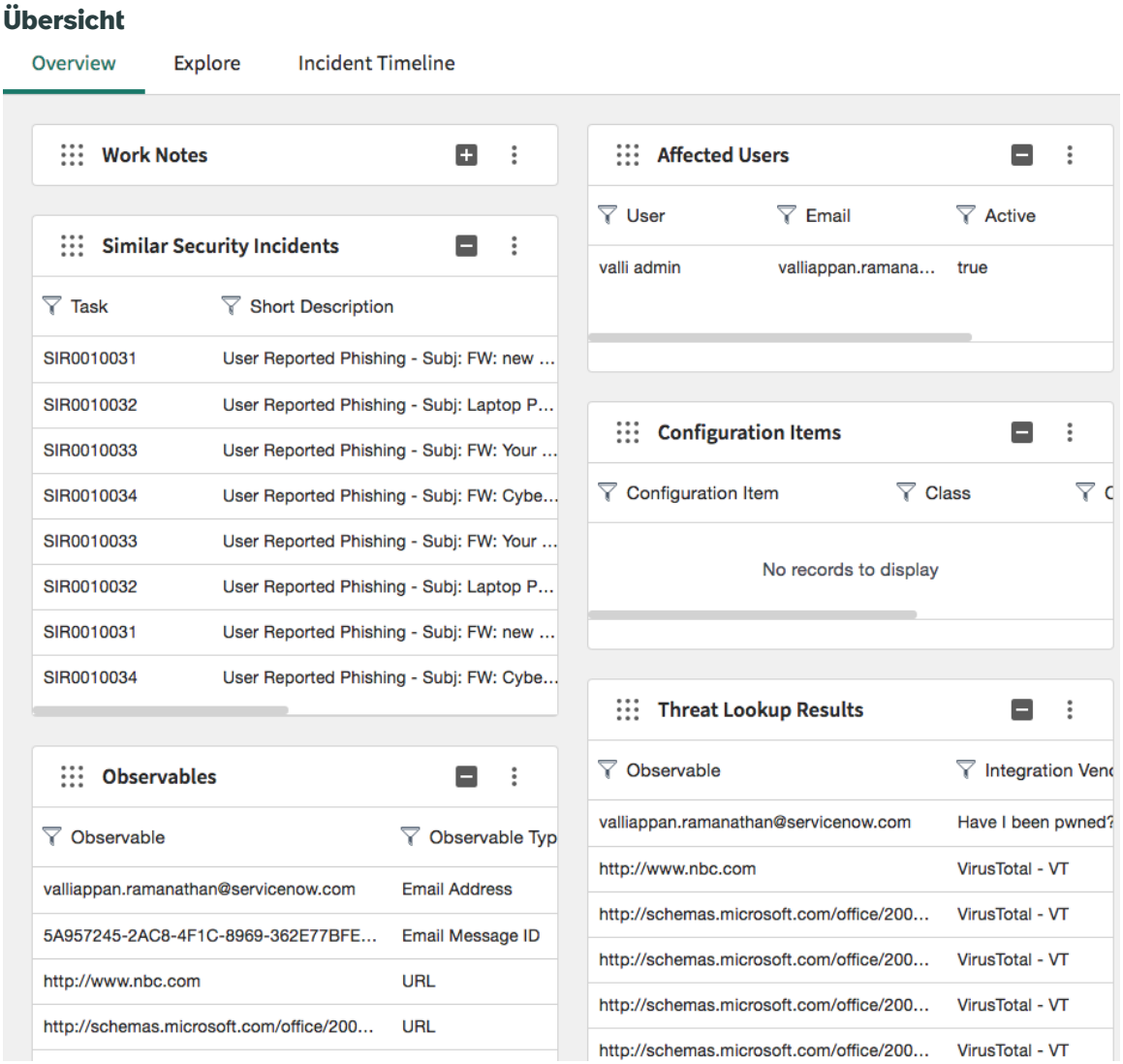
- Übersicht
- Erkunden
- Incident-Zeitleiste

## Registerkarte „Übersicht“

Verwenden Sie die Registerkarte **Übersicht**, um Informationen zu einem Security Incident an einem einzigen Ort anzuzeigen. Sie müssen keine andere Anwendung oder Konsole öffnen.

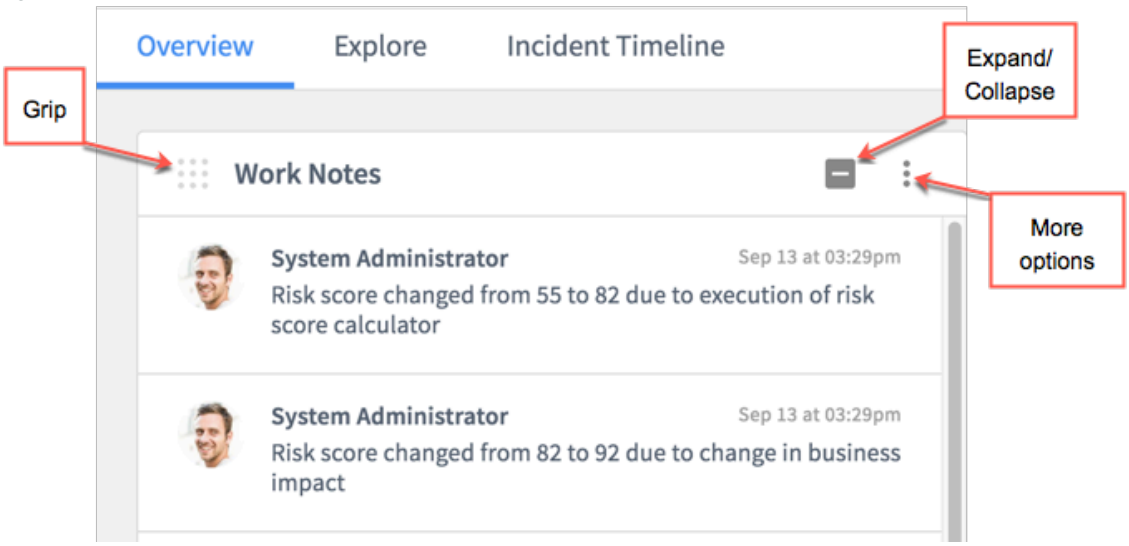


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die Kacheln, die auf der Registerkarte **Übersicht** angezeigt werden, sind anpassbar. Sie können sie nach Bedarf reduzieren und erweitern, und Sie können sie verschieben, indem Sie das **Griffsymbol** ziehen. Klicken Sie auf das Symbol **Weitere Optionen**, um eine Kachel zu löschen oder ihren Überschriftentext zu ändern.

**Registerkarte „Übersicht“**



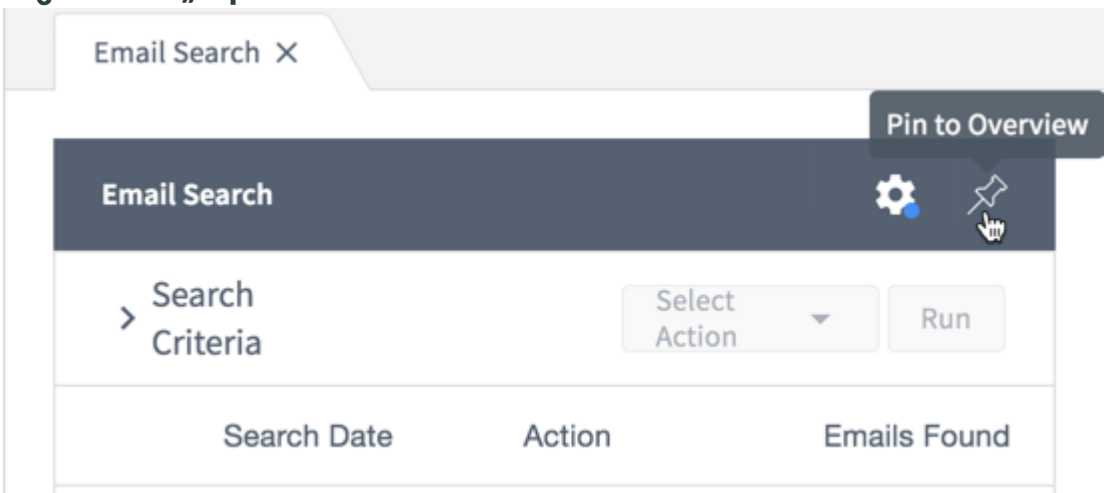

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Untersuchen“.

Konfigurieren Sie die auf der Registerkarte **Übersicht** angezeigten Kacheln mithilfe der Registerkarte **Erkunden**. Wählen Sie einfach im linken Bereich die Kacheln aus, die Sie anzeigen möchten, und **klicken** Sie auf das Symbol „Anheften“. Angeheftete Kacheln werden automatisch auf der Registerkarte **Übersicht** angezeigt.

**Registerkarte „Exportieren“.**




Der linke Bereich der **Registerkarte** „Durchsuchen“ enthält eine Vielzahl von Informationen, die Sie auf der Registerkarte „ **Übersicht** “ anzeigen können. Erweitern Sie beispielsweise Erkennbare **Elemente**, um diese zugehörigen Listen anzuzeigen.

- Erkennbare Elemente
- Suche nach Bedrohungen – Ergebnisse
- Ergebnisse des Sicherheitsscans
- Domänensuchen
- Anreicherung erkennbarer Elemente

Zusätzliche zugehörige Listen sind unter **Benutzer**, **Konfigurationselemente**und **Incidents**verfügbar.

## Registerkarte „Incident-Zeitleiste“.

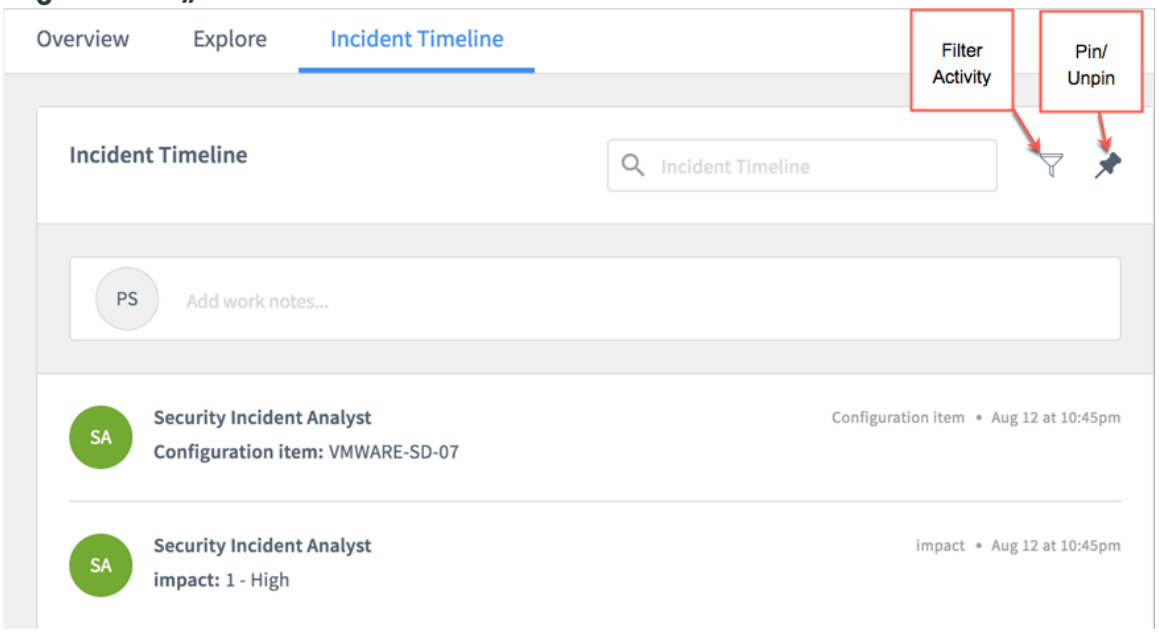
Verwenden Sie die Registerkarte **Incident-Zeitleiste** während Ihrer Untersuchung zu Nachverfolgungszwecken. Jede Aktion, die für einen Security Incident ausgeführt wird, wird vom System in der Incident-Zeitleiste aufgezeichnet.

- Sie können Arbeitsnotizen auch manuell zur Zeitleiste hinzufügen, indem Sie sie in das Feld **Arbeitsnotizen** hinzufügen eingeben und auf Veröffentlichen **klicken**.
- Sie können mithilfe des Suchfelds nach einer bestimmten Zeitleistenaktivität suchen.
- Mit dem Symbol „ **Aktivität** filtern“ können Sie nur die Arten von Zeitleistenaktivitäten anzeigen, die Sie anzeigen möchten (z. B. nur Incidents, die von einem bestimmten Analysten erstellt wurden).
- Sie können die Incident-Zeitleiste mithilfe des Symbols **„Anheften/Lösen“** auf der Registerkarte „ **Übersicht** “ hinzufügen oder entfernen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Incident-Zeitleiste“.**




## Behandeln Sie Security Incidents mit dem Playbook

Beheben Sie bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt mit den integrierten Security Analyst Playbooks. Beispielsweise kann ein Analyst das Playbook verwenden, um Phishing-Angriffe und Bedrohungen zu beheben, die durch Aktivitäten mit böswilligem Code verursacht werden. Weitere Informationen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

## Beheben Sie Sicherheitsbedrohungen mit dem Playbook

Verwenden Sie das Playbook, um bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt zu beheben. Sie können beispielsweise Phishing-Angriffe und -Bedrohungen, die durch böswillige Codeaktivitäten verursacht werden, mithilfe von Playbooks beheben.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder admin

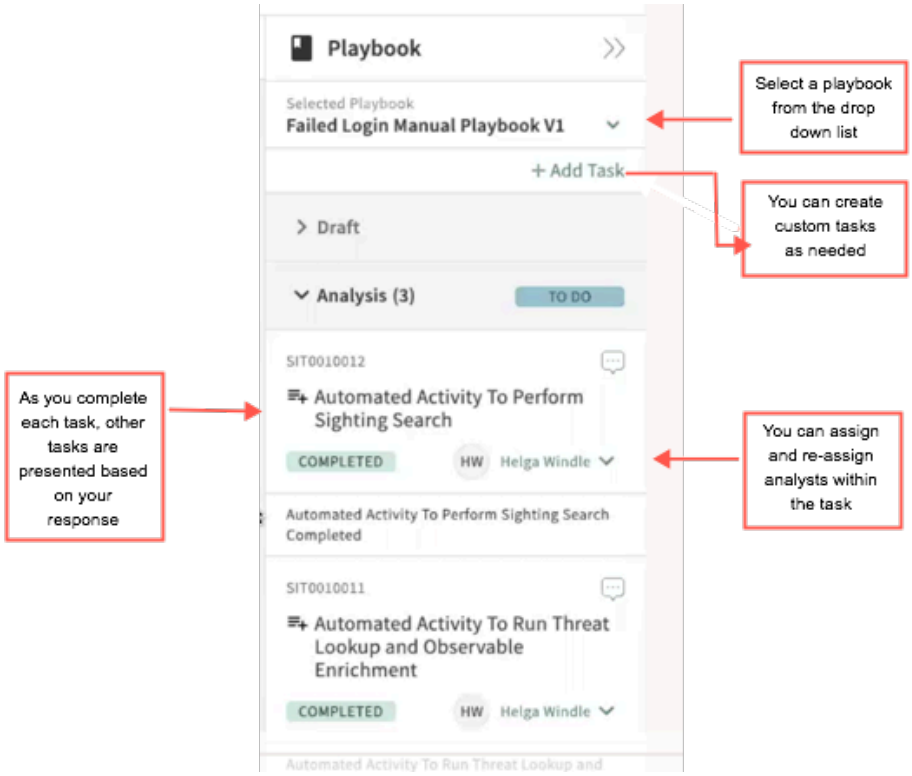
### Warum und wann dieser Vorgang ausgeführt wird

Jede Gruppe von Aufgaben (Analyse, Eindämmung usw.) führt Sie durch eine Reihe von Fragen und anderen Aktivitäten zur Lösung der Bedrohung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

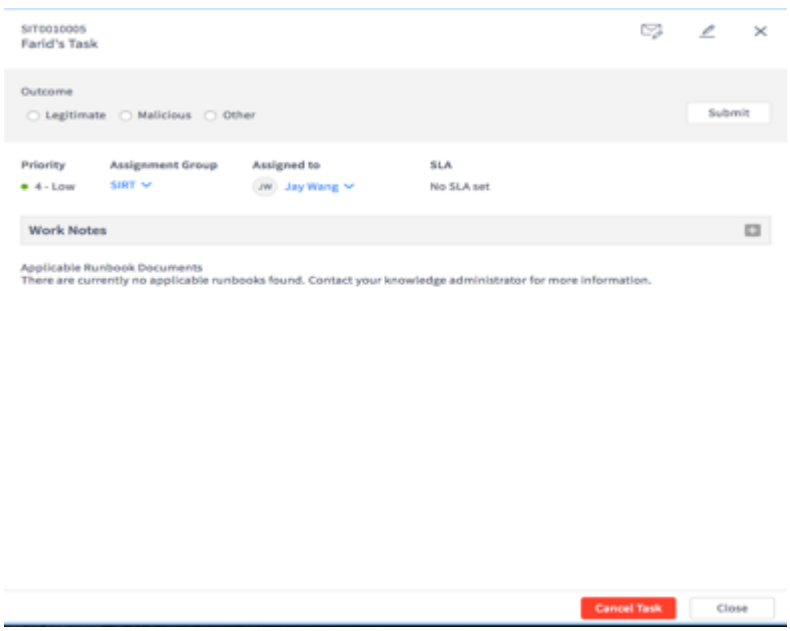
### Playbook




Geben Sie beim Durcharbeiten der einzelnen Aufgaben Arbeitsnotizen ein, um in Zukunft ähnliche Angriffe zu analysieren. Nachdem eine Bedrohung identifiziert wurde, können Sie die Informationen im Playbook auch verwenden, um die Bedrohung unter Quarantäne zu stellen, ähnlich betroffene Assets zu isolieren und Malware zu entfernen.

Wissensartikel, die in jeder Aufgabe enthalten sind, enthalten Tipps und andere Informationen, die Sie bei der Ausführung der erforderlichen Schritte unterstützen.

### Wissensartikel




Das Basissystem enthält Wissensartikel für jede der Playbook-Aufgaben. Sie können jedoch eigene Wissensartikel schreiben und sie Playbook-Aufgaben zuordnen.

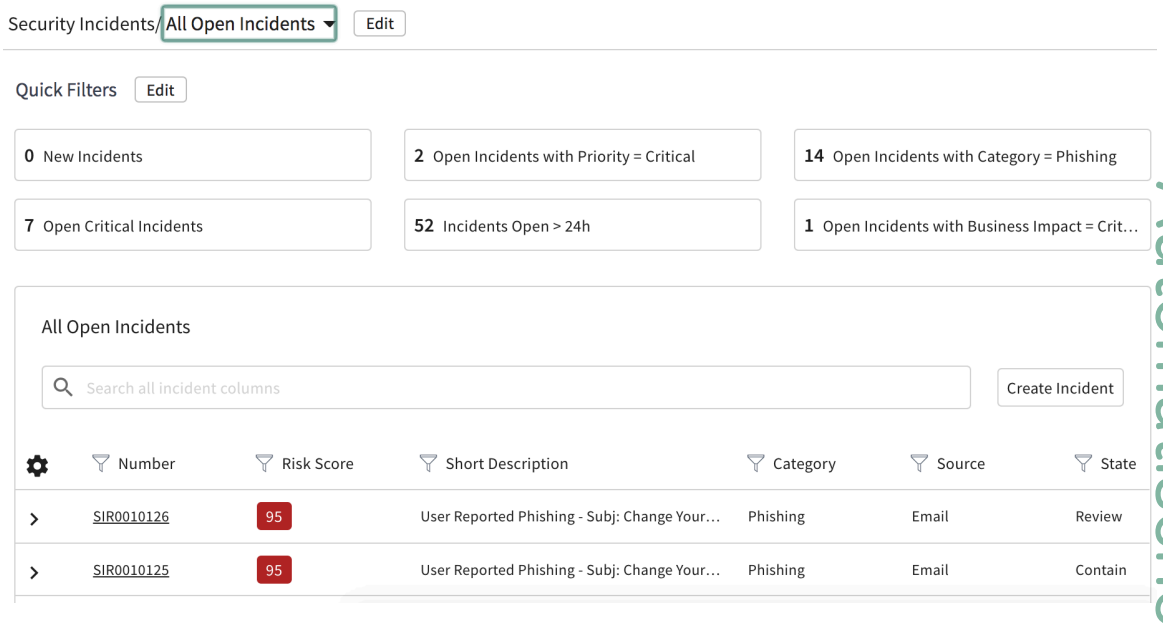


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ein Beispiel für die Verwendung des Playbooks zum Analysieren und Beheben einer bestimmten Bedrohung finden Sie unter Behebung von von Benutzern gemeldeten Phishing-Angriffen mit dem Playbook.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents (neue UI)**.
   Der Bildschirm „Security Incidents“ zeigt Security Incidents, die Ihnen zugewiesen wurden.



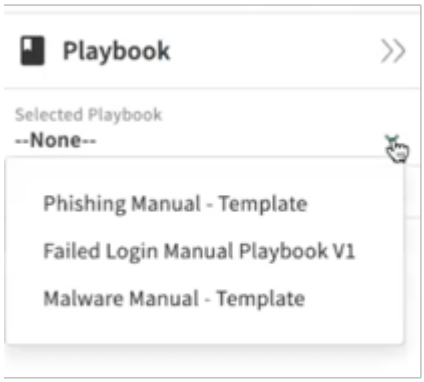

2. Sie können auf die **Auswahlliste Mir zugewiesen** klicken, um einen anderen Filter auszuwählen, z. B. alle offenen Incidents oder alle nicht zugewiesenen Incidents.
   Alternativ können Sie auf einen der Schnellfilter klicken, um Security Incidents eines bestimmten Typs anzuzeigen, z. B. nur kritische Incidents.
3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

   Erwägen Sie die Priorisierung von Security Incidents mit hohen Risikopunktzahlen.

4. Wenn der Playbook-Bereich am rechten Rand des Bildschirms geschlossen ist, klicken Sie auf das Playbook-Symbol ( ), um ihn zu öffnen.
   Wenn dem Security Incident kein Playbook zugewiesen ist, können Sie wie unten gezeigt ein Playbook aus der Auswahlliste Ausgewähltes Playbook auswählen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






Sie können dem Security Incident auch ein anderes Playbook zuweisen. Wie Sie ein Playbook in die Auswahlliste Ausgewähltes Playbook aufnehmen oder das Playbook für einen Security Incident ändern, erfahren Sie unter Aktivieren Sie Playbooks für die Analystenauswahl.

Das für den Typ der Sicherheitsbedrohung spezifische Playbook wird geöffnet. Sie ist in Kategorien mit ähnlichen Aufgaben unterteilt. Verwenden Sie beispielsweise die Aufgaben in der Gruppe „ **Analyse** “, um die Gültigkeit und den Umfang der Bedrohung zu bestimmen. Die Gruppe „ **Enthalten** “ enthält Aufgaben zum Eingrenzen der Bedrohung für einen bestimmten Benutzer oder ein bestimmtes Asset. Die Aufgaben in der Gruppe „ **Beseitigen** “ führen Sie durch den Prozess zum Entfernen der Malware oder zum erneuten Erstellen eines Host-Images.

5. Klicken Sie auf die erste Gruppe (**Analyse**), und klicken Sie dann auf die erste Aufgabe im Playbook.
6. Befolgen Sie die Anweisungen in der Aufgabe.
   - Einige Aufgaben stellen eine Frage, z. B. „Ist E-Mail Teil der Kampagne?“. Führen Sie die erforderliche Analyse durch, um die Frage zu beantworten, und wählen Sie **Ja** oder **Nein**.
   - Wenn Sie Wissensartikel definiert und Playbook-Aufgaben zugeordnethaben, werden die Artikel angezeigt, wenn Sie mit der Arbeit an einer Aufgabe beginnen.
   - Einige Aufgaben sind Übergangsaufgaben. Sie weisen Sie einfach an, eine Aktion auszuführen, z. B. einem Security Incident erkennbare Elemente hinzuzufügen. Klicken Sie nach Abschluss der Aktion auf **Als abgeschlossen markieren**.

   Wenn Sie Aufgaben abschließen, werden Ihnen basierend auf den von Ihnen getroffenen Entscheidungen nachfolgende Aufgaben angezeigt. Ausgegraute Gruppen (z. B. **Wiederherstellen**, **Überprüfen**usw.) können durch Ihre Auswahl aktiviert werden.
7. Setzen Sie die Arbeit an jeder Aufgabe fort, bis Sie alle Aufgaben abgeschlossen haben, um die Bedrohung zu beheben und den Security Incident zu schließen.

**Zugehörige Informationen**

Fügen Sie dem Playbook eine benutzerdefinierte Aufgabe hinzu

## Behebung von von Benutzern gemeldeten Phishing-Angriffen mit dem Playbook

Das Phishing-Playbook führt Sie durch die Aufgaben, die für die Analyse und Lösung eines von einem Mitarbeiter Ihres Unternehmens gemeldeten Phishing-Angriffs erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

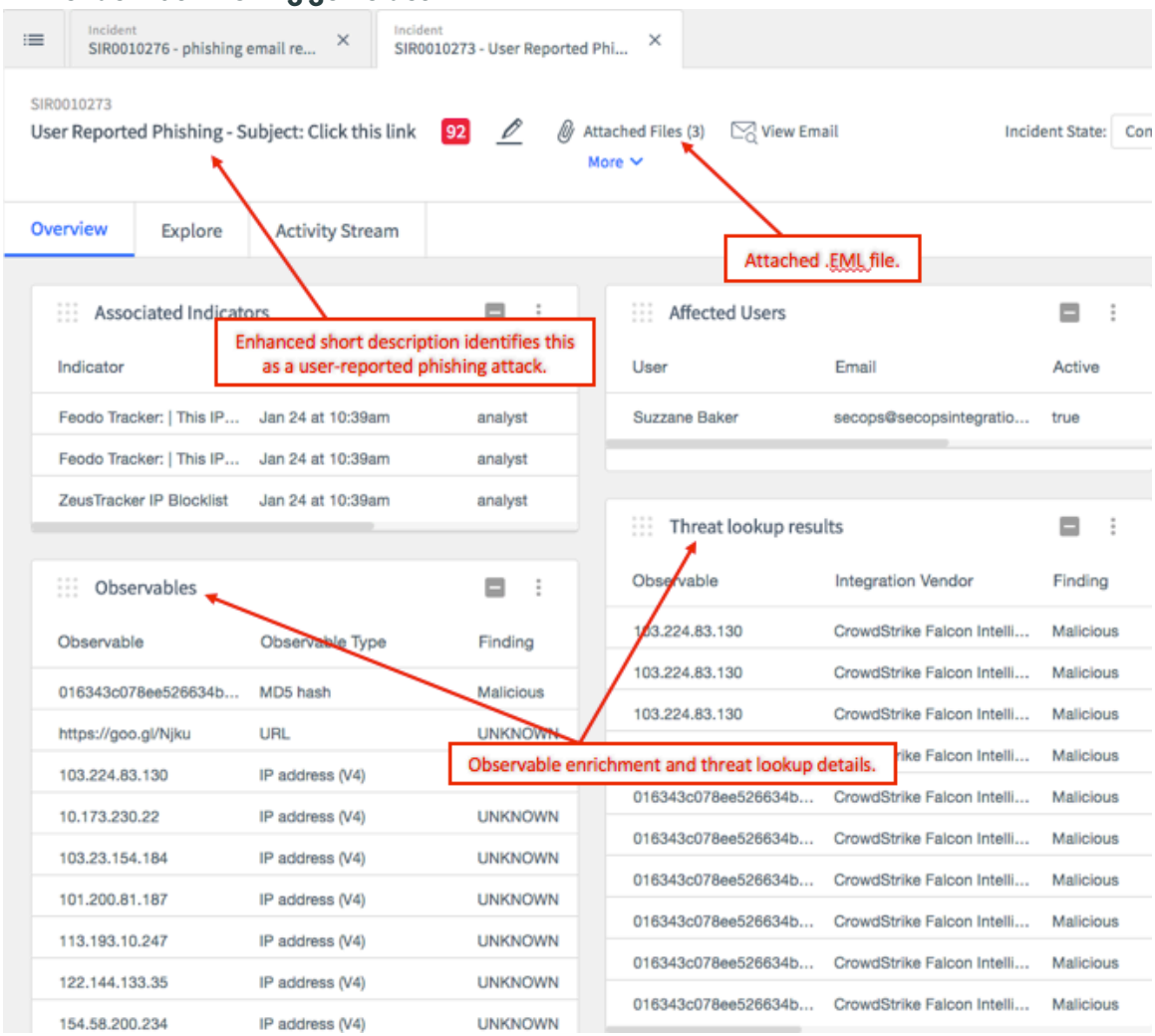
## Wie Security Incidents aus von Benutzern gemeldeten Phishing-Angriffen erstellt werden

Während der Einrichtung von Security Incident Response erstellt Ihr Systemadministrator eine Reihe von E- Mail-Abgleichregeln, die E-Mails identifizieren können, die Anzeichen eines Phishing-Angriffs enthalten. Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die häufigsten Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie sie als EML-Anhang an die von Ihrer Organisation festgelegte Phishing-E-Mail-Adresse senden.

Wenn die E-Mail an der Phishing-E-Mail-Adresse empfangen wird, wird der EML-Anhang analysiert und seine Informationen werden mit den E-Mail-Abgleichregeln verglichen. Wenn eine Übereinstimmung gefunden wird, wird ein Security Incident mit den folgenden Informationen erstellt:

- Die Kurzbeschreibung enthält Phishing vom Anwender gemeldet, gefolgt vom eigentlichen Betreff der ursprünglichen E-Mail.
- Die EML-Datei wird an den Security Incident angehängt.
- Wenn die EML-Datei erkennbare Elemente enthielt, werden diese analysiert, und Ergänzungs- und Bedrohungssuchen werden automatisch durchgeführt.

### Anwender hat Phishing gemeldet

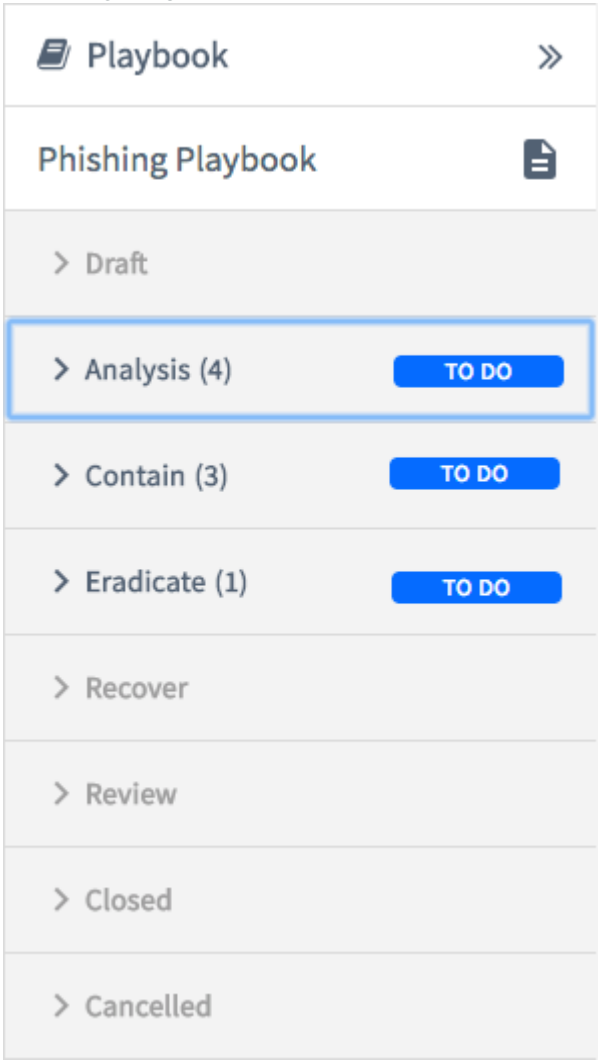





© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Security Incident der Kategorie „Phishing“ geöffnet wird, ist das Phishing-Playbook automatisch verfügbar. Klicken Sie einfach auf das Playbook-Symbol ( ), um das Playbook zu öffnen.

**Phishing-Playbook**




Das Phishing-Playbook enthält Aufgaben, die Sie bei der Analyse, Eindämmung und Beseitigung einer Phishing-Bedrohung unterstützen. Die Aufgaben sind in Status organisiert (z. B. **Analyse**, **Eindämmen**usw.). Wenn alle Aufgaben für einen Status abgeschlossen wurden, führt Sie das Playbook zum nächsten Status.

## Details zu Security Incidents werden analysiert

Wenn sich der Security Incident im Status „Analyse“ befindet, erhalten Sie Aufgaben zur Durchführung grundlegender Untersuchungen des Incidents, einschließlich:

- Bestimmen der Gültigkeit des Incident.
- Untersuchung der Auswirkungen der potenziellen Bedrohung.
- Eine effektive Reaktion auf den Incident koordinieren.

Während Sie die Aufgaben durcharbeiten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Machen Sie sich mit den Wissensartikeln vertraut.
- Öffnen Sie den E-Mail-Anhang, und untersuchen Sie ihn auf Anzeichen für häufige Phishing-Elemente.
- Überprüfen Sie die Ergebnisse der Bedrohungssuche.

### Eindämmung des Security Incident

Wenn sich der Security Incident im Status „ **Eindämmen** “ befindet, erhalten Sie Aufgaben zur Überprüfung der Details der E-Mail. Um sicherzustellen, dass Bedrohungen nicht in Ihre Organisation gelangen können, aktualisieren Sie Ihre Netzwerkabwehr in Form von Signaturen und Regeln für das Angriffsabwehrsystem (IDS) und das Angriffsverhinderungssystem (IPS).

Während Sie die Aufgaben durcharbeiten:

- Ergreifen Sie Maßnahmen, um die Auswirkungen von Bedrohungen zu begrenzen, z. B. die Isolierung der betroffenen Geräte.
- Überprüfen Sie die an die E-Mail angehängten erkennbaren Elemente.
- Stellen Sie fest, ob E-Mail-Inhalte einer bekannten Bedrohung zugeordnet sind, einschließlich:
  - URL
  - E-Mail-Absender
  - Phishing-URL
  - IP-Adresse des SMTP-Servers des Absenders

### Die Malware wird entfernt

Nachdem Sie aktualisierte Signaturen und Regeln für Ihre Antivirenlösung bereitgestellt haben, verwenden Sie die Aufgaben im Status „ **Beseitigen** “, um festzustellen, ob Malware vorhanden ist, und sie entsprechend zu behandeln.

Während Sie die Aufgaben durcharbeiten:

- Scannen Sie die Endpunkte der betroffenen Geräte auf Malware.
- Entfernen Sie die gefundene Malware.
- Als letzten Ausweg können Sie die Hostgeräte löschen und ein neues Image erstellen.

### Überprüfen des Security Incident

Wenn Sie bei der Ausführung der Analyseaufgaben festgestellt haben, dass ein Phishing-Angriff ein falscher Alarm war, wird der Security Incident in den **Überprüfungsstatus** versetzt, und Sie müssen Ihre Benutzer benachrichtigen, damit sie wissen, dass der E-Mail-Anhang sicher geöffnet werden kann.

### Der Security Incident wird geschlossen

Wenn alle Aufgaben im Playbook abgeschlossen sind, wird der Security Incident in den Status „ **Geschlossen** “ verschoben. Sie müssen Abschlusskommentare eingeben, bevor der Incident geschlossen werden kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Abbruch eines Security Incident

Wenn sich ein Security Incident im **Überprüfungsstatus** befindet und Sie Ihre Benutzer erfolgreich darüber informiert haben, dass die E-Mail keine Bedrohung darstellt, wird der Status **Abgebrochen aktiviert**, und Sie können den Security Incident abbrechen.

**Hinweis:**
Die Aufgabe „Wiederherstellen“ wird im Phishing-Playbook nicht verwendet.

### Verknüpfen Sie einen Wissensartikel mit einer Playbook-Aufgabe

Wenn Sie Sicherheitsbedrohungen mit dem Playbook Security Incident Response analysieren, können Sie Wissensartikel für jede Aufgabe anzeigen, sofern dies von Ihrer Organisation definiert wurde. Wenn keine Wissensartikel vorhanden sind, können Sie sie erstellen und Playbook-Aufgaben zuordnen.

#### Vorbereitungen

Wenn Sie das Playbook in Security Incident Responseverwenden, beachten Sie den Text, der jeder Aufgabe zugeordnet ist. Zum Beispiel lautet die erste Aufgabe in der Phishing-Kategorie „ **Wurde vom Mitarbeiter benachrichtigt?“ – Übermittelt?** Dies ist die Kurzbeschreibung der Aufgabe. Sie benötigen diesen Text (genau so, wie er im Playbook angezeigt wird), um der Aufgabe einen Wissensartikel zuzuordnen.

Erforderliche Rolle: sn_sir.knowledge_admin und entweder sn_si.admin oder admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**.
2. Erstellen und veröffentlichen Sie einen Wissensartikel für eine bestimmte Playbook-Aufgabe.
3. Navigieren zu **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**.
4. Erstellen Sie ein Runbook, indem Sie die folgenden Informationen ausfüllen:

| Feld | Beschreibung |
|---|---|
| Wissensartikel | Wählen Sie den veröffentlichten Wissensartikel aus, den Sie der Playbook-Aufgabe zuordnen möchten. |
| Tabelle | Wählen Sie Security Incident Response Aufgabe [sn_si_task]. |
| Bedingung | Legen Sie den Bedingungsgenerator fest auf:<br>○ **Option:** Wählen Sie **Kurzbeschreibung aus**.<br>○ **Operator:**Wählen Sie **ist**aus.<br>○ **Eingabewert:** Geben Sie die Kurzbeschreibung für die Aufgabe genau so ein, wie sie im Playbook angezeigt wird. |

5. Klicken Sie auf **Absenden**.
   Wenn Sie das Playbook das nächste Mal ausführen und diese Aufgabe auswählen, wird der zugehörige Wissensartikel angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zugehörige Informationen**

Erstellen Sie einen Wissensartikel zu Security Incidents

Erstellen Sie ein Security Incident Response-Runbook

### Fügen Sie dem Playbook eine benutzerdefinierte Aufgabe hinzu

Das Security Analyst Workspace Basissystem enthält eine Reihe von Aufgaben für jede Bedrohungskategorie. Sie können benutzerdefinierte Aufgaben erstellen, die den spezifischen Anforderungen Ihres Systems oder Ihrer Kunden entsprechen.

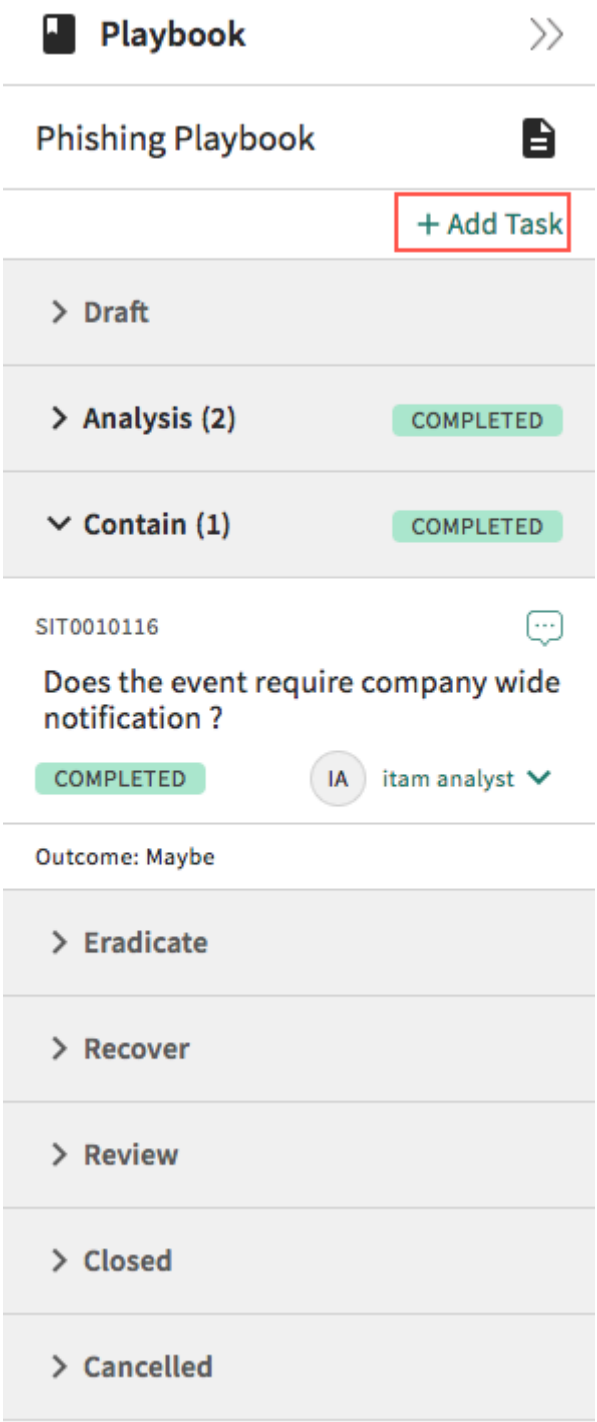
**Vorbereitungen**
Erforderliche Rolle: sn_si.basic oder security_admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

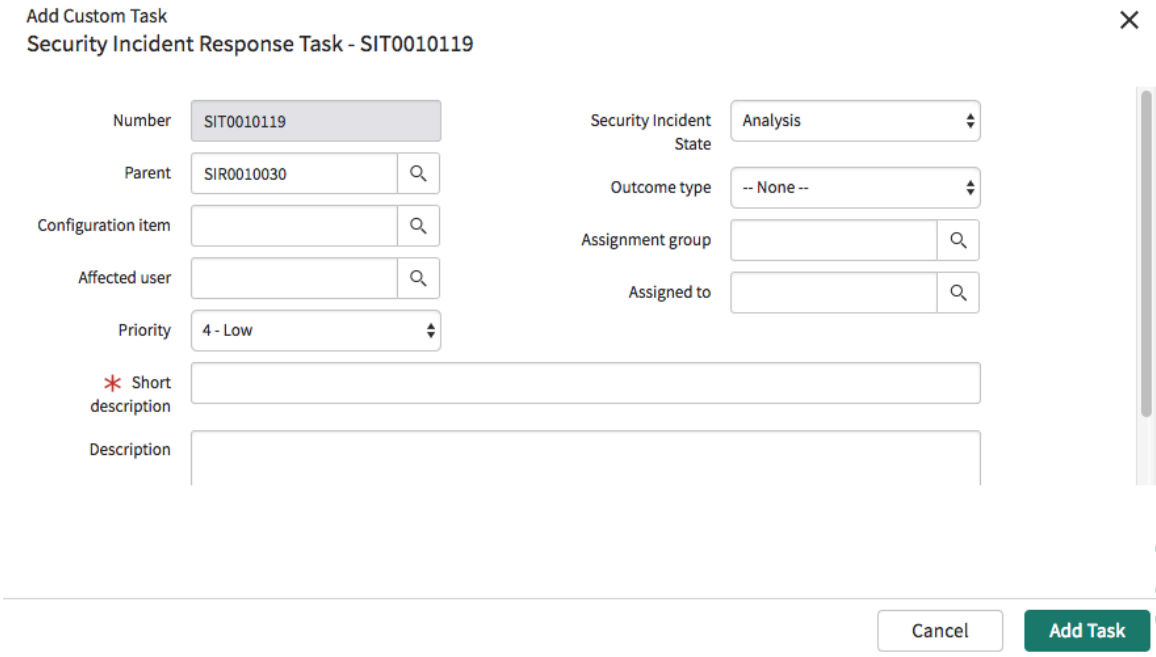
**1.** Klicken Sie bei geöffnetem Playbook auf **Aufgabe hinzufügen**.




Der Bildschirm Benutzerdefinierte Aufgabe hinzufügen wird geöffnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**2.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Nummer | [Nur Lesen] Die automatisch generierte Nummer der Security Incident-Aufgabe. |
| Übergeordnet | Die Nummer des zugehörigen Security Incidents. |
| Konfigurationselement | Das vom Sicherheitsproblem betroffene Konfigurationselement, falls vorhanden. |
| Betroffener Anwender | Der vom Sicherheitsproblem betroffene Benutzer, falls vorhanden. |
| Priorität | Wählen Sie die Priorität aus, die bestimmt, wann diese Aufgabe ausgeführt werden soll. |
| Status des Security Incidents | Aktueller Status der Sicherheitsreaktionsaufgabe Sie können bei Bedarf einen zukünftigen Status auswählen. |
| Ergebnistyp | Wenn Sie die Rolle „sn_si.basic“ haben, wählen Sie **Ja/Nein** als Ergebnistyp aus.<br><br>Wenn Sie die Rolle „security_admin“ haben, können Sie einen benutzerdefinierten Ergebnistyp mit mehreren benutzerdefinierten Ausgabewerten erstellen. Sie können beispielsweise eine Aufgabe mit abhängigen Werten basierend auf der Bedrohungskategorie definieren. Weitere Informationen finden Sie unter Auswahllisten |
| Zuweisungsgruppe | Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird. |
| Zugewiesen an | Die Person, der die Aufgabe zugewiesen wurde. |
| Kurzbeschreibung | Eine Beschreibung der Security Incident-Playbook-Aufgabe. |
| Beschreibung | Geben Sie eine Beschreibung für die ausgewählte Aufgabe ein. |

**3.** Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie auf **Aufgabe hinzufügen**.
Die Aufgabe wird nach der aktuellen Aufgabe in das Playbook eingefügt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Sichtungssuchen nach von Benutzern gemeldeten Phishing- und Malware-Angriffen

Führen Sie Sichtungssuchen für E-Mails oder erkennbare Elemente durch, um zu bestimmen, wie oft bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder Kommunikation mit einer schädlichen IP oder URL, in Ihrem Netzwerk auftreten. Jedes Vorkommen wird als Sichtung betrachtet. Sichtungssuchen nach erkennbaren Elementen müssen für Ihre Protokollspeicher oder Security Information and Event Management (SIEM) konfiguriert werden.

So verwenden Sie die Sichtungssuchfunktion, um Phishing-Anwender zu finden und erkennbare Phishing- und Malware-Elemente im Protokollspeicher in Ihrem Netzwerk nachzuverfolgen.

Sehen Sie sich dieses dreiminütige Video an, um zu erfahren, wie Sie die Sichtungssuchfunktion verwenden, um Phishing-Anwender zu finden und erkennbare Phishing- und Malware-Elemente im Protokollspeicher in Ihrem Netzwerk nachzuverfolgen.

Die folgenden Begriffe werden verwendet, um von Benutzern gemeldete Phishing-Angriffe zu beschreiben:

- Phishing-Anwender: Ein Anwender, der eine Phishing-E-Mail erhalten hat.
- Opferanwender: Ein Anwender, der mit der Phishing-URL interagiert hat, in der Regel durch Klicken auf einen Link in der Phishing-E-Mail. Mit dieser Aktion werden dem Angreifer möglicherweise Anmeldeinformationen zur Verfügung gestellt.

Wenn Sie mit der Analyse eines Phishing-Incident beginnen, können Sie eine E-Mail-Sichtungssuche durchführen oder eine Suche nach erkennbaren Sichtungen durchführen, um andere Benutzer in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind. Durchsuchen Sie Ihre Protokollspeicher, um Phishing-Anwender und Anwender zu identifizieren. Nachdem Sie die Liste der betroffenen Benutzer identifiziert haben, erstellen Sie untergeordnete Security Incidents, um mit den in Security Incident Responseverfügbaren Tools umfassende Verfahren zur Reaktion auf Incidents durchzuführen.

**Hinweis:**
Sie können auch den folgenden Ansatz verwenden, um eine Sichtungssuche durchzuführen:

- Navigieren zu **Security Incidents** > **Alle Incidents anzeigen** und klicken Sie auf einen Security Incident.
- Klicken Sie unter Zugehörige Links auf **IoC** anzeigen. Eine Liste der erkennbaren Elemente wird angezeigt.
- Wählen Sie ein erkennbares Element aus der Liste aus, und wählen Sie in der Liste **Aktionen** eine der folgenden Optionen aus:
  - Führen Sie eine Webdatenverkehrs-Sichtungssuche aus
  - Führen Sie die Suche nach Sichtungen des E-Mail-Datenverkehrs aus
- Geben Sie den Zeitrahmen an, und klicken Sie auf **Suche**, um eine Sichtungssuche durchzuführen.

## Sichtungssuchkonfigurationen gespeichert

Konfigurieren Sie Sichtungssuchen, und erstellen Sie gespeicherte Konfigurationen für SIEMs oder andere Protokollspeicher für Instanzen von erkennbaren Elementen, um das Vorhandensein schädlicher erkennbarer Elemente in Ihrer Umgebung zu bestimmen.

**Hinweis:**
Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zugehörige Informationen**

Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

## Führen Sie eine E-Mail-Sichtungssuche nach von Benutzern gemeldeten Phishing-Angriffen durch

Suchen Sie nach Benutzern, die Phishing-E-Mails erhalten haben, basierend auf erkennbaren Elementen wie E-Mail-Betreff, Absendername oder Nachrichten-ID. Anschließend können Sie diese Phishing-E-Mails in Ihrer Organisation eindämmen und entfernen.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Durchsuchen Sie die Splunk-E-Mail-Datenverkehrsprotokolle, um die Liste der Empfänger einer verdächtigen E-Mail zu erfassen. Die Suche kann anhand des E-Mail-Absenders, der E-Mail-Nachrichten-ID oder des E-Mail-Betreffs, der einem Security Incident zugeordnet ist, als Kriterien durchgeführt werden.

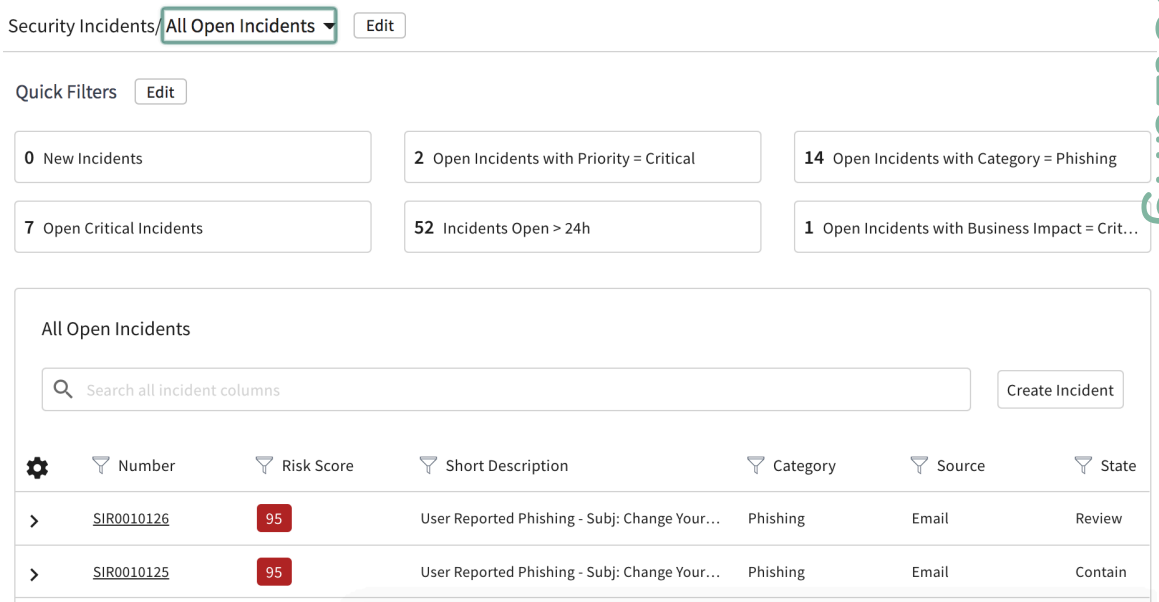
**Hinweis:**

- Diese Implementierung der Sichtungssuche für E-Mail-basierte erkennbare Elemente wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokoll-Events müssen mit dem Common Information Model (CIM) kompatibel sein, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

### Prozedur

1. Um die Ihrem Team zugewiesenen Security Incidents anzuzeigen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.
2. Wählen Sie in der Liste „ **Security Incidents** “ einen der Filter aus, z. B. alle **offenen Incidents**, **alle Ihnen zugewiesenen Incidents**oder **alle Incidents**.

   Um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails, klicken Sie auf einen der **Schnellfilter**.

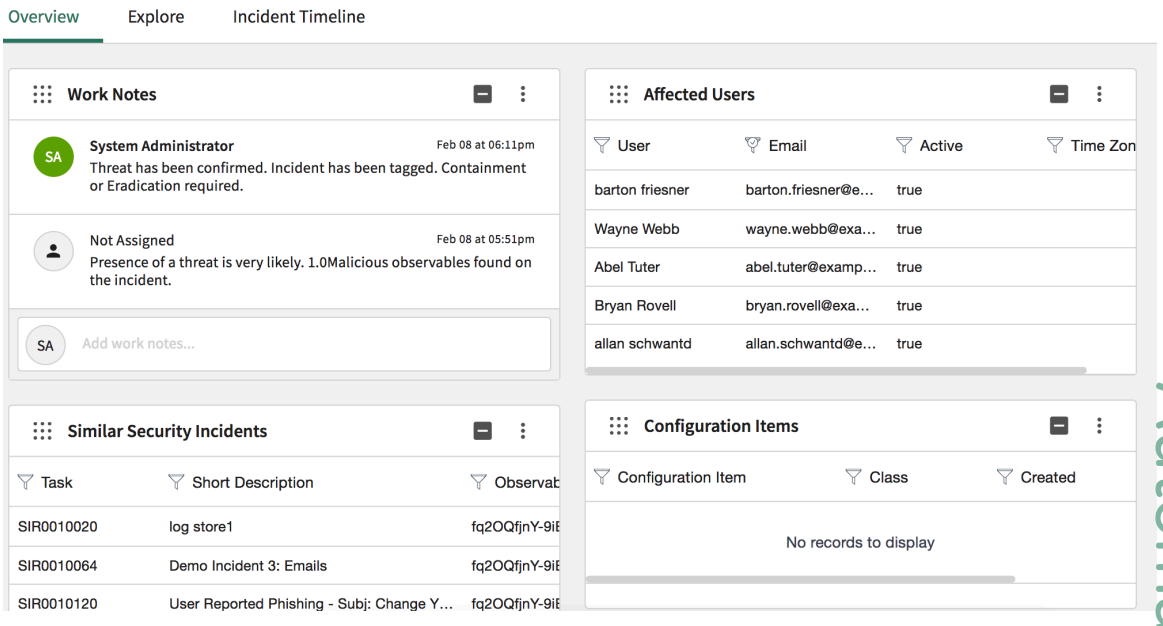



3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

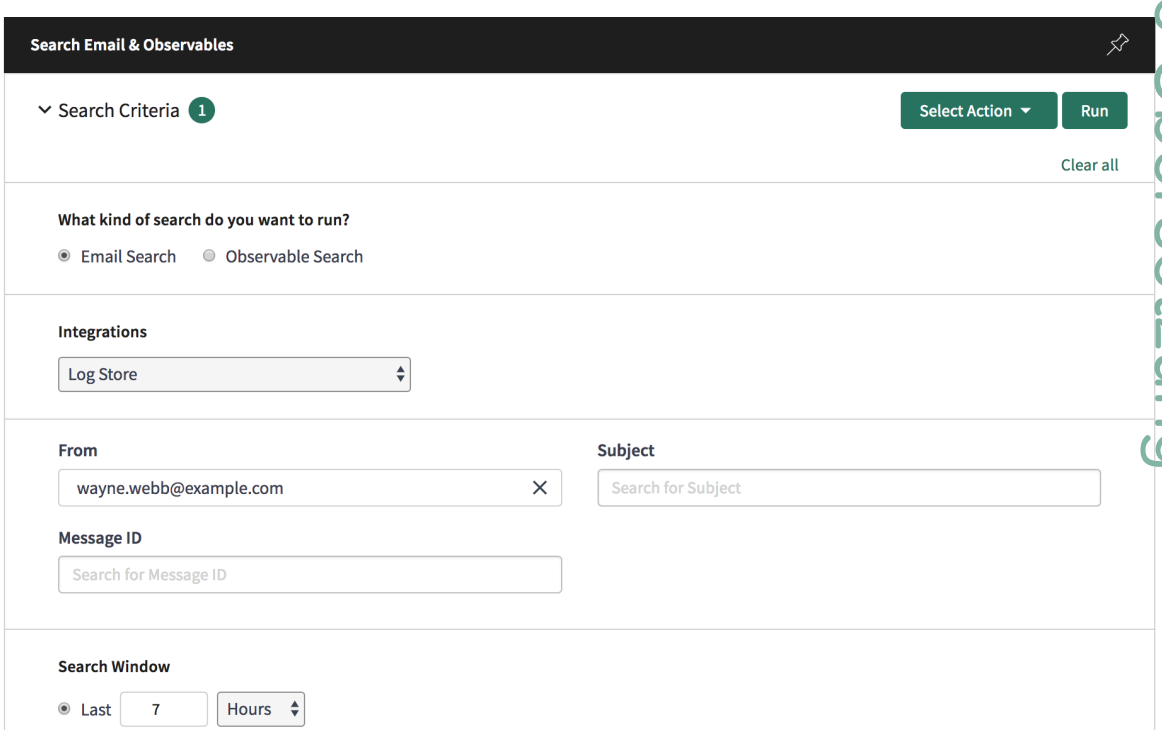
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Registerkarte Übersicht bietet eine Übersicht über den Security Incident, einschließlich einer Liste von erkennbaren Elementen, betroffenen Benutzern und ähnlichen Security Incidents.




4. Klicken Sie auf die Registerkarte **Erkunden**.
5. Navigieren Sie unter **Incident-Daten**zu **Ermittlung** > **E-Mail und erkennbare Elemente durchsuchen**.




6. Erweitern Sie den Abschnitt Suchkriterien.
7. Wählen Sie E- **Mail-Suche** als Suchtyp aus, den Sie ausführen möchten, und geben Sie die restlichen Suchkriterien an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Suchkriterien“.**

| Feld | Beschreibung |
|---|---|
| Integrationen | Integrationstyp. Wählen Sie **Protokollspeicher** aus der Liste aus.<br><br>**Hinweis:**<br>Diese Funktion wird nur mit dem Splunk-Protokollspeicher unterstützt. |
| Von | Vollständige E-Mail-Adresse des Absenders (z. B. jane.doe@example.com). |
| Nachrichten-ID | E-Mail-Nachrichten-ID aus dem Protokollspeicher. |
| Betreff | Betreff der Phishing-E-Mail. |
| Suchfenster | Zeitfenster für die Suche (z. B. die letzten 24 Stunden). |

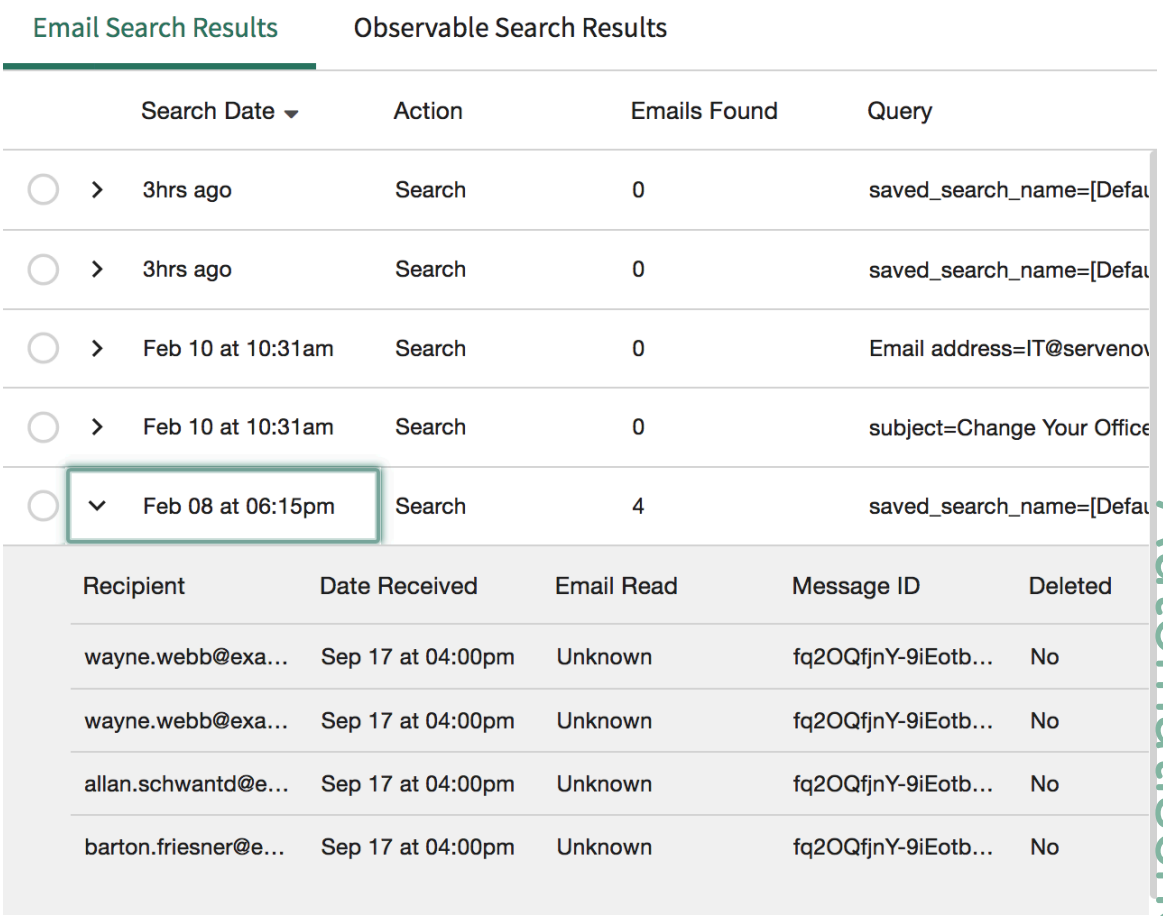
8. **Wählen Sie in der Liste Aktion** auswählen die Option **Suche** aus, und klicken Sie dann auf **Ausführen**.

   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die Benutzer, die Ziel des Phishing-Angriffs sind, werden auf der Registerkarte „E- **Mail-Suchergebnisse** “ angezeigt. Die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum, Empfänger und Nachrichten-ID, werden angezeigt.

9. Um die Liste der Benutzer anzuzeigen, die die Phishing-E-Mail erhalten haben, klicken Sie in der Spalte „Suchdatum“ auf das Symbol **>**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




10. Um eine Liste der Benutzer anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Benutzer**.

    Die Spalte Phishing-Benutzer identifiziert die E-Mail-Empfänger.

    **Hinweis:**
    Auf der Seite „Betroffene Benutzer“ werden nur die Benutzerdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

11. Führen Sie die folgenden Schritte aus, um die Benutzer, die Ziele des Phishing-Angriffs sind, weiter zu untersuchen:

    a. Aktivieren Sie die Kontrollkästchen neben den Benutzernamen.

    b. Wählen Sie in der Liste die **Option Untergeordneten Security Incident erstellen**aus und klicken Sie auf **Ausführen**.

    Eine Nachricht wird angezeigt, die angibt, dass ein untergeordneter Security Incident erstellt wurde. Um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind, klicken Sie auf die Registerkarte **Erkunden**, und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**.

### Ergebnisse

Die Liste der Phishing-Benutzer wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Führen Sie eine Suche nach erkennbaren Sichtungen nach von Benutzern gemeldeten Phishing- und Malware-Angriffen durch

Führen Sie Sichtungssuchen für erkennbare Elemente durch, um herauszufinden, wie viele Benutzer innerhalb eines bestimmten Zeitraums eine schädliche oder verdächtige Website besucht haben.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Suche nach Netzwerkdatenverkehr für erkennbare Elemente wie URL, Zielhost oder Ziel-IP-Adresse durchführen, die einem Security Incident zugeordnet sind.

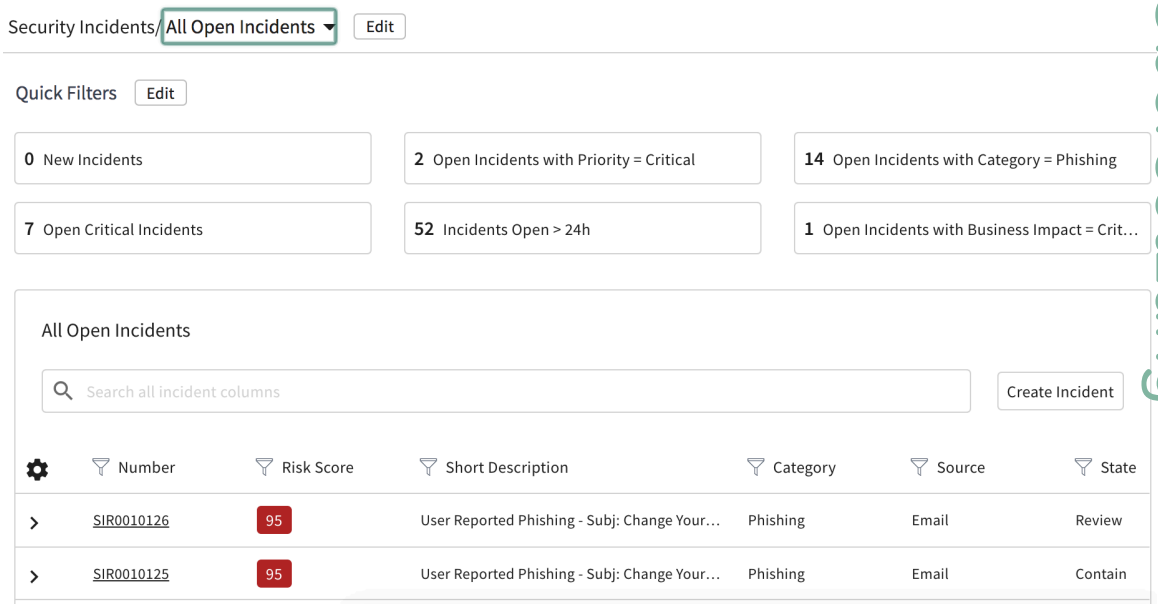
**Hinweis:**

- Diese Implementierung der Sichtungssuche für erkennbare Elemente wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokoll-Events müssen mit dem Common Information Model (CIM) kompatibel sein, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

### Prozedur

1. Um die Ihrem Team zugewiesenen Security Incidents anzuzeigen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**.
2. Wählen Sie in der Liste „ **Security Incidents** “ einen anderen Filter aus, z. B. „all **Mir zugewiesene Incidents“**, „ **Alle offenen Incidents**“ oder „ **Alle Incidents**“.

   Um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails, klicken Sie auf einen der **Schnellfilter**.

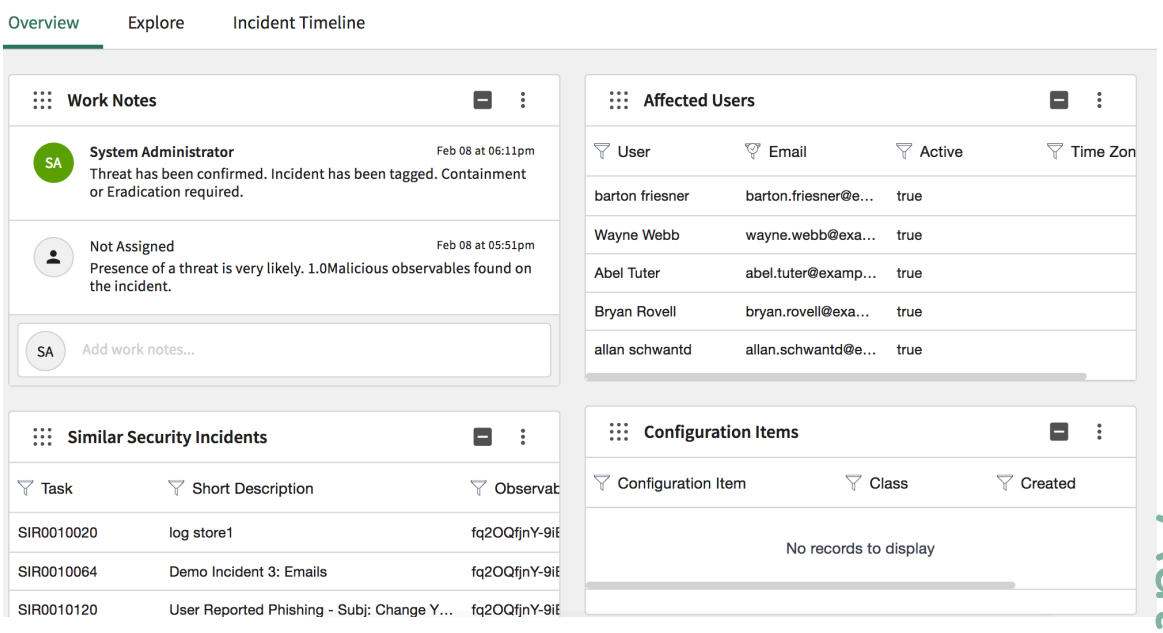



3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

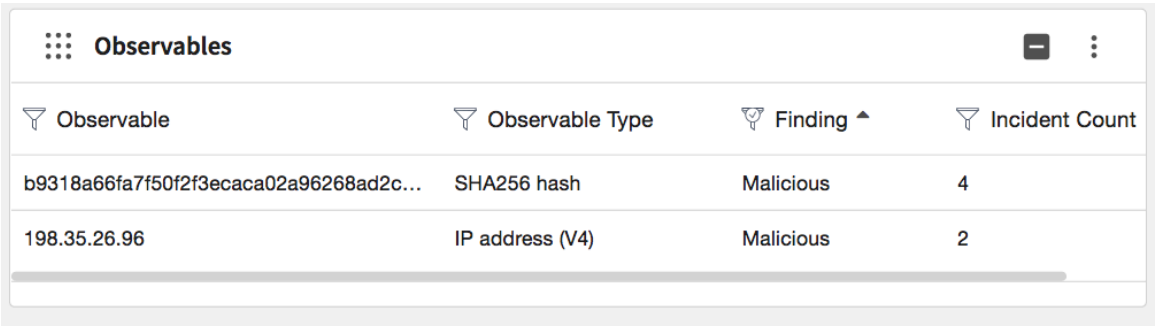
   Sie sehen eine Übersicht über den Security Incident, einschließlich einer Liste der erkennbaren Elemente, betroffenen Benutzer und ähnlichen Security Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



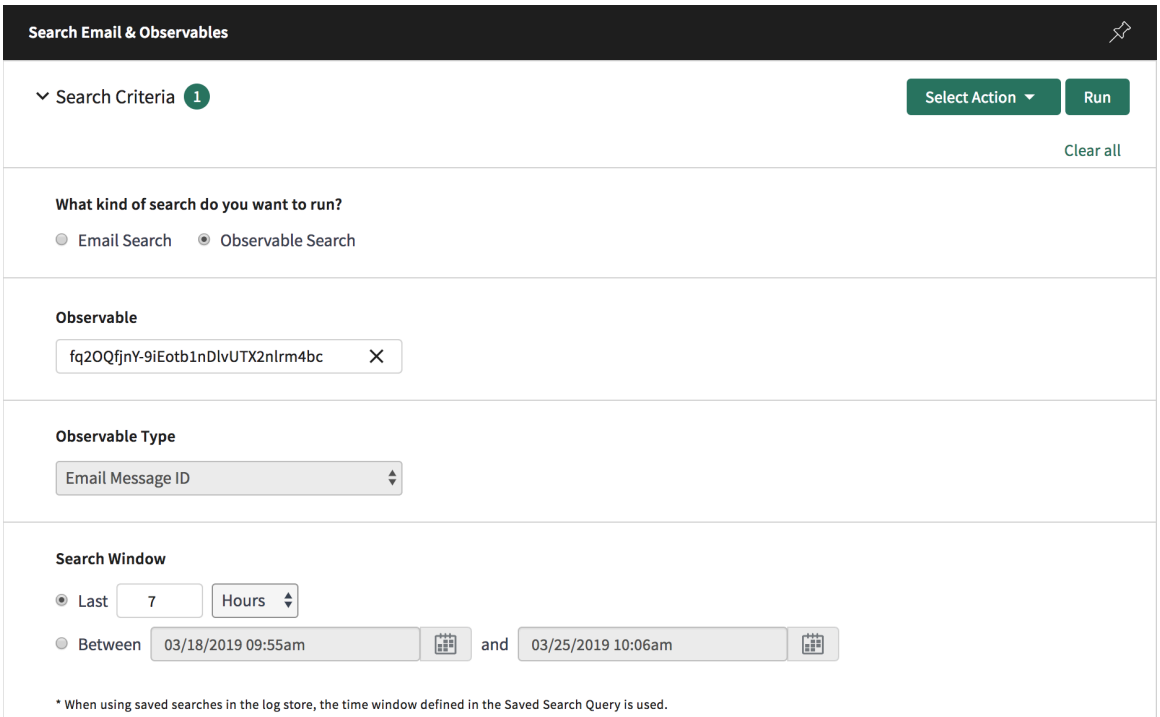

Beachten Sie im Abschnitt „Erkennbare Elemente“, dass in der Spalte „Erkennbares Element“ die E-Mail-Adresse, der Betreff und die URL angezeigt werden. Beachten Sie auch, dass die Spalte „Ergebnis“ zeigt, dass die URL beim Senden der Phishing-E-Mail automatisch gescannt und als bekanntermaßen schädliche URL eingestuft wurde. Die Spalte Incident-Anzahl zeigt die anderen Incidents, die dasselbe erkennbare Element verwenden. Diese Artefakte weisen darauf hin, dass Sie wahrscheinlich bereit sind, zu Eindämmungsverfahren für diesen Phishing-Angriff überzugehen, einschließlich der Bestimmung, wie viele Benutzer in der Organisation betroffen waren.




4. Navigieren zu **Erkunden** > **Ermittlung** > **E-Mail und erkennbare Elemente durchsuchen**.
5. Erweitern Sie den Abschnitt Suchkriterien, und klicken Sie auf **Suche**nach erkennbaren Elementen.

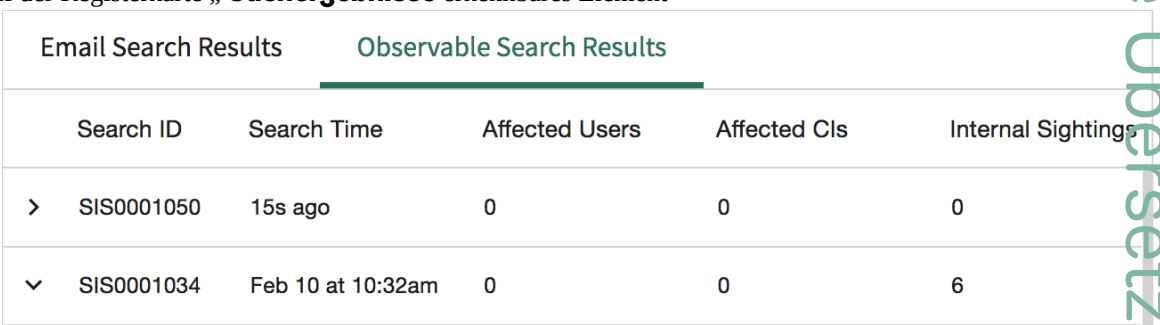


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Geben Sie das erkennbare Element ein, nach dem Sie suchen, und ein Zeitfenster für die Suche (z. B. Letzte 24 Stunden).

7. **Wählen Sie in der Liste Aktion** auswählen die Option **Suchen**aus.
   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die wichtigsten Benutzer, auf die der böswillige Angriff abzielt, werden auf der Registerkarte „ **Suchergebnisse** erkennbares Element“




   angezeigt.

8. Um die Benutzer anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Benutzer**.

   Die Spalte Phishing-Benutzer identifiziert die Empfänger der Phishing-E-Mail, und die Spalte Benutzerinteraktion identifiziert Benutzer, die auf eine Phishing-URL geklickt oder mit einer verdächtigen E-Mail-Adresse interagiert haben. Die Spalte „Benutzerinteraktion“ wird auf „true“ oder „false“ festgelegt, je nachdem, ob der Benutzer auf den schädlichen Link oder die IP geklickt hat.

   **Hinweis:**
   Auf der Seite „Betroffene Benutzer“ werden nur die Benutzerdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

9. Um die Benutzer weiter zu untersuchen, die auf die Phishing-E-Mail geklickt und möglicherweise ihre Anmeldeinformationen gefährdet haben:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Aktivieren Sie in den Spalten Phishing-Benutzer und Benutzerinteraktion die Checkboxen neben den Benutzernamen, die **true**anzeigen.

**b.** Klicken Sie auf **Untergeordneten Security Incident erstellen** und dann auf **Ausführen**.
Eine Nachricht wird angezeigt, die angibt, dass ein untergeordneter Security Incident erstellt wurde. Um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind, klicken Sie auf die Registerkarte **Erkunden**, und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**.

### Ergebnisse
Die Liste der Phishing-Benutzer wird angezeigt.

## Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Erstellen Sie mehrere Konfigurationsdatensätze für die Sichtungssuche, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter ändern.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss in der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.

### Warum und wann dieser Vorgang ausgeführt wird
Sie können auch Konfigurationsdatensätze für Sichtungssuchen erstellen, um gespeicherte Suchen im Protokollspeicher von Splunk Enterprise aufzurufen.

**Hinweis:**
Die Suchkonfigurationsabfragen stützen sich auf Splunk-Protokolldaten, um mit Splunk Common Information Model (CIM) konform zu sein.

Mit gespeicherten Suchkonfigurationen können Sie:

- Erstellen Sie benutzerdefinierte Suchen, die mehrere Event-Datensätze kombinieren.
- Designeffiziente und effektive Suchvorgänge.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das Basissystem enthält die in der folgenden Abbildung gezeigten Beispielkonfigurationen:

**Gespeicherte Suchkonfigurationen**

| | | Name | Observable type | Search | Is saved search |
|---|---|---|---|---|---|
| | | Search | Search | Search | Search |
| ☐ | ⓘ | Default Proofpoint Inplace Search-Emails | Email | tag=email [\| search tag="email" AND (sub... | false |
| ☐ | ⓘ | Default Saved Search - Emails | Email | args.email.subject=${email.subject}&args... | true |
| ☐ | ⓘ | Default PAN Inplace Search - URLs | URL | tag=network url=${observable} \| table us... | false |

Die gespeicherten Such- und Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der gespeicherten Konfiguration übereinstimmen, die in Ihrer Splunk-Instanz definiert ist. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

**Hinweis:**
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Searches, Reports, and Alerts (Suchen, Berichte und Warnungen), und suchen Sie nach Ihrer gespeicherten Suchabfrage. Klicken Sie auf den Link **Berechtigungen**, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie das Optionsfeld **Alle Apps** aus, und aktivieren Sie die Option **Leseberechtigung** für **Jeder**. Dadurch wird der Wert der Spalte „Freigabe“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn diese Option nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

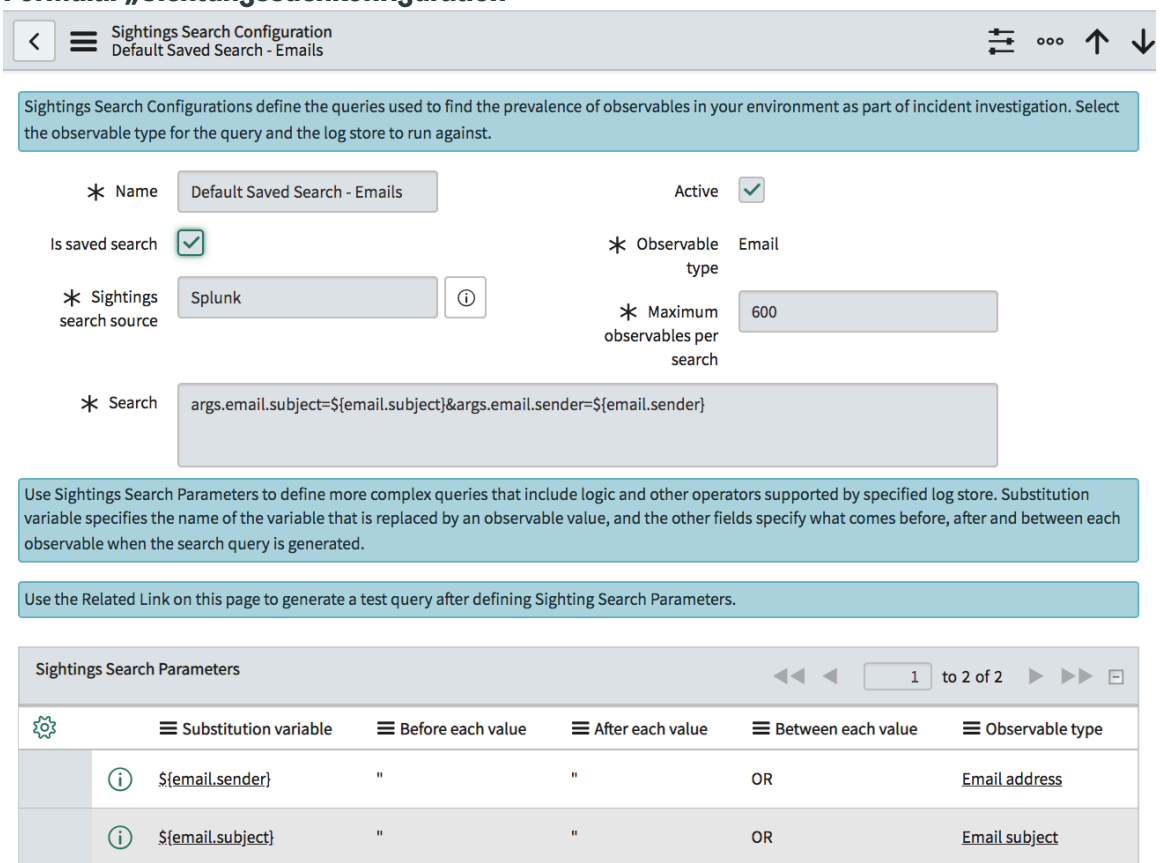
So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**.
2. Ändern Sie den **App-Kontext** in **Alle**.

   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Beispielsweise enthält das Formular „Sichtungssuchkonfiguration“ die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:

**Formular „Sichtungssuchkonfiguration“**




Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit demselben Namen, Standardmäßige gespeicherte Suche – E-Mails, und denselben Suchparametern für die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Adresse und den E-Mail-Betreff. Wenn der Name und die Suchparameter nicht identisch sind, generiert die Sichtungssuche kein genaues Ergebnis.

### Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

**Formular „Sichtungssuchkonfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Konfiguration |
| Ist gespeicherte Suche | Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt. |
| Sichtungssuchquelle | Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus. |
| Aktiv | Option für den gespeicherten Suchstatus. Für die Suche nach Sichtungen können nur aktive Suchkonfigurationen verwendet werden. |
| Erkennbarer Typ | Erkennbarer Typ kann ein beliebiger erkennbarer Typ sein, z. B. IP, Hash-Wert, URL, Domänenname usw. |
| Maximale erkennbare Elemente pro Suche | Maximale Anzahl der erkennbaren Elemente, die von der Suche zurückgegeben werden sollen. |
| Suchen | Die Standardsuchzeichenfolge ist `$(observable)`, Sie können jedoch eine eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden. |

2. Klicken Sie auf **Absenden**.

### Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

### Nächste Maßnahme
Klicken Sie nach dem Definieren der Suchabfrage auf **Testabfrage für Sichtungssuche generieren**, und geben Sie eine Liste von Werten für erkennbare Elemente an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

## Playbook-Ressourcen

Security Incident Response bietet eine Vielzahl von Playbook-Ressourcen, darunter eine umfassende Bibliothek mit Playbooks, Subflows und Aktionen. Sie können Playbooks schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen Schritt für Schritt zu beheben.

Zu den Playbook-Ressourcen gehören:

| Security Incident Response Playbooks | Security Incident Response-Playbook-Aktionen |
|---|---|
| Die mit dem Basissystem bereitgestellten Playbooks sollen den Untersuchungsprozess für Security Incidents beschleunigen, | Komplexe Aktionen, die für die Erstellung von Playbooks von entscheidender Bedeutung sind, sind als **Aktionsbibliotheken**verfügbar. Mit diesen Aktionsbibliotheken können Sicherheitsadministratoren Playbooks erstellen, |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Security Incident Response Playbooks | Security Incident Response-Playbook-Aktionen |
|---|---|
| indem komplexe und alltägliche Aufgaben automatisiert werden.<br><br>Playbooks sind in hohem Maße konfigurierbar und werden mit der Flow Designer-Technologie von ServiceNow erstellt. Kopieren Sie zum Konfigurieren das mit dem Basissystem bereitgestellte Playbook, und ändern Sie es mithilfe der einfachen grafischen Drag-and-Drop-Oberfläche. Weitere Informationen finden Sie unter Security Incident Response Playbooks. | ohne komplizierten Code zu schreiben. Weitere Informationen finden Sie unter Security Incident Response-Playbook-Aktionen. |

## Aktivieren Sie einen Security Incident Response -Flow

Sicherheitsadministratoren und Flow Designer können die Security Incident Response -Flows verwenden, um den Prozess der Lösung von Security Incidents in der Organisation zu automatisieren.

### Vorbereitungen

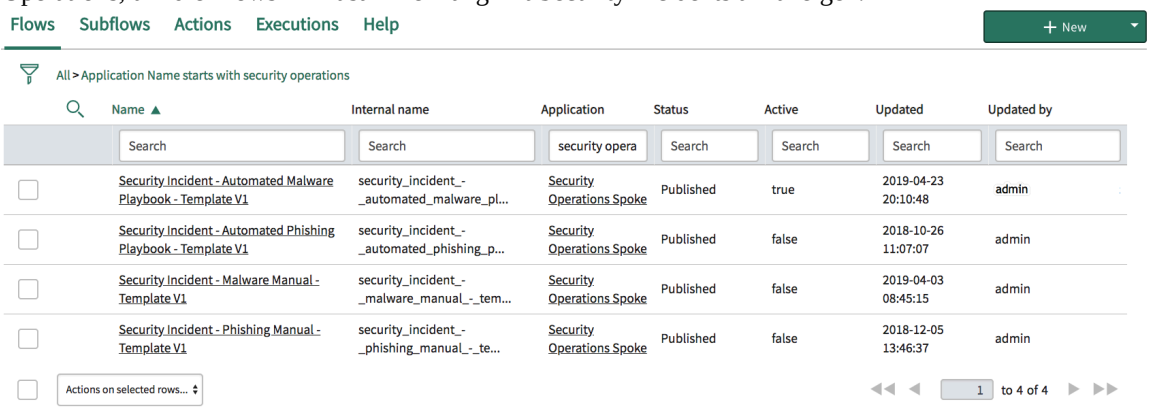
Erforderliche Rolle: sn_si.admin, action_designer und flow_designer

### Warum und wann dieser Vorgang ausgeführt wird

Die mit dem Basissystem bereitgestellten Flows befinden sich in einem inaktiven Status. Aktivieren Sie diese Flows, bevor Sie sie verwenden.

### Prozedur

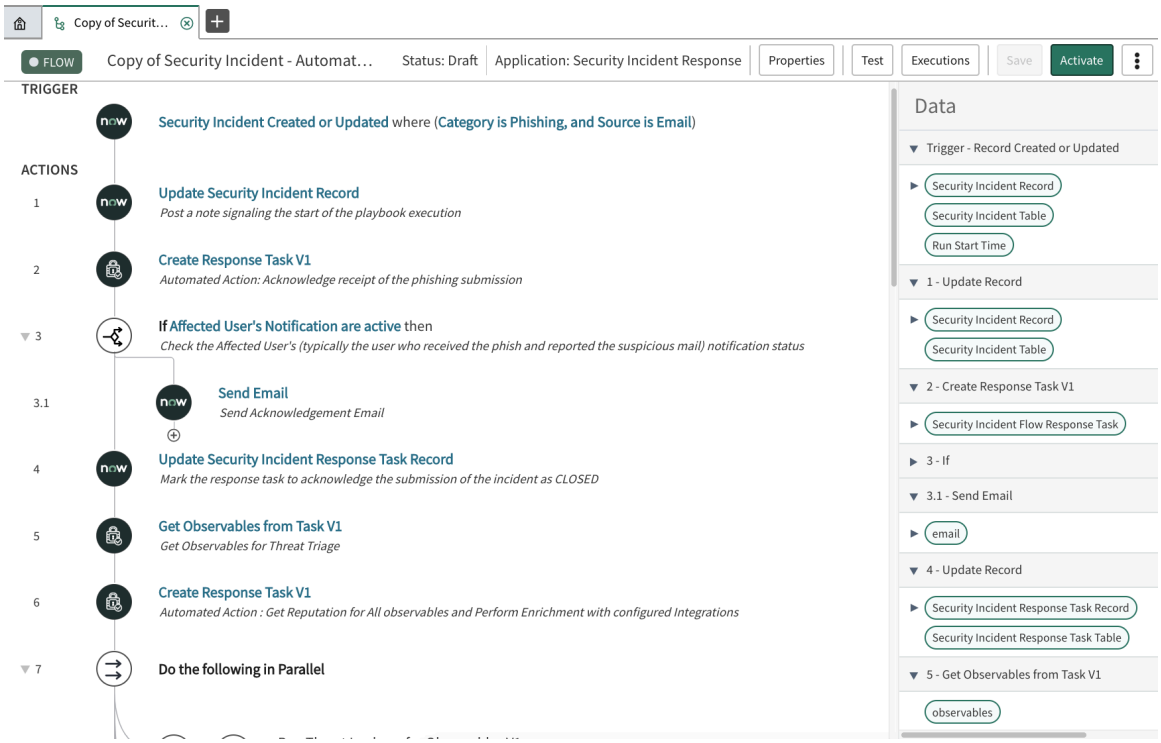
1. Laden Sie die Anwendung Security Operations Spoke herunter,und installieren Sie sie.
   Diese Spoke-Anwendung bietet Aktionen für Sicherheitsvorgänge, die Sie beim Definieren von Security Incident Response -Flows verwenden können.
2. Navigieren zu **Flow Designer** > **Designer** und suchen Sie nach der Spoke-Anwendung Security Operations, um die Flows im Zusammenhang mit Security Incidents anzuzeigen.




   Beachten Sie, dass die Flows den Status „Veröffentlicht“ haben und inaktiv sind.
3. Wenn Sie beispielsweise den automatisierten Malware-Playbook-Flow aktivieren möchten, klicken Sie auf den Link **Security Incident – Automated Phishing Playbook – Template V1** (Security Incident – Automated Phishing Playbook – Template V1), um den Flow anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Sie können die mit dem Basissystem bereitgestellten Flows nicht bearbeiten, da es sich um schreibgeschützte Flows handelt. Sie können diese Flows unverändert verwenden oder eine Kopie erstellen und sie nach Bedarf ändern.

4. Klicken Sie auf **Aktivieren**, um den Flow zu aktivieren.

### Ergebnisse
Der Flow des automatisierten Phishing-Playbooks ist aktiv und einsatzbereit.

## Security Incident Response Playbooks

Sie können den Security Incident-Playbook-Flow automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn mindestens ein Playbook einem Security Incident zugeordnet ist. Die Playbook-Komponente funktioniert nur für die mit PAD (Process Automation Designer) erstellten Prozesse und nicht für die mit Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert sie weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response unterstützt zwei Arten von Playbooks:

- Prozessbasierte Playbooks
- Flow-basierte Playbooks

Zusätzlich zu den aufgeführten Playbooks gibt es in Security Operations Spoke auch Subflows, die aus dem Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Security Incident Response-Flow aktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozessbasierte Playbooks

Die Playbook-Komponente funktioniert nur für die mit PAD (Process Automation Designer) erstellten Prozesse und nicht für die mit Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert sie weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit.

### Playbook für manuelles Phishing

Das Playbook für manuelles Phishing bietet eine Schritt-für-Schritt-Anleitung für Ihre Analysten, wie sie bestimmte Arten von Sicherheitsbedrohungen in Ihren Phishing-Aktivitäten manuell beheben können.

## Übersicht

Die Vorlage „Manuelles Phishing-Playbook“ wurde entwickelt, um die Phishing-Antwortaufgaben manuell auszuführen, und enthält eine Reihe von Aktionen, die Auslöserbedingungen enthalten. Sie können die PAD-Vorlagen verwenden, um die Schritte im Phishing-Antwort-Playbook auszuführen und diese Incidents effizient zu lösen.

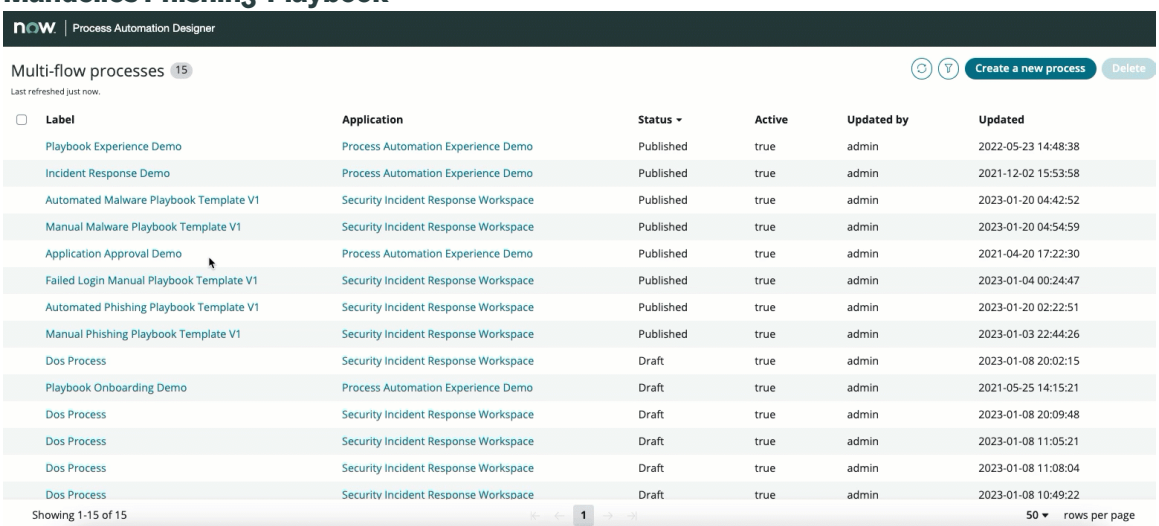
Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das manuelle Phishing-Playbook im Prozessautomatisierungs-Designer (PAD) aktivieren und dann alle Aufgaben wie Analyse, Eindämmung, Beseitigung und Überprüfung ausführen.

Im Folgenden sind die Spuren der Prozessdefinition aufgeführt, die dem Security Incident-Status entsprechen:

- Analyse
- Beinhalten
- Beseitigen
- Prüfen

Jede Spur enthält Aktivitäten.

### Manuelles Phishing-Playbook




Sobald Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbook zeigt alle Daten, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um die Erstellung der Berechtigung abzuschließen.

### Erstellen Sie Prozesse für manuelles Phishing in PAD

Gehen Sie wie folgt vor, um Prozesse für manuelles Phishing im Prozessautomatisierungs-Designer (PAD) zu erstellen.

#### Vorbereitungen

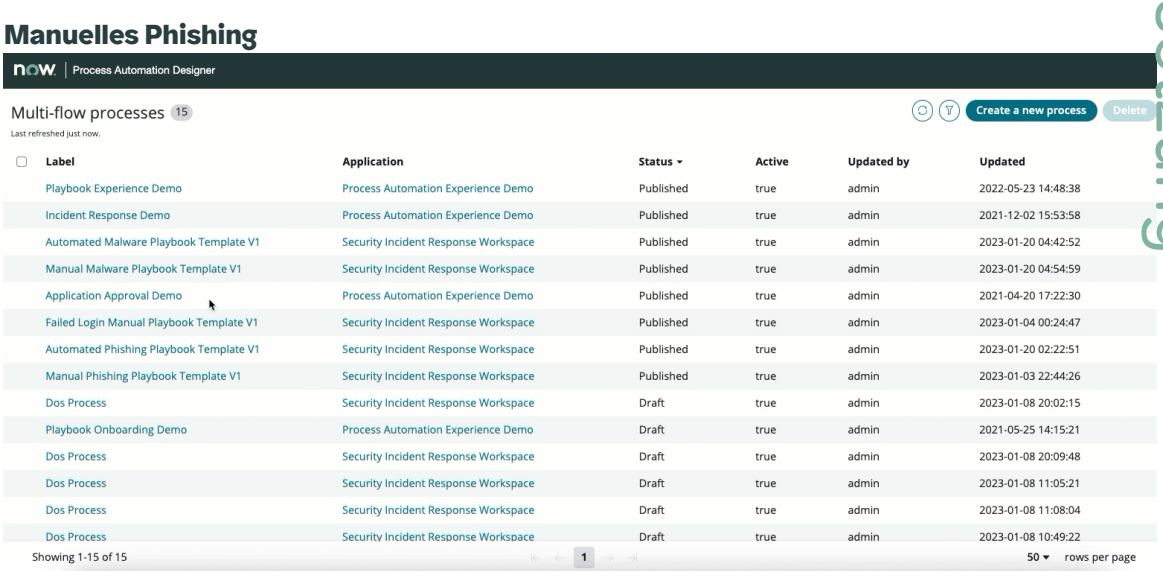
Erforderliche Rolle: sn_si.admin oder sn_si.manager

#### Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

   Beispiel: Manuelle Phishing-Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken **Sie auf Einen Auslöser auswählen**.
4. Wählen **Sie Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken **Sie auf Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie „Phishing“ erstellt wird.



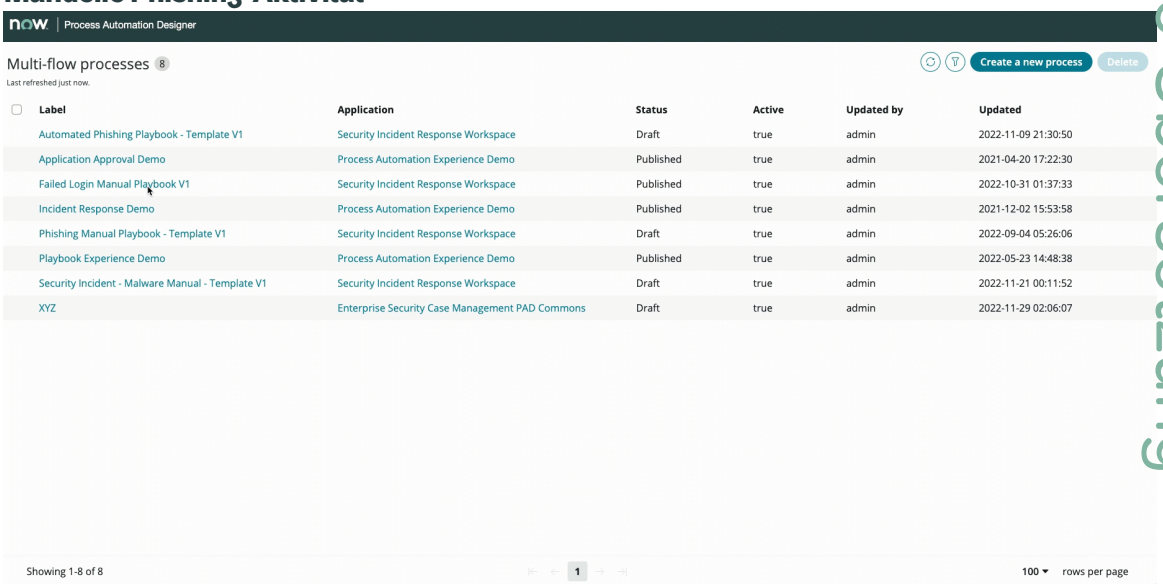

7. Klicken **Sie auf Zu Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Neue Spalte hinzufügen**.
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Benutzeroberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name**, **Beschreibung**, **Bedingung**ausführen und **Geben Sie an, wann gestartet werden soll**.
   Die Felder Ausführungsbedingung und **Angeben, wann gestartet** werden soll implizieren, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte**hinzufügen.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spur für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel beginnt die **Analysespalte** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Spaltenstart, nachdem die vorherige Spalte abgeschlossen ist, und weist eine Ausführungsbedingung auf, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spur hinzufügen.
12. Klicken Sie unter einer bestimmten Spur (z. B. Analysespalte) **auf Weitere Prozessaktivität hinzufügen**.
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken **Sie auf Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Ebenso können Sie weitere Prozessaktivitäten unter jeder Spur erstellen.

**Manuelle Phishing-Aktivität**




14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (beinhaltet konfigurierte Eingaben im Automatisierungsplan) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie auf **Alle Eigenschaften** anzeigen, und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie parallele Aktivitäten hinzu

Wenn das Feld **Startzeitpunkt** auf **Mit vorherigem**festgelegt ist, können parallele Aktivitäten initiiert werden.

## Zum Wechseln von einer Spur zur nächsten Spur

Wenn keine Ausführungsbedingung definiert ist, werden die Spuren und Aktivitäten nacheinander ausgeführt.

Sie können die Ausführungsbedingung verwenden, um Aktivitäten oder Spuren zu überspringen. In diesem Beispiel **beginnt die Spur „Enthalten“, wenn das Ergebnis von „Verfügt die E-Mail über Bedrohungsindikatoren?“ ist Ja**.

Um von einer Spur zu einer anderen zu wechseln, können Sie die von der Plattform bereitgestellte **Aktivitätsdefinition „Datensatz aktualisieren**“ verwenden. Dadurch wird das Statusfeld des Security Incident aktualisiert, und die Playbook-Ausführung wird in der nächsten Spur fortgesetzt.

Die Herausforderung bei dieser Aktivitätsdefinition besteht jedoch darin, dass, wenn sich das Playbook beispielsweise in der Analysespur befindet und der Benutzer den Status manuell auf „Überprüfung“ aktualisiert hat, die Aktivität „Datensatz aktualisieren“ den Status erneut in „Enthalten“ ändert, um das Playbook fortzusetzen Ausführung. Dadurch wird die vorgenommene manuelle Änderung überschrieben.

Um dies zu umgehen, wird im Basissystem eine Aktivitätsdefinition namens „ **Aufgabenstatus aktualisieren“** bereitgestellt. Diese Aktivität überschreibt den Security Incident-Status nicht, wenn der aktuelle Sicherheitsstatus im Playbook vor der Spur liegt.

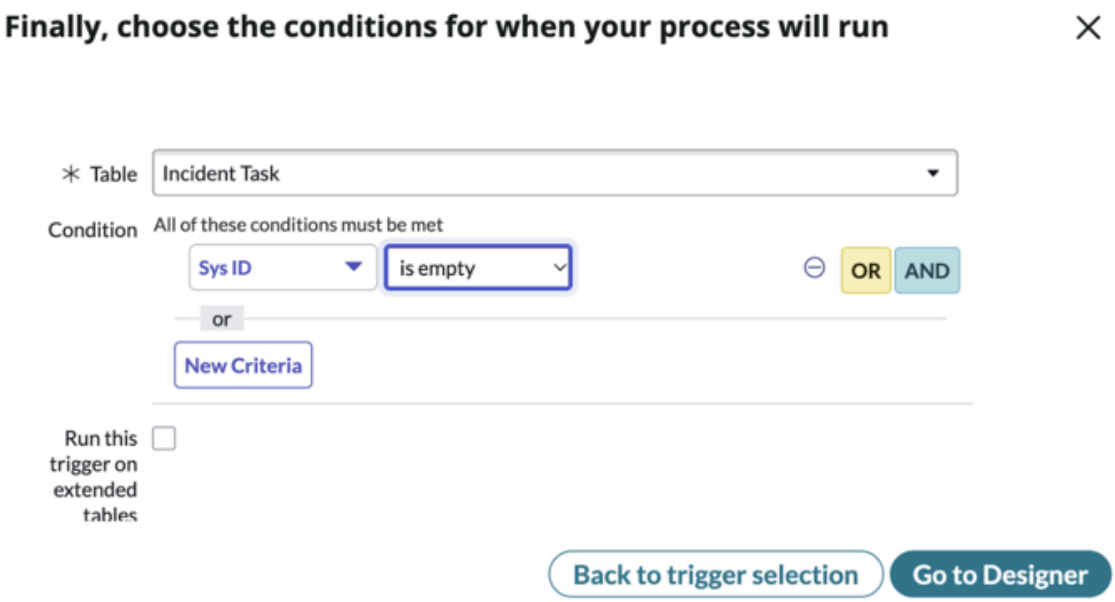
## Erstellen Sie eine Prozessdefinition mit Dummy-Auslöserbedingung

Eine Prozessdefinition erfordert immer eine Auslöserbedingung. Wenn Sie jedoch nicht sicher sind, wann der Prozess ausgelöst werden soll, können Sie dennoch eine Prozessdefinition mit einer Dummy-Auslöserbedingung erstellen. Legen Sie die Auslösebedingung fest, da **sys_id leer ist**. Diese Bedingung wird niemals erfüllt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prozessbedingungen**






### Verwenden des Playbooks für manuelles Phishing

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook „Manuelles Phishing“ im SIR-Analystenarbeitsbereich und seinen Funktionen verwenden können.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

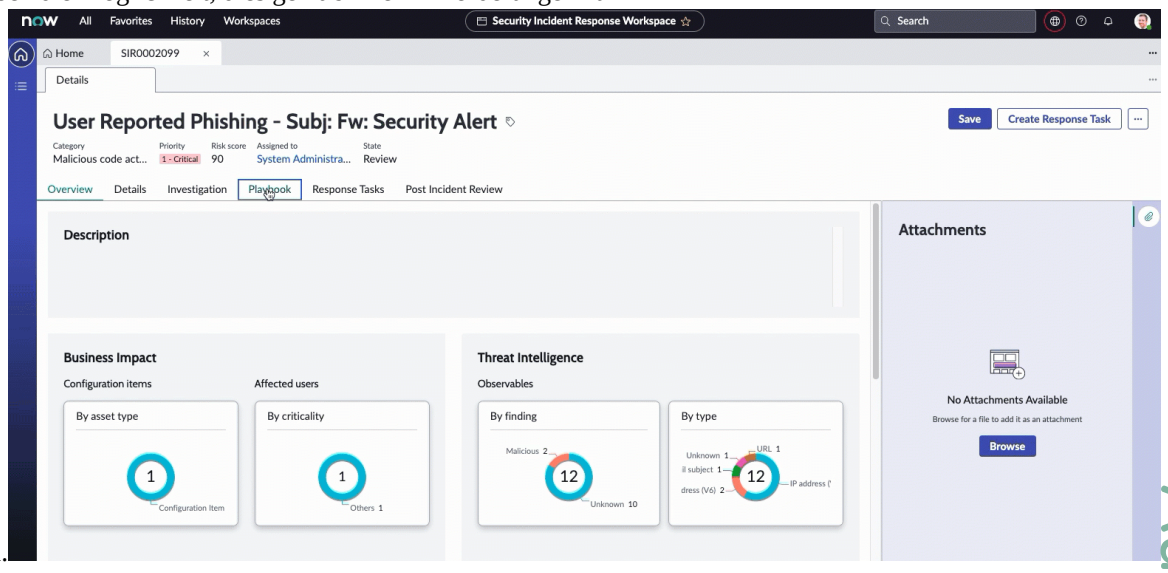
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incident und die Risikopunktzahl anzeigen.

   **Hinweis:**
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie aktivieren, damit sie sie auf der Registerkarte **„Playbook“** anzeigen können.

3. Klicken Sie auf das **Playbook für manuelles Phishing**.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies gemäß Ihren Anforderungen zu ändern.




6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Benutzeraktion vorhanden ist, die Sie ausführen müssen, wird sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Benutzeraktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

### Zusammenfassung des Arbeitsbereich-Playbooks

Im Folgenden wird die Prozesszusammenfassung beschrieben.

- Machen Sie sich mit dem veralteten Flow-basierten Playbook vertraut.
- Listen Sie mögliche Aktivitäten und Spuren nach der Analyse des Flows auf. Suchen Sie nach den Schritten, in denen eine echte Orchestration erstellt werden kann.
- Nehmen Sie jede Aktivität und überprüfen Sie, ob die vom Basissystem bereitgestellte Aktivitätsdefinition den Anwendungsfall erfüllen kann oder nicht.
- Listen Sie Aktivitätsanwendungsfälle auf, für die neue Aktivitätsdefinitionen implementiert werden müssen. Klassifizieren Sie sie – Interaktiv, nicht interaktiv oder automatisiert. So erstellen Sie eine Aktivitätsdefinition:
  - Erstellen Sie einen Subflow oder eine Aktion für den Anwendungsfall.
  - Entscheiden Sie, ob die zugeordneten Daten in der Flow-Datentabelle oder einer benutzerdefinierten Tabelle erfasst werden müssen.
  - Wenn Sie die Flow-Datentabelle verwenden, erstellen Sie eine Flow-Datendefinition in **sys_flow_data_definition**. Wählen Sie beim Erstellen eines Flow-Datensatzes im Subflow die erstellte Flow-Datendefinition aus.
  - Erstellen Sie eine **Aktivitätsdefinition**.
  - Ordnen Sie den Automatisierungsplan zu.
  - Füllen Sie die Eigenschaften der **Aktivitäts-Experience** aus.
  - Erstellen Sie eine Aktion unter Playbook-Aktionen. Es sollte eine Aktivitätsaktion vorhanden sein, um sie der Aktivitätsdefinition zuzuweisen.
  - Um die Standardkarten-Experience basierend auf dem ausgewählten Experience-Typ zu überschreiben, fügen Sie die Playbook-Überschreibung mithilfe des Aktivitäts-UI-Konzepts hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Einige Aktivitäten können so festgelegt werden, dass sie sowohl automatisch als auch interaktiv verarbeitet werden, indem die Kennzeichnung „Warten auf Benutzereingabe“ im Subflow verwendet wird. Diese Eingabe kann beim Konfigurieren der Aktivität in der Prozessdefinition übergeben werden.
- Nachdem Sie alle für Ihren Prozess erforderlichen Aktivitätsdefinitionen erstellt haben, beginnen Sie mit der Erstellung der Prozessdefinition mit PAD Studio.

### Playbook für automatisiertes Phishing

Das Playbook für automatisiertes Phishing bietet Ihren Analysten eine Schritt-für-Schritt-Anleitung, wie sie bestimmte Arten von Sicherheitsbedrohungen in Ihren automatisierten Phishing-Aktivitäten beheben können.

## Übersicht

Die Playbook-Vorlage für automatisiertes Phishing wurde entwickelt, um die Phishing-Antwortaufgaben zu automatisieren. Sie enthält eine Reihe von Aktionen, die Auslösebedingungen enthalten. Sie können die PAD-Vorlagen verwenden, um die Schritte im Phishing-Antwort-Playbook zu automatisieren und diese Incidents effizient zu lösen. Diese Playbook-Vorlage enthält eine Reihe von wiederverwendbaren Aktionen, die als Reaktion auf Phishing-Angriffe entwickelt wurden. Jeder Flow hat einen Auslöser (eine Bedingung), eine Sequenz von Aktionen und Subflows, die Sie mit Anmerkungen versehen können.

In diesem Playbook findet keine Benutzerinteraktion statt, wenn die Kategorie eines Security Incident auf „Phishing“ festgelegt ist. Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das automatisierte Phishing-Playbook im Prozessautomatisierungs-Designer (PAD) aktivieren. Dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

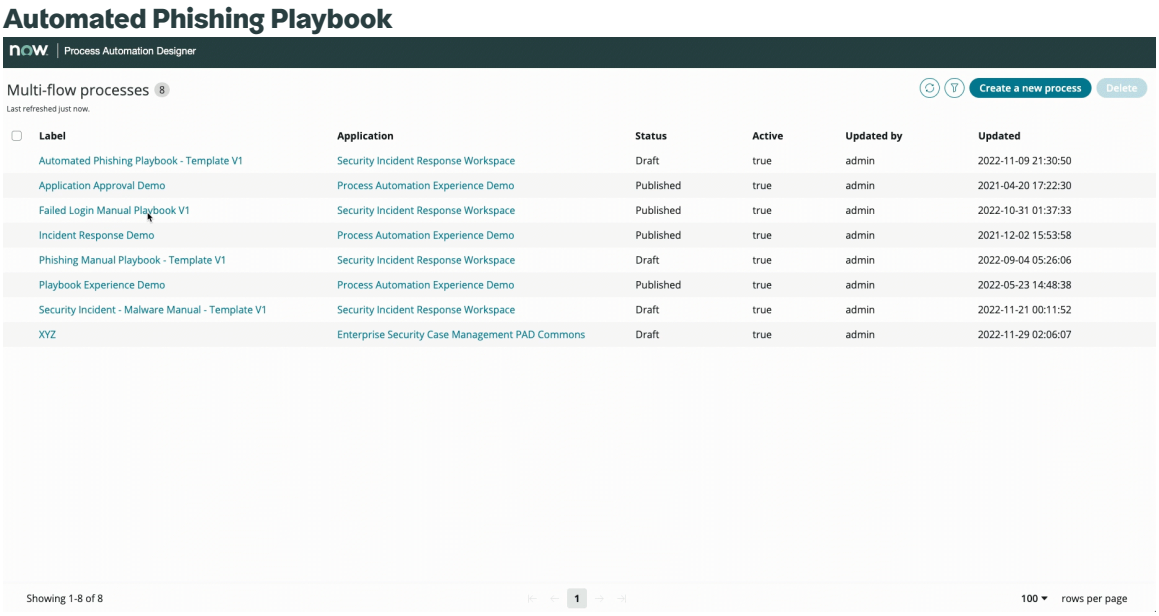
Im Folgenden sind die Spuren der Prozessdefinition aufgeführt, die dem Security Incident-Status entsprechen:

- Analyse
- Beinhalten
- Beseitigen
- Prüfen

Jede Spur enthält Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sobald Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbook zeigt alle Daten, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um die Erstellung der Berechtigung abzuschließen.

### Erstellen Sie Prozesse für automatisiertes Phishing in PAD

Gehen Sie wie folgt vor, um Prozesse für automatisiertes Phishing im Prozessautomatisierungs-Designer (PAD) zu erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

#### Prozedur

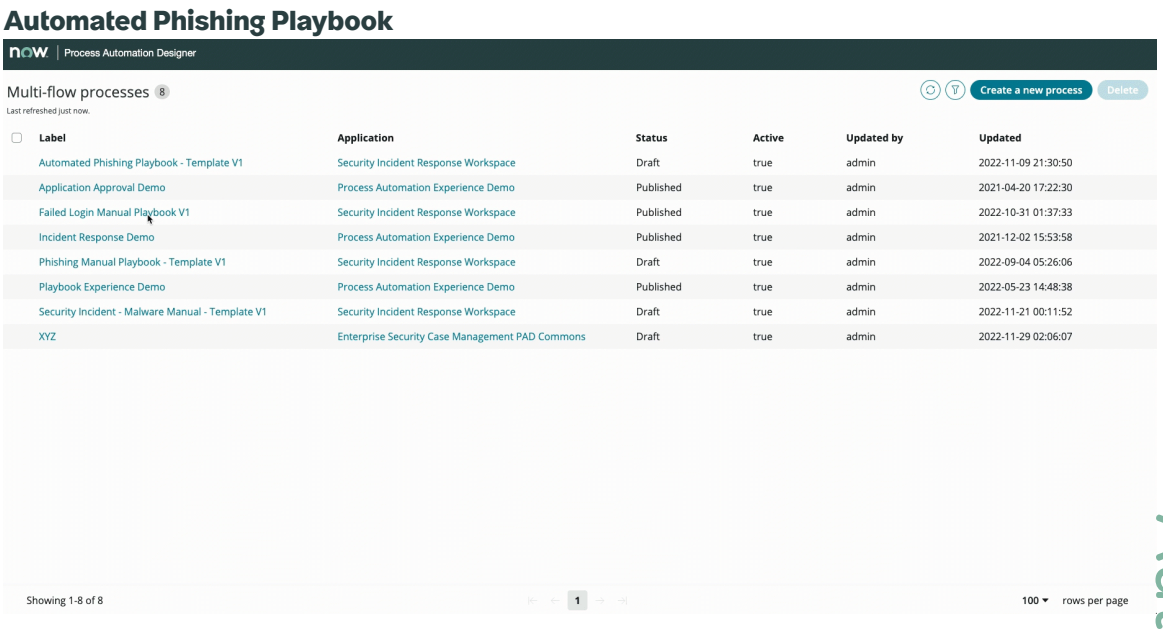
1. Klicken **Alle** > **Prozessautomatisierungs-Designer** >  > **Einen neuen Prozess erstellen**.

   Beispiel: Automated Phishing Playbook Template V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken **Sie auf Einen Auslöser auswählen**.
4. Wählen **Sie Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken **Sie auf Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie „Phishing“ erstellt wird.



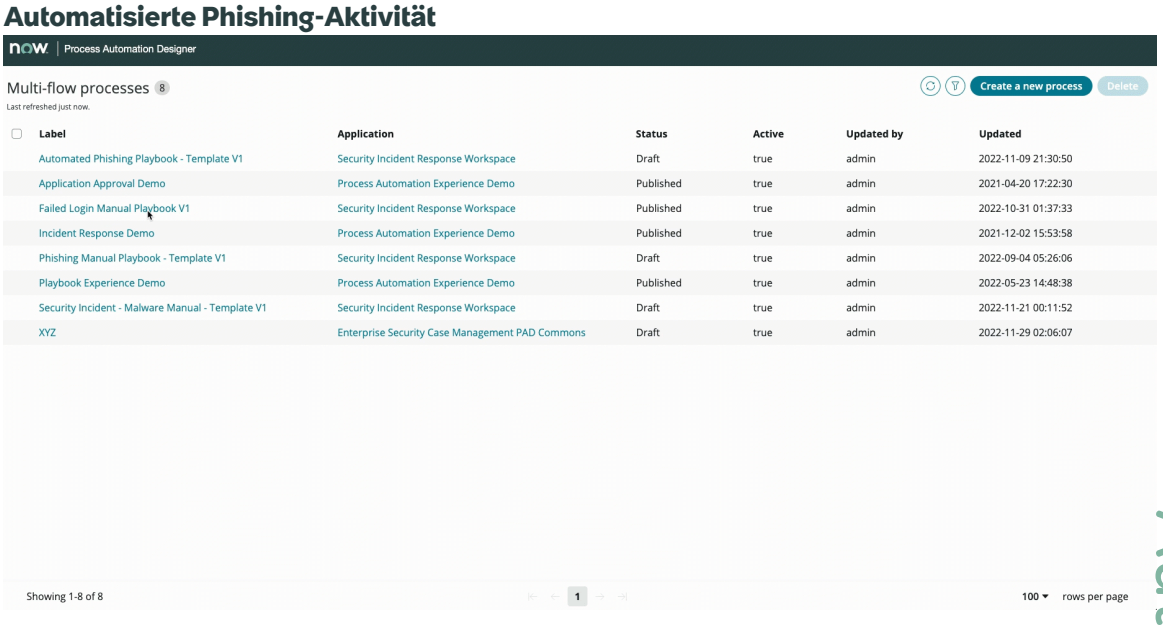
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Klicken **Sie auf Zu Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Neue Spalte hinzufügen**.
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Benutzeroberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name**, **Beschreibung**, **Bedingung**ausführen und **Geben Sie an, wann gestartet werden soll**.
   Die Felder Ausführungsbedingung und **Angeben, wann gestartet** werden soll implizieren, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte**hinzufügen.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spur für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel beginnt die **Analysespalte** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Spaltenstart, nachdem die vorherige Spalte abgeschlossen ist, und weist eine Ausführungsbedingung auf, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spur hinzufügen.
12. Klicken Sie unter einer bestimmten Spur (z. B. Analysespalte) **auf Weitere Prozessaktivität hinzufügen**.
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken **Sie auf Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Ebenso können Sie weitere Prozessaktivitäten unter jeder Spur erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (beinhaltet konfigurierte Eingaben im Automatisierungsplan) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie auf **Alle Eigenschaften** anzeigen, und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

## Verwenden des Automated Phishing-Playbooks

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook für automatisiertes Phishing im SIR-Analystenarbeitsbereich und seinen Funktionen verwenden können.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incident und die Risikopunktzahl anzeigen.

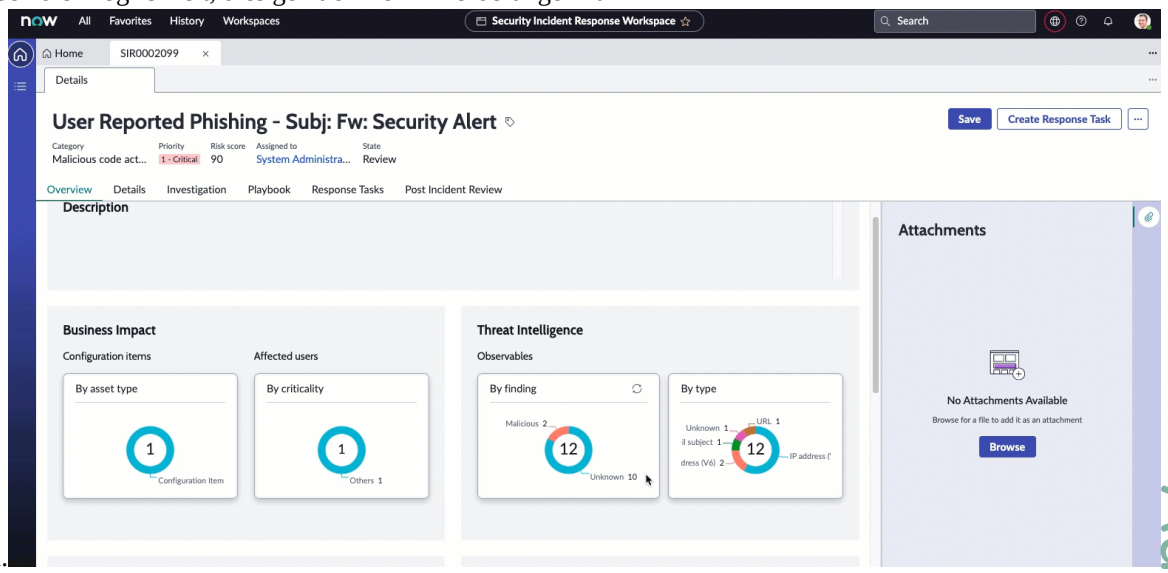
   **Hinweis:**
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie aktivieren, damit sie sie auf der Registerkarte **„Playbook“** anzeigen können.

3. Klicken Sie auf das **automatisierte Phishing-Playbook**.
   Beim automatisierten Phishing werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies gemäß Ihren Anforderungen zu ändern.




6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Benutzeraktion vorhanden ist, die Sie ausführen müssen, wird sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Benutzeraktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

### Playbook für manuelle Malware

Das Playbook „Manual Malware“ (Manuelle Malware) enthält eine Schritt-für-Schritt-Anleitung dazu, wie Analysten Malware-Warnungen manuell effizienter lösen können.

Die Playbook-Vorlage „Manuelle Malware“ wurde entwickelt, um die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk manuell auszuführen. Sie können die PAD-Vorlagen verwenden, um die Schritte im manuellen Malware-Playbook auszuführen und diese Warnungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie mit Anmerkungen versehen können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, die als Reaktion auf Malware-Angriffe entwickelt wurden. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn Malware erstellt oder aktualisiert wird. Sie müssen das manuelle Malware-Playbook im Prozessautomatisierungs-Designer (PAD) aktivieren und alle Aufgaben erstellen, z. B. Analysieren, Eindämmen, Entfernen und Überprüfen.

Im Folgenden sind die Spuren der Prozessdefinition aufgeführt, die dem Status der Malware-Warnung entsprechen:

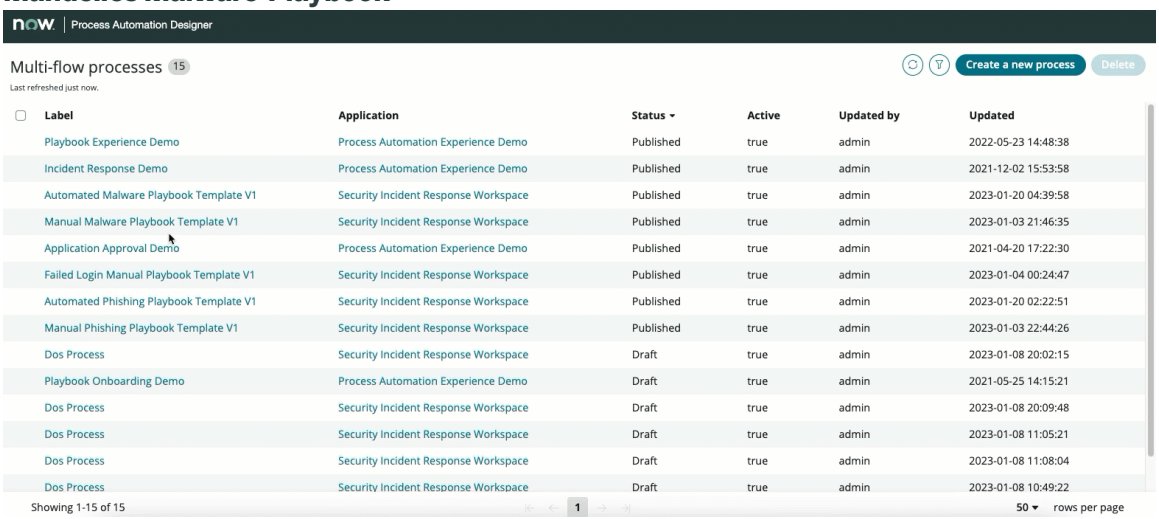
- Analyse
- Beinhalten
- Beseitigen
- Prüfen

Jede Spur enthält Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Manuelles Malware-Playbook**




Nachdem Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbook zeigt alle Daten, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um die Erstellung der Berechtigung abzuschließen.

### Erstellen Sie Prozesse für manuelle Malware in PAD

Führen Sie diese Schritte aus, um Prozesse für manuelle Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

### Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**.

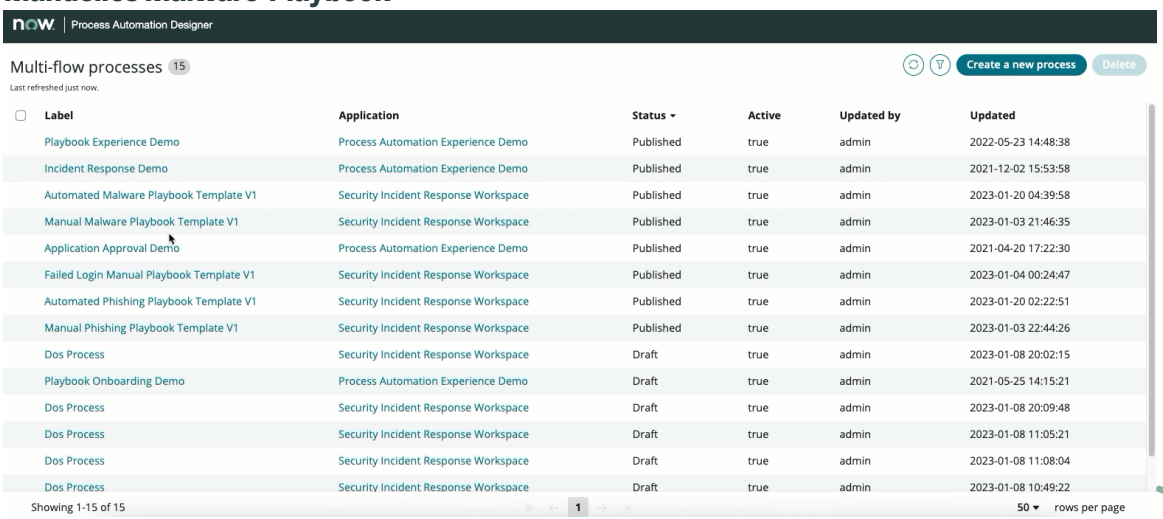
   Beispiel: Manuelle Malware-Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken **Sie auf Einen Auslöser auswählen**.
4. Wählen **Sie Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken **Sie auf Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie „Phishing“ erstellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

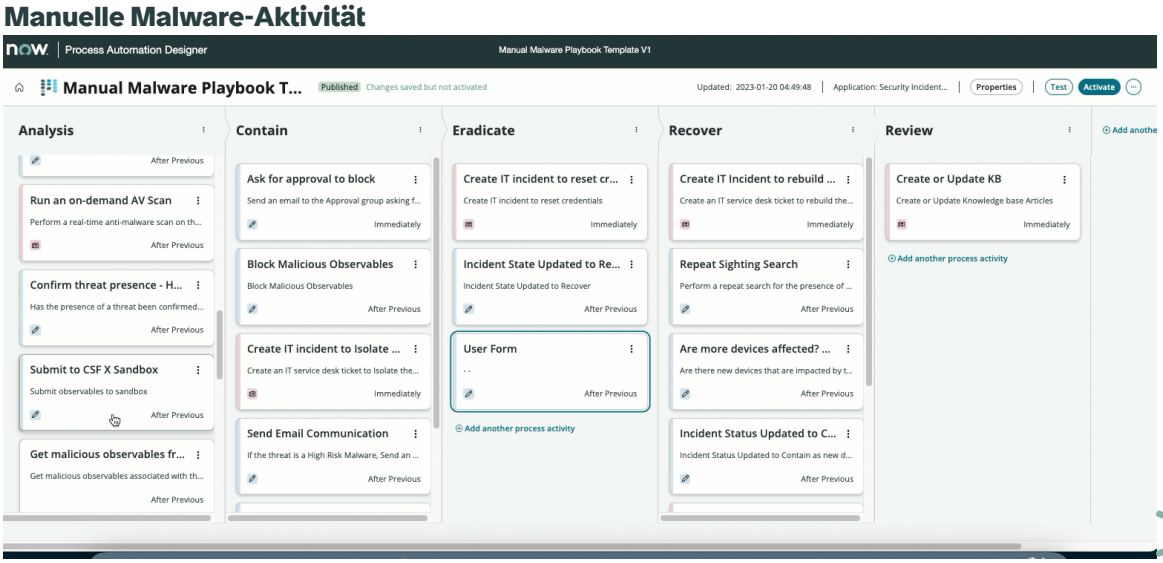
**Manuelles Malware-Playbook**




7. Klicken **Sie auf Zu Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Neue Spalte hinzufügen**.
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Benutzeroberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name**, **Beschreibung**, **Bedingung**ausführen und **Geben Sie an, wann gestartet werden soll**.
   Die Felder Ausführungsbedingung und **Angeben, wann gestartet** werden soll implizieren, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte**hinzufügen.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spur für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel beginnt die **Analysespalte** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Spaltenstart, nachdem die vorherige Spalte abgeschlossen ist, und weist eine Ausführungsbedingung auf, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spur hinzufügen.
12. Klicken Sie unter einer bestimmten Spur (z. B. Analysespalte) **auf Weitere Prozessaktivität hinzufügen**.
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken **Sie auf Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Ebenso können Sie weitere Prozessaktivitäten unter jeder Spur erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (beinhaltet konfigurierte Eingaben im Automatisierungsplan) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie auf **Alle Eigenschaften** anzeigen, und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

### Verwenden des manuellen Malware-Playbooks

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das manuelle Malware-Playbook im SIR-Analystenarbeitsbereich und seine Funktionen verwenden können.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

#### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incident und die Risikopunktzahl anzeigen.

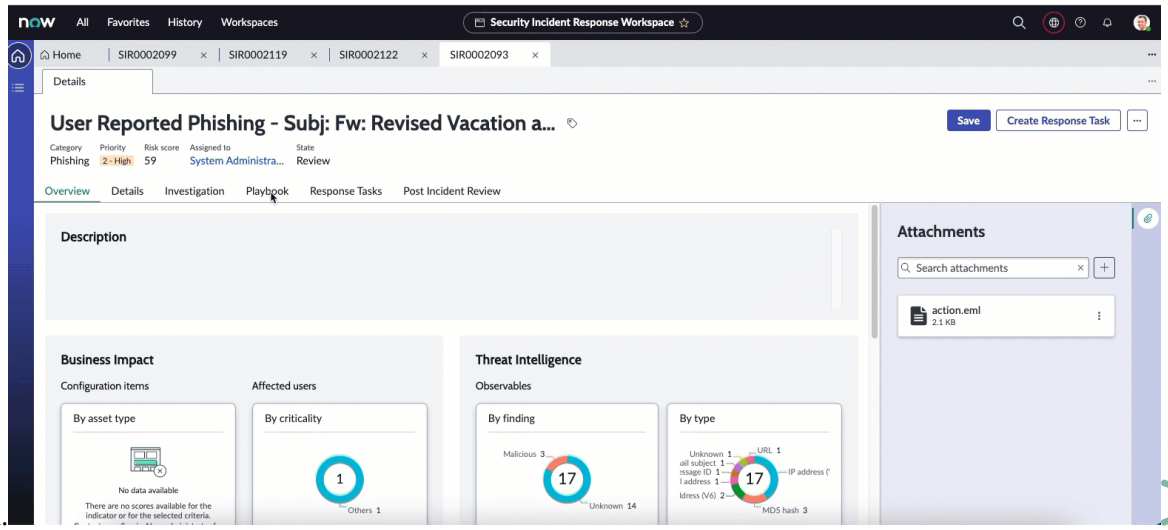
   **Hinweis:**
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie aktivieren, damit sie sie auf der Registerkarte **„Playbook“** anzeigen können.

3. Klicken Sie auf das **manuelle Malware-Playbook**.
   Bei manueller Malware werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies gemäß Ihren Anforderungen zu ändern.




6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Benutzeraktion vorhanden ist, die Sie ausführen müssen, wird sie in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Benutzeraktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

### Playbook für automatisierte Malware

Das automatisierte Malware-Playbook bietet eine Reihe automatisierter Schritte, mit denen Analysten Malware-Warnungen effizienter lösen können.

Die Vorlage „Automatisiertes Malware-Playbook“ wurde entwickelt, um die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk zu automatisieren. Sie können die PAD-Vorlagen verwenden, um die Schritte im automatisierten Malware-Playbook zu automatisieren und diese Warnungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie mit Anmerkungen versehen können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, die als Reaktion auf Malware-Angriffe entwickelt wurden. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das automatisierte Malware-Playbook im Prozessautomatisierungs-Designer (PAD) aktivieren. Dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Im Folgenden sind die Spuren der Prozessdefinition aufgeführt, die dem Security Incident-Status entsprechen:

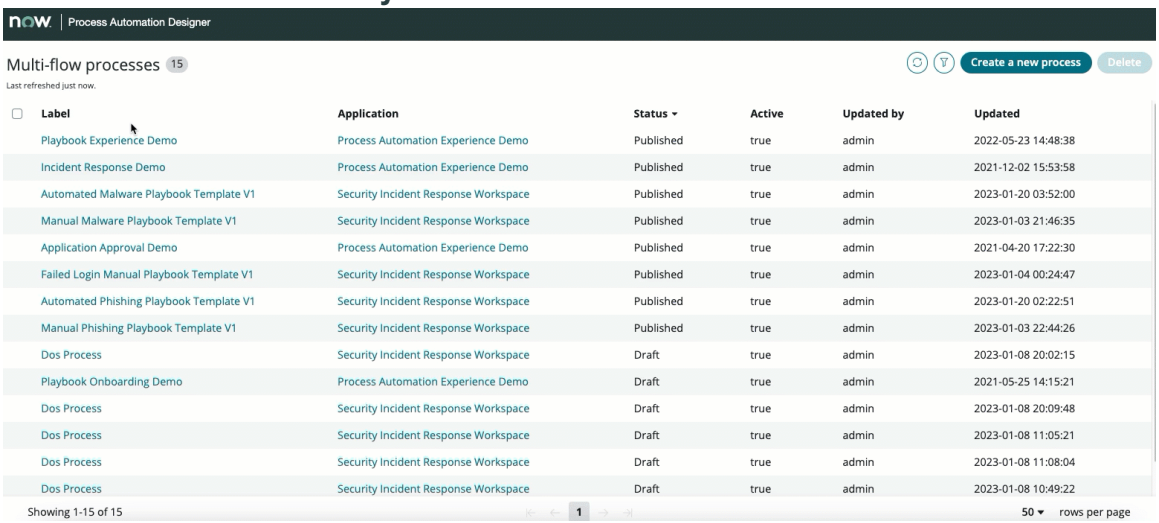
- Analyse
- Beinhalten
- Beseitigen
- Prüfen

Jede Spur enthält Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Automatisiertes Malware-Playbook**




Sobald Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbook zeigt alle Daten, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um die Erstellung der Berechtigung abzuschließen.

### Erstellen Sie Prozesse für automatisierte Malware in PAD

Führen Sie diese Schritte aus, um Prozesse für automatisierte Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

#### Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** >  > **Einen neuen Prozess erstellen**.

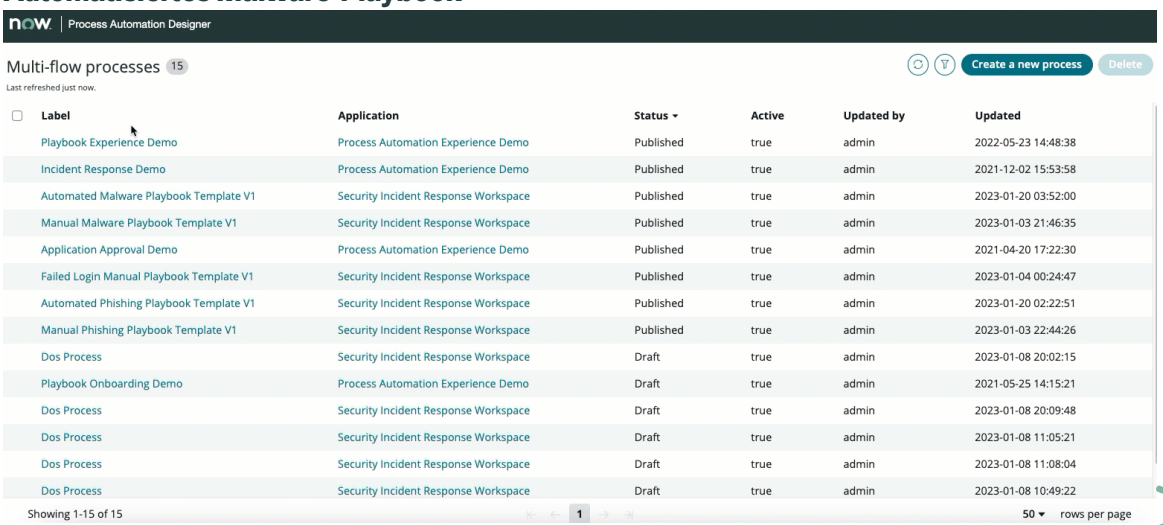
   Beispiel: Automated Malware Playbook Template V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken **Sie auf Einen Auslöser auswählen**.
4. Wählen **Sie Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken **Sie auf Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie „Phishing“ erstellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Automatisiertes Malware-Playbook**

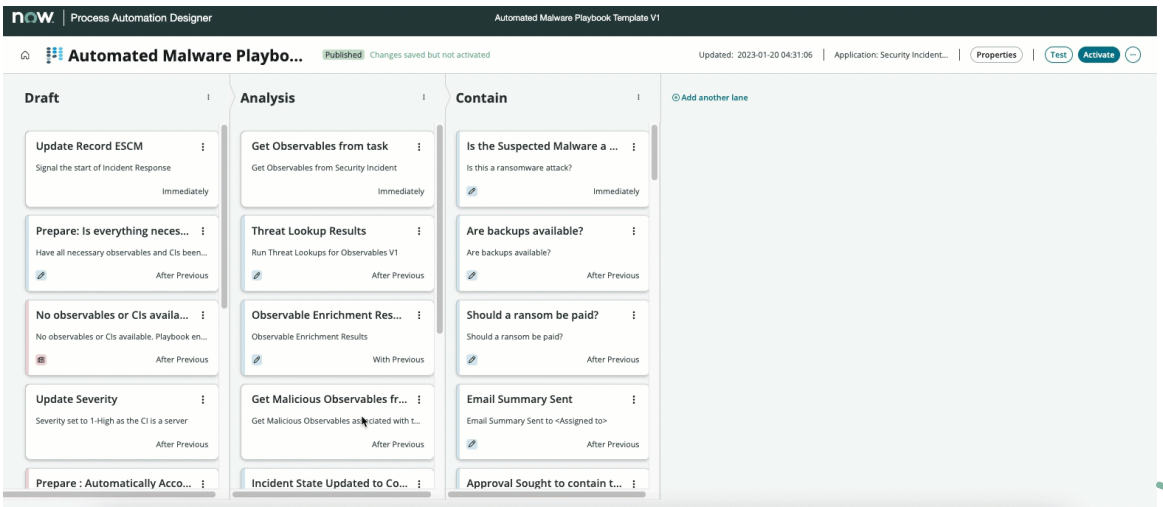



7. Klicken **Sie auf Zu Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Neue Spalte hinzufügen**.
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Benutzeroberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name**, **Beschreibung**, **Bedingung**ausführen und **Geben Sie an, wann gestartet werden soll**.
   Die Felder Ausführungsbedingung und **Angeben, wann gestartet** werden soll implizieren, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte**hinzufügen.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spur für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel beginnt die **Analysespalte** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Spaltenstart, nachdem die vorherige Spalte abgeschlossen ist, und weist eine Ausführungsbedingung auf, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spur hinzufügen.
12. Klicken Sie unter einer bestimmten Spur (z. B. Analysespalte) **auf Weitere Prozessaktivität hinzufügen**.
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken **Sie auf Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Ebenso können Sie weitere Prozessaktivitäten unter jeder Spur erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Automatisierte Malware-Aktivität**




14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (beinhaltet konfigurierte Eingaben im Automatisierungsplan) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie auf **Alle Eigenschaften** anzeigen, und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

## Verwenden des automatisierten Malware-Playbooks

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das automatisierte Malware-Playbook im SIR Analyst Workspace und seinen Funktionen verwenden können.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incident und die Risikopunktzahl anzeigen.

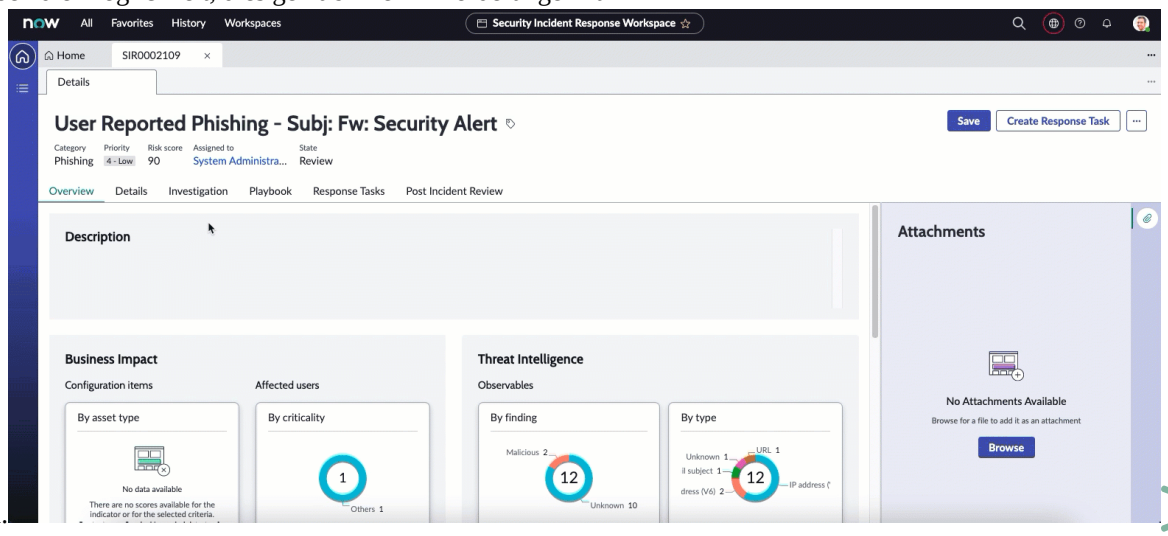
   **Hinweis:**
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie aktivieren, damit sie sie auf der Registerkarte **„Playbook“** anzeigen können.

3. Klicken Sie auf das **automatisierte Malware-Playbook**.
   Bei automatisierter Malware werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, dies gemäß Ihren Anforderungen zu ändern.




6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie gemäß Ihren Anforderungen zu ändern. Wenn Sie noch eine Aktivität oder Benutzeraktion ausführen müssen, wird diese in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Benutzeraktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

### Playbook für fehlgeschlagene Anmeldung – manuell

Das Playbook „Manuelles Failed Login“ bietet Anleitungen und hilft bei der Optimierung der Untersuchung von Security Incidents mit fehlgeschlagenen Anmeldungen.

Wenn ein Benutzer bestimmte erfolglose Anmeldeversuche unternimmt (gemäß SIM-Konfiguration), wird ein Security Incident erstellt. Bei diesen erfolglosen Anmeldeversuchen kann es sich entweder um Falschmeldungen oder um Versuche von Angreifern handeln, sich Zugriff auf die E-Mail-Accounts der Benutzer zu verschaffen.

Sie können die PAD-Vorlagen verwenden, um die Schritte im Playbook „Fehlgeschlagene Anmeldung“ auszuführen und Security Incidents mit fehlgeschlagener Anmeldung effizient zu beheben. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie mit Anmerkungen versehen können. Dieses Playbook enthält eine Reihe von wiederverwendbaren Aktionen, die darauf ausgelegt sind, auf Security Incidents mit fehlgeschlagener Anmeldung zu reagieren. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident mit fehlgeschlagener Anmeldung erstellt oder aktualisiert wird. Sie müssen das manuelle Playbook für fehlgeschlagene Anmeldungen im Prozessautomatisierungs-Designer (PAD) aktivieren und alle Aufgaben erstellen, z. B. Analysieren, Eindämmen, Entfernen und Überprüfen.

Im Folgenden sind die Spuren der Prozessdefinition aufgeführt, die dem Security Incident-Status entsprechen:

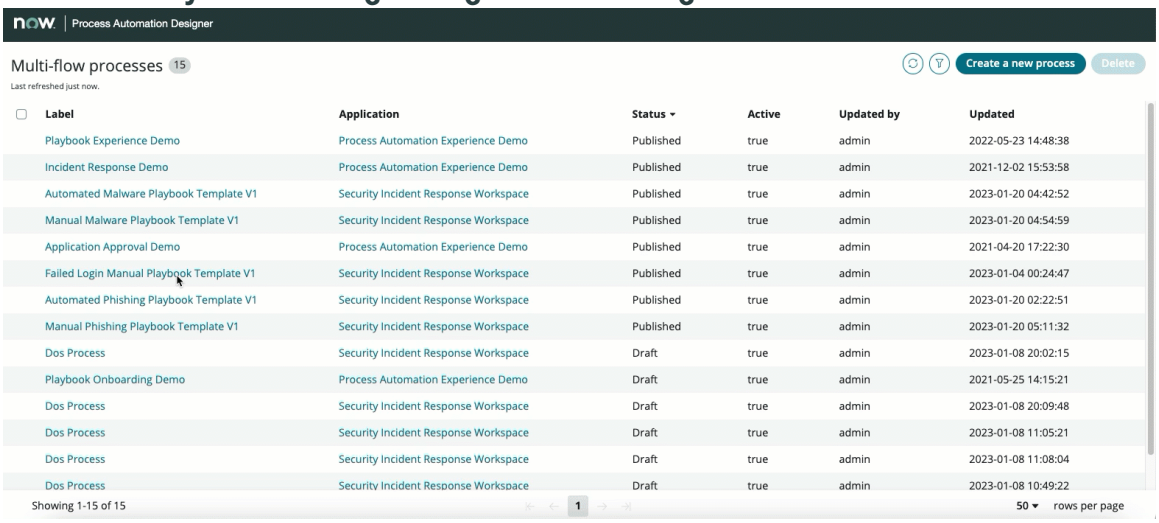
- Analyse
- Beinhalten
- Beseitigen
- Prüfen

Jede Spur enthält Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Manuelles Playbook bei fehlgeschlagener Anmeldung




Sobald Sie eine Aufgabe in einer Spur als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spur abgeschlossen haben, können Sie zur nächsten Spur wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie weiterhin Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbook zeigt alle Daten, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die Details zu überprüfen, die Sie in allen Spuren eingegeben haben. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um die Erstellung der Berechtigung abzuschließen.

### Erstellen Sie Prozesse für die manuelle fehlgeschlagene Anmeldung in PAD

Gehen Sie wie folgt vor, um Prozesse für die manuelle fehlgeschlagene Anmeldung im Prozessautomatisierungs-Designer (PAD) zu erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager

#### Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** >  > **Einen neuen Prozess erstellen**.

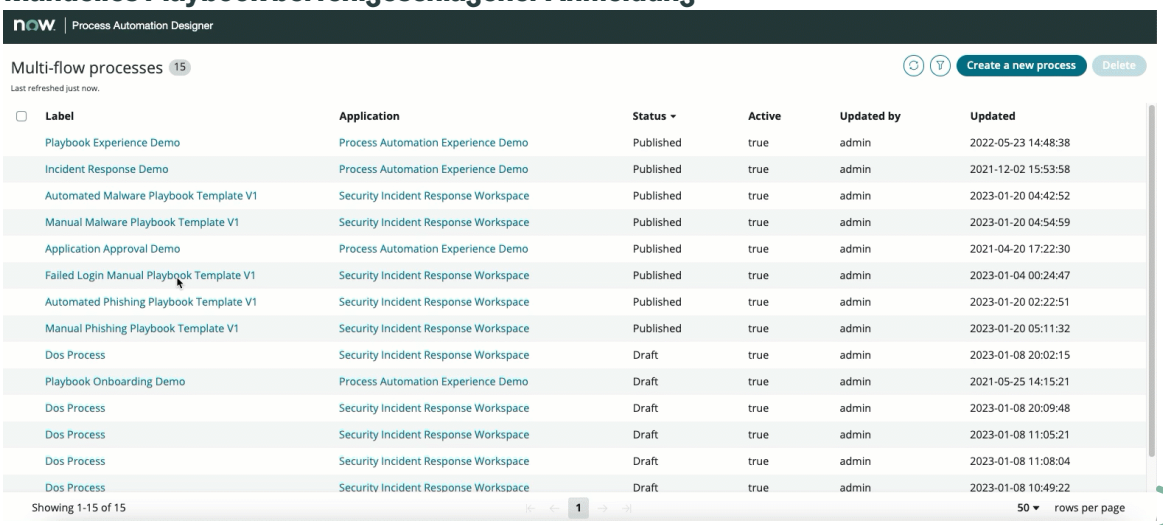
   Beispiel: Manuelle Playbook-Vorlage für fehlgeschlagene Anmeldung V1.

2. Geben Sie einen Namen für den Prozess, eine Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken **Sie auf Einen Auslöser auswählen**.
4. Wählen **Sie Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses**, und wählen Sie die Auslöserbedingung für die Ausführung des Prozesses aus.
5. Klicken **Sie auf Ihre Auslöserbedingungen festlegen**.
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie „Phishing“ erstellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

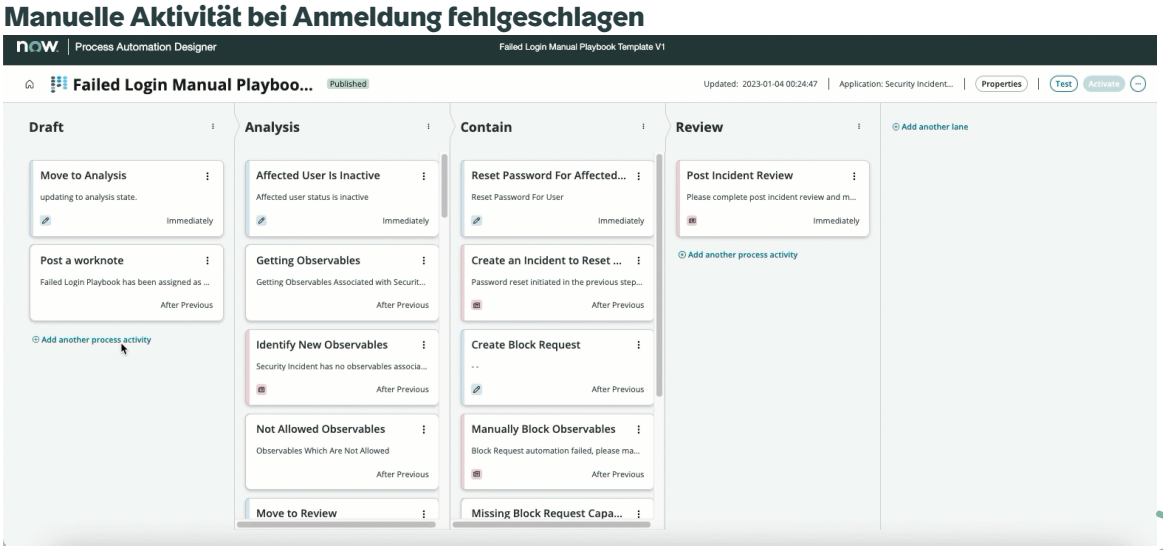
**Manuelles Playbook bei fehlgeschlagener Anmeldung**




7. Klicken **Sie auf Zu Designer wechseln**.
   Die Seite „Prozessautomatisierungs-Designer“ wird geöffnet.
8. Um mit dem Entwurf Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Neue Spalte hinzufügen**.
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Benutzeroberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name**, **Beschreibung**, **Bedingung**ausführen und **Geben Sie an, wann gestartet werden soll**.
   Die Felder Ausführungsbedingung und **Angeben, wann gestartet** werden soll implizieren, wann die Spalte ausgeführt wird.
10. Klicken Sie auf **Speichern und schließen**.
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Weitere Spalte**hinzufügen.
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spur für „Analyse“, „Eindämmen“, „Beseitigen“ und „Überprüfen“ erstellen. Im folgenden Beispiel beginnt die **Analysespalte** sofort und weist keine Ausführungsbedingung auf. **Enthält** den Spaltenstart, nachdem die vorherige Spalte abgeschlossen ist, und weist eine Ausführungsbedingung auf, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spur hinzufügen.
12. Klicken Sie unter einer bestimmten Spur (z. B. Analysespalte) **auf Weitere Prozessaktivität hinzufügen**.
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken **Sie auf Neue Aktivität erstellen**.
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Ebenso können Sie weitere Prozessaktivitäten unter jeder Spur erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (beinhaltet konfigurierte Eingaben im Automatisierungsplan) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie auf **Alle Eigenschaften** anzeigen, und aktivieren Sie den Umschalter **Erweiterte Eigenschaften**, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

## Verwenden des Playbooks „Manuelles Failed Login“.

Führen Sie diese Schritte aus, um zu erfahren, wie Sie das Playbook „Manuelles fehlgeschlagenes Login“ im SIR-Analystenarbeitsbereich und seinen Funktionen verwenden können.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.manager oder sn_si.analyst

### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf die Registerkarte **Playbook**.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incident und die Risikopunktzahl anzeigen.

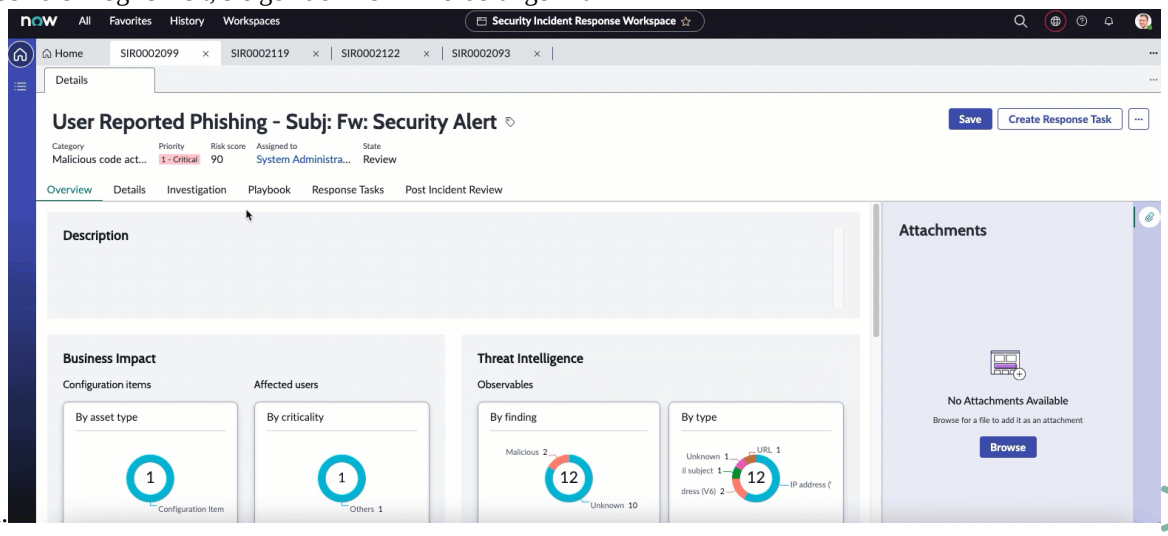
   **Hinweis:**
   Wenn keine Playbooks aufgelistet sind, müssen Sie zu PAD wechseln und sie aktivieren, damit sie sie auf der Registerkarte **„Playbook“** anzeigen können.

3. Klicken Sie auf das **Playbook bei fehlgeschlagener Anmeldung**.
   Bei „Manuelle fehlgeschlagene Anmeldung“ werden die Aufgaben automatisch für den Security Incident ausgeführt.
4. Klicken Sie auf jede Spur, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie auf **Analyse**, um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, sie gemäß Ihren Anforderungen zu ändern.




6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn Sie noch eine Aktivität oder Benutzeraktion ausführen müssen, wird diese in der entsprechenden Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Benutzeraktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

### Flow-basierte Playbooks

Mit Flow Designer können Sicherheitsadministratoren und Flow-Design-Autoren einfacher von manuellen oder undokumentierten Playbooks zu automatisierten und wiederholbaren Playbooks wechseln. Die Drag-and-Drop-Funktion bietet Flexibilität beim Verschieben von Objekten, Bedingungsprüfungen, parallelen Verzweigungen, Entscheidungstabellen und mehr.

Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit.

Zusätzlich zu den aufgeführten Playbooks gibt es in Security Operations Spoke auch Subflows, die aus dem Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Security Incident Response-Flow aktivieren.

### Playbook für automatisiertes Phishing

Das Playbook Automated Phishing hilft Ihnen, bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt zu beheben. Mit den Flow Designer-Vorlagen können Sie die Schritte im Phishing-Antwort-Playbook automatisieren und Incidents schnell und effizient lösen.

Sie können mit Flow Designer erstellte Vorlagen verwenden, um die Aufgaben im Phishing-Antwort-Playbook zu automatisieren und Phishing-Angriffe in Ihrer Organisation zu analysieren und zu beheben.

Das Phishing-Antwort-Playbook enthält die folgenden Flows und Subflows:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident – Automated Phishing Response Template: Diese Vorlage dient zur Automatisierung der Phishing-Antwortaufgaben und enthält eine Reihe von Aktionen, einschließlich eines Auslösers.
- Security Incident – Phishing – Manuelle Vorlage: Diese Vorlage ist der vorhandene manuelle Phishing-Antwort-Workflow. Legen Sie die Kategorie auf Phishing fest, um den Flow zu aktivieren.

Diese Vorlagen enthalten eine Reihe von wiederverwendbaren Aktionen, die als Reaktion auf Phishing-Angriffe entwickelt wurden. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows, die Sie zur besseren Lesbarkeit mit Anmerkungen versehen können. Um auf diese Flows zuzugreifen, müssen Sie dieSecurity Operations-Spoke installieren.

**Hinweis:**
Aktivieren Sie diese Vorlagen, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter Security Incident Response-Flow aktivieren.

- Bedrohungssuchen für erkennbare Elemente ausführen: Führt Bedrohungssuchen für ausgewählte erkennbare Elemente durch.
- Erkennbare Elemente anreichern: Ermöglicht das Anreichern von erkennbaren Elementen mit zusätzlichen Informationen aus verschiedenen Quellen.
- Phishing-E-Mail-Auswirkung bewerten: Ermöglicht die Bewertung der Auswirkungen der Phishing-E-Mail. Wenn Sie eine E-Mail an die Phishing-E-Mail-Adresse erhalten, analysiert dieser Subflow den EML-Anhang und vergleicht die Informationen mit den E-Mail-Abgleichregeln.
- Phishing-E-Mails beseitigen: Ermöglicht das Löschen oder Entfernen von Phishing-E-Mails, um die Gefährdung durch einen bestimmten Angriff zu reduzieren.
- Sichtungssuche für erkennbare Elemente ausführen: Ermittelt die Verbreitung einer Bedrohung im Laufe der Zeit oder testet Korrektur- oder Beseitigungsmaßnahmen.
- Blockierungsanforderungen erstellen: Blockiert die Kommunikation mit erkennbaren Elementen, die dem Incident zugeordnet sind.

Diese Subflows stellen eine Reihe von wiederverwendbaren Vorgängen dar, die Sie in mehreren Playbooks verwenden können. Sie können diese Subflows verwenden, um benutzerdefinierte Vorlagen (Flows) gemäß Ihren Anforderungen zu definieren.

Um benutzerdefinierte Vorlagen (Flows) zu erstellen, befolgen Sie die Anweisungen unter Flows .

### Führen Sie den automatisierten Phishing-Antwort-Playbook-Flow aus

Mit dem Flow Designer können Sie Aufgaben im Playbook definieren und automatisieren, um Phishing-Angriffe auf Ihre Organisation zu analysieren und zu lösen.

### Vorbereitungen

- Erforderliche Rolle: sn_si.admin, flow_designer und action_designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Blockanforderung (Security Operations Palo Alto Networks NGFW-Integration)
  - Anreicherung erkennbarer Elemente
  - Sichtungssuche



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuche
- Microsoft Office Exchange

### Warum und wann dieser Vorgang ausgeführt wird

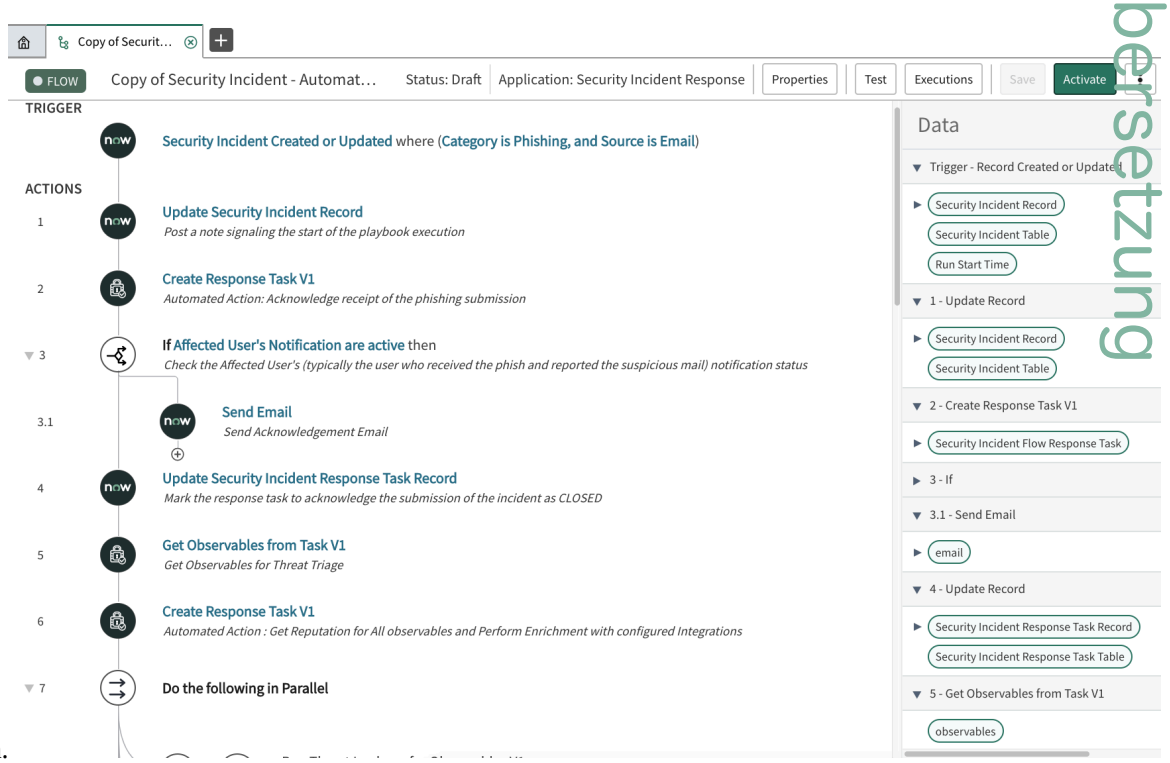
Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die häufigsten Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie sie als EML-Anhang an die von Ihrer Organisation festgelegte Phishing-E-Mail-Adresse senden. Mit den im automatisierten Phishing-Playbook-Flow definierten Aufgaben können Sie eine Phishing-Bedrohung selektieren, analysieren, eindämmen und beseitigen. Diese Aufgaben können als Teil verschiedener Incident-Status aufgerufen werden (z. B. „Analyse“, „Eindämmen“ usw.). Wenn ein Phishing-Security Incident erstellt wird, kann der automatisierte Phishing-Flow automatisch ausgelöst werden. Mit Flow Designer können Sie die Details der verschiedenen Incident-Antwortaktionen anzeigen, wenn sie aufgerufen werden.

**Hinweis:**
Der Playbook-Flow „Security Incident – Automated Phishing Response Template V1“ (Security Incident – Automated Phishing Response Template V1) ist schreibgeschützt. Sie können eine Kopie des Flow erstellen und nach Bedarf Änderungen vornehmen.

Die folgenden Schritte beschreiben, wie Sie eine Kopie der Phishing-Playbook-Vorlage erstellen, und führen Sie durch einige der Aufgaben im Flow.

### Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** , um die mit der Spoke Security Operations verfügbaren Flows anzuzeigen.
2. Klicken Sie auf den Link **Security Incident – Automated Phishing Response Template VI**.
3. Klicken Sie auf der Seite „Flow“ auf das Symbol „ “ Symbol „Mehr“ , erstellen Sie eine Kopie des Flows, und öffnen Sie sie zur Verwendung.
   Sie können die Auslöserbedingungen ändern, Aktionen hinzufügen oder entfernen und andere Änderungen am Flow



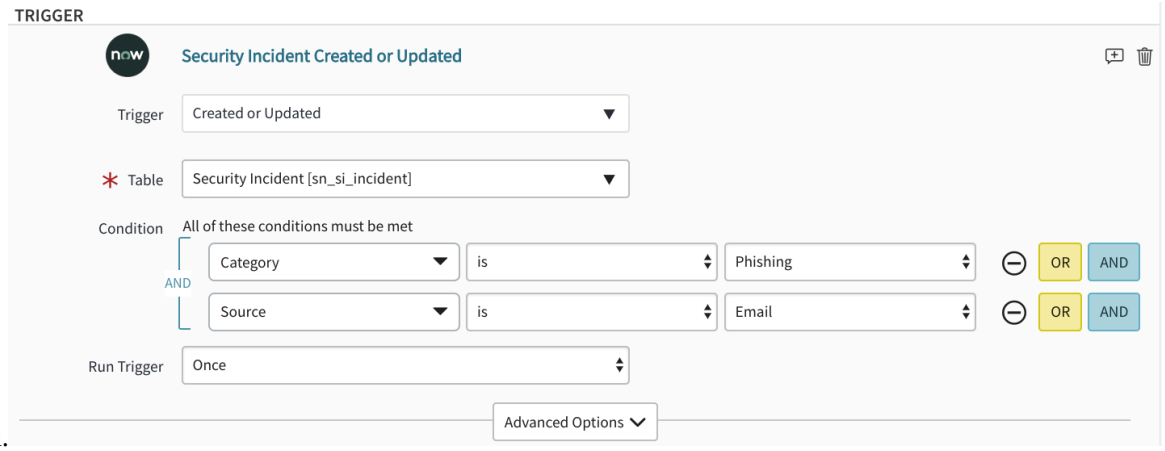

vornehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

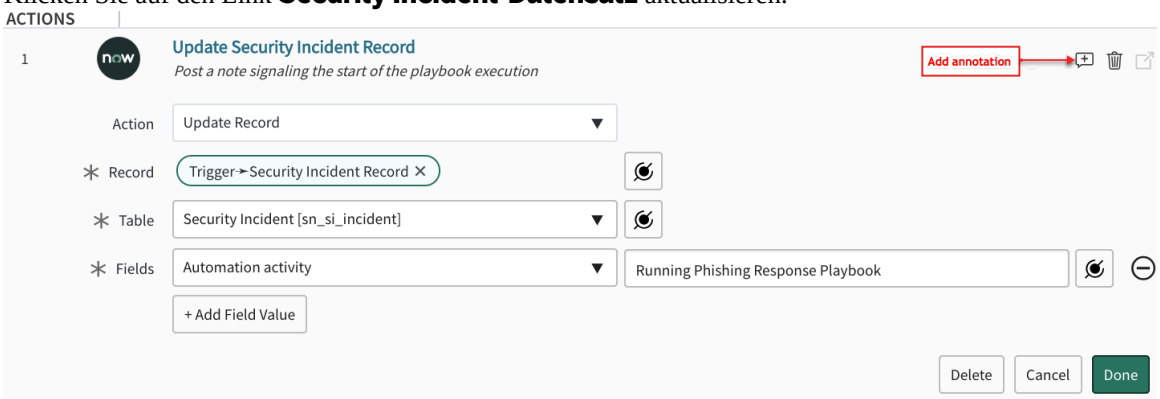
Diese Abbildung zeigt die Auslösebedingungen und die Schritte, die der Flow ausführt. Im rechten Bereich wird der Datenfluss angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

4. Klicken Sie auf das **Auslösersymbol**.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser an und wie oft der Flow den Auslöser ausführen soll.




   Wenn die im Flow definierten Bedingungen (Kategorie ist Phishing und Quelle ist E-Mail) im Incident-Datensatz erfüllt sind, werden die Aufgaben im automatisierten Phishing-Flow nacheinander ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Klicken Sie auf den Link **Security Incident-Datensatz** aktualisieren.



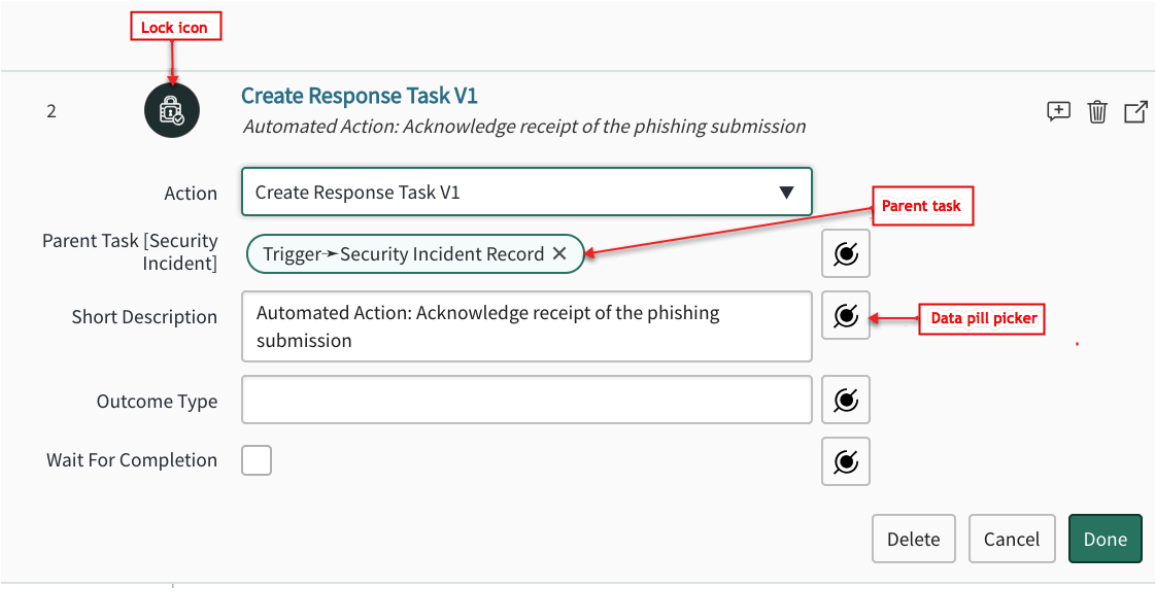

   „Security Incident-Datensatz aktualisieren“ ist der erste Schritt in diesem Flow. Klicken Sie auf das Anmerkungssymbol , um dem Sicherheitsanalysten eine Notiz hinzuzufügen, die angibt, dass ein Phishing-Incident aufgetreten ist und die Ausführung des automatisierten Phishing-Playbook-Flows begonnen hat.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf den Link **Antwortaufgabe erstellen**.

   In diesem Schritt erstellt der Flow eine automatisierte Antwortaufgabe, um der Person, die den Incident übermittelt hat, oder dem betroffenen Benutzer den Empfang zu bestätigen.



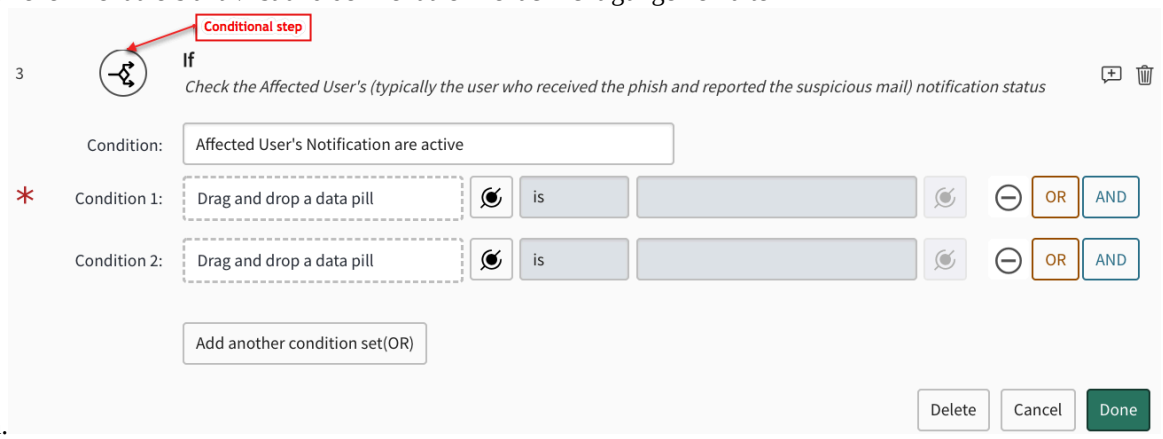
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Beachten Sie, dass das Feld **Übergeordnete Aufgabe [Security Incident]**auf den übergeordneten Datensatz verweist, der diesem Schritt zugeordnet ist. Sie können einen beliebigen Referenzdatensatz auswählen, indem Sie das Datenpillenauswahl-Symbol verwenden oder das relevante Referenzelement aus dem rechten Bereich ziehen.

Beachten Sie das Schlosssymbol . Das Sperrsymbol zeigt an, dass für diesen Schritt kein Benutzereingriff erforderlich ist.

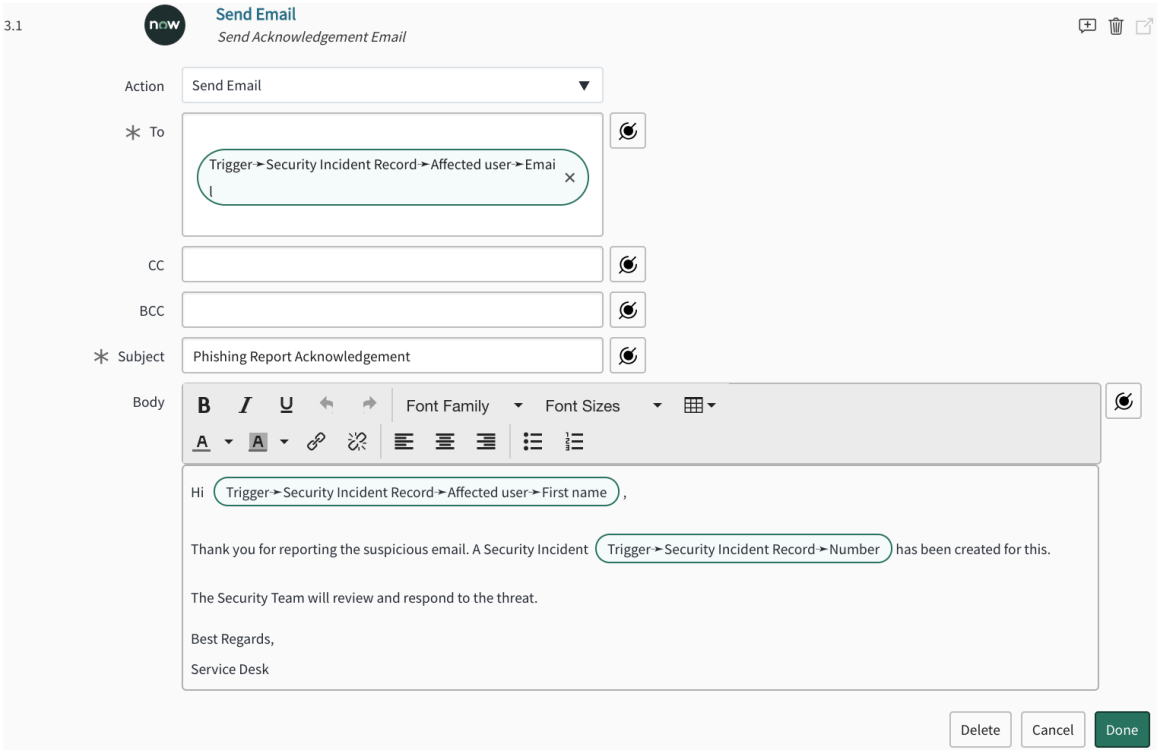
7. In Schritt 3 erfasst der Flow zusätzliche Details des betroffenen Benutzers (normalerweise der Benutzer, der den Incident übermittelt hat), um sicherzustellen, dass eine Benachrichtigung erfolgreich gesendet werden kann.
   Sie können Bedingungen angeben, um zu überprüfen, ob der Status des betroffenen Benutzers aktiv ist und der Benutzer Benachrichtigungen erhalten kann.




Beachten Sie das Symbol für den bedingten Schritt Symbol für den in Schritt 3. Der Flow führt den nächsten Schritt (3.1) nur aus, wenn die angegebenen Bedingungen erfüllt sind.

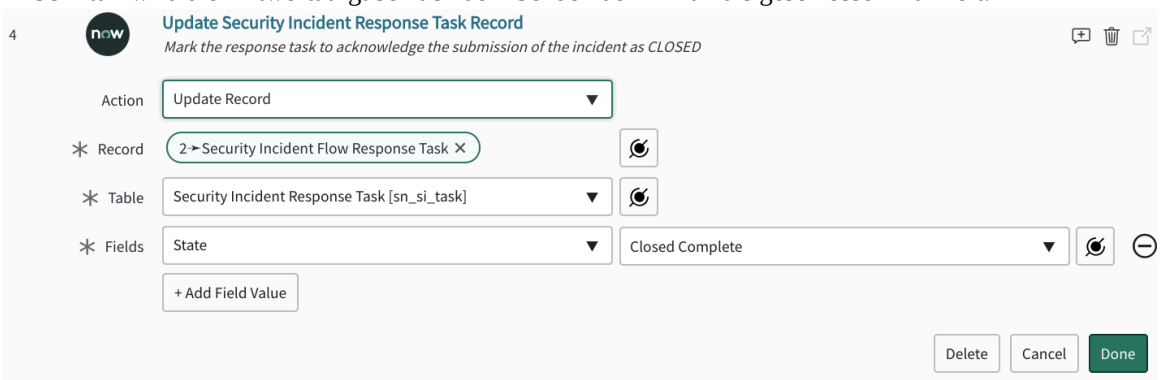


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

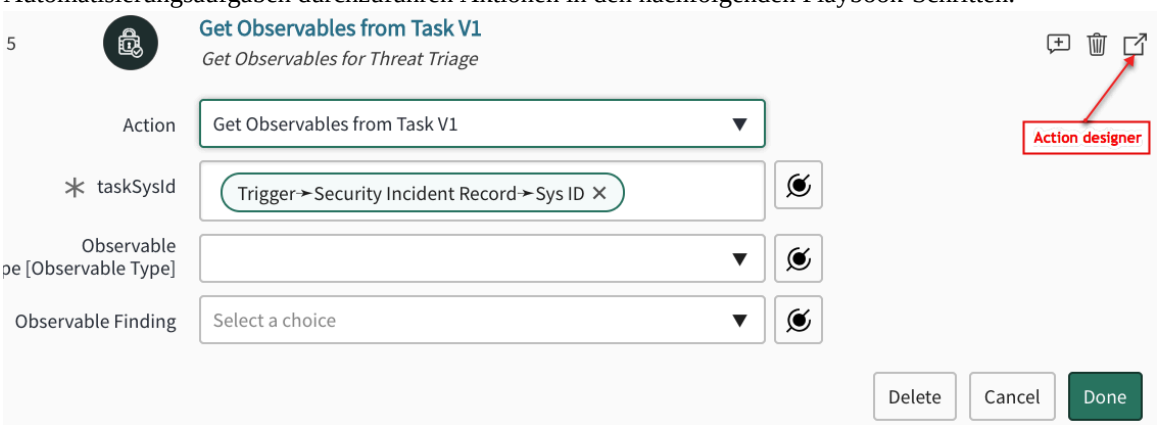



Wenn die in Schritt 3 definierten Bedingungen erfolgreich erfüllt wurden, wird die E-Mail gesendet.

**8.** In Schritt 4 wird die Antwortaufgabe nach dem Senden der E-Mail als geschlossen markiert.




**9.** In Schritt 5 werden alle am Incident beteiligten erkennbaren Elemente (z. B. E-Mail-Betreff, E-Mail-Adresse, von der die Phishing-E-Mail gesendet wurde, Phishing-URL) oder erkennbare Elemente, die zu einer ausgewählten Kategorie (Hash, Datei oder Domäne) gehören, erfasst, um zusätzliche Automatisierungsaufgaben durchzuführen Aktionen in den nachfolgenden Playbook-Schritten.



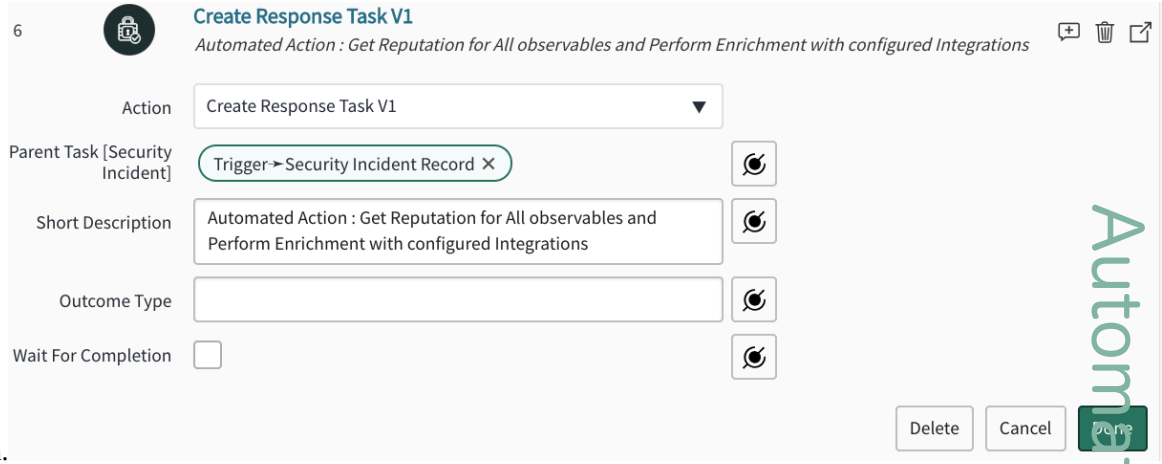



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

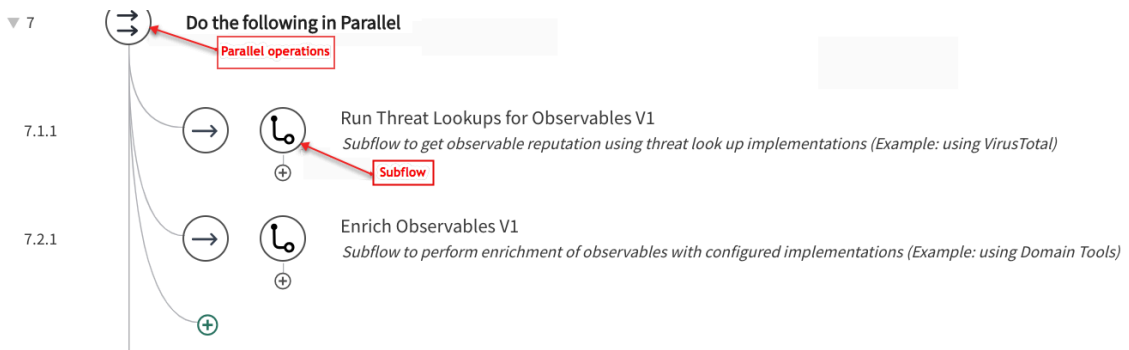
Klicken Sie auf das Aktionsdesigner-Symbol , um eine detaillierte Ansicht der Aktion anzuzeigen.

Um die Seite „Aktionsdesigner“ anzuzeigen, erweitern Sie einen Schritt im Flow, und klicken Sie auf das Aktionsdesigner-Symbol.

10. In Schritt 6 wird eine automatisierte Antwortaufgabe erstellt.
Diese Aufgabe erfasst den Beginn des Prozesses zum Abrufen der Reputation aller erkennbaren Elemente und zur Ergänzung mit konfigurierten Integrationen.



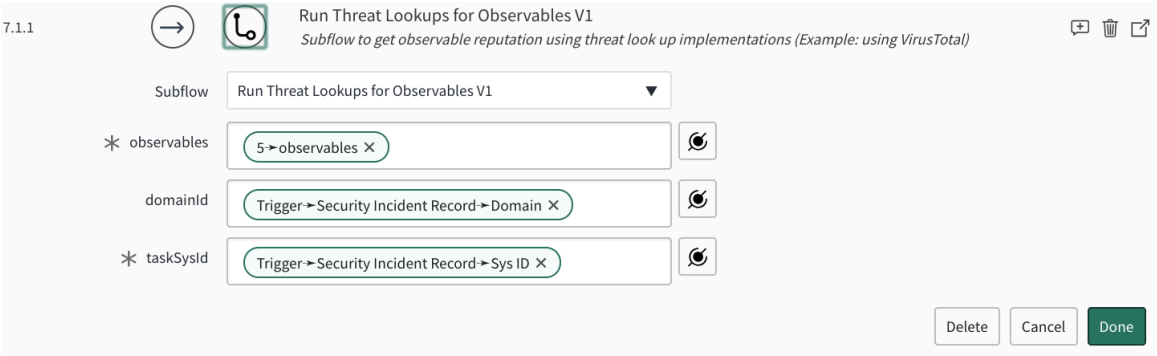

11. In Schritt 7 werden zwei Subflows aufgerufen:
    - Bedrohungssuche für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Implementierungen der Bedrohungssuche abzurufen.
    - Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung von erkennbaren Elementen mit konfigurierten Implementierungen durchzuführen.




Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge Symbol für zeigt an, dass beide Aufgaben parallel ausgeführt werden, und das Subflow-Symbol zeigt an, dass die ausgeführte Aufgabe ein Subflow ist, wie unten dargestellt:

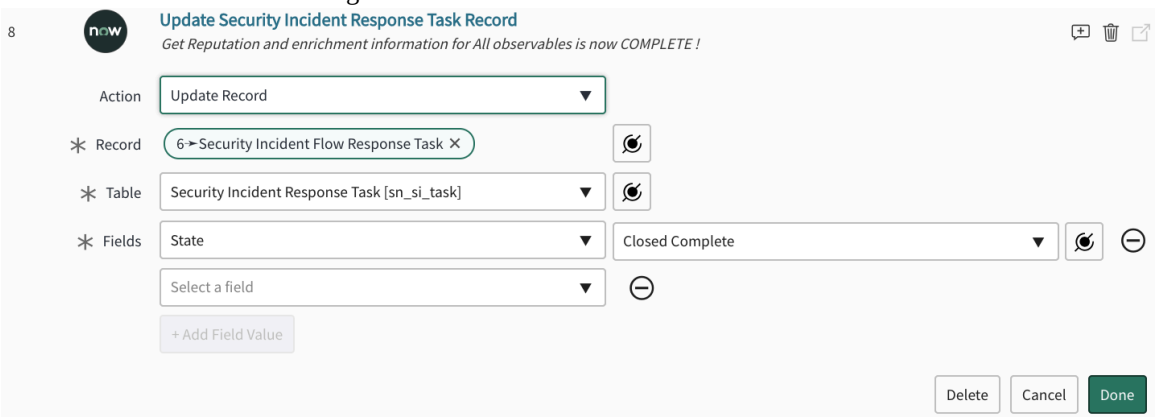
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

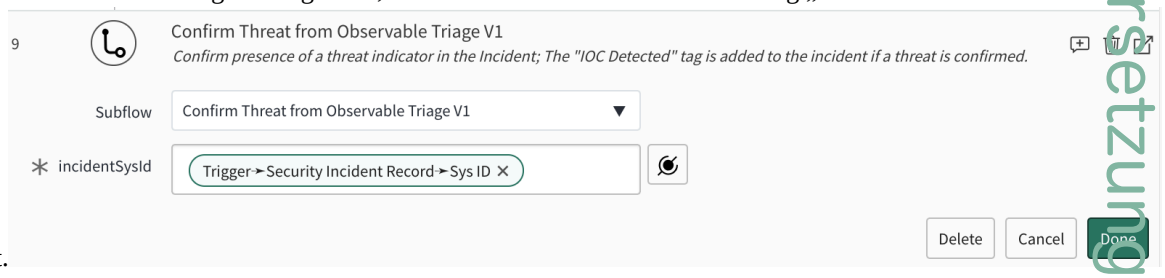



Beachten Sie die Zahl 5 im Feld „Erkennbare Elemente“. Dies gibt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf, wie im Subflow Designergezeigt.

**12.** In Schritt 8 wird die Antwortaufgabe nach Abschluss der Subflows als Geschlossen markiert.

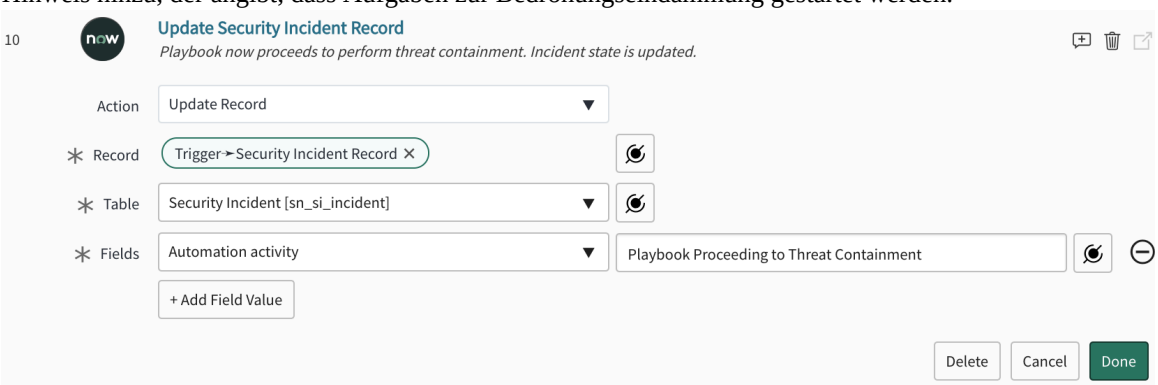



**13.** In Schritt 9 wird der Subflow „Bedrohung aus Selektierung erkennbarer Elemente bestätigen“ aufgerufen. Dieser Subflow wird verwendet, um das Vorhandensein eines Bedrohungsindikators im Incident zu bestätigen. Wenn die Bedrohung bestätigt wird, wird dem Incident die Kennzeichnung „IOC erkannt“




hinzugefügt.

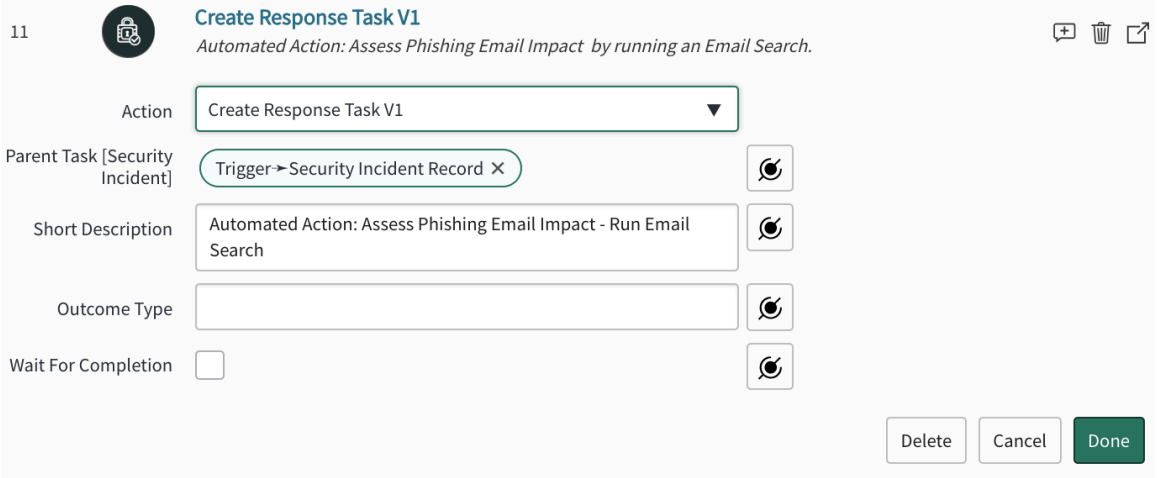
**14.** Wenn die Bedrohung bestätigt wird, aktualisieren Sie in Schritt 10 den Security Incident und fügen einen Hinweis hinzu, der angibt, dass Aufgaben zur Bedrohungseindämmung gestartet werden.



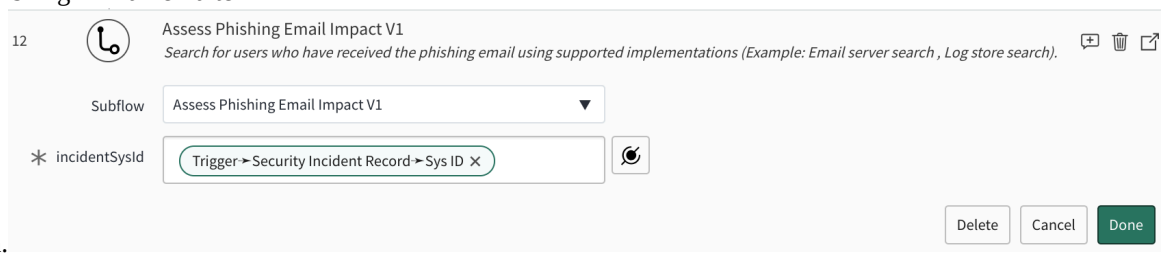

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Schritt 11 ist eine automatisierte Antwortaufgabe, die den Beginn und Abschluss der Aufgabe erfasst, die zur Bewertung der Auswirkungen der Phishing-E-Mails verwendet wird.

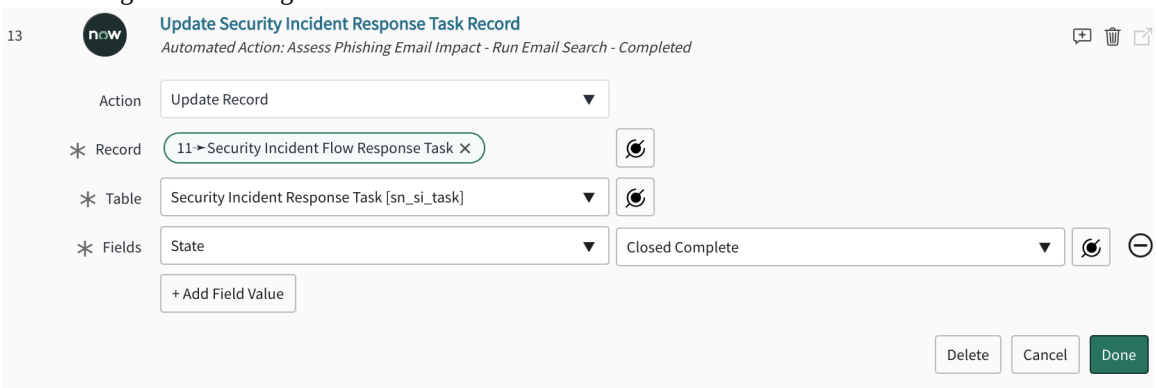



16. In Schritt 12 wird der Subflow Phishing-E-Mail-Auswirkung bewerten aufgerufen.
Dieser Subflow wird verwendet, um mithilfe unterstützter Implementierungen nach Benutzern zu suchen, die die Phishing-E-Mail erhalten

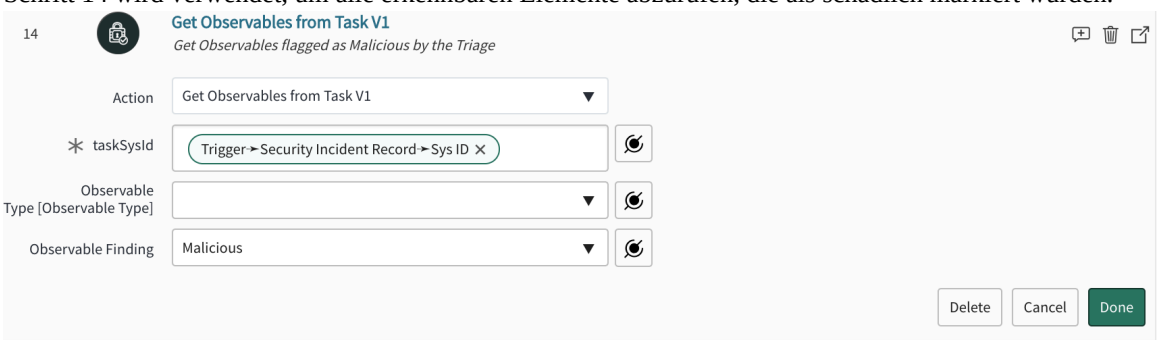



haben.

17. In Schritt 13 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow Phishing-E-Mail-Auswirkung bewerten ausgeführt wurde.



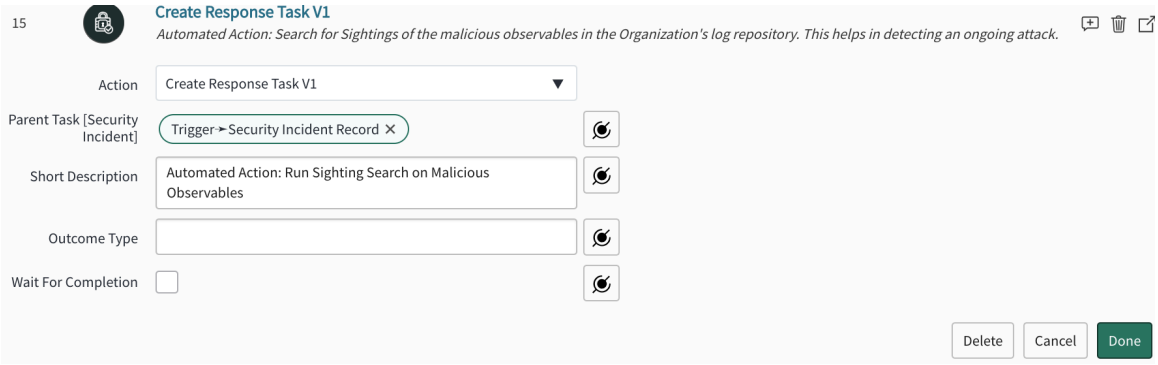

18. Schritt 14 wird verwendet, um alle erkennbaren Elemente abzurufen, die als schädlich markiert wurden.



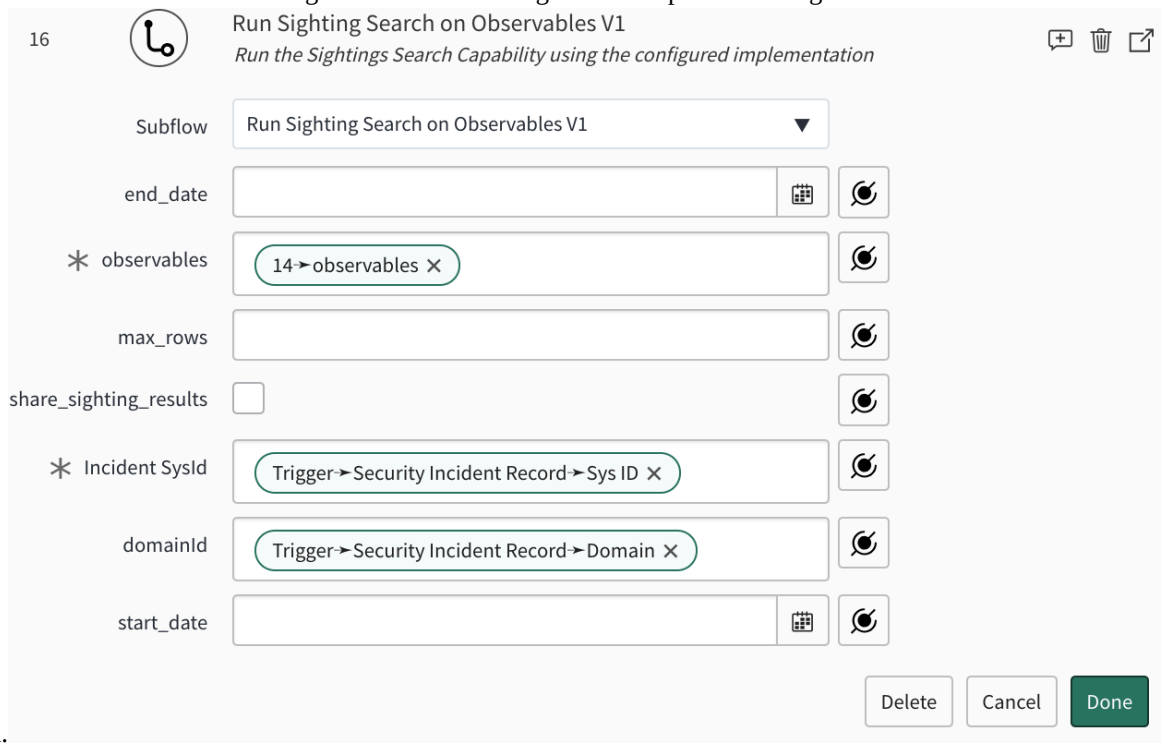

19. Schritt 15 ist eine automatisierte Antwortaufgabe, die den Beginn und Abschluss der Aufgabe „Sichtungssuche nach erkennbaren Elementen“ erfasst.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

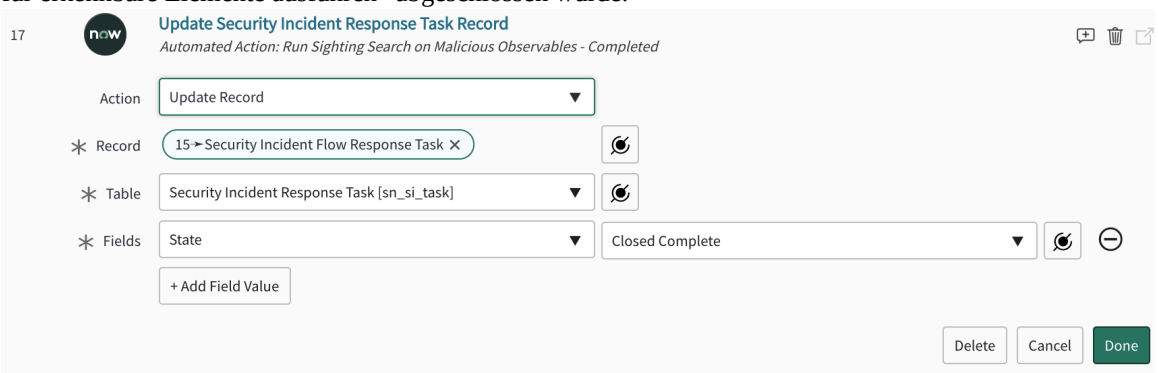



**20.** In Schritt 16 wird der Subflow „Sichtungssuche für erkennbare Elemente ausführen“ aufgerufen. Dieser Subflow führt eine Sichtungssuche mit der konfigurierten Implementierung




durch.

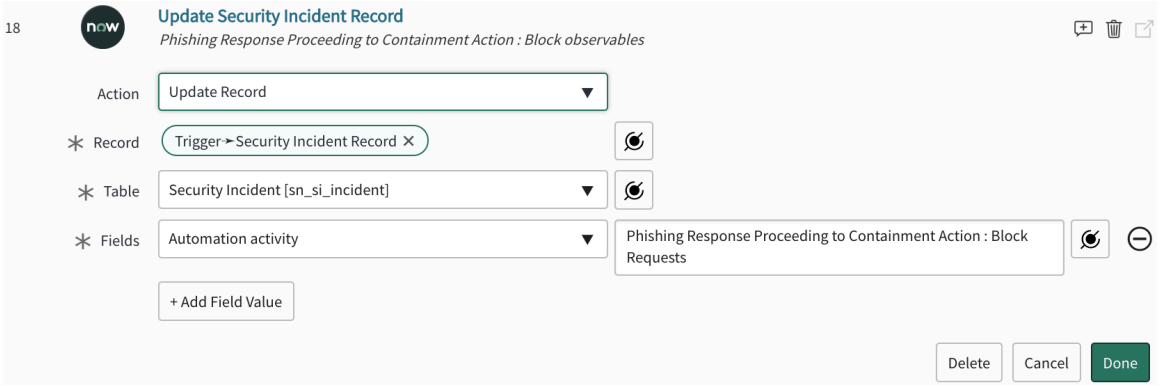
**21.** In Schritt 17 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow „Sichtungssuche für erkennbare Elemente ausführen“ abgeschlossen wurde.



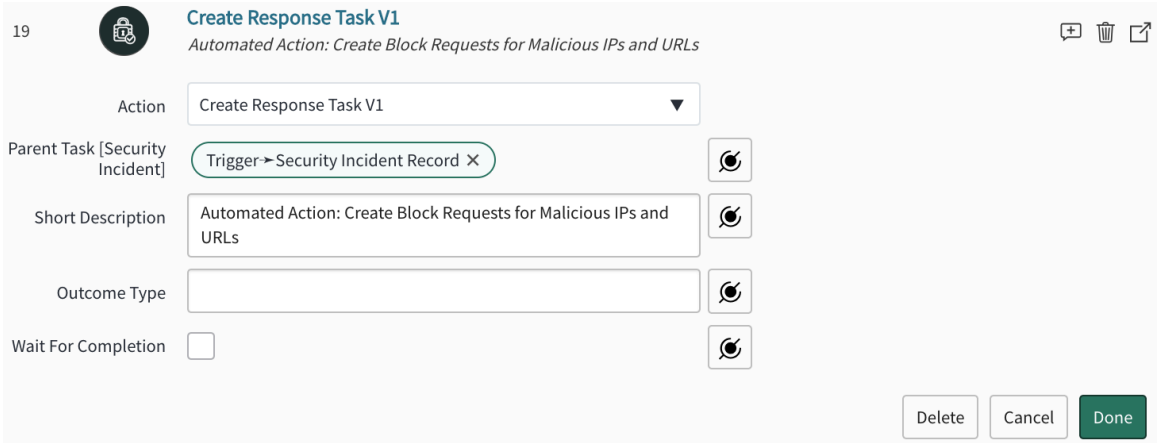

**22.** Nachdem Sie die schädlichen erkennbaren Elemente identifiziert haben, aktualisieren Sie in Schritt 18 den Security Incident-Datensatz, um anzugeben, dass die Eindämmungsmaßnahmen jetzt beginnen.



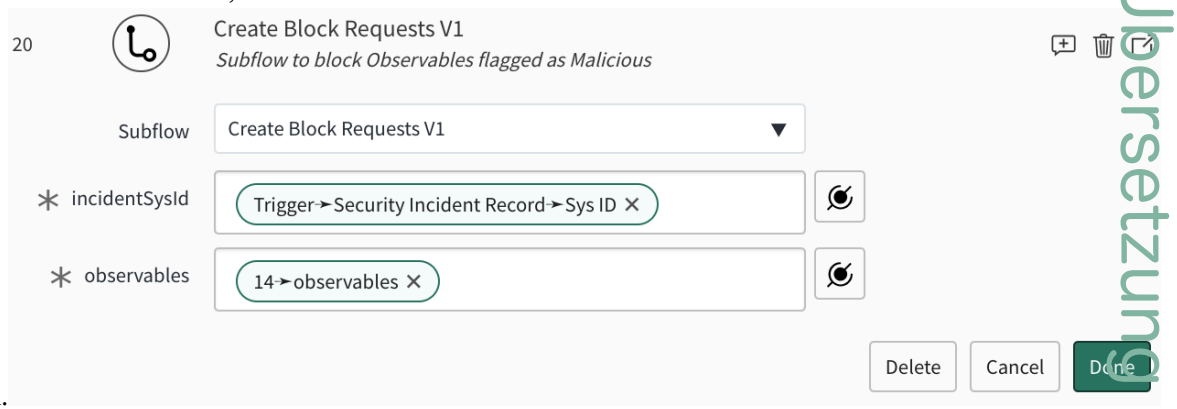
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**23.** Schritt 19 ist eine automatisierte Antwortaufgabe, die den Start und Abschluss der Blockanforderungsaufgabe erfasst.

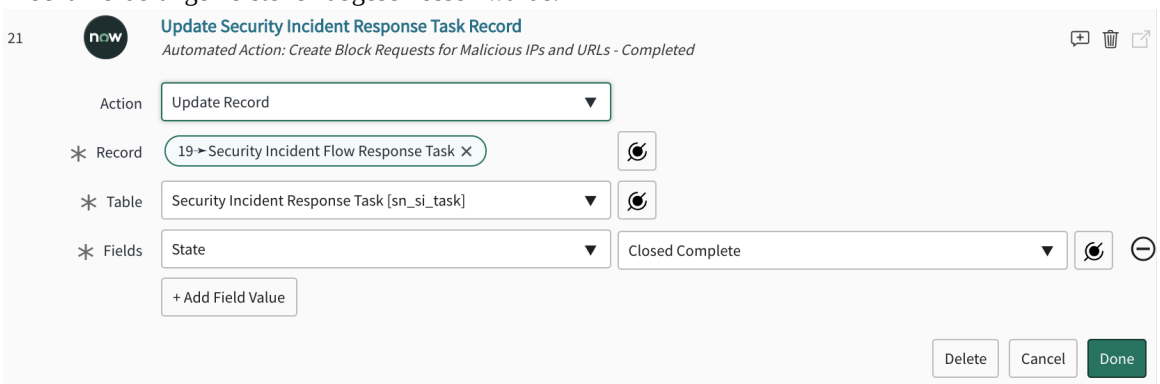



**24.** In Schritt 20 wird der Subflow Blockanforderungen erstellen aufgerufen. Dieser Subflow wird verwendet, um schädliche erkennbare Elemente zu




blockieren.

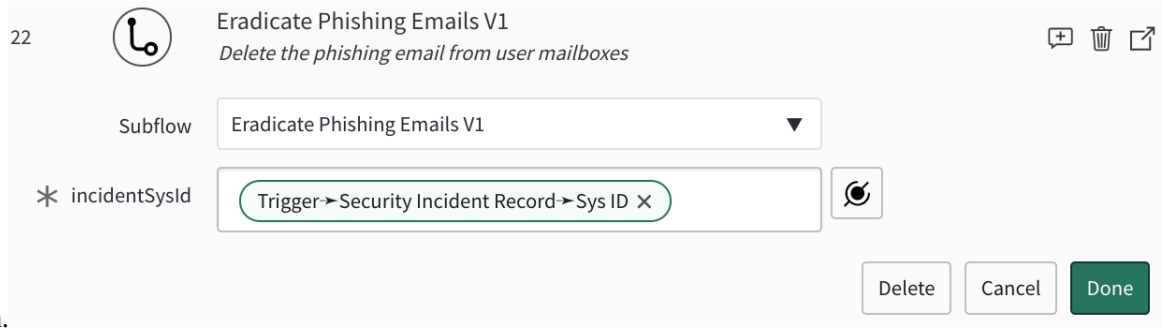
**25.** In Schritt 21 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow Blockanforderungen erstellen abgeschlossen wurde.




Automatische Übersetzung

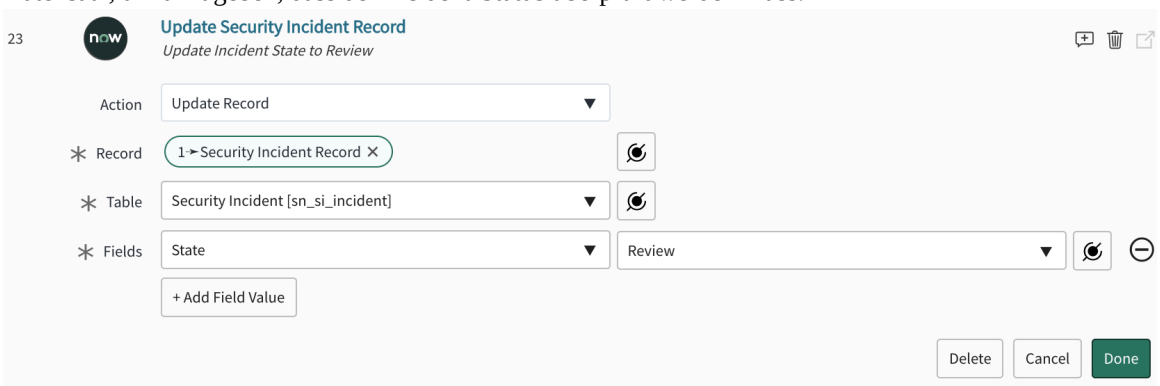
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**26.** In Schritt 22 wird der Subflow Phishing-E-Mails beseitigen aufgerufen.
Dieser Subflow wird verwendet, um Phishing-E-Mails aus Benutzerpostfächern zu

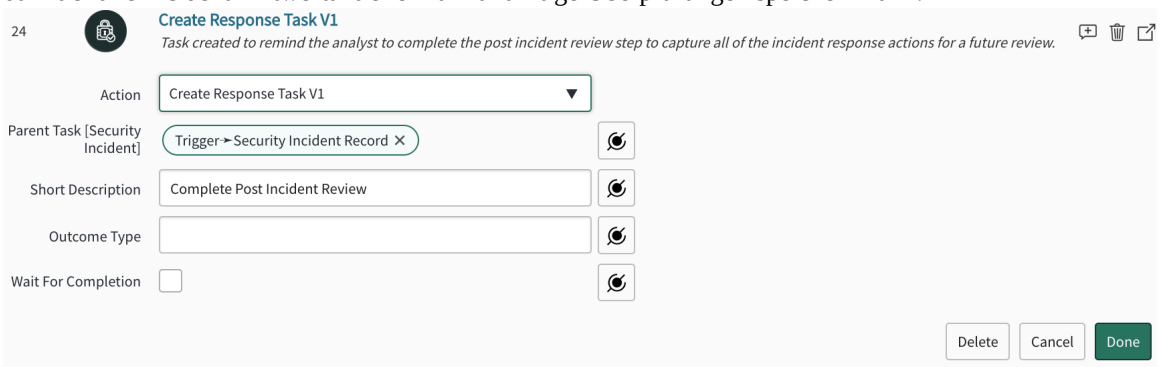



löschen.

**27.** Nachdem die Phishing-E-Mails gelöscht wurden, aktualisieren Sie in Schritt 23 den Security Incident-Datensatz, um anzugeben, dass der Incident-Status überprüft werden muss.




**28.** Im letzten Schritt erstellt der Flow eine automatisierte Antwortaufgabe.
Diese Aufgabe wird verwendet, um eine Erinnerung an den Sicherheitsanalysten zu senden, damit er alle Incident-Antwortaktionen für zukünftige Überprüfungen speichern kann.



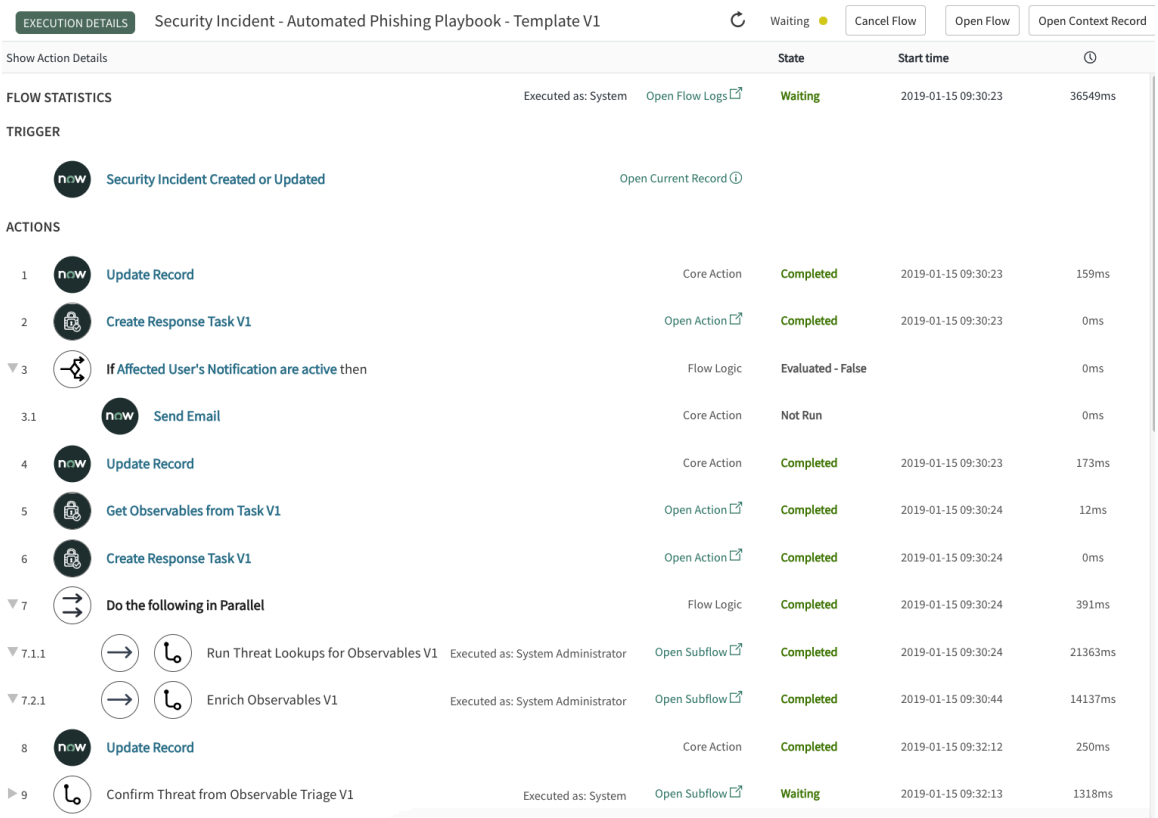

## Nächste Maßnahme

Sie können auf **Testen** klicken, um die Aktionen im Flow zu simulieren, bevor Sie ihn veröffentlichen. Klicken Sie nach dem Testen des Flow auf **Aktivieren**, um den Flow zu aktivieren und auszuführen.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



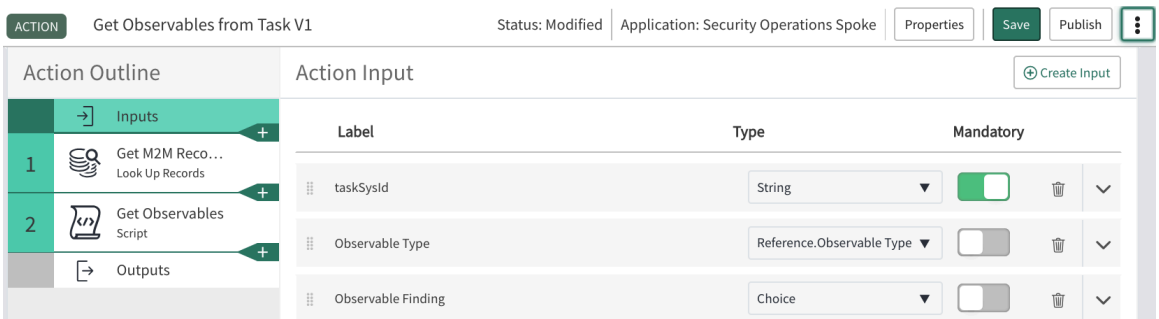

### Zeigen Sie den Flow-Aktionsdesigner des automatisierten Phishing-Antwort-Playbook-Flows an

Sie können Detailinformationen zum Aktionsdesigner anzeigen, um detaillierte Informationen zu den Aktionen anzuzeigen, die für einen bestimmten Schritt im automatisierten Phishing-Antwort-Playbook-Flow ausgeführt werden.

Auf dieser Seite wird die Seite „Aktionsdesigner“ für den Schritt „Erkennbare Elemente aus Aufgabe abrufen“ beschrieben. Klicken Sie im Bereich „Aktionsgliederung“ auf eine Aufgabe, um die Details anzuzeigen.

## Aktionseingabe

Dieser Abschnitt zeigt Details dazu, wie die Aktion erstellt wurde, einschließlich der Incident-ID, des Typs des erkennbaren Elements (Hash oder IP) und der Suche nach erkennbaren Elementen (nur böswillige E-Mails).

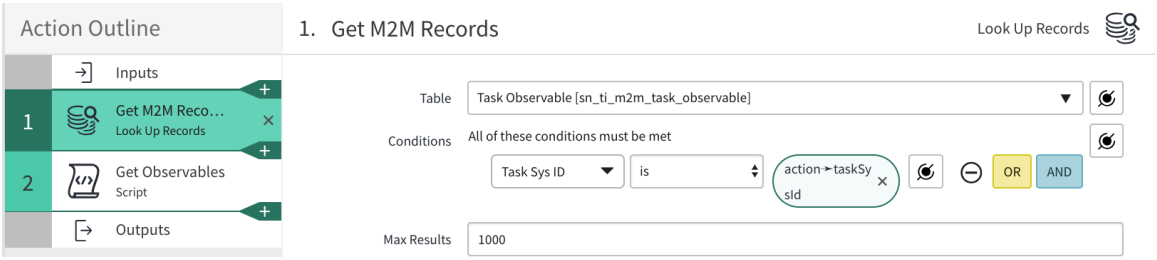



## M2M-Datensätze abrufen

In diesem Abschnitt werden die Bedingungen angezeigt, die für die Suche nach erkennbaren Elementen in einer angegebenen Tabelle definiert wurden.

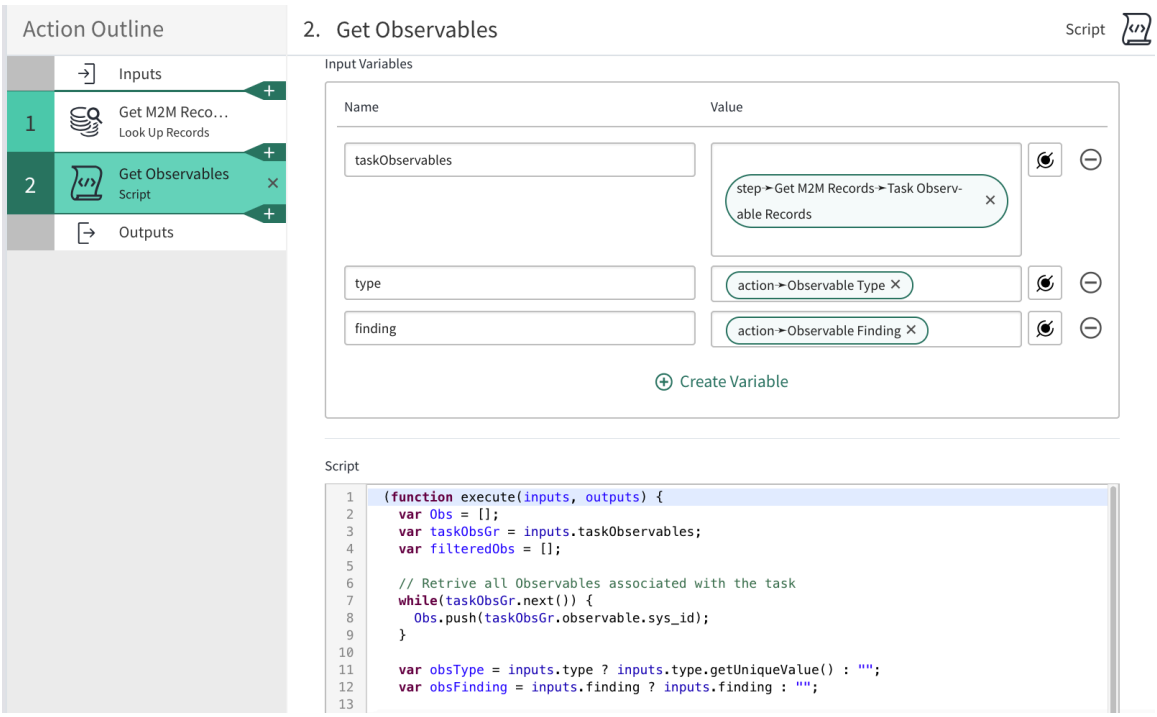


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Erkennbare Elemente abrufen

Dieser Abschnitt zeigt das Skript, das zum Abrufen von erkennbaren Elementen basierend auf den angegebenen Filterbedingungen verwendet wird. Schließlich werden die erkennbaren Elemente, die diese Kriterien erfüllen, und die Anzahl angezeigt.




**Hinweis:**
Alle in diesem Flow definierten Aktionen sind wiederverwendbar und können entsprechend Ihren Anforderungen geändert werden.

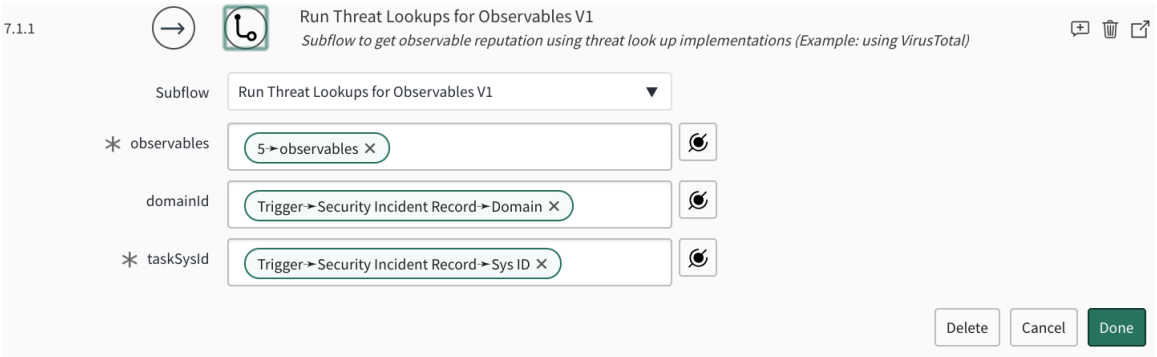
### Zeigen Sie den Subflow-Designer des automatisierten Phishing-Antwort-Playbooks an

Sie können Detailinformationen zum Subflow-Designer anzeigen, um detaillierte Informationen zum Subflow anzuzeigen, der als Teil des Playbook-Flows für die automatisierte Phishing-Antwort ausgeführt wird.

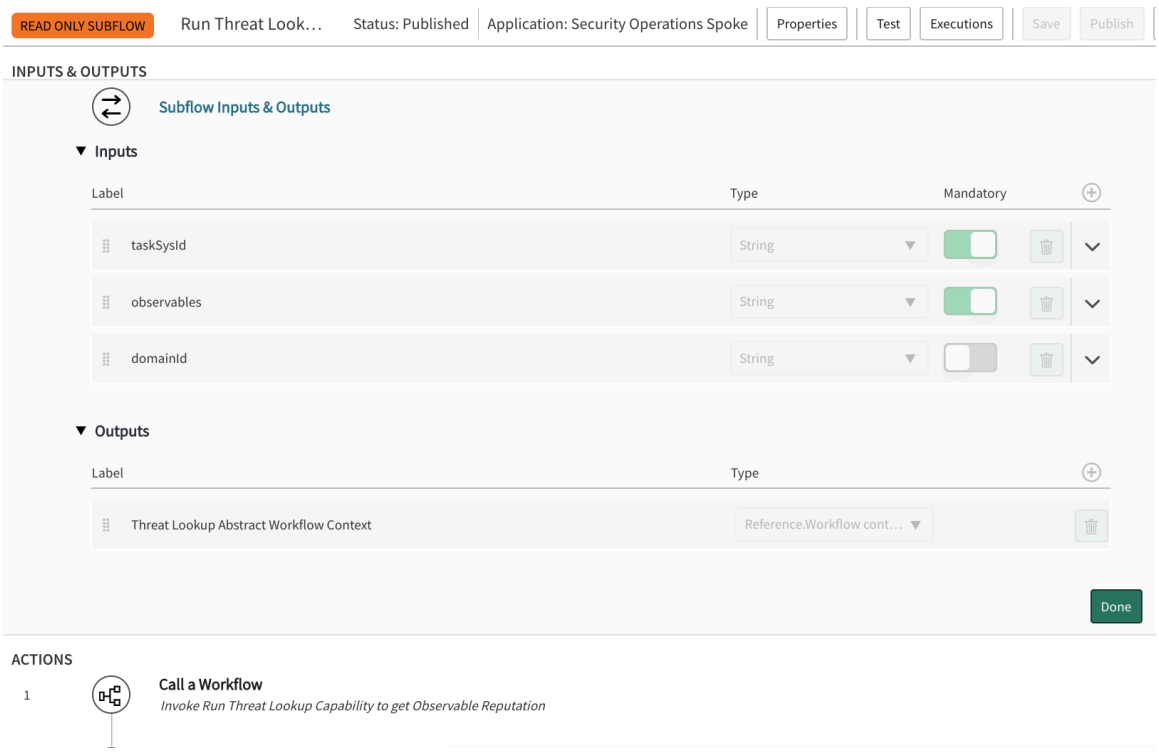
Sie können den Subflow-Designer starten, um zusätzliche Details eines Subflows anzuzeigen. Die Seite „Subflow Designer“ für den Subflow „Bedrohungssuchen für erkennbare Elemente ausführen“ wird hier angezeigt. Klicken Sie in der Abbildung unten auf das Symbol, um den Subflow-Designer anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Auf der Seite „Subflow Designer“ sehen Sie die Eingaben und Ausgaben für diesen Subflow und die zugrunde liegenden Workflow-Aktionen, die ausgeführt werden.




**Hinweis:**
Dieser Subflow ist schreibgeschützt und kann nicht bearbeitet werden. Sie können dem Schritt Subflows hinzufügen oder löschen, aber Sie können den Subflow nicht ändern.

### Playbook für automatisierte Malware

Das automatisierte Malware-Playbook bietet eine Reihe automatisierter Schritte, mit denen Sie Malware-Warnungen schnell und effizient lösen können.

Verwenden Sie den Malware-Playbook-Flow, um die Schritte zur Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk zu automatisieren. Die Flow-Vorlage enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die zur besseren Lesbarkeit mit Anmerkungen versehen sind.

Diese Vorlagen enthalten eine Reihe von wiederverwendbaren Aktionen, die als Reaktion auf Phishing-Angriffe entwickelt wurden. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows, die zur besseren Lesbarkeit mit Anmerkungen versehen sind. Um auf diese Flows zuzugreifen, müssen Sie dieSecurity Operations-Spoke und die Security Operations Palo Alto Networks - WildFire-App aus dem ServiceNow Storeinstallieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie müssen diese Vorlagen aktivieren, bevor Sie sie verwenden können.

Die folgenden Flows und Subflows sind enthalten:

- Security Incident – Automated Malware Playbook Template: Diese Vorlage wurde entwickelt, um die Reaktionen auf Malware-Warnungen zu automatisieren, und enthält eine Reihe von Aktionen, einschließlich eines Auslösers.
- Security Incident – Malware – Manuelle Vorlage: Diese Vorlage ist der vorhandene manuelle Malware-Antwort-Workflow, der aktiviert wird, wenn die Kategorie auf Böswillige Codeaktivität festgelegt wird.

**Subflows**

- Bedrohung durch erkennbares Element bestätigen: Überprüft, ob das erkennbare Element böswillig ist und behoben werden muss.
- Incident-Schweregrad festlegen: Legt einen Schweregradstatus für den Incident fest.
- Ransomware-Playbook: Ermittelt, ob es sich um einen Ransomware-Angriff handelt.

Diese Subflows stellen eine Reihe von wiederverwendbaren Vorgängen dar, die in mehreren Playbooks verwendet werden können. Sie können diese Subflows verwenden, um benutzerdefinierte Vorlagen (Flows) gemäß Ihren Anforderungen zu definieren.

Um benutzerdefinierte Vorlagen (Flows) zu erstellen, befolgen Sie die Anweisungen unter Flows .

### Führen Sie den automatisierten Malware-Playbook-Flow aus

Verwenden Sie diesen Flow, um Aufgaben im Playbook zu automatisieren, um Malware-Angriffe auf Ihre Organisation zu analysieren und zu beheben.

**Vorbereitungen**

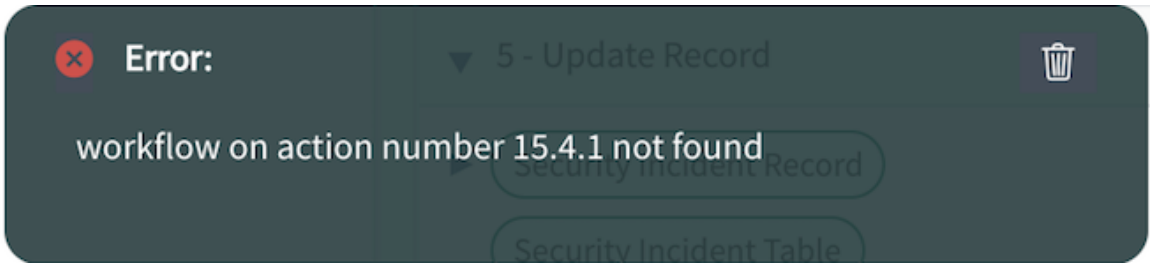
- Erforderliche Rolle: sn_si.admin, flow_designer und action_designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Palo Alto Networks WildFire for Security Operations
  - Sichtungssuche (Splunk)
  - Anforderungen blockieren
  - Bedrohungssuche
  - Erkennbare Elemente ergänzen

  Vergewissern Sie sich, dass diese Integrationen ordnungsgemäß funktionieren, bevor Sie Security Incident – Automated Malware Playbook Template aktivieren.

- Security Operations Palo Alto Networks Wildfire-App: Um auf den automatisierten Malware-Playbook-Flow zuzugreifen, müssen Sie die Spoke von Security Operations und die App Security Operations Palo Alto Networks - WildFire aus dem ServiceNow Storeinstallieren. Wenn die Wildfire-App „Security Operations Palo Alto Networks“ nicht installiert ist, wird der Fehler „Workflow für Aktionsnummer 15.4.1 nicht gefunden“ angezeigt, wie unten gezeigt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn Sie diese App nicht installieren möchten, löschen Sie die Schritte **15.2, 15.3 und 15.4** aus dem automatisierten Malware-Playbook-Flow.

- Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:
  - Der Security Incident wurde einem Sicherheitsanalysten zugewiesen, der zur entsprechenden Genehmigungsgruppe gehört.
  - Der Sicherheitsanalyst, der den Incident bearbeitet, muss über eine gültige E-Mail-Adresse verfügen.
  - Die erforderlichen Konfigurationselemente und erkennbaren Elemente wurden dem Security Incident hinzugefügt.
- Ändern **Sie für Schritt 21 (Genehmigung anfordern)**die Gruppe von **Security Incident-Zuweisung** in Ihre bevorzugte Gruppe.
- Schritt 21 des Flows ist ein obligatorischer Aufgabengenehmigungsschritt, bei dem eine Genehmigungsanforderung an den Administrator gesendet wird. Um die Anforderung zu genehmigen, muss der Administrator zur Seite „Aufgabengenehmigungen“ navigieren und das Feld Status auf **Genehmigt**festlegen. Wenn die Aufgabe nicht genehmigt wird, kann der Flow Designer nicht fortfahren, und der Prozess wird beendet.

### Warum und wann dieser Vorgang ausgeführt wird

Wenn im Netzwerk eine Aktivität mit schädlichem Code erkannt wird, wird ein Security Incident erstellt und der automatisierte Malware-Playbook-Flow gestartet. Sie können die im automatisierten Malware-Playbook-Flow definierten Aufgaben verwenden, um die Bedrohung zu selektieren, zu analysieren, einzudämmen und zu beseitigen.

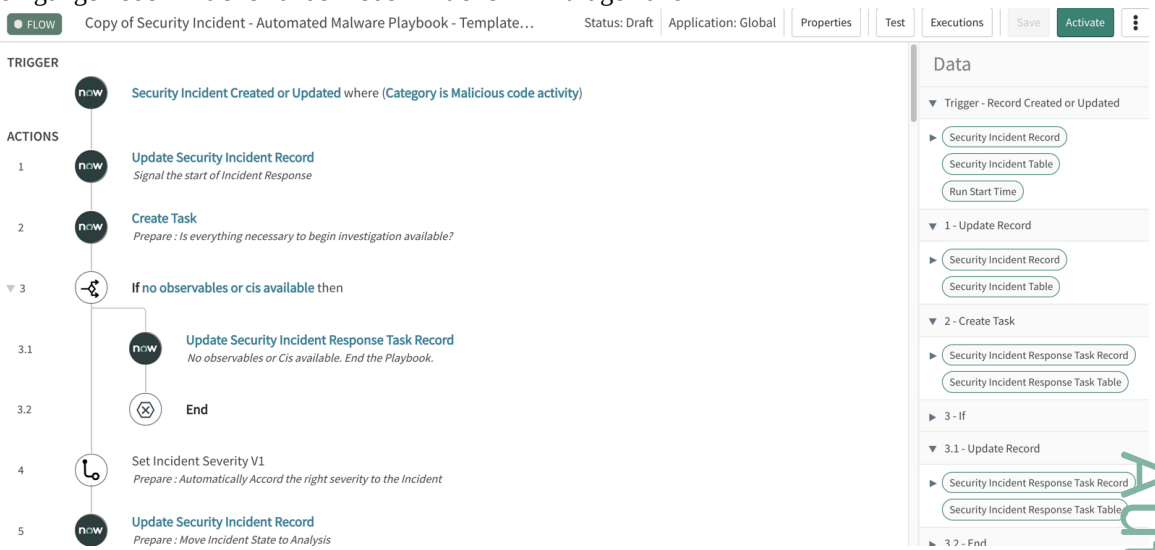
### Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** , um die mit der Security Operations-Spoke verfügbaren Flows anzuzeigen.
2. Klicken Sie auf den Link **Security Incident – Automatisierte Malware-Playbook-Vorlage VI**.
3. Klicken Sie auf der Seite „Flow“ auf das Symbol „ “ Symbol „Mehr“ , erstellen Sie eine Kopie des Flows, und öffnen Sie sie zur Verwendung.



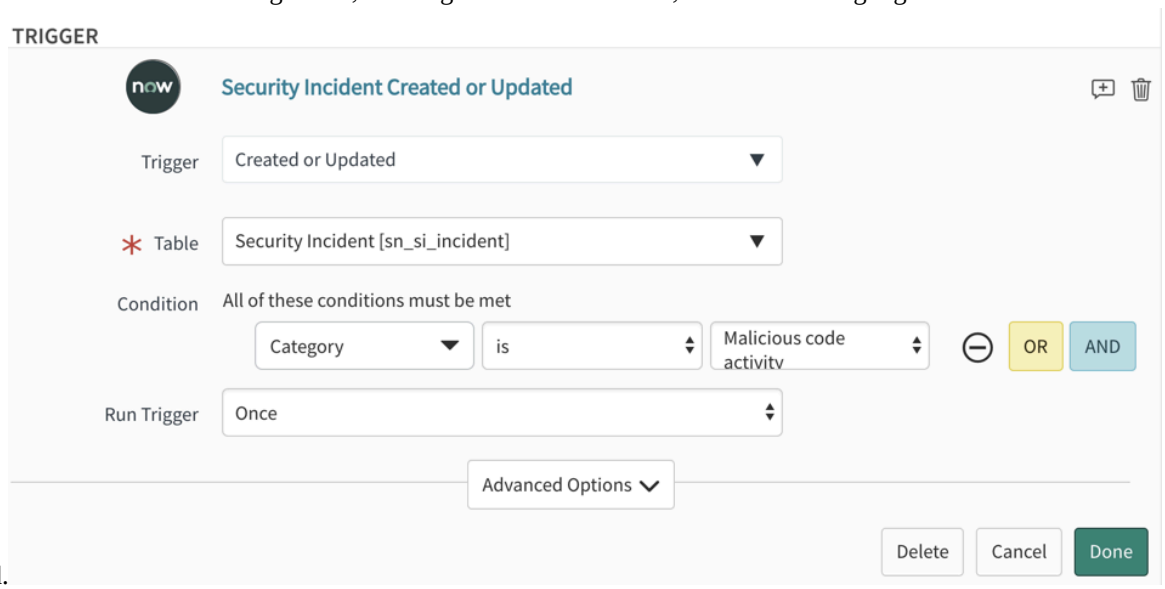
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslösebedingungen oder Aktionen ändern oder Aktionen hinzufügen und entfernen.




Dies zeigt den Auslöser und die Schritte, die mit dem Flow ausgeführt werden. Im rechten Bereich wird der Datenfluss angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

4. Klicken Sie auf das **Auslösersymbol**.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind.

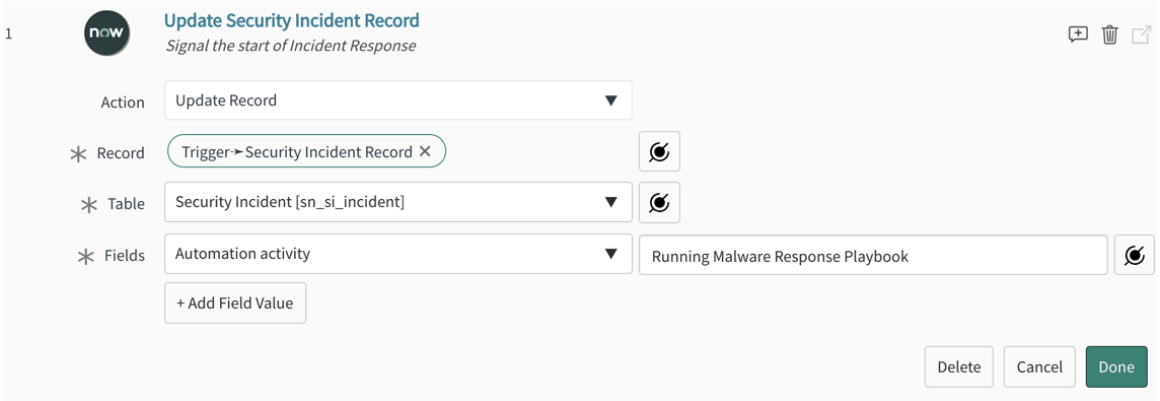



Wenn die im Flow definierte Bedingung (Aktivität „Kategorie ist schädlicher Code“) im Incident-Datensatz erfüllt ist, werden die Aufgaben im automatisierten Phishing-Flow nacheinander ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Der erste Schritt im Flow ist **„Security Incident-Datensatz aktualisieren“**.



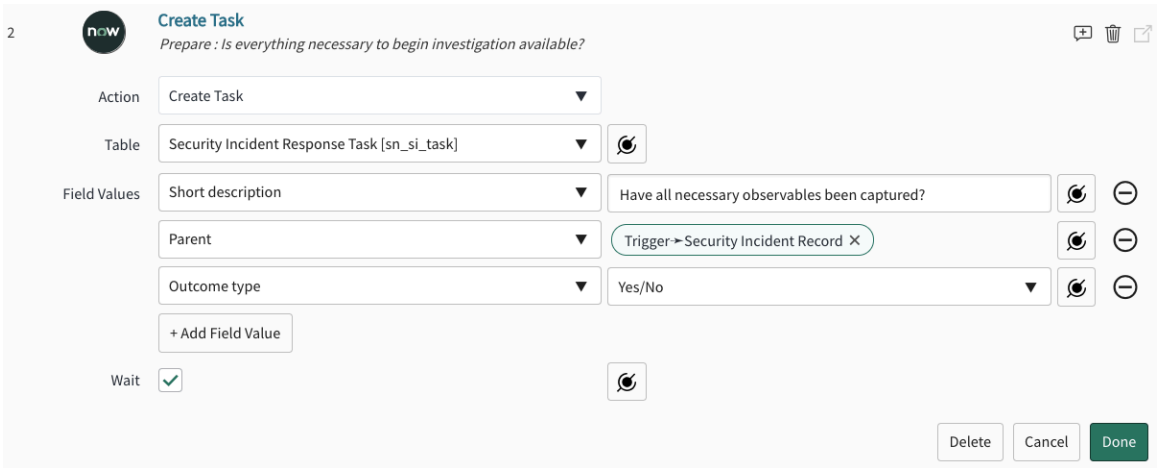
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Klicken Sie auf den Link und dann auf das Anmerkungssymbol , um dem Sicherheitsanalysten eine Notiz hinzuzufügen, die angibt, dass böswilliger Code aktiv war und die Ausführung des automatisierten Playbook-Flows für die Reaktion auf Malware gestartet wurde.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf den Link **Aufgabe erstellen**.

   In diesem Schritt wird eine automatisierte Antwortaufgabe erstellt, um zu überprüfen, ob alle erforderlichen erkennbaren Elemente erfasst wurden und die Untersuchung beginnen kann.

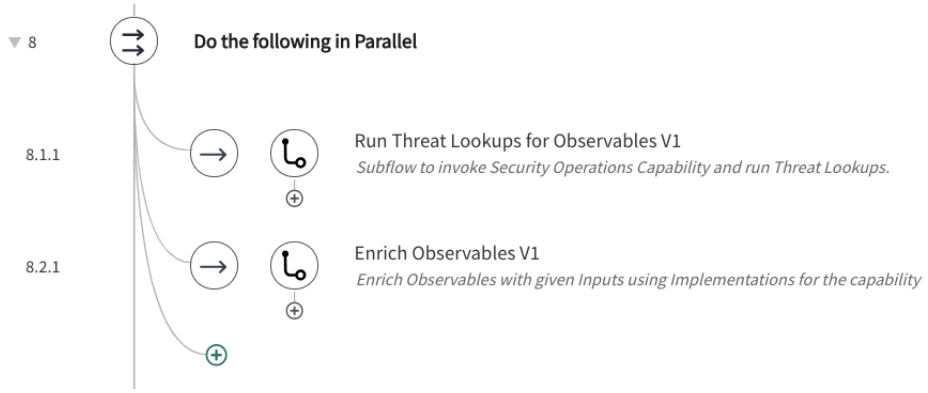



7. Wenn der Ergebnistyp **Nein**ist, bedeutet dies, dass keine erkennbaren Elemente und CIs zum Initiieren der Untersuchung verfügbar sind.
   Aktualisieren Sie den Security Incident-Datensatz, um anzugeben, dass das Playbook nicht fortgesetzt werden kann.
8. Wenn der Ergebnistyp **Ja**ist, weist der Subflow „Incident-Schweregrad festlegen“ dem Security Incident automatisch den richtigen Schweregrad zu.
9. Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert.
10. Im nächsten Schritt werden alle am Incident oder einer ausgewählten Kategorie beteiligten erkennbaren Elemente erfasst, um in den nachfolgenden Playbook-Schritten zusätzliche automatisierte Aktionen auszuführen.
11. Im nächsten Schritt wird eine automatisierte Antwortaufgabe erstellt.
    Diese Aufgabe erfasst den Beginn des Prozesses zum Abrufen der Reputation aller erkennbaren Elemente und zur Ergänzung mit konfigurierten Integrationen.
12. In Schritt 8 werden zwei Subflows aufgerufen:

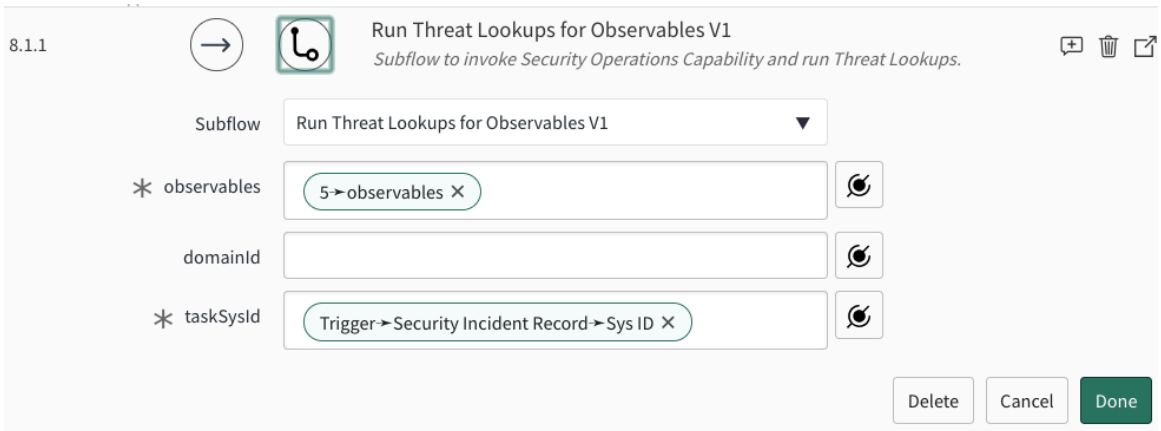


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuche für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Implementierungen der Bedrohungssuche abzurufen.
- Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung von erkennbaren Elementen mit konfigurierten Implementierungen durchzuführen.




Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge Symbol für zeigt an, dass beide Aufgaben parallel ausgeführt werden, und das Subflow-Symbol zeigt an, dass die ausgeführte Aufgabe ein Subflow ist, wie unten dargestellt:




Beachten Sie die Zahl 5 im Feld „Erkennbare Elemente“. Dies gibt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf.

13. Im nächsten Schritt wird die Aktion „Datensätze nachschlagen ausführen“ ausgeführt.
Diese Aktion wird verwendet, um nach Workflow-Kontextdatensätzen zu suchen, in denen die übergeordneten Workflows einer der folgenden sein können.
    - Bedrohungssuche – abstrakter Workflow-Kontext
    - Anreicherung erkennbarer Elemente – abstrakter Workflow-Kontext
14. Im nächsten Schritt werden die Reputations- und Ergänzungsergebnisse für alle 8 Datensätze überprüft.
15. Überprüfen Sie die nächsten Schritte weiter:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Security Incident-Datensatz aktualisieren: Aktualisiert den Security Incident-Datensatz, um anzuzeigen, dass die Aktivitäten zur Reputationssuche und -anreicherung abgeschlossen wurden.

b. Erkennbare Elemente aus Aufgabe abrufen: Ruft alle mit dem Security Incident verknüpften schädlichen erkennbaren Elemente ab.

c. Aufgabe erstellen: Überprüft und bestätigt, ob die automatisierten Selektierungsläufe erfolgreich waren.

16. Wenn erkennbare Elemente vorhanden sind, die als schädlich gekennzeichnet wurden:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass eine Bedrohung erkannt wurde.

b. Eingabeabfrage aus erkennbaren Elementen erstellen: Wenn mehr als zehn erkennbare Elemente als schädlich gekennzeichnet wurden, wird der Subflow „Sichtungssuche für erkennbare Elemente“ (unter Splunk oder Carbon Black) ausgeführt.

17. Wenn die erkennbaren Elemente nicht als schädlich gekennzeichnet sind, wird der Flow mit den folgenden Schritten fortgesetzt:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass keine Bedrohung erkannt wurde

b. Erkennbare Elemente aus Aufgabe abrufen: Identifiziert alle SHA256-Hash-IDs aus dem Incident.

c. Datensätze für erkennbare Elemente suchen: Sucht nach Datensätzen, die diese Kriterien erfüllen.

18. Überprüfen Sie die nächsten Schritte weiter:

a. Für jedes schädliche erkennbare Element wird der Workflow **„Security Operations Palo Alto Networks – Wildfire-Datenanreicherung** abrufen“ ausgeführt.

b. Überprüft die Untersuchungsergebnisse, um festzustellen, ob sie zufriedenstellend sind.
Eine Antwortaufgabe wird erstellt, um zu überprüfen, ob es sich bei der vermuteten Malware um einen Ransomware-Angriff handelt. Wenn ja, wird der Subflow „Ransomware-Playbook“ ausgeführt.

c. Im nächsten Schritt wird eine E-Mail mit einer Zusammenfassung der Analyse und einer Genehmigungsanforderung gesendet, um Containment-Verfahren zu initiieren.

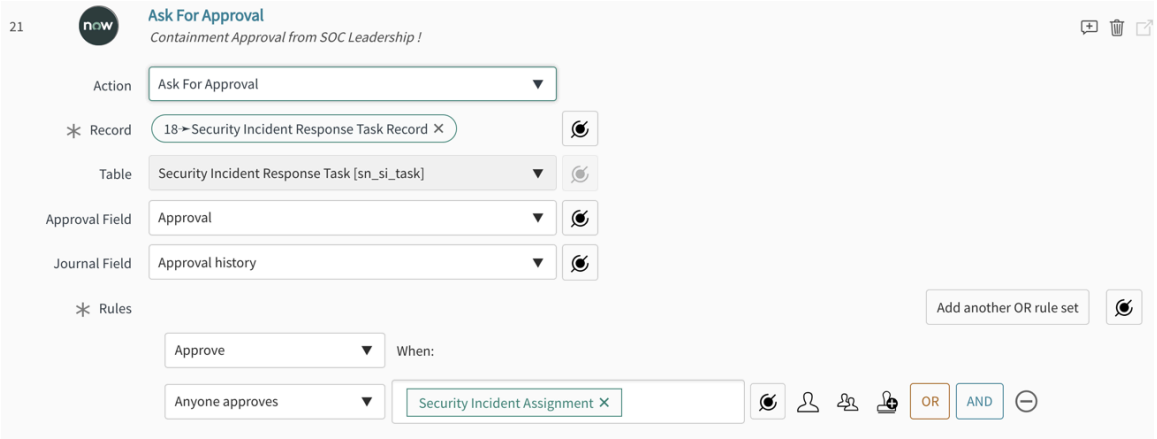
d. Eine Aufgabe wird erstellt, um Details der angeforderten Genehmigung zu erfassen.

e. Der nächste Schritt besteht darin, den Security Incident-Datensatz zu aktualisieren.
Veröffentlichen Sie eine Arbeitsnotiz, die den Sicherheitsanalysten darüber informiert, dass die Genehmigungsanforderung erfolgt ist.

f. Fordert die Genehmigung zur Eindämmung der Malware-Angriffe von Ihrem SOC-Manager an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn eine Genehmigungsanforderung vom Flow generiert wird, wird die Arbeitsnotiz mit der folgenden Meldung aktualisiert:

Für wurde eine Genehmigungsanforderung gestellt<task id> wird mit Containment fortgesetzt. Führen Sie die folgenden Schritte manuell aus, um diese Aufgabe als SOC-Manager zu genehmigen:

- Navigieren Sie zur Seite „Aufgabengenehmigungen“.
- Die Liste der Genehmigungen wird angezeigt. Klicken Sie auf<task id> , der genehmigt werden soll.
- Ändern Sie den Status in **„Genehmigen** und speichern“.<task id> .

**g.** Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert, um den Genehmigungsstatus nachzuverfolgen.

**h.** Als Nächstes wird eine Aufgabe erstellt, um Containment-Verfahren zu initiieren.

**i.** Der Subflow „Blockierungsanforderungen für schädliche erkennbare Elemente ausführen“ wird ausgeführt, und ein Incident-Datensatz wird mit der Anforderung erstellt, das infizierte Gerät und seine Assets neu zu erstellen.

**j.** Als Nächstes wird eine Aufgabe zum Ausführen der Sichtungssuche erstellt, um zu bestätigen, ob die Umgebung sicher ist.
Die Sichtungssuche wird wiederholt, bis keine Sichtungen gefunden werden.

**k.** Als Nächstes wird eine Aufgabe erstellt, um anzugeben, dass der Security Incident-Datensatz zur Überprüfung bereit ist.

**l.** Abschließend wird der Datensatz aktualisiert und in die Überprüfungsphase verschoben.

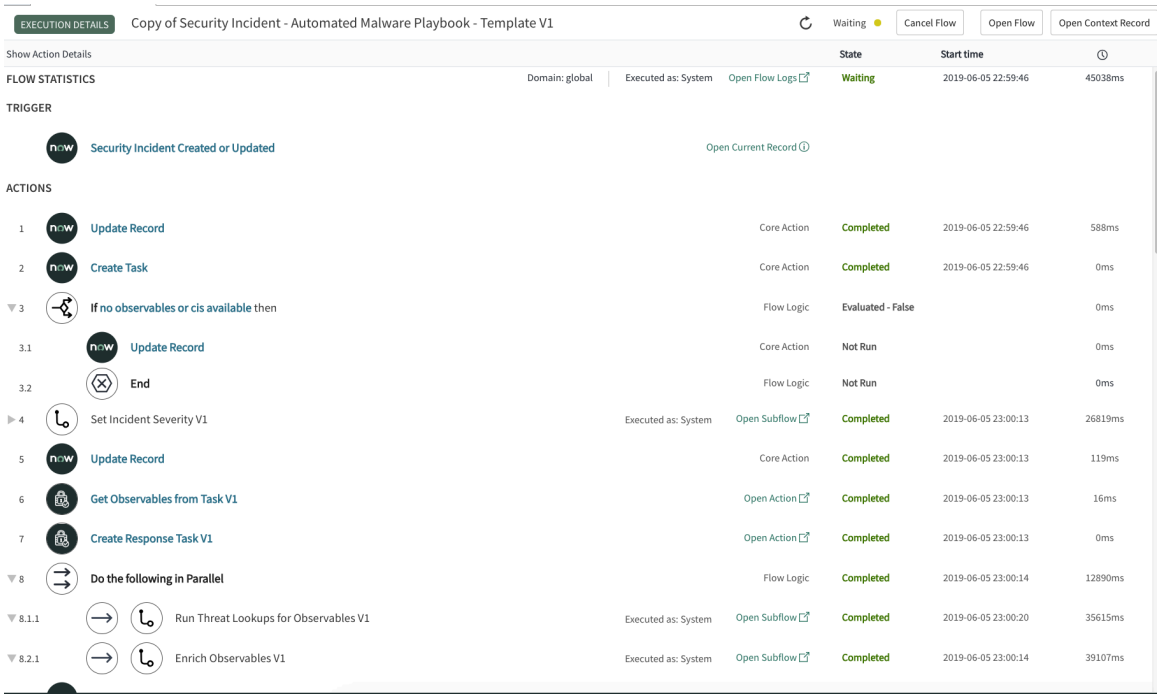
## Nächste Maßnahme

Sie können auf **Test** klicken, um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flow auf **Aktivieren**, um den Flow zu aktivieren und auszuführen.

Klicken Sie auf **Ausführungen**, um die Ausführungsdetails des Flow anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Playbook für fehlgeschlagene Anmeldung – manuell

Wenn ein Benutzer (je nach SIM-Konfiguration) bestimmte erfolglose Anmeldeversuche unternimmt, wird ein Security Incident erstellt.

Bei diesen erfolglosen Anmeldeversuchen kann es sich entweder um Falschmeldungen oder um Versuche von Angreifern handeln, sich Zugriff auf die E-Mail-Accounts der Benutzer zu verschaffen. In solchen Szenarien kann das Playbook „Manuelles Failed Login“ als Anleitung dienen und dazu beitragen, die Untersuchung von Security Incidents mit fehlgeschlagenen Anmeldungen zu optimieren.

## Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_spoke)

## Wichtige Funktionen

Das Playbook „Fehlgeschlagene Anmeldung“ umfasst die folgenden Funktionen zur Untersuchung von Security Incidents:

1. Überprüft, ob der betroffene Anwender ein aktiver/inaktiver Anwender ist
2. Filter zulässige Liste erkennbarer Elemente
3. Reichert die erkennbaren Elemente an
4. Führt eine automatisierte Bedrohungssuche durch.
5. Sendet eine automatisierte E-Mail an den Anwender, um den fehlgeschlagenen Anmeldeversuch zu bestätigen.
6. Weist Analysten Aufgaben zu, um den Benutzerzugriff zu untersuchen
7. Identifiziert schädliche erkennbare Elemente und blockiert IPs und URLs.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Setzt das Anwenderpasswort zurück.
9. Aktualisiert den Status des Security Incident
10. Weist einem Sicherheitsanalysten Aufgaben zur Überprüfung nach Incidents zu.

### Erforderliche Fähigkeiten

- Bedrohungssuche (Viren gesamt, Hybridanalyse)
- Ergänzung erkennbarer Elemente (Whhois, ReverseWhhois)
- Sichtungssuche (Splunk, QRadar)
- Blockierung erkennbarer Elemente (CheckPoint, Palo Alto)

Weitere Informationen finden Sie im ServiceNow Store .

### Erfahrung von Sicherheitsanalysten

Informationen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

### Verwenden des Playbooks „Fehlgeschlagene Anmeldung“ mit Flow Designer-Fähigkeiten

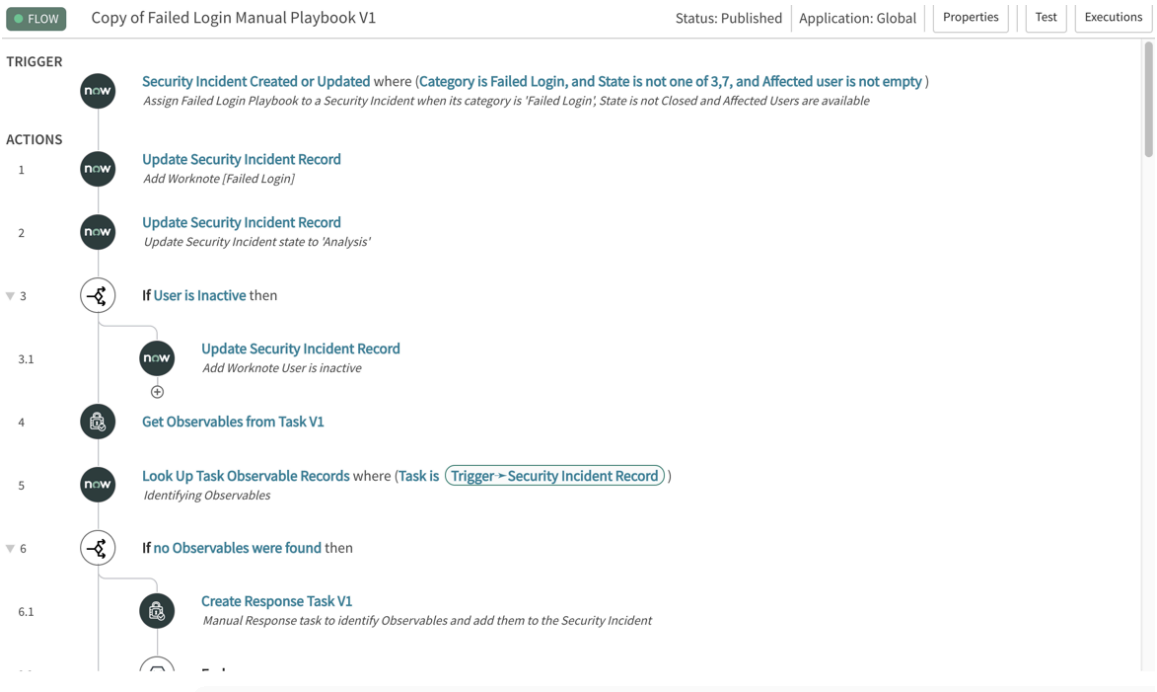
#### Erste Schritte

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Flow Designer** > **Designer** und klicken Sie auf das Playbook **Fehlgeschlagene** Anmeldung.
3. Erstellen Sie eine Kopie der folgenden Flows, um das Playbook für fehlgeschlagene Anmeldungen zu kopieren und die erforderlichen Änderungen vorzunehmen. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.
   - Manuelles Playbook V1 bei fehlgeschlagener Anmeldung
   - Fehlgeschlagene Anmeldung – Antwort des Anwenders analysieren und Antwortaufgabe aktualisieren V1
4. Nehmen Sie die erforderlichen Änderungen gemäß Ihren Anforderungen vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.
5. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das mit dem Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie Änderungen gemäß Ihren Anforderungen vorgenommen haben.

Die folgende Abbildung zeigt eine Kopie des Playbooks bei fehlgeschlagener Anmeldung. Überprüfen Sie die folgenden Schritte, um sich mit den verschiedenen Aktionen im Playbook vertraut zu machen.

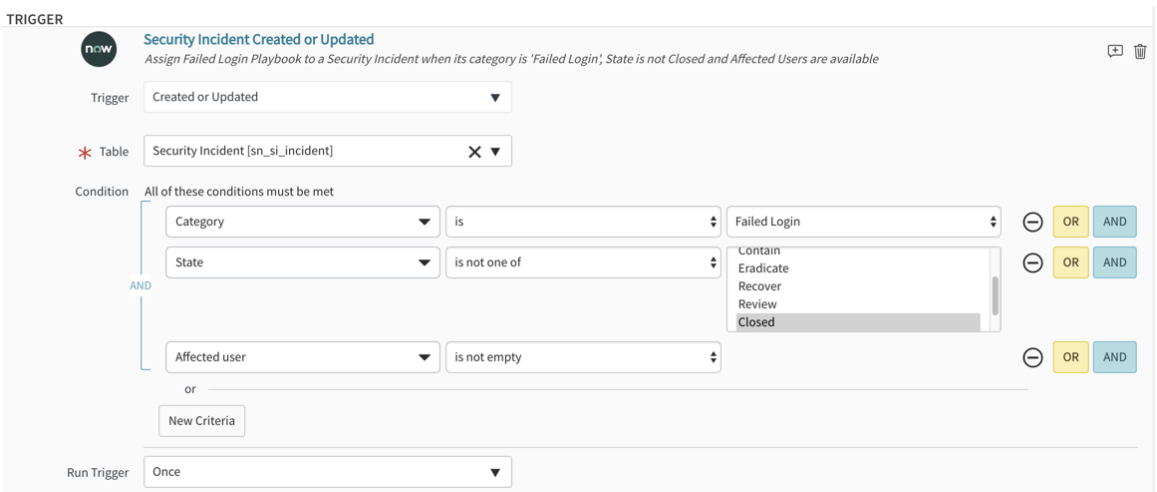


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

- Kategorie ist „Fehlgeschlagene Anmeldung“.
- Hat einen oder mehrere betroffene Benutzer
- Security Incident wurde nicht geschlossen oder abgebrochen

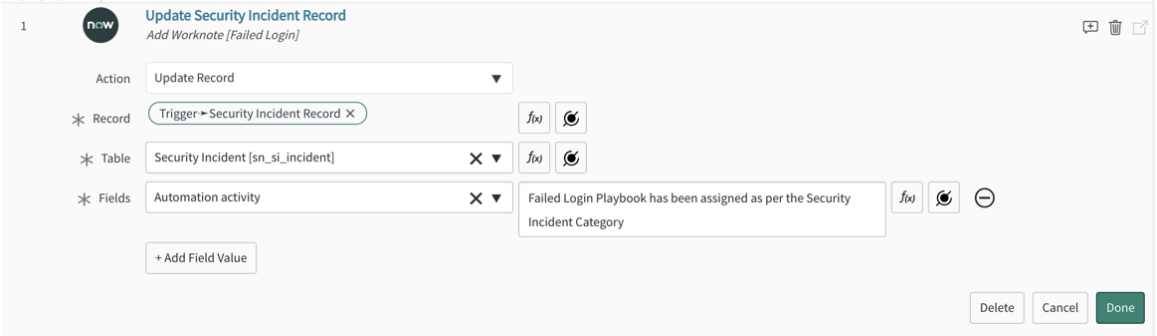



Die folgenden Schritte führen Sie durch die Aktionen, Aufgaben und Subflows, die im Playbook „Failed Login Manuell“ verfügbar sind.

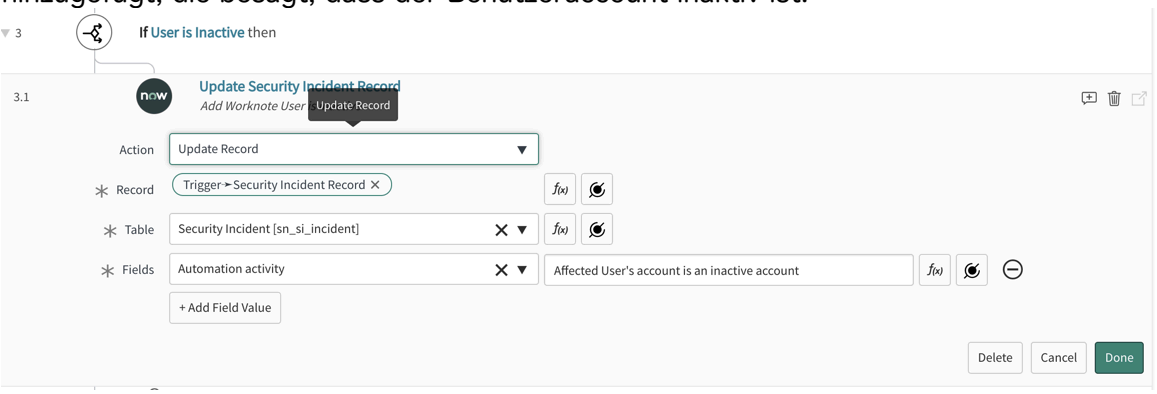


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn die Ausführung des Playbooks in Schritt 1 gestartet wird, wird das Playbook automatisch mit einer Arbeitsnotiz aktualisiert, aus der hervorgeht, dass der Security Incident mit der Kategorie „Fehlgeschlagene Anmeldung“ zugewiesen wurde.




2. In Schritt 2 wird das Playbook aktualisiert und in den Status „Analyse“ verschoben.
3. In Schritt 3 überprüft das Playbook, ob der betroffene Benutzer ein aktiver oder inaktiver Benutzer ist. Wenn der Benutzer inaktiv ist, wird dem Security Incident eine Arbeitsnotiz hinzugefügt, die besagt, dass der Benutzeraccount inaktiv ist.




**Hinweis:**

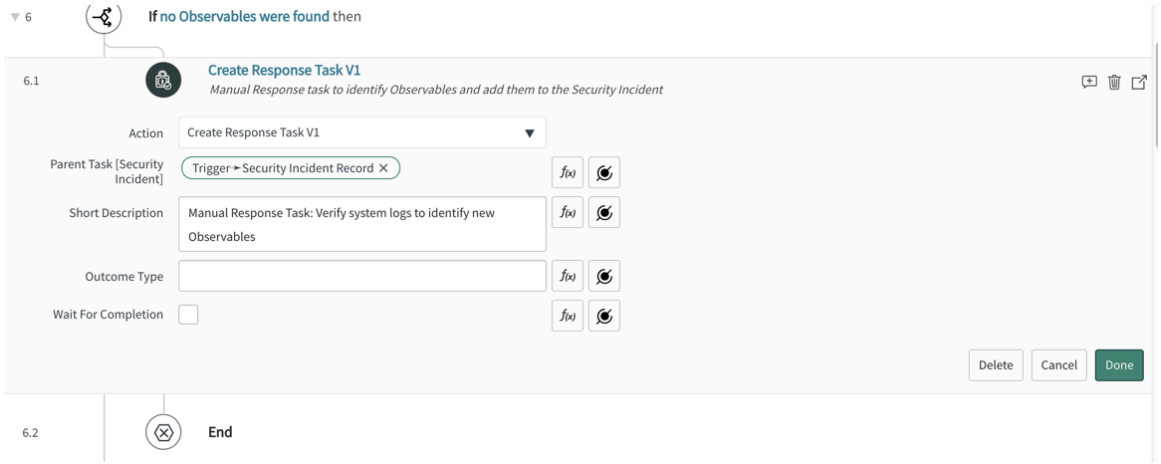
In Schritt 3 des Flows werden inaktive Benutzer in der Tabelle „ `sn_si_incident` “ überprüft, die in ServiceNowverfügbar ist. Dieser Schritt wird als Leitlinie bereitgestellt und muss für Ihre spezifische Umgebung geändert werden. Wenn Sie diese Funktionalität verwenden möchten, empfehlen wir die Einrichtung einer Active Directory-Integration in Ihrer Umgebung. Sie können bei Ihrer Active Directory-Integration nach dem Benutzerstatus suchen und abhängig von der Antwort die nächsten Schritte für Ihr Playbook entwerfen.

Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe für den Sicherheitsanalysten, der mit dem IT-Team zusammenarbeitet, um den Benutzer zu blockieren und mit den restlichen Schritten im Playbook fortzufahren.

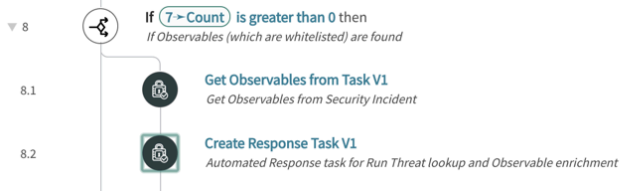
4. In Schritt 4 werden die erkennbaren Elemente für den Security Incident abgerufen.
5. In Schritt 5 werden die erkennbaren Elemente identifiziert.
6. Wenn keine erkennbaren Elemente gefunden werden, wird in Schritt 6 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.



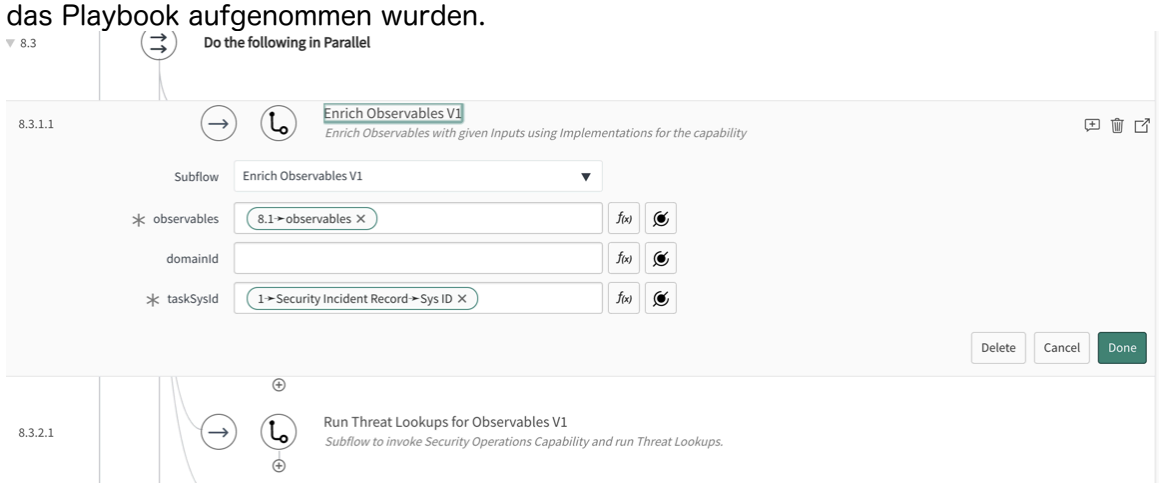
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Wenn in Schritt 7 erkennbare Elemente gefunden werden, werden die nicht zulässigen erkennbaren Elemente identifiziert.
8. Wenn mindestens eines der erkennbaren Elemente in der Liste nicht zulässig ist, werden die folgenden Schritte ausgeführt:
   a. Die Schritte 8.1 und 8.2 werden ausgeführt. Erkennbare Elemente werden abgerufen und eine automatisierte Antwortaufgabe wird initiiert.




   b. Nachdem die automatisierte Aufgabe erstellt wurde, wird Schritt 8.3 (8.3.1.1 und 8.3.2.1) ausgeführt und die Integrationen „Erkennbare Elemente anreichern“ und „Bedrohungssuche“ werden ausgeführt. Beachten Sie, dass dies Subflows sind, die in das Playbook aufgenommen wurden.




   c. In Schritt 8.4 wird der Security Incident-Datensatz nach Abschluss der Integrationen aktualisiert.
   d. In Schritt 8.5 wird eine neue Antwortaufgabe erstellt, um die nächste automatisierte Aufgabe anzugeben, die ausgeführt wird.
   e. In Schritt 8.6 wird die Integration der Sichtungssuche für die erkennbaren Elemente ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**f.** Nachdem der Subflow „Sichtungssuche“ in Schritt 8.7 abgeschlossen wurde, wird der Security Incident aktualisiert.

**g.** In Schritt 8.8 werden die erkennbaren Elemente daraufhin überprüft, ob sie schädlich sind.

**h.** Wenn die erkennbaren Elemente nicht böswillig sind und das Benutzerkonto aktiv ist, wird eine automatisierte E-Mail an den Benutzer gesendet, um die nicht erfolgreichen Anmeldeversuche zu bestätigen. Eine manuelle Antwortaufgabe wird erstellt, um die erkennbaren Elemente zu identifizieren und dem Security Incident hinzuzufügen. Das Playbook endet dann in dieser Phase.

**i.** Wenn die erkennbaren Elemente schädlich sind, werden drei Antwortaufgaben erstellt:

  **i.** Eine automatisierte E-Mail wird an den Benutzer gesendet, um die nicht erfolgreichen Anmeldeversuche zu bestätigen **(Ja oder Nein)**. Wenn der Benutzer mit Ja antwortet:

    **1.** Der Status des Security Incident wird auf **Contain**aktualisiert.

    **2.** Eine automatisierte E-Mail wird an den Benutzer gesendet, um das Passwort zurückzusetzen.

    **3.** Der Subflow „Passwort zurücksetzen“ wird initiiert und eine E-Mail wird an den Benutzer gesendet, wenn die Aufgabe abgeschlossen wurde.

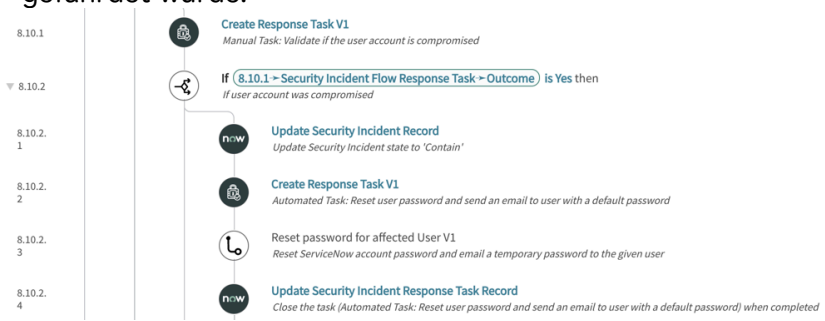
> **Hinweis:**
> Der Schritt „Passwort zurücksetzen“ wird als Leitlinie bereitgestellt. Die Schritte im Flow setzen das Passwort für den Account des Benutzers im ServiceNow-System zurück. Der Vorgang zum Zurücksetzen des Passworts kann jedoch je nach Umgebung unterschiedlich sein. Sie können bei Ihrer Active Directory-Integration überprüfen, ob das Passwort von Benutzern automatisch zurückgesetzt werden soll. Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe für den Sicherheitsanalysten, der mit dem jeweiligen IT-Team zusammenarbeitet, um das Passwort des Benutzers zurückzusetzen und nach Abschluss der jeweiligen mit den restlichen Schritten im Playbook fortzufahren Aufgabe.

  **ii.** Wenn der Benutzer mit Nein antwortet, wird eine automatisierte E-Mail an den Benutzer gesendet, um die Antwort erneut zu bestätigen. Der Sicherheitsanalyst muss die entsprechenden Maßnahmen manuell ergreifen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

iii. Wenn der Benutzer nicht auf die automatisierte E-Mail antwortet, muss der Sicherheitsanalyst den Security Incident manuell aktualisieren und eine Antwort geben. Eine manuelle Aufgabe wird erstellt, um zu überprüfen, ob das Benutzerkonto gefährdet wurde.




9. In Schritt 8.10.3 wird der Status des Security Incident aktualisiert.
10. In Schritt 8.10.4 wird eine automatisierte Aufgabe erstellt, um zu überprüfen, ob die Implementierung der Fähigkeit Blockanforderungen für schädliche IPs und URLs erstellen verfügbar ist. Wenn die Fähigkeitsimplementierung verfügbar ist, wird der Subflow Blockanforderungen erstellen ausgeführt. Wenn diese Option nicht verfügbar ist, wird der Security Incident aktualisiert und eine Arbeitsnotiz veröffentlicht, um anzugeben, dass die Fähigkeitsimplementierung nicht verfügbar ist.
11. In Schritt 9 wird der Security Incident aktualisiert, und der Status wird auf **Überprüfen**festgelegt.
12. In Schritt 10 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

### Playbook für die Automatisierung von untergeordneten Security Incidents

Doppelte Security Incidents werden als untergeordnete Security Incidents kategorisiert und per Rollup zu den übergeordneten Security Incidents zusammengefasst.

Das Playbook „Automatisierung von untergeordneten Security Incidents“ trägt dazu bei, die Zeit für die Untersuchung und das Schließen doppelter Security Incidents zu reduzieren. Dieses Playbook führt automatisch ein Rollup für bestimmte eindeutige Artefakte des untergeordneten Security Incident (erkennbare Elemente, betroffene Benutzer, CIs) zum übergeordneten Security Incident durch.

## Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_spoke)

## Wichtige Funktionen

Das Playbook „Untergeordnete Automatisierung“ deckt die folgenden Funktionen ab:

1. Verschiebt den Security Incident in die **Analysephase**.
2. Beseitigt Duplikate und fügt die betroffenen Benutzer und CIs dem übergeordneten Security Incident hinzu (führt ein Rollup durch).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügt dem übergeordneten Security Incident erkennbare Elemente aus dem untergeordneten Incident hinzu.
4. Schließt oder bricht den untergeordneten Security Incident ab, wenn der übergeordnete Security Incident geschlossen wird.

## Erforderliche Fähigkeiten

Weitere Informationen finden Sie im ServiceNow Store .

## Erfahrung von Sicherheitsanalysten

Informationen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Beheben Sie Sicherheitsbedrohungen mit dem Playbook.

## Vertieftes Verständnis des Playbooks für die Automatisierung von untergeordneten Security Incidents mit Flow Designer-Funktionen

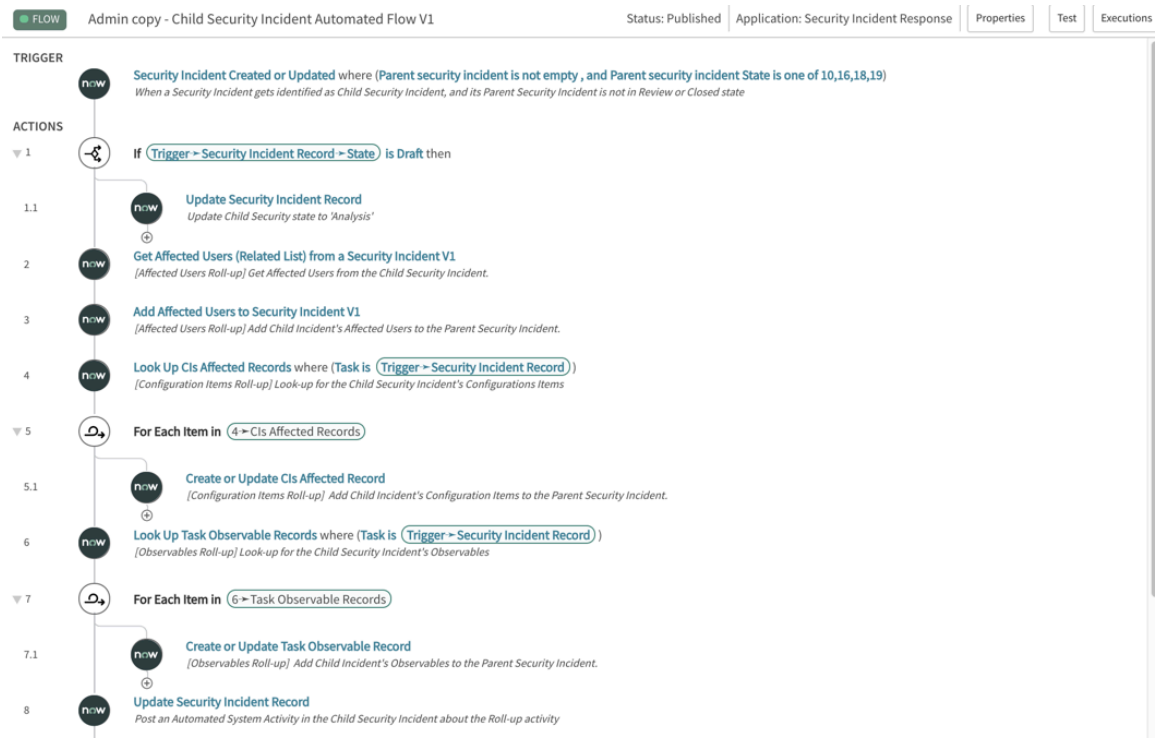
### Erste Schritte

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Flow Designer** > **Designer** und klicken Sie auf das Playbook Fehlgeschlagene Anmeldung.
3. Erstellen Sie eine Kopie des Child Security Incident Automation-Playbooks, und nehmen Sie die erforderlichen Änderungen vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.
4. Nehmen Sie die erforderlichen Änderungen gemäß Ihren Anforderungen vor. (Dies ist ein optionaler Schritt.) Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.
5. Aktivieren Sie das Playbook.
   - Aktivieren Sie den Haupt-Flow, um das mit dem Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie den kopierten Flow, nachdem Sie Änderungen gemäß Ihren Anforderungen vorgenommen haben.

Die folgende Abbildung zeigt eine Kopie des Playbooks „Automatisierung von untergeordneten Sicherheitsvorfällen“. Überprüfen Sie die folgenden Schritte, um sich mit den verschiedenen Aktionen im Playbook vertraut zu machen.

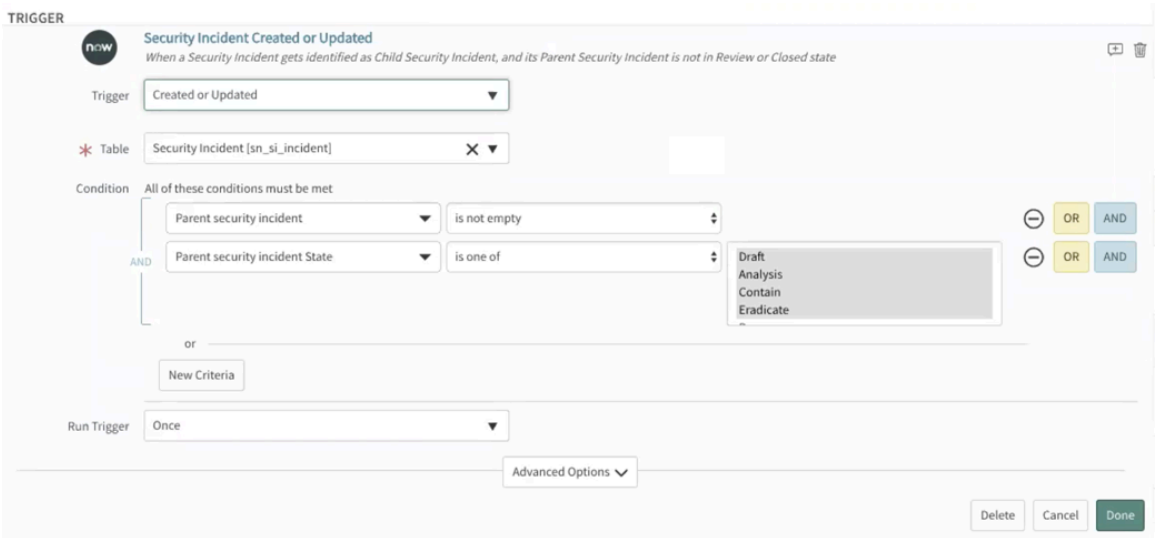


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Dieses Playbook wird ausgelöst, wenn:

- Das Feld „Übergeordneter Security Incident“ ist nicht leer.
- Der übergeordnete Security Incident befindet sich im Status „Entwurf“, „Analyse“, „Eindämmen“ oder „Beseitigen“.

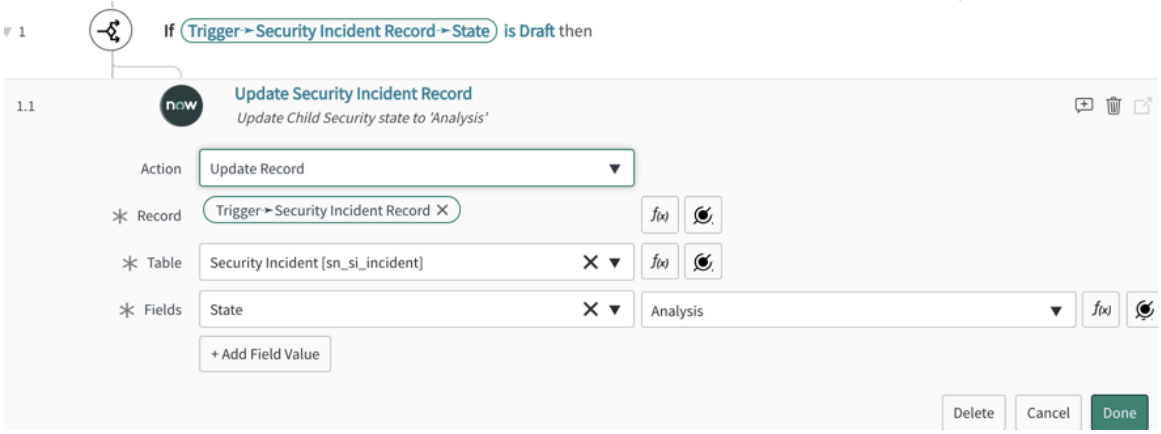



Die folgenden Schritte führen Sie durch die Aktionen und Aufgaben, die im Playbook für die Automatisierung von untergeordneten Security Incidents verfügbar sind.

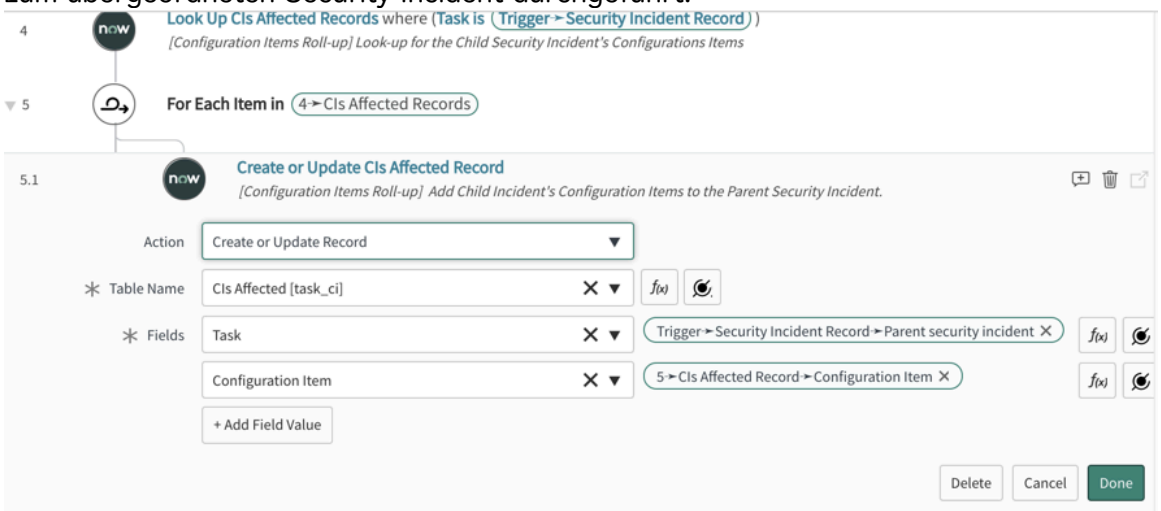


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

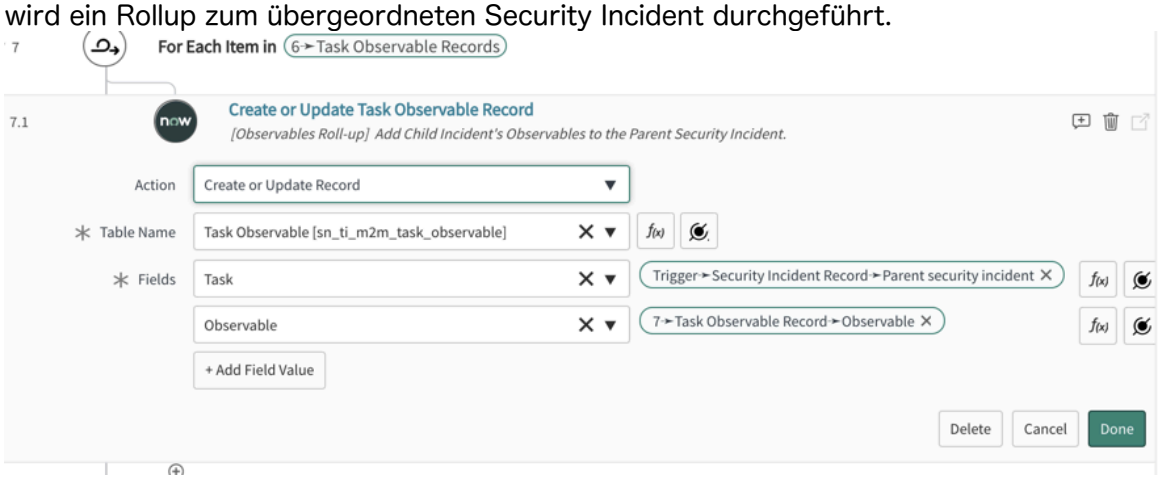
1. Wenn die Ausführung des Playbooks in Schritt 1 beginnt und sich der Security Incident im Status „Entwurf“ befindet, wird er aktualisiert und in den Status „Analyse“ versetzt.




2. In den Schritten 2 und 3 werden die betroffenen Benutzer für den Security Incident abgerufen und ein Rollup zum übergeordneten Security Incident durchgeführt. Alle doppelten Benutzer werden eliminiert.
3. In den Schritten 4 und 5 werden Konfigurationselemente abgerufen, die dem untergeordneten Security Incident zugeordnet sind, und für eindeutige CIs wird ein Rollup zum übergeordneten Security Incident durchgeführt.




4. In den Schritten 6 und 7 werden die dem untergeordneten Security Incident zugeordneten erkennbaren Elemente abgerufen und für eindeutige erkennbare Elemente wird ein Rollup zum übergeordneten Security Incident durchgeführt.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In den Schritten 8 und 9 werden automatisierte Arbeitsnotizen in den übergeordneten und nachfolgenden Security Incidents veröffentlicht, die angeben, dass für die betroffenen Benutzer, Konfigurationselemente und erkennbaren Elemente ein Rollup vom untergeordneten zum übergeordneten Security Incident durchgeführt wurde.

### Playbook für Office 365 – Schädliche Datei erkannt

Dieses Playbook bietet systematische Korrekturschritte für die Untersuchung schädlicher Dateien, die in Office 365 erkannt wurden

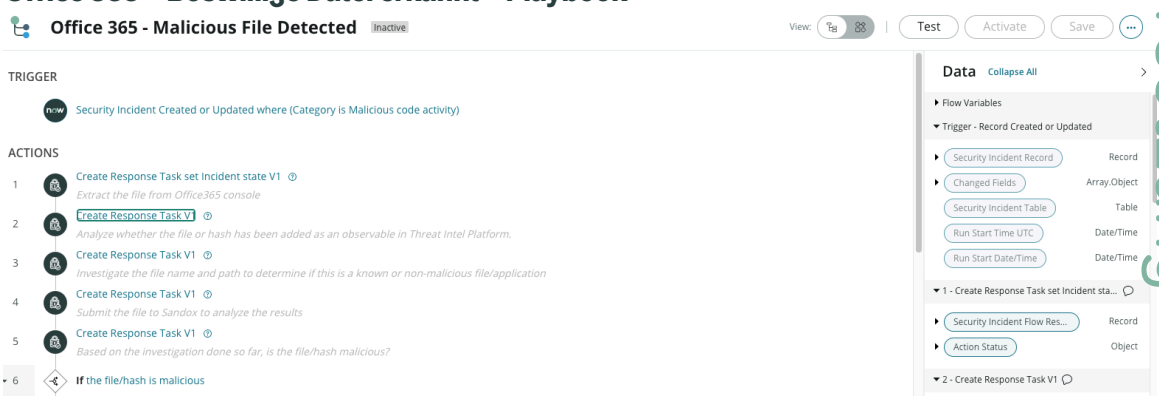
Wenn in Office 365 schädliche Dateien erkannt werden, können Sie das Playbook „365 – Malicious File Detected“ im Flow Designer als Anleitung und zur Optimierung der Untersuchung dieser schädlichen Dateien verwenden.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Playbook „Office 365 – Malicious File Detected“.

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Office 365 – Böswillige Datei erkannt** “ aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows „Office 365 – Böswillige Datei erkannt“ erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

**Office 365 – Böswillige Datei erkannt – Playbook**

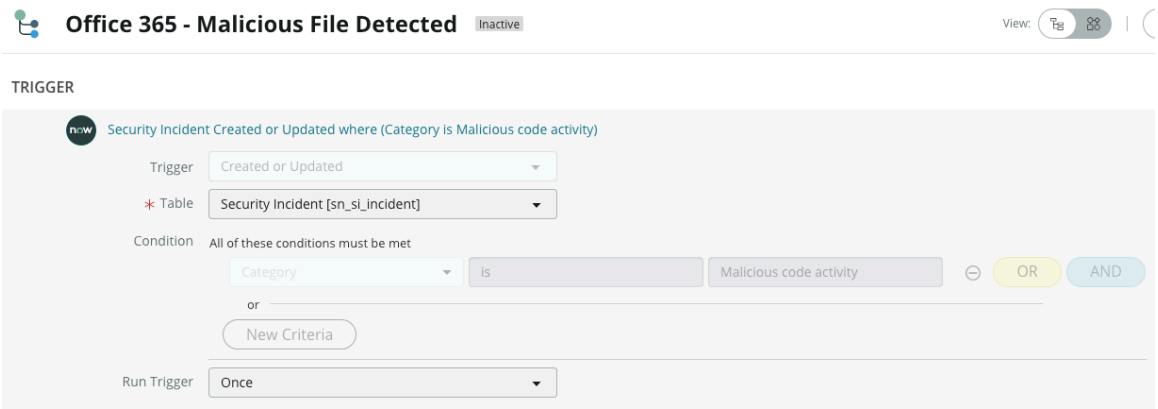



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslösebedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die Aktivität „ **Kategorie“ Böswilliger Code**lautet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Richten Sie die erkannte Office-Datei mit schädlicher Datei ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

Navigieren zu **Alle** > > .

### Verwenden Sie das Office 365-Playbook „Böswillige Datei erkannt“.

Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Playbook Office 365 Böswillige Datei erkannt verfügbar sind.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

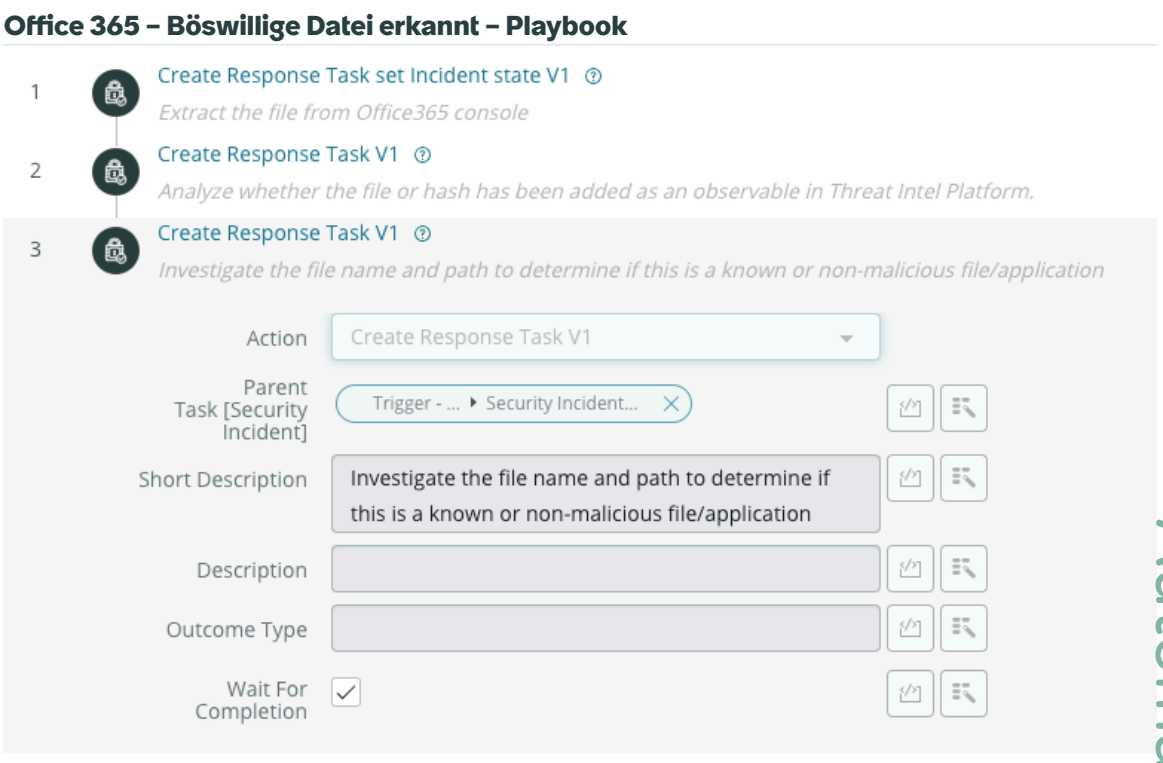
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 die schädliche Datei aus der Office 365-Konsole extrahieren.
2. In Schritt 2 müssen Sie analysieren, ob die Datei oder der Hash als erkennbares Element in der Threat Intel Platform hinzugefügt wurde.
3. In Schritt 3 müssen Sie den Dateinamen und den Pfad untersuchen, um festzustellen, ob es sich um eine bekannte oder nicht schädliche Datei/Anwendung handelt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. In Schritt 4 müssen Sie die Datei zur Analyse der Ergebnisse an Sandbox senden.
5. In Schritt 5 müssen Sie basierend auf den bisher durchgeführten Untersuchungen überprüfen, ob die Datei oder der Hash böswillig ist oder nicht.
   Wenn die Datei oder der Hash nicht böswillig ist, wird in Schritt 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
6. Wenn in Schritt 6 die Datei oder der Hash böswillig ist, werden die Schritte 7 und 8 ausgeführt.
7. In Schritt 7 müssen Sie den Endbenutzer um eine gültige geschäftliche Begründung bitten, warum er eine schädliche Datei auf dem Gerät hat.
   Wenn die Datei oder der Hash böswillig ist, können Sie die bereits vorhandene E-Mail-Vorlage im Playbook verwenden, um den Endbenutzer per E-Mail um Klärung zu bitten.
8. In Schritt 8 müssen Sie überprüfen, ob der Endbenutzer eine gültige geschäftliche Begründung angegeben hat.
   Wenn der Endbenutzer eine gültige geschäftliche Begründung angegeben hat, wird in Schritt 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
9. Wenn der Benutzer in Schritt 9 keine gültige geschäftliche Begründung angegeben hat, werden die Schritte 10, 11 und 12 ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Da in Schritt 10 keine gültige geschäftliche Begründung vorlag, können Sie die schädliche Datei oder den schädlichen Hash zur Überprüfung an das Threat Intel-Team weiterleiten.
11. In Schritt 11 müssen Sie das Malware-Bytes-Scanner-Skript ausführen, um zu überprüfen, ob die Datei oder der Hash böswillig ist.
12. In Schritt 12 müssen Sie eine forensische Analyse durchführen, um zu überprüfen, ob die Datei oder der Hash böswillig ist.
13. In Schritt 13 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

### Playbook für Wiederholungserkennung

Mit diesem Playbook können Sie feststellen, ob die Incident-Antwort in der Vergangenheit für einen genauen oder ähnlichen Phishing-Bericht bereitgestellt wurde, und funktioniert automatisch für den neuen Bericht.

Das Playbook „Erkennung wiederholen“ überprüft, ob der neu gemeldete Phishing-Incident einem früheren Incident ähnelt. Wenn die wiederholte Erkennung identifiziert wird, werden der übereinstimmende Security Incident und die Lösungsdetails dem Analysten zur Verfügung gestellt, der sie für den neu gemeldeten Incident verwenden kann, was zu einer schnellen Behebung des Security Incident führt.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Wiederholungserkennungs-Playbook

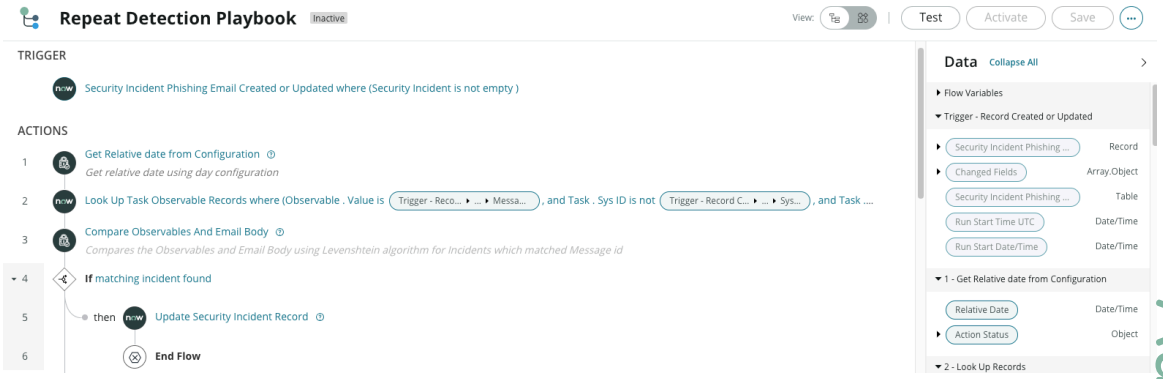
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Erkennung wiederholen** “ aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows für Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

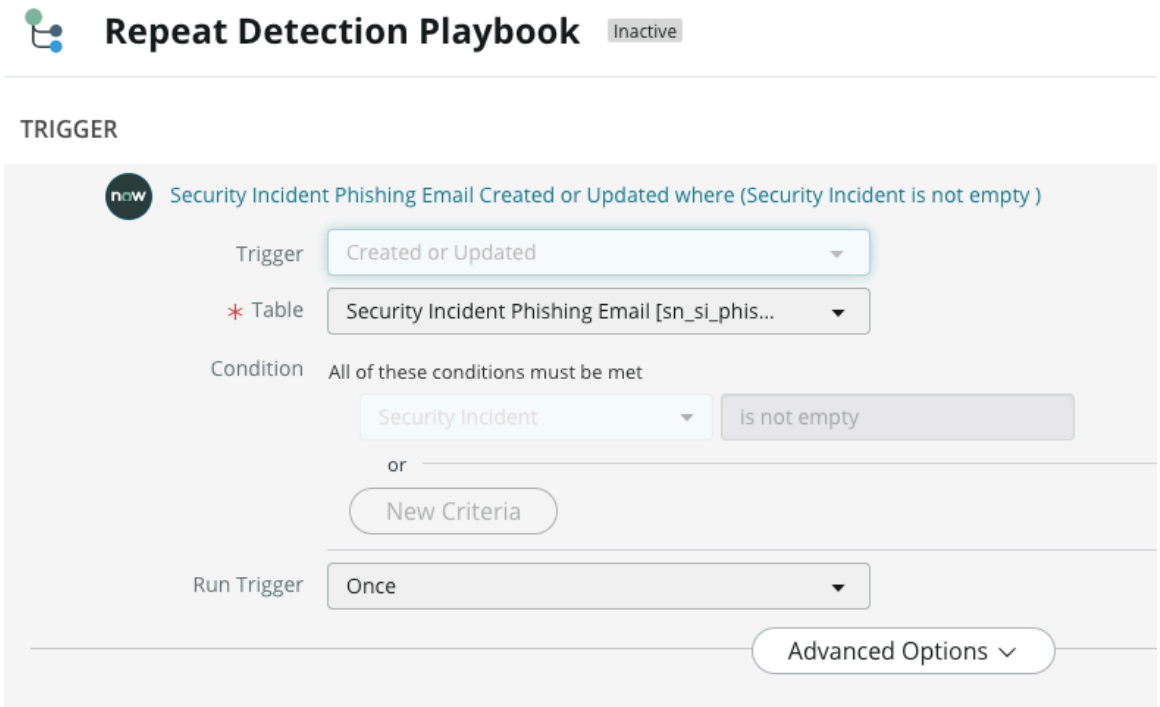
Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

**Playbook „Erkennung wiederholen“.**




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst, wenn der **Security Incident nicht leer ist**.




### Richten Sie das Playbook „Wiederholungserkennung“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

Navigieren zu **Alle** > > .

#### Verwenden Sie das Playbook „Erkennung wiederholen“.

Die folgenden Schritte zeigen Ihnen die Aktionen, Aufgaben und Subflows, die im Playbook „Wiederholungserkennung“ verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben. Sie haben die Möglichkeit, die folgenden Systemeigenschaften zu ändern:

- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

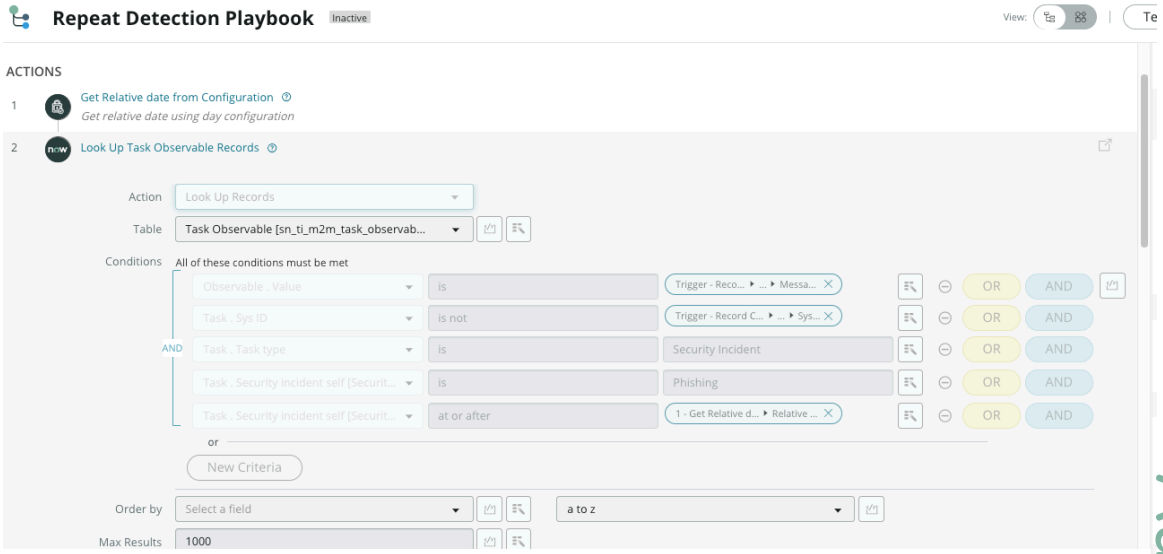
### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, ruft das Playbook in Schritt 1 das relative Datum des Security Incident anhand der Tageskonfiguration ab.
2. In Schritt 2 sucht das Playbook in der Tabelle *„sn_ti_m2m_task_observable* “ nach den Datensätzen des erkennbaren Aufgabenelements, die dem Incident basierend auf der Nachrichten-ID entsprechen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

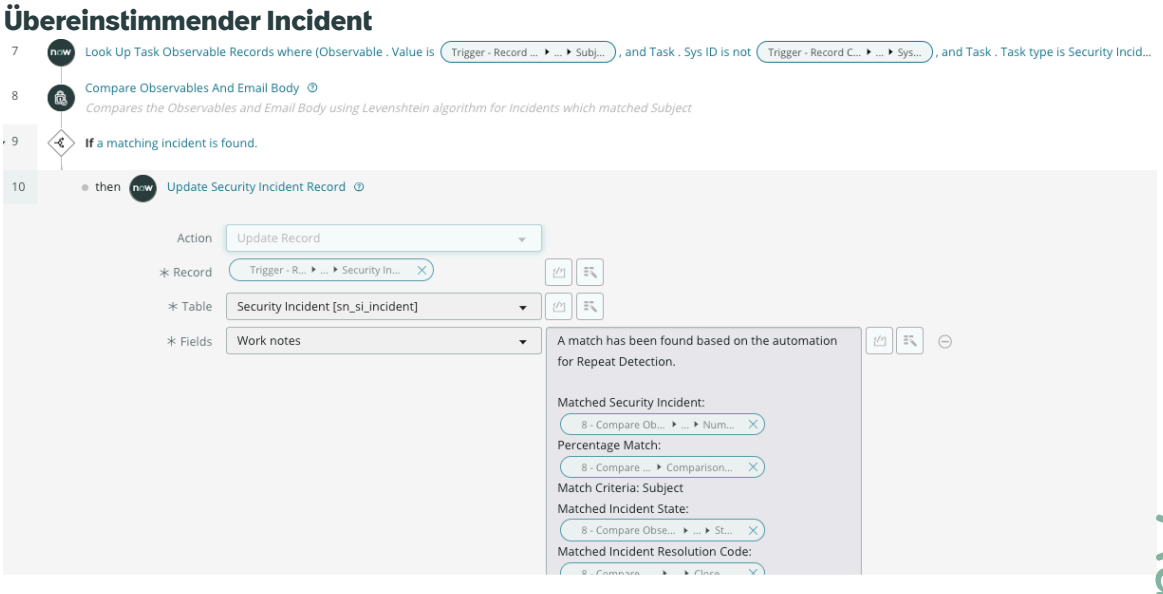
**Playbook „Erkennung wiederholen“.**




3. In Schritt 3 vergleicht das Playbook die erkennbaren Aufgabenelemente und den E-Mail-Text mit dem Levenshtein-Algorithmus für Incidents, die der Nachrichten-ID entsprechen.
4. In Schritt 4 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob der übereinstimmende Incident basierend auf der Nachrichten-ID gefunden wurde oder nicht.
   Wenn in Schritt 5 ein übereinstimmender Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, in der basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Schritt 6 endet der Flow.
5. Wenn der übereinstimmende Incident nicht gefunden wird, sucht das Playbook in Schritt 7 in der Tabelle *„`sn_ti_m2m_task_observable`“* nach den Datensätzen des erkennbaren Aufgabenelements, die dem Incident basierend auf dem Betreff entsprechen.
6. In Schritt 8 vergleicht das Playbook die erkennbaren Elemente der Aufgabe und den E-Mail-Text mit dem Levenshtein-Algorithmus für Incidents, die dem Betreff entsprechen.
7. In Schritt 9 überprüft das Playbook, ob der übereinstimmende Incident gefunden wurde.
   Wenn in Schritt 10 ein übereinstimmender Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, in der basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Schritt 11 endet der Flow.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




8. In Schritt 12 sucht das Playbook in der Tabelle *„sn_ti_m2m_task_observable“* nach den Datensätzen für erkennbare Aufgabenelemente, die dem Incident basierend auf der Adresse entsprechen.
9. In Schritt 13 vergleicht das Playbook die erkennbaren Elemente der Aufgabe und den E-Mail-Text mit dem Levenshtein-Algorithmus für Incidents, die mit der Adresse übereinstimmen.
10. In Schritt 14 überprüft das Playbook, ob der übereinstimmende Incident basierend auf der Adresse gefunden wurde oder nicht.
    Wenn in Schritt 15 ein übereinstimmender Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, in der basierend auf der Automatisierung für die Wiederholungserkennung eine Übereinstimmung gefunden wurde. In Schritt 16 endet der Flow.

### Playbook für gefälschte E-Mails (mit demselben Anzeigenamen)

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung gefälschter E-Mails, die ausgelöst werden, wenn gefälschte Namen für E-Mails an die Mitarbeiter des Unternehmens gesendet werden.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

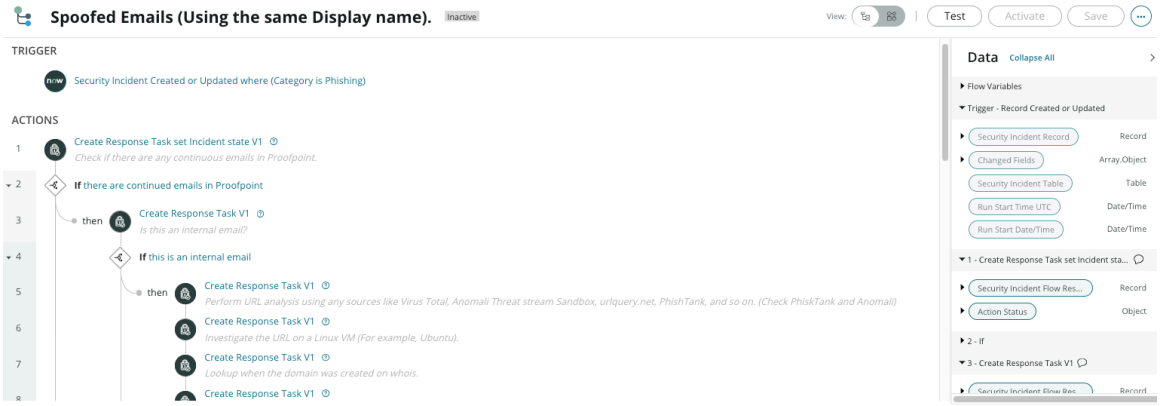
## Erste Schritte mit dem Playbook „Gefälschte E-Mails (mit demselben Anzeigenamen)“.

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook „Spoofed Emails (with the same Display name)“ (Spoofed Emails (mit demselben Anzeigenamen))** aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows für Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.



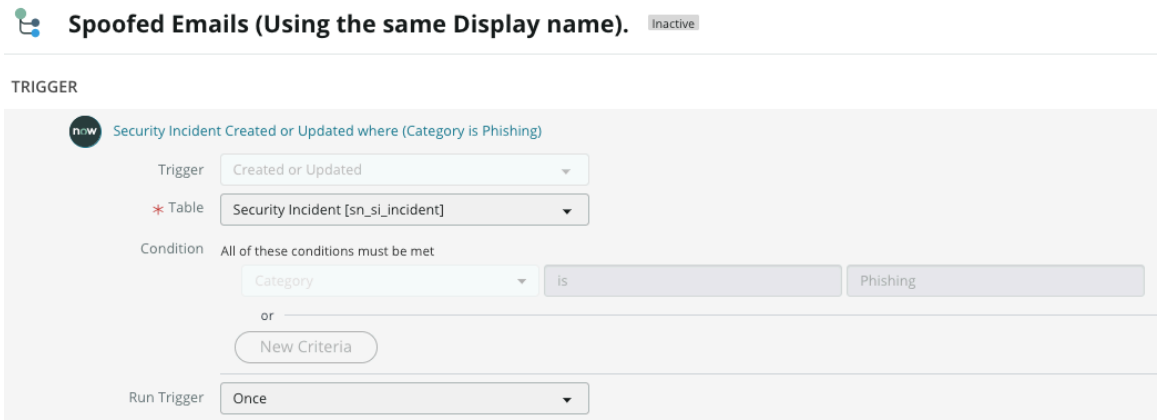
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook „Gefälschte E-Mails“.**




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategoriePhishing**lautet.




## Richten Sie gefälschte E-Mails ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

Navigieren zu **Alle** > > .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden Sie das Playbook „Gefälschte E-Mails (mit demselben Anzeigenamen)“.

Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Gefälschte E-Mails (mit demselben Anzeigenamen)“ verfügbar sind.

## Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

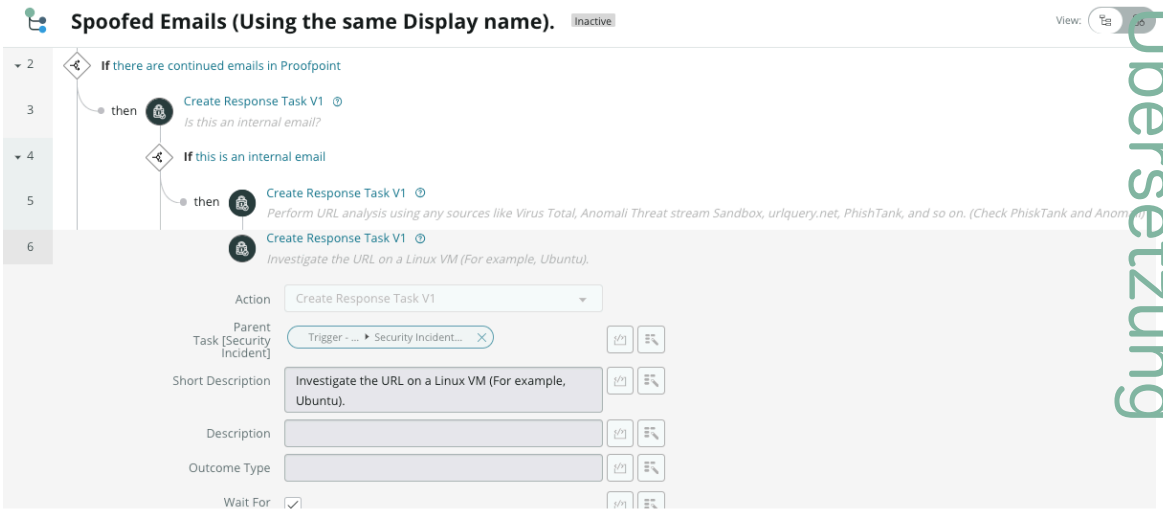
## Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 überprüfen, ob in Proofpoint kontinuierlich gefälschte E-Mails vorhanden sind.
2. Wenn in Schritt 2 fortlaufende E-Mails in Proofpoint vorhanden sind, überprüfen Sie, ob es sich um eine interne gefälschte E-Mail handelt oder nicht.
3. Wenn es sich um eine interne gefälschte E-Mail handelt, führen Sie in Schritt 3 die folgenden Schritte aus:

   a. In Schritt 5 müssen Sie eine URL-Analyse mit beliebigen Quellen wie Virus Total, Anomali Threat Stream Sandbox, urlquery.net, PhishTank durchführen (prüfen Sie beispielsweise PhiskTank und Anomali).

   b. In Schritt 6 müssen Sie die URL auf einer Linux-VM (z. B. Ubuntu) untersuchen.

**Playbook für gefälschte E-Mails (mit demselben Anzeigenamen).**

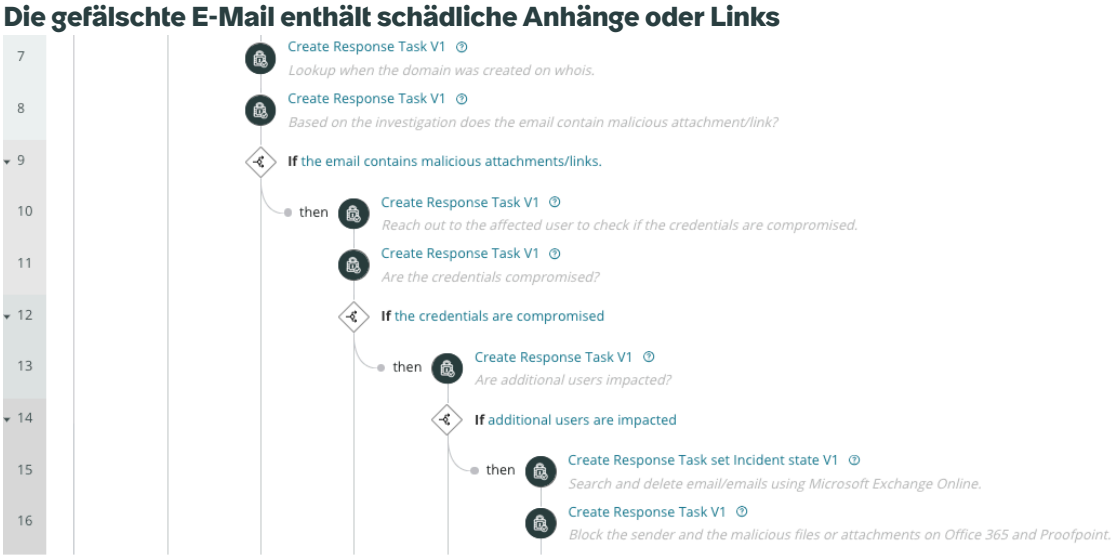



   c. In Schritt 7 müssen Sie nachschlagen, wann die Domäne in WHOIS erstellt wurde.
   Suchen Sie nach kürzlich registrierten Domänen (innerhalb der letzten Woche), die verdächtig sind und eine hohe Wahrscheinlichkeit von Phishing-Angriffen aufweisen.

   d. In Schritt 8 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob diese E-Mail einen schädlichen Anhang oder Link enthält.
   Wenn diese E-Mail keinen schädlichen Anhang oder Link enthält, wird der Flow beendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**e.** Wenn die E-Mail in Schritt 9 schädliche Anhänge oder Links enthält, führen Sie die folgenden Schritte aus.

**i.** In Schritt 10 müssen Sie den betroffenen Benutzer kontaktieren, um zu überprüfen, ob die Anmeldeinformationen gefährdet sind. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Benutzer zu kontaktieren.

**ii.** In Schritt 11 müssen Sie überprüfen, ob die Anmeldeinformationen basierend auf der E-Mail-Antwort gefährdet sind. Wenn die Anmeldeinformationen nicht gefährdet waren, wird der Flow beendet.

**1.** Wenn in Schritt 12 die Anmeldeinformationen gefährdet sind, müssen Sie in Schritt 13 überprüfen, ob weitere Benutzer betroffen sind. Wenn keine weiteren Benutzer betroffen sind, wird der Flow beendet.

**2.** Wenn in Schritt 14 weitere Benutzer betroffen sind, führen Sie die folgenden Schritte aus:

**a.** In Schritt 15 müssen Sie E-Mails mit Microsoft Exchange Online suchen und löschen.

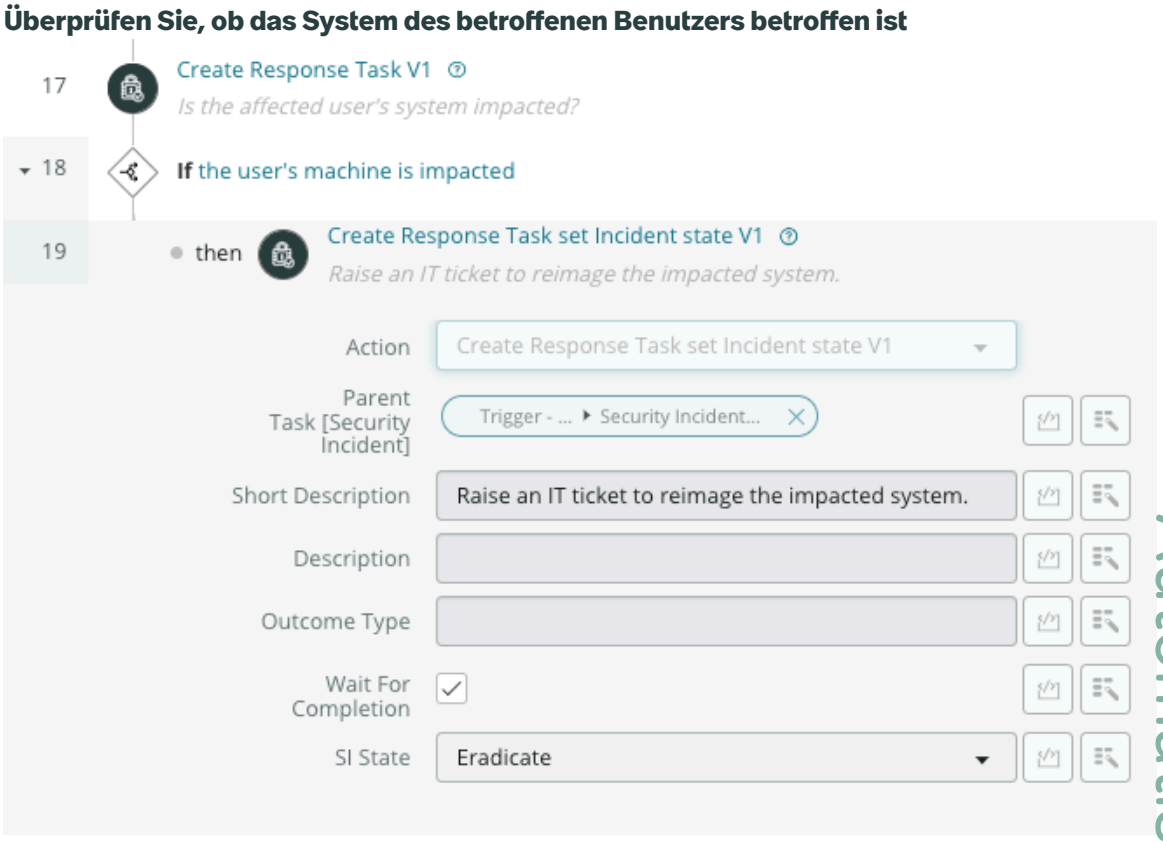
**b.** In Schritt 16 müssen Sie den Absender und die schädlichen Dateien oder Anhänge in Office 365 und Proofpoint blockieren.

**4.** Wenn es sich in Schritt 17 nicht um eine interne gefälschte E-Mail handelt, müssen Sie überprüfen, ob das System des betroffenen Benutzers betroffen ist.

**5.** Wenn in Schritt 18 das System des Benutzers betroffen ist, lösen Sie in Schritt 19 ein IT-Ticket aus, um ein neues Image des betroffenen Systems durchzuführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. In Schritt 20 wird eine Antwortaufgabe erstellt, damit Sie die Überprüfung nach dem Incident abschließen, bevor die Aufgabe geschlossen wird.

### Playbook für Endpunkterkennung

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Malware-Warnungen, die auf einem Host oder Endpunkt ausgelöst werden (z. B. Erkennung schädlicher Dateien).

Wenn CrowdStrike-Warnungen auf einem Host oder Endpunkt ausgelöst werden, können Sie das Endpunkterkennungs-Playbook im Flow Designer als Anleitung und zur Optimierung der Untersuchung dieser schädlichen Dateien verwenden.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Endpunkterkennungs-Playbook

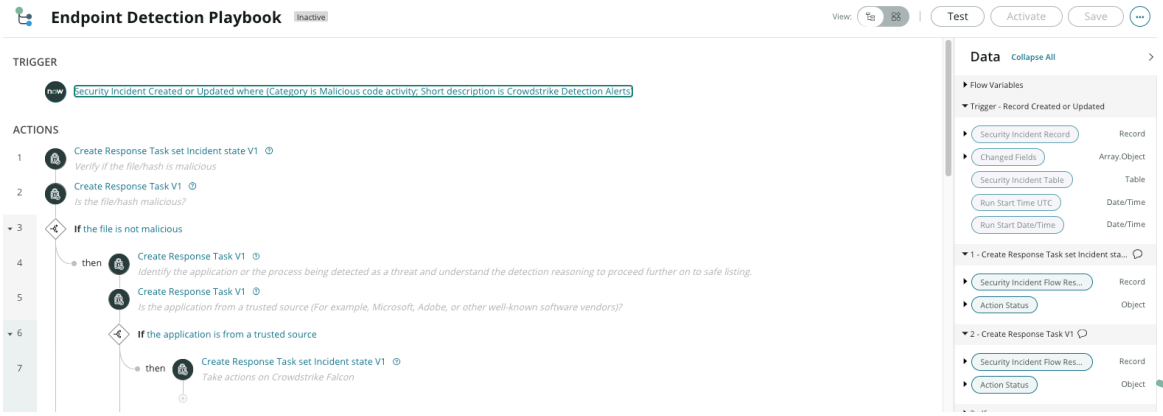
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Endpunkterkennungs-** Playbook aus.
3. (Optional) Sie können eine Kopie des Endpunkterkennungs-Playbook-Flows erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

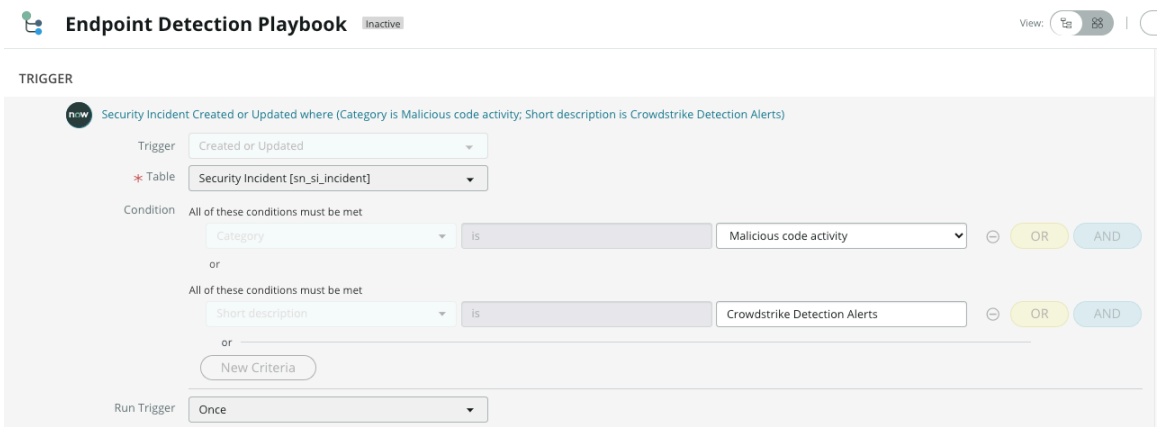
**Endpunkterkennungs-Playbook**




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

- **Kategorie** ist **„Böswillige Codeaktivität“**.
- **Die Kurzbeschreibung** lautet **CrowdStrike-Erkennungswarnungen**.




### Richten Sie die Endpunkterkennung ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

Navigieren zu **Alle** > > .

### Verwenden Sie das Endpunkterkennungs-Playbook

Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Endpunkterkennungs-Playbook verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

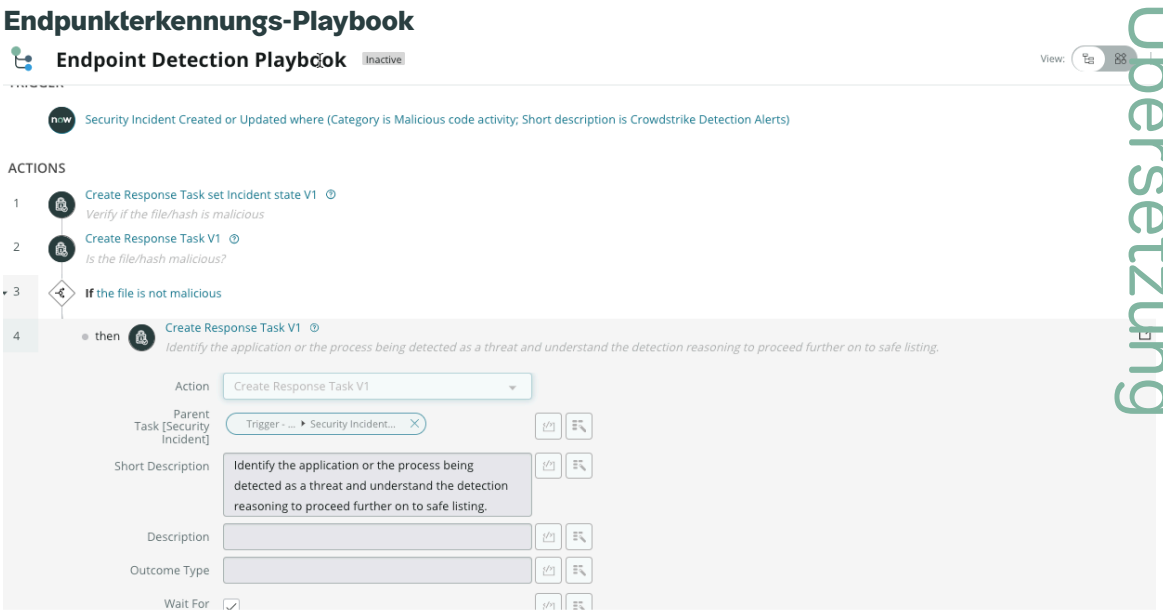
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

## Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 überprüfen, ob die Datei oder der Hash böswillig ist, indem Sie die Ergebnisse der Bedrohungssuche in SIR analysieren und Informationen von VirusTotal, WildFire, ThreatCrowd usw. sammeln.
2. In Schritt 2 müssen Sie überprüfen, ob die Datei oder der Hash böswillig ist oder nicht.
3. Wenn die Datei oder der Hash in Schritt 3 schädlich ist, führen Sie die folgenden Schritte aus:

   a. In Schritt 4 müssen Sie die Anwendung oder den erkannten Prozess als Bedrohung identifizieren und Informationen über die Gründe für die Erkennung sammeln, um mit der sicheren Auflistung fortzufahren.

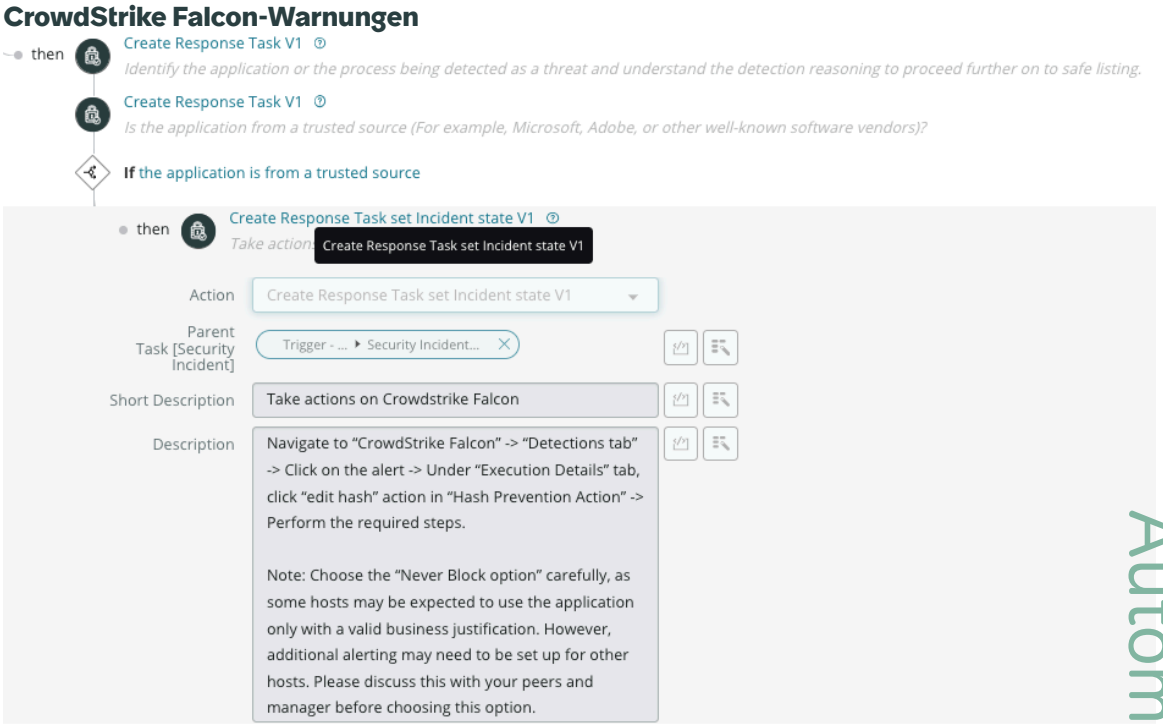



   b. In Schritt 5 müssen Sie überprüfen, ob die Anwendung aus einer vertrauenswürdigen Quelle stammt (z. B. Microsoft, Adobe oder andere bekannte Softwareanbieter).

   c. Wenn die Anwendung in Schritt 6 aus einer vertrauenswürdigen Quelle stammt, müssen Sie Maßnahmen für die CrowdStrike Falcon-Warnungen ergreifen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Führen Sie in Schritt 7 die folgenden Schritte aus:

**i.** Navigieren zu **CrowdStrike Falcon** > **Erkennungen** Registerkarte.

**ii.** Klicken Sie auf die CrowdStrike Falcon-Warnung.

**iii.** Klicken Sie auf der Registerkarte Ausführungsdetails auf Hash-Aktion **bearbeiten** in Hash-Verhinderungsaktion.

**iv.** Führen Sie die erforderlichen Schritte aus.

> **Hinweis:**
> Wählen Sie die Option **Nie blockieren** mit Bedacht aus, da nur bestimmte Hosts die Anwendung mit einer gültigen geschäftlichen Begründung verwenden dürfen. Möglicherweise müssen jedoch zusätzliche Warnungen für andere Hosts eingerichtet werden.

**e.** Wenn die Anwendung in Schritt 8 nicht aus einer vertrauenswürdigen Quelle stammt, müssen Sie auswählen, ob Sie lokal auf die Datei oder Anwendung auf dem Gerät verzichten möchten.
Wenn Sie in Schritt 10 auf die Datei oder Anwendung auf dem Gerät lokal verzichten möchten, führen Sie die folgenden Schritte aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Navigieren Sie in Schritt 11 zur Registerkarte **Dateien in Quarantäne**, und filtern Sie den Endpunkt, indem Sie nach dem Gerätenamen suchen.

ii. Wählen Sie die Datei aus, die lokal entfernt werden muss, und klicken Sie auf **Release**.

**Hinweis:**

- Die Datei wird weiterhin auf diesem spezifischen Endpunkt ausgeführt. Erkennung und Quarantäne erfolgen jedoch weiterhin auf allen anderen Hosts.
- Um die Quarantänedatei auf mehreren Hosts in einem Massenvorgang freizugeben, wählen Sie die entsprechenden Dateinamen und Status aus. Klicken Sie auf **Auswählen**und dann auf **Release**.

Wenn Sie in Schritt 12 nicht lokal auf dem Gerät auf die Datei oder Anwendung verzichten möchten, können Sie den Benutzer an den IT-Support umleiten, um die Installation der genehmigten Anwendungen anzufordern.

**4.** Wenn die Datei oder der Hash in Schritt 14 nicht schädlich ist, führen Sie die folgenden Schritte aus:

**a.** In Schritt 15 müssen Sie basierend auf der Rolle des Benutzers (Abteilung oder Position, die vertrauliche Informationen verarbeitet), dem Typ der Anwendung (Ransomware, Rootkit usw.) und den Auswirkungen bestimmen, ob die Datei/der Hash ein hohes oder niedriges Risiko aufweist der Anwendung (wie viele Anwender waren betroffen).

**b.** Wenn es sich bei der Datei in Schritt 16 um eine Datei mit hohem Risiko handelt, führen Sie die folgenden Schritte aus:

i. Überprüfen Sie in Schritt 17 die Ergebnisse mit dem Threat Intel-Team.

ii. Führen Sie in Schritt 18 den Malwarebyte-Scan für die Datei aus.

iii. Initiieren Sie in Schritt 19 die forensische Analyse.

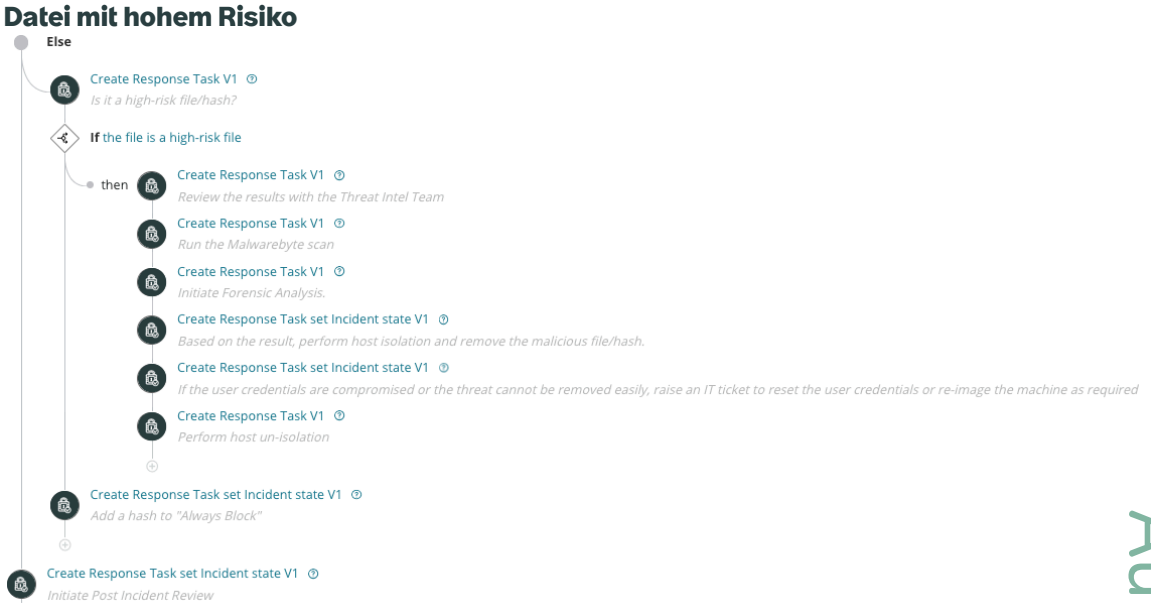
iv. Führen Sie in Schritt 20 basierend auf dem Ergebnis der forensischen Analyse eine Hostisolierung durch, und entfernen Sie die schädliche Datei/den schädlichen Hash.

v. Wenn in Schritt 21 die Benutzeranmeldeinformationen gefährdet sind oder die Bedrohung nicht einfach entfernt werden kann, lösen Sie ein IT-Ticket aus, um die Benutzeranmeldeinformationen zurückzusetzen, oder führen Sie ein erneutes Image des Computers durch.

vi. Führen Sie in Schritt 22 die Isolierung des Hosts durch.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**c.** Wenn es sich bei der Datei in Schritt 23 nicht um eine Datei mit hohem Risiko handelt, führen Sie die folgenden Schritte aus:

**i.** Navigieren zu **CrowdStrike Falcon** > **Konfigurationen** Registerkarte.

**ii.** Navigieren Sie auf der Registerkarte Konfigurationen zu **Präventions-Hashes** > > **Hash hochladen** > **Fügen Sie den Hash hinzu**.

**iii.** Wählen Sie das erforderliche Betriebssystem und dann **Immer blockieren**aus.

**5.** In Schritt 24 wird eine Antwortaufgabe erstellt, damit der Benutzer die Überprüfung nach dem Incident abschließen kann, bevor die Aufgabe geschlossen wird.

### Playbook für mögliches Passwort-Spray

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Passwort-Spray-Warnungen, die durch mehrere fehlgeschlagene Anmeldungen ausgelöst werden (zu viele Authentifizierungsfehler von mehr als einer IP-Adresse für denselben Benutzer).

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Playbook „Mögliches Passwort-Spray“.

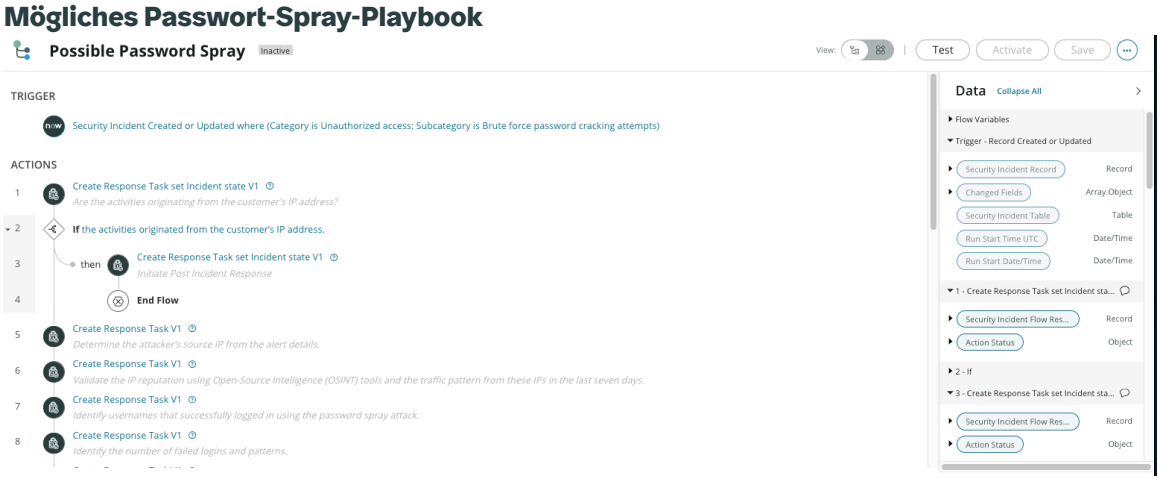
**1.** Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.

**2.** Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook „ **Mögliches Passwort-Spray** “ aus.

**3.** (Optional) Sie können eine Kopie des Playbook-Flows „Mögliches Passwort-Spray“ erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.



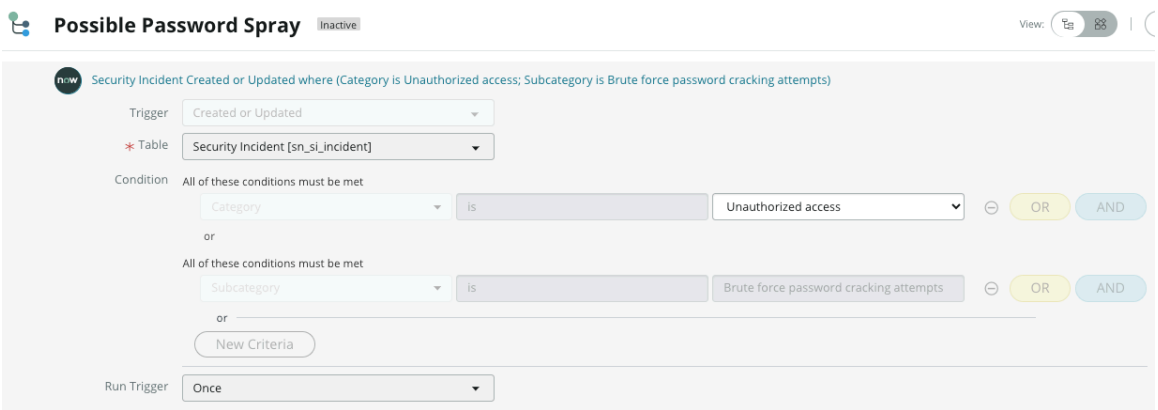
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

- **Kategorie** ist **„Nicht autorisierter Zugriff“**.
- **Unterkategorie** ist **Brute-Force-Angriffe auf Passwörter**.




## Richten Sie das mögliche Passwort-Spray ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

Navigieren zu **Alle** > > .

#### Verwenden Sie das Playbook „Mögliches Passwort-Spray“.

Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Mögliches Passwort-Spray“ verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

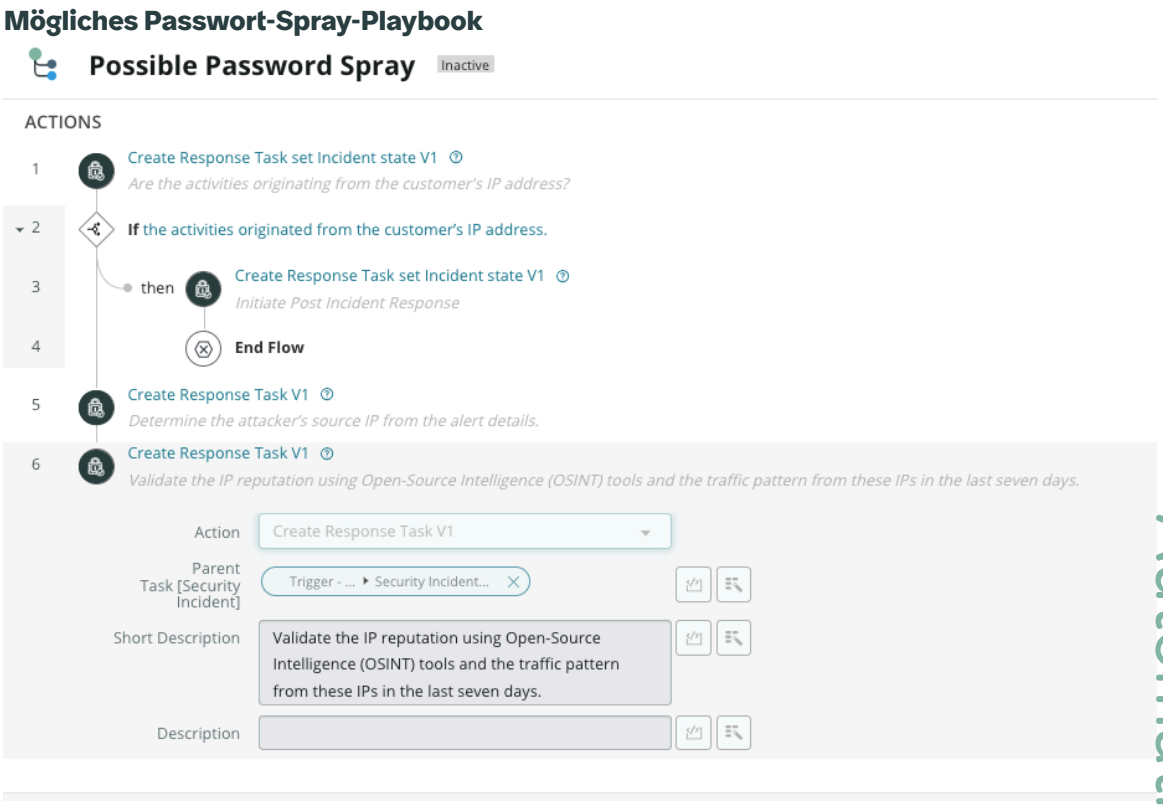
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 überprüfen, ob die Aktivitäten von der IP-Adresse des Kunden stammen.
   Identifizieren Sie die IP-Adressen, die den Passwort-Spray-Angriff ausführen. Verwenden Sie beispielsweise die TXIDs (Transaktions-IDs) aus der Warnung, und vergleichen Sie sie mit den F5-Protokollen.
2. Wenn die Aktivitäten in Schritt 2 von der IP-Adresse des Kunden stammen, führen Sie die folgenden Schritte aus:
   a. In Schritt 3 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach dem Incident initiieren.
   b. In Schritt 4 endet der Flow.
3. Wenn die Aktivitäten in Schritt 5 nicht von der IP-Adresse des Kunden stammen, bestimmen Sie die Quell-IP des Angreifers anhand der Warnungsdetails.
4. In Schritt 6 müssen Sie die IP-Reputation mit Open Source Intelligence-Tools (OSINT) und das Datenverkehrsmuster dieser IPs in den letzten sieben Tagen validieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

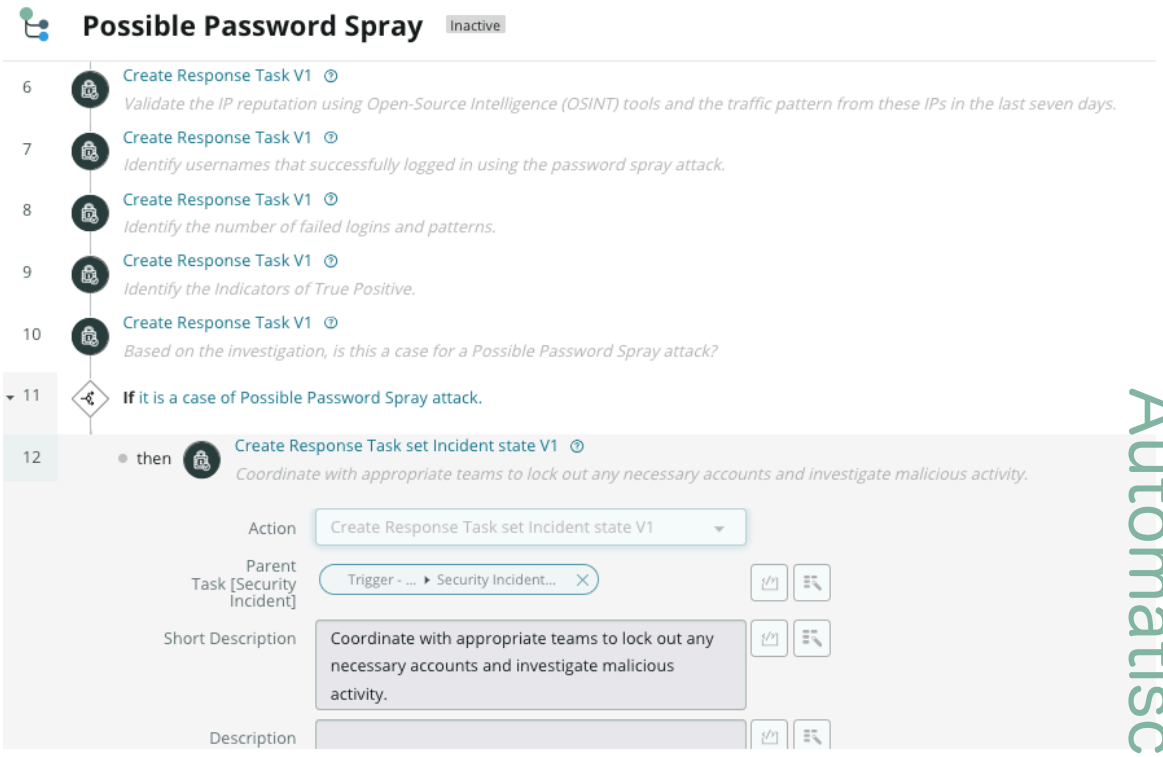



5. In Schritt 7 müssen Sie die Benutzernamen identifizieren, die sich erfolgreich mit dem Passwort-Spray-Angriff angemeldet haben.
6. In Schritt 8 müssen Sie die Anzahl der fehlgeschlagenen Anmeldungen und Muster identifizieren.
7. In Schritt 9 müssen Sie die Indikatoren für „wahr positiv“ identifizieren.
   - Überprüfen Sie den Datenverkehr von den Quell-IPs in den letzten 60 Tagen. Kein Verlaufsdatenverkehr kann ein Hinweis auf ein richtig positives Ergebnis sein.
   - Überprüfen Sie die Benutzernamenmuster mit Authentifizierungsfehlern und die Anzahl. Je höher die Anzahl, desto höher die Wahrscheinlichkeit, dass es sich um ein richtig positives Ergebnis handelt.
   - Der Benutzername sieht aus wie eine Wörterbuchbasis (von A bis Z) und enthält möglicherweise allgemeine Administratornamen wie admin, sysadmin, root usw
   - Derselbe Benutzername kann unterschiedliche Muster im -Spray-Angriff aufweisen, z. B. kann dieselbe Warnung Fehler für john.doe, johnd, jdoe, john_doe, jdoe7 usw. aufweisen, was darauf hinweist, dass Angreifer das Benutzernamenmuster basierend auf häufigen Anwendungsfällen erraten haben.
   - Beachten Sie den Benutzer-Agent und die URIs aus den F5-Protokollen im obigen Schritt, und prüfen Sie, ob die IoCs mit den Red-Condor-Warnungen zusammenhängen. Wenn sie übereinstimmen, handelt es sich um ein echtes positives Event.
8. In Schritt 10 müssen Sie basierend auf den bisher durchgeführten Untersuchungen überprüfen, ob es sich um einen möglichen Passwort-Spray-Angriff handelt oder nicht.
9. Führen Sie in Schritt 11 bei einem möglichen Passwort-Spray-Angriff die folgenden Schritte aus:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** In Schritt 12 müssen Sie sich mit den entsprechenden Teams abstimmen, um alle erforderlichen Konten zu sperren und böswillige Aktivitäten zu untersuchen.




**b.** In Schritt 13 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach dem Incident initiieren.

**c.** In Schritt 14 endet der Flow.

**10.** In Schritt 15 müssen Sie überprüfen, ob es sich nicht um einen möglichen Passwort-Spray-Angriff handelt.

**11.** Wenn es sich in Schritt 16 nicht um einen möglichen Passwort-Spray-Angriff handelt, führen Sie die folgenden Schritte aus:

**a.** In Schritt 17 müssen Sie die bisherigen Ergebnisse dokumentieren.

**b.** In Schritt 18 müssen Sie eine Überprüfung des möglichen Passwort-Spray-Angriffs nach dem Incident initiieren.

**c.** In Schritt 19 endet der Flow.

**12.** In Schritt 20 müssen Sie die Kollegen und den GIR-Manager um Rat fragen.

**13.** In Schritt 21 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

### Playbook für T1003 – Tools zum Speichern von Anmeldeinformationen erkennen

Dieses Playbook hilft bei der frühzeitigen Selektierung von von Benutzern gemeldeten Phishing-Übermittlungen, indem der Analyst auf die Möglichkeit einer Doppelgänger-Domäne in der E-Mail-Adresse des Phishing-Angriffs aufmerksam gemacht wird.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder



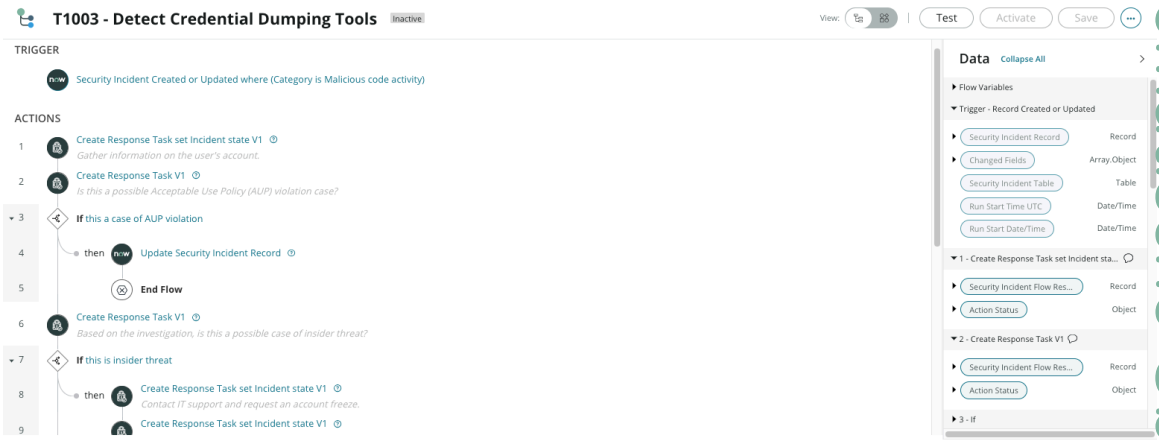
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Playbook „T1003 – Detect Credential Dumping Tools“.

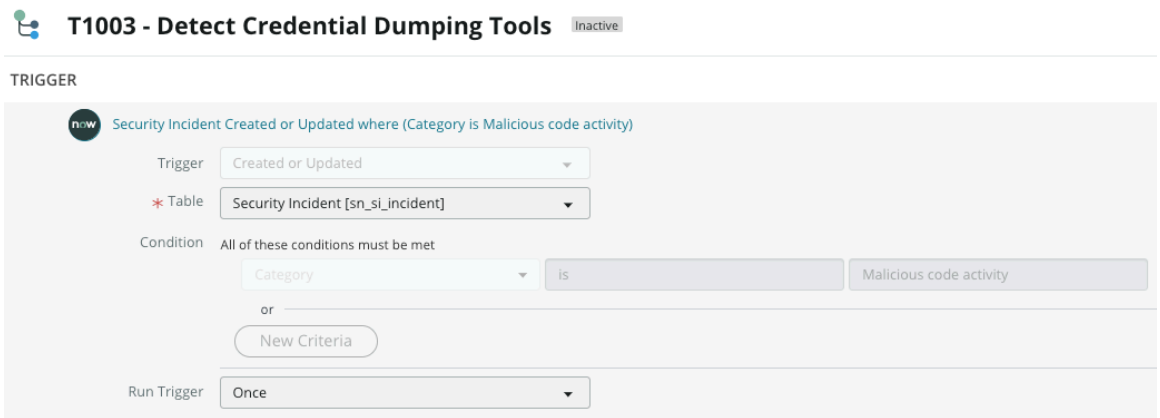
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook T1003 – Detect Credential Dumping Tools** aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows T1003 – Detect Credential Dumping Tools erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

### T1003 – Playbook „Erkennen Sie Tools für das Dumping von Anmeldeinformationen“.




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslösebedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die Aktivität „ **Kategorie“ Böswilliger Code**lautet.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie „Anmeldeinformations-Dumping erkennen“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

Navigieren zu **Alle** > > .

### Verwenden Sie das Playbook „T1003 – Detect Credential Dumping Tools“.

Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „T1003 – Detect Credential Dumping Tools“ verfügbar sind.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

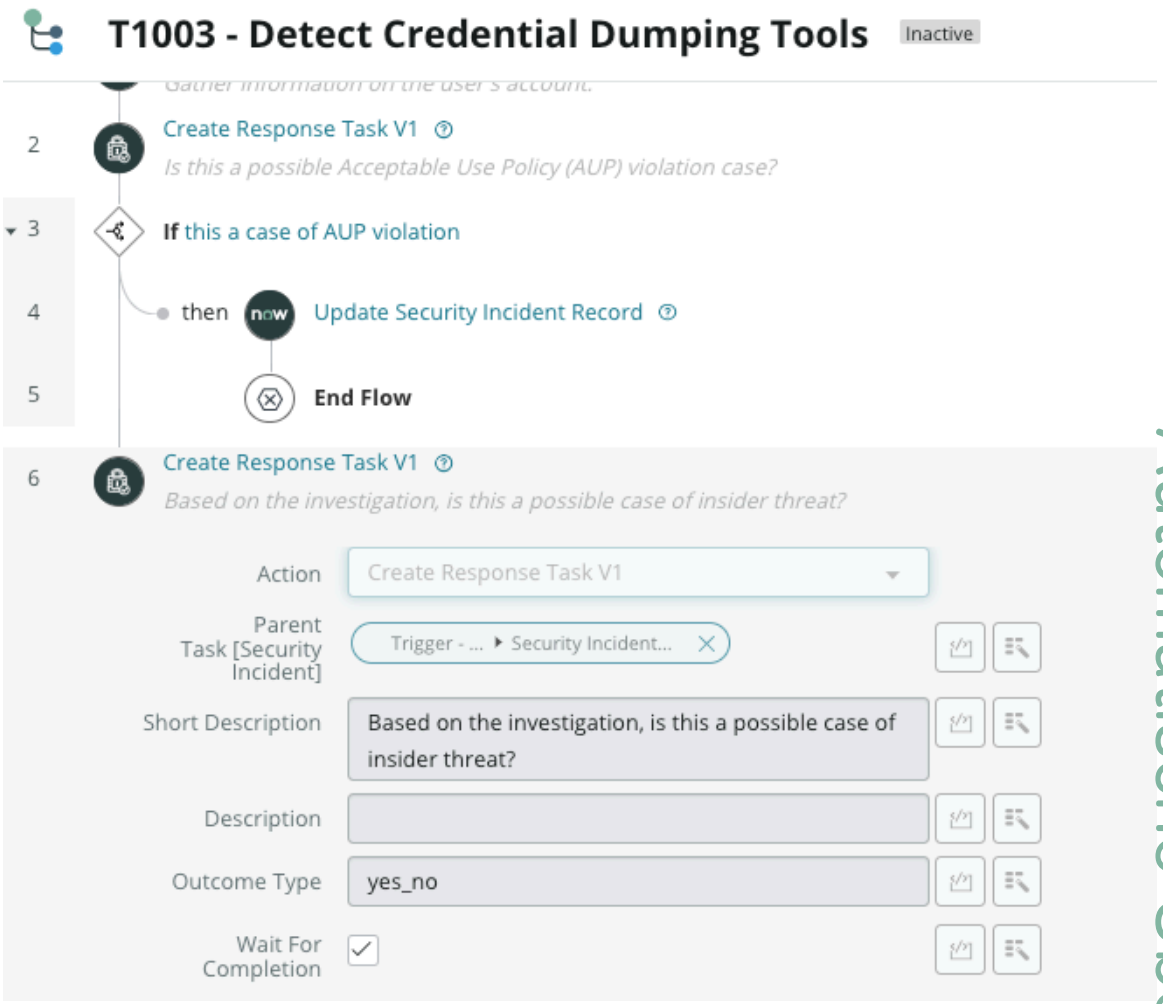
**Prozedur**

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 Informationen zum Konto des Benutzers erfassen.
   - Sie müssen die Hostaktivität überprüfen, um nach verdächtigen Aktivitäten zu suchen.
   - Sie müssen den Besitzer des Servers/Endpunkts/der VM identifizieren und die Daten erfassen, die dem Tool entsprechen.
   - Sie müssen Informationen zu den anderen Accounts des Benutzers sammeln.
2. In Schritt 2 müssen Sie überprüfen, ob dies ein möglicher Verstoßfall für die Richtlinie zur zulässigen Nutzung (AUP) ist.
   Sie können eine Peer-Review mit den gesammelten Nachweisen durchführen und sich mit Ihrem regionalen Incident Manager beraten, ob Sie den Benutzer kontaktieren sollen.
3. Wenn es sich in Schritt 3 um einen Verstoß gegen die Richtlinie zur zulässigen Nutzung (AUP) handelt, führen Sie die folgenden Schritte aus:
   a. In Schritt 4 müssen Sie den Security Incident so aktualisieren, dass es sich um einen AUP-Verstoß handelt
   b. In Schritt 5 endet der Flow.
4. In Schritt 6 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob dies ein möglicher Fall einer internen Bedrohung ist oder nicht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**T1003 – Playbook „Erkennen Sie Tools für das Dumping von Anmeldeinformationen“.**




**5.** Wenn es sich um eine interne Bedrohung handelt, führen Sie in Schritt 7 die folgenden Schritte aus:

**a.** In Schritt 8 müssen Sie sich an den IT-Support wenden und eine Kontosperre anfordern.

**b.** In Schritt 9 müssen Sie schädliche IPs blockieren.

**c.** In Schritt 10 müssen Sie interne Mitarbeiter per E-Mail kontaktieren.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um Ihre internen Mitarbeiter zu kontaktieren.

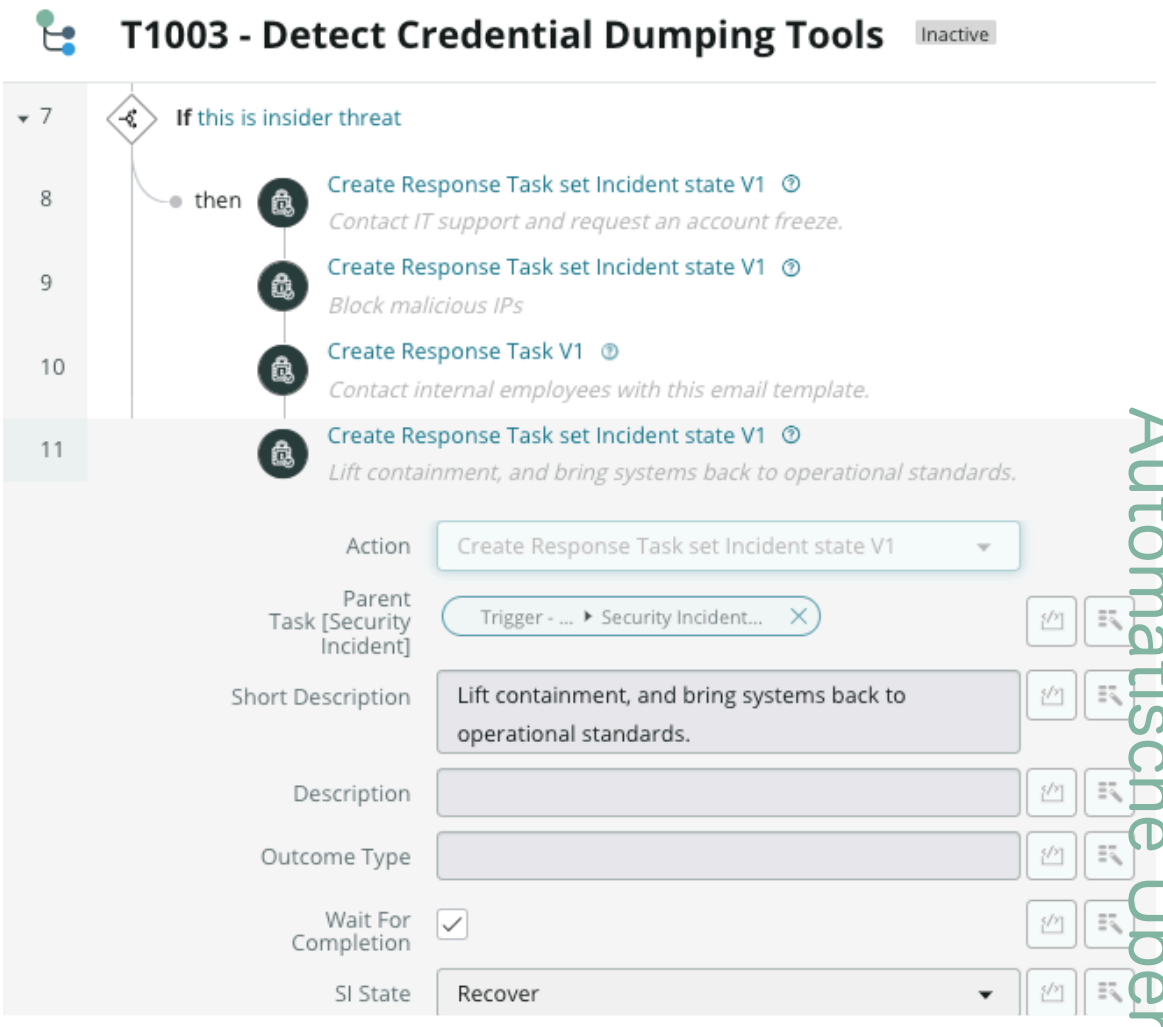
**d.** In Schritt 11 müssen Sie das Containment aufheben und die Systeme wieder in den Betriebszustand versetzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Flow endet.

**Antwortaufgaben zum Aufheben des Containments**




6. Wenn es sich in Schritt 12 nicht um eine interne Bedrohung handelt, müssen Sie in Schritt 13 eine Peer-Überprüfung durchführen, um festzustellen, ob dies der Ausschlussliste hinzugefügt werden muss.
   Der Flow endet.
7. In Schritt 14 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

### Playbook für die Erkennung von E-Mail-Domänen-Spoofing

Dieses Playbook hilft bei der frühzeitigen Selektierung von von Benutzern gemeldeten Phishing-Übermittlungen, indem der Analyst auf die Möglichkeit einer Doppelgänger-Domäne in der E-Mail-Adresse des Phishing-Angriffs aufmerksam gemacht wird.

Das Playbook zur Erkennung von E-Mail-Domänen-Spoofing sucht nach einer Ähnlichkeitsübereinstimmung zwischen der Absender-E-Mail-Domäne des Phishers und einem vertrauenswürdigen Domänennamen, der im Repository für erkennbare Elemente vorhanden ist. Wenn das Playbook eine gefälschte Absender-E-Mail-Domänenübereinstimmung identifiziert hat, werden die Analysten mit einem Tag benachrichtigt.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder

Automatische Übersetzung

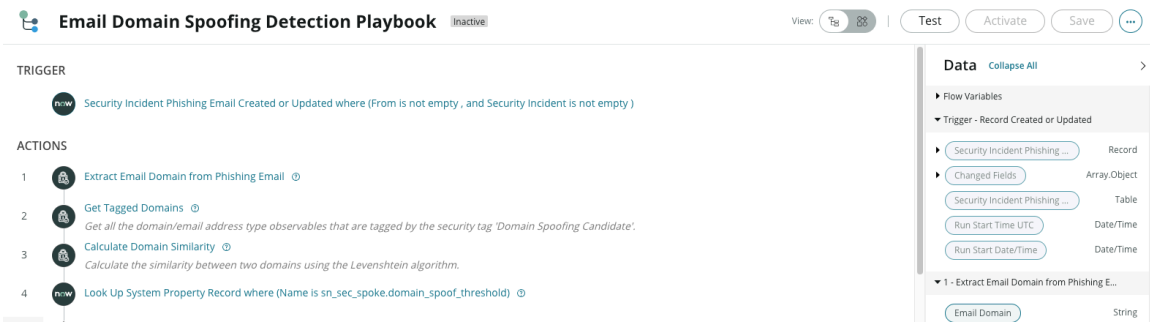
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

## Erste Schritte mit dem Playbook zur Erkennung von E-Mail-Domänen-Spoofing

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook „E-Mail-Domänen-Spoofing-Erkennung** “ aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows zur Erkennung von E-Mail-Domänen-Spoofing erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

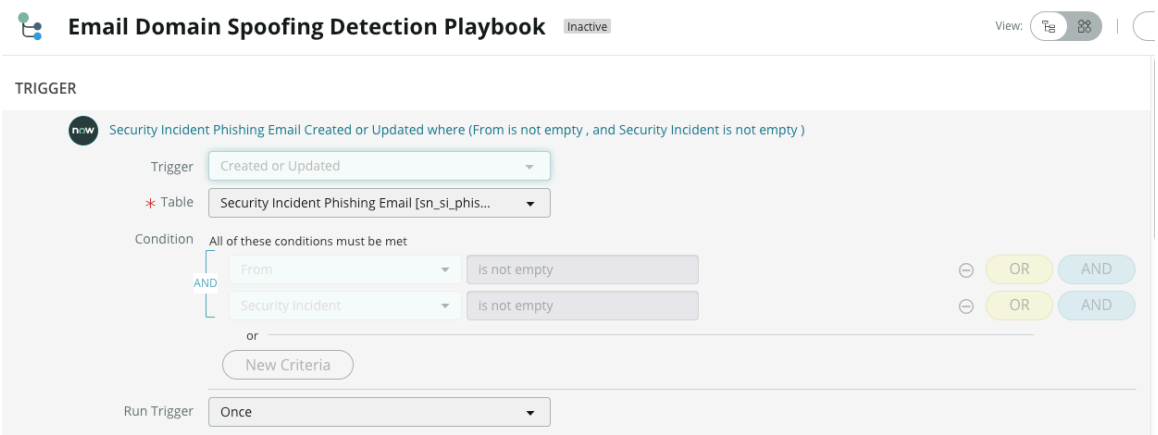
**Playbook „E-Mail-Domänen-Spoofing-Erkennung“.**




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

- **„Von “ ist nicht leer**.
- **Security Incident ist nicht leer**.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie die E-Mail-Spoof-Erkennung ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

Navigieren zu **Alle** > > .

### Verwenden Sie das Playbook „E-Mail-Domänen-Spoofing-Erkennung“.

Die folgenden Schritte zeigen Ihnen die Aktionen, Aufgaben und Subflows, die im Playbook „E-Mail-Domänen-Spoofing-Erkennung“ verfügbar sind.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

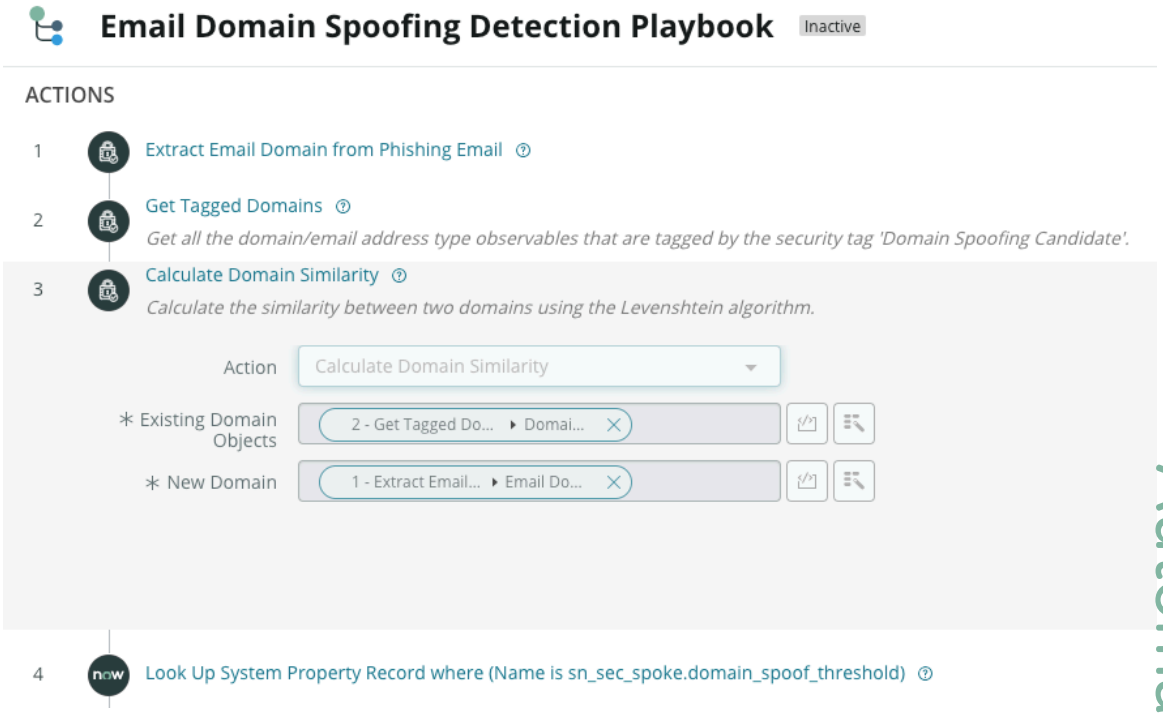
**Prozedur**

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, extrahiert das Playbook in Schritt 1 die E-Mail-Domäne aus der Phishing-E-Mail.
2. In Schritt 2 ruft das Playbook alle erkennbaren Elemente des Domänen-/E-Mail-Adresstyps ab, die mit dem Sicherheits-Tag „Domänen-Spoofing-Kandidat“ gekennzeichnet sind.
3. In Schritt 3 berechnet das Playbook die Ähnlichkeit zwischen der Domäne „Get Tagged“ und der E-Mail-Domäne mithilfe des Levenshtein-Algorithmus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

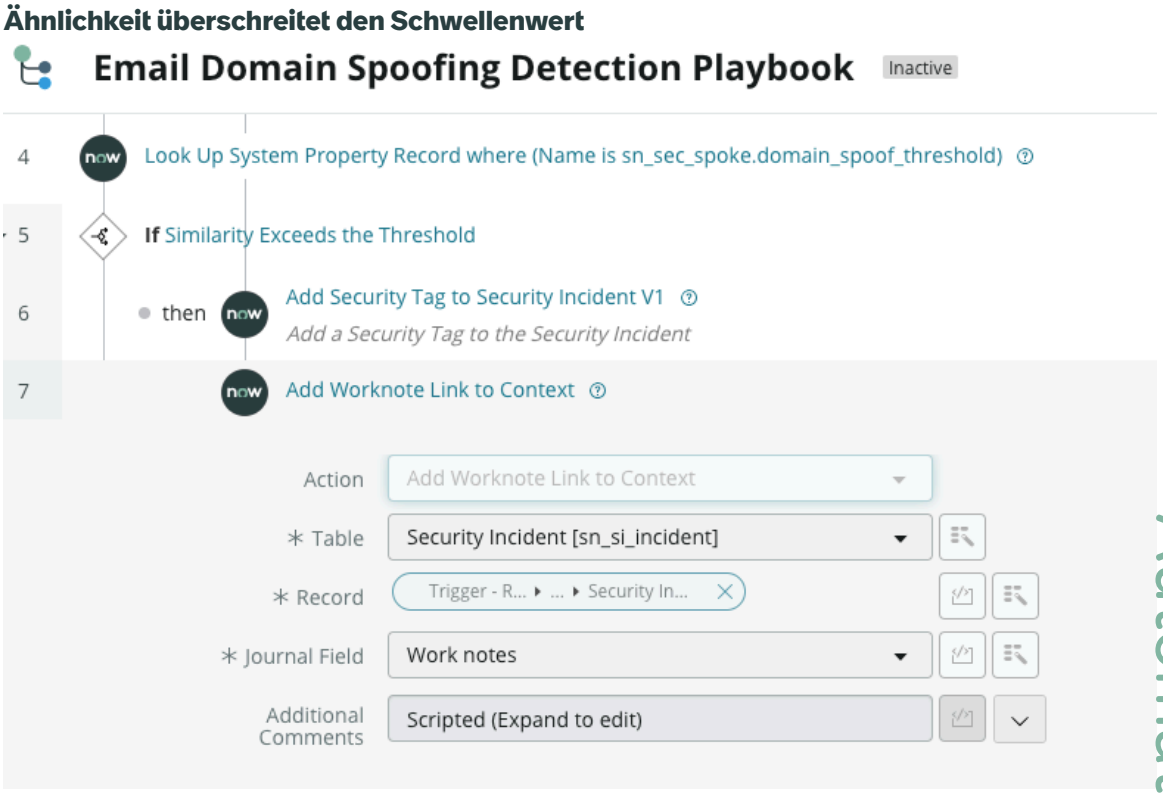
**Playbook „E-Mail-Domänen-Spoofing-Erkennung“.**




4. In Schritt 4 sucht das Playbook basierend auf den folgenden Bedingungen nach dem Systemeigenschaften-Datensatz:
   - Name ist sn_sec_spoke.domain_spoof_threshold, (OR)
   - Der Name reicht von a bis z. Wenn mehrere Datensätze gefunden werden, wird nur der erste Datensatz zurückgegeben.
5. In Schritt 5 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet oder nicht.
   Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert nicht überschreitet, wird in Schritt 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet. Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet, werden die Schritte 6 und 7 ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. In Schritt 6 fügt das Playbook dem Security Incident das Sicherheits-Tag „Email Domain Spoofing“ hinzu.
7. In Schritt 7 fügt das Playbook dem Kontext mithilfe der Skriptoption einen Arbeitsnotizlink hinzu.
8. In Schritt 8 endet der Flow.

### Playbook für Tippfehler in besetzter Domäne

Tippfehler-Squatted-Domänen sind absichtlich falsch geschriebene Domänennamen, die echten Domänen sehr ähnlich sind. Angreifer nutzen Rechtschreibfehler aus, um auf eine schädliche Website zu gelangen, um sie finanziell oder für andere böswillige Aktivitäten auszunutzen.

Die besetzten Domänen für Tippfehler werden dem Sicherheitsbetriebsteam aus verschiedenen Quellen wie Lösungen zum Schutz vor digitalen Risiken (Digital Shadows) und Threat Intelligence-Plattformen (Anomali Threatstream) gemeldet. Nachdem ein Security Incident erstellt wurde, hilft diese Lösung zu identifizieren, ob die Domäne tatsächlich eine Tippfehler-Squatted-Domäne ist. Wenn es sich um einen Tippfehler in der Domäne handelt, kann der Analyst dies der Rechtsabteilung melden, damit weitere Maßnahmen ergriffen werden können.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Untersuchung von Incidents bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisabhängige Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis dieser Aufgaben.

### Erste Schritte mit dem Playbook „Tippfehlerbesetzte Domäne“.

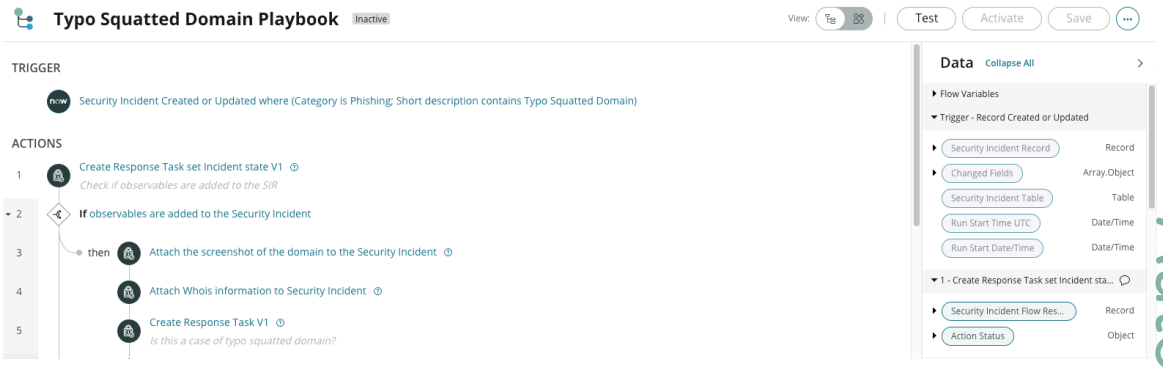
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **Typo Squatted Domain aus**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. (Optional) Sie können eine Kopie des Playbook-Flows „Tippfehlerbesetzte Domäne“ erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

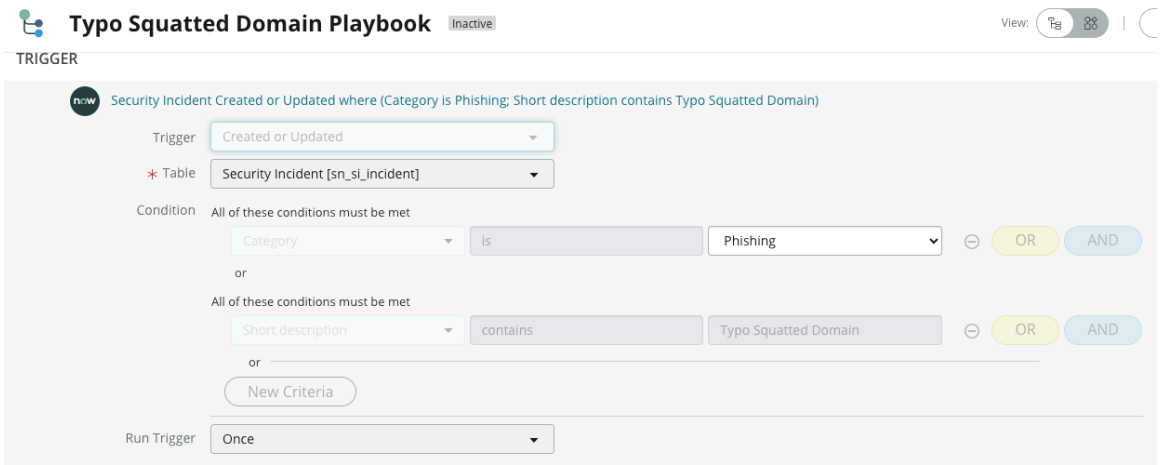
**Playbook „Tippfehlerbesetzte Domäne“.**




4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

- **Kategorie** ist **Phishing**.
- **Kurzbeschreibung** enthält **Tippfehler in der Domäne „Squatted“**.




## Richten Sie das Playbook für Tippfehler-besetzte Domänen ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

### Vorbereitungen

Erforderliche Rolle:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

Navigieren zu **Alle** > > .

### Verwenden Sie das Playbook „Tippfehlerbesetzte Domäne“.

Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Playbook „Typo Squatted Domain“ verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

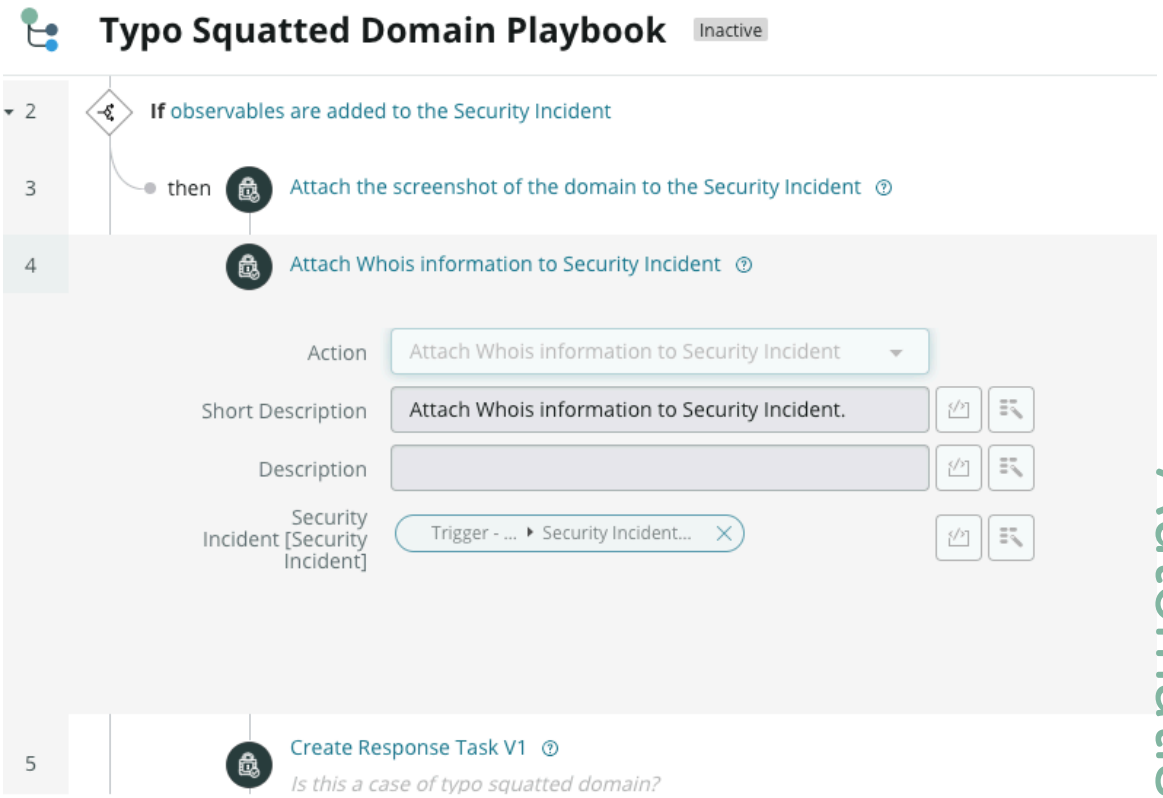
### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Schritt 1 überprüfen, ob die erkennbaren Elemente Security Incident Response (SIR) hinzugefügt wurden.
   Wenn die erkennbaren Elemente nicht zu SIR hinzugefügt werden, fügen Sie die erkennbaren Elemente hinzu, bevor Sie fortfahren. Wenn die erkennbaren Elemente nicht verfügbar sind, wird Schritt 10 ausgeführt, und der Security Incident wird geschlossen.
2. Wenn in Schritt 2 die erkennbaren Elemente dem Security Incident hinzugefügt werden, werden die folgenden Schritte ausgeführt.
3. In Schritt 3 müssen Sie den Screenshot der Domäne „Tippfehler besetzt“ an den Security Incident anhängen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook „Tippfehlerbesetzte Domäne“.**




4. In Schritt 4 müssen Sie die Whois-Informationen an den Security Incident anhängen.
5. In Schritt 5 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob es sich um einen Fall von „Tippfehler in der Domäne handelt“ oder nicht.
   Wenn es sich nicht um eine Tippfehler-Domäne handelt, wird in Schritt 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.
6. Wenn es sich in Schritt 6 um eine Tippfehler-Domäne handelt, wird Schritt 7 ausgeführt.
7. In Schritt 7 müssen Sie die Rechtsabteilung und andere erforderliche Teams per E-Mail darüber informieren, dass es sich um einen Tippfehler in der Domäne handelt, und die erforderlichen Schritte unternehmen, um ihn zu beheben.
   Wenn es sich nicht um eine Tippfehler-Domäne handelt, wird in Schritt 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Fall von Tippfehler in Domäne**

8. In Schritt 9 wird eine Antwortaufgabe erstellt, damit Sie die Überprüfung nach dem Incident abschließen, bevor die Aufgabe geschlossen wird.

### Playbook für das Ausspionieren von Anmeldeinformationen

Dieses Playbook enthält Systemkorrekturschritte zur Untersuchung eines Incident mit Aktivitäten zum Erfassen von Anmeldeinformationen, die über die Tabelle `sys_installation_exit` in einer ServiceNow-Instanz ausgeführt werden.

Das Playbook „Sniffing von Anmeldeinformationen“ bietet ein Skriptfeld, um die Datenbankanmeldungen (DB), Single Sign-on (SSO) und LDAP (Lightweight Directory Access Protocol) mithilfe der Datensätze in der Tabelle `sys_installation_exit` zu verarbeiten. Diese privilegierten Skriptfelder ermöglichen das Abhören von Benutzeranforderungen und Parametern für die Instanzen während der Anmeldung, einschließlich Benutzeranmeldeinformationen wie Benutzername und Passwort.

Ein böswilliger Benutzer kann ein Skript erstellen, um die Benutzeranforderungen abzuhören und diese Anforderungen in der Instanz zu protokollieren. Die Tabelle `sys_installation_exit` in einer Instanz definiert die Regeln für die Verarbeitung der Anmelde- und Abmeldeaktivitäten aller Benutzer in dieser Instanz.

### Richten Sie das Credential Sniffing-Playbook ein

Führen Sie die folgenden Schritte aus, um das Credential Sniffing-Playbook einzurichten.

**Vorbereitungen**
Erforderliche Rolle:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

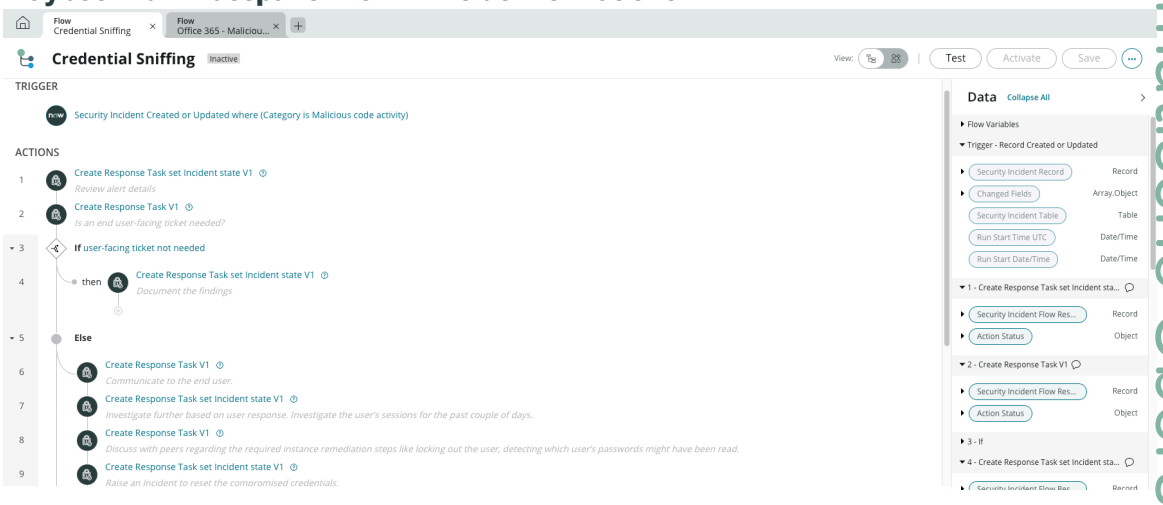
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **Credential Sniffing** aus.
3. Erstellen Sie eine Kopie des Playbook-Flows zum Ausspionieren von Anmeldeinformationen, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **Playbook zum Ausspähen von Anmeldeinformationen**

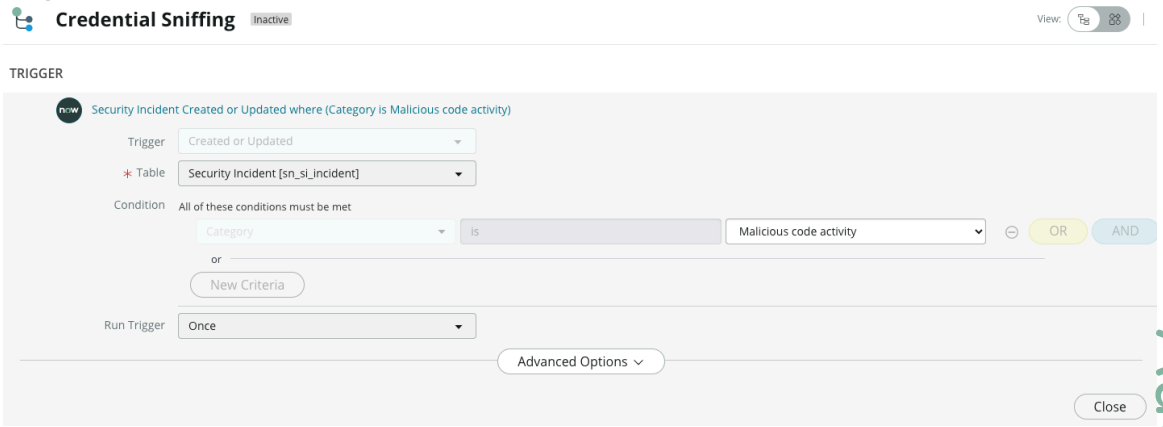
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieAktivität mit böswilligem Code**lautet.

**Auslöserbedingung für das Sniffing von Anmeldeinformationen für das Playbook**




### Verwenden Sie das Playbook Credential Sniffing

Verwenden Sie dieses Playbook, um einen Incident zu untersuchen, bei dem es um das Erfassen von Anmeldeinformationen geht, die über die Tabelle *sys_installation_exit* in einer ServiceNow-Instanz ausgeführt werden. Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Playbook zum Ausspionieren von Anmeldeinformationen verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, überprüfen Sie in Aktion 1 die folgenden Warnungsdetails.
   - Instanz
   - Sitzungs-ID
   - Transaktion-ID
   - _raw: Stellt das gesamte Skript bereit.

   Beispielskript:

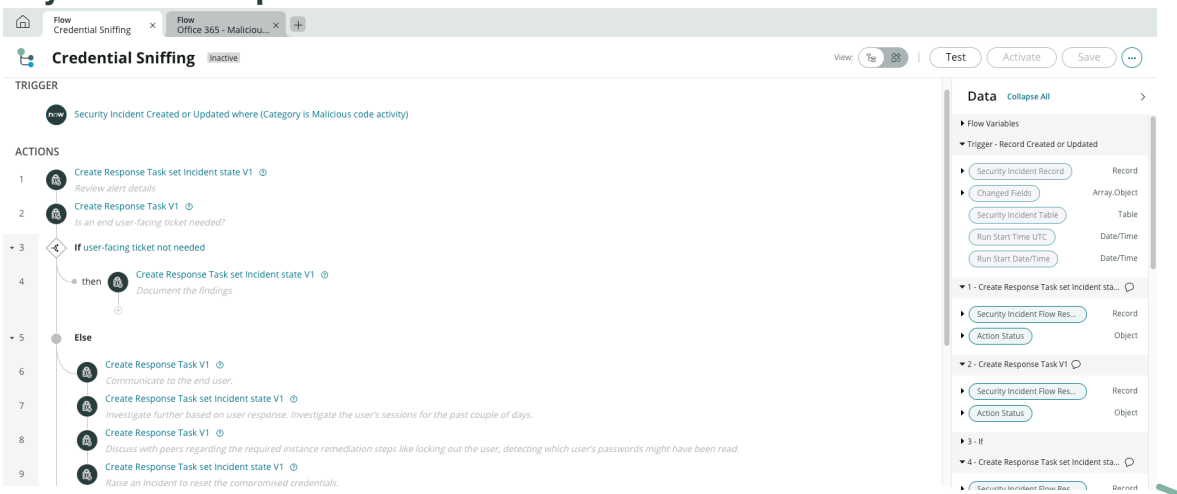
```
Var pass= request.getParameter(“user_password”);
Gs.log(pass);
```

2. Überprüfen Sie in Aktion 2 basierend auf den bisher erfassten Daten, ob für diese Warnung ein Endbenutzerticket erforderlich ist oder nicht.
3. Wenn in Aktion 3 für die Warnung kein Endbenutzerticket erforderlich ist, dokumentieren Sie in Aktion 4 die bisherigen Ergebnisse.
   Der Flow endet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook zum Ausspähen von Anmeldeinformationen**




4. Wenn für die Warnung in Aktion 5 ein Endbenutzerticket erforderlich ist, führen Sie die folgenden Schritte aus:

   a. Informieren Sie den Endbenutzer in Aktion 6, dass für die Warnung ein Endbenutzerticket erforderlich ist.

   b. Untersuchen Sie in Aktion 7 basierend auf der Antwort des Benutzers und den Sitzungen des Benutzers in den letzten Tagen weitere.

   c. Diskutieren Sie in Aktion 8 mit Kollegen über die Korrekturschritte für die Instanz, z. B. das Sperren des Benutzers und das Erkennen, ob die Passwörter des Benutzers gelesen wurden.

   d. Lösen Sie in Aktion 9 einen Incident oder ein Ticket aus, um die gefährdeten Benutzeranmeldeinformationen zurückzusetzen.

   e. Heben Sie in Aktion 10 die Eindämmung auf, und bringen Sie die Systeme wieder in den Betriebszustand Der Flow endet.

5. Schließen Sie in Aktion 11 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

### Playbook für T1070 – Windows-Ereignisprotokolle gelöscht

Dieses Playbook enthält Korrekturschritte zur Untersuchung von Incidents, die Ereignistypen nachverfolgen, bei denen der Benutzer Sicherheitsprotokolle entfernt. Wenn das Sicherheitsprotokoll gelöscht wird, werden die Events 517 und 1102 unabhängig vom Status der Audit System Event-Richtlinie protokolliert.

Diese Warnung kann die folgenden Arten von Events nachverfolgen:

- **Event 517**: Die Felder Primärer Benutzername und Client-Benutzername identifizieren den Benutzer, der das Protokoll gelöscht hat. Der primäre Benutzername entspricht dem System, und der Client-Benutzername gibt den Benutzer an, der das Protokoll gelöscht hat.
- **Event 1102**: Die Felder Account-Name und Domänenname identifizieren den Benutzer, der das Protokoll gelöscht hat. Mit der Anmelde-ID können Sie rückwärts mit dem Anmeldeereignis und anderen während derselben Anmeldesitzung protokollierten Ereignissen korrelieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie das Playbook „T1070 – Windows Events Logs Cleared“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „T1070 – Windows Event Logs Cleared“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

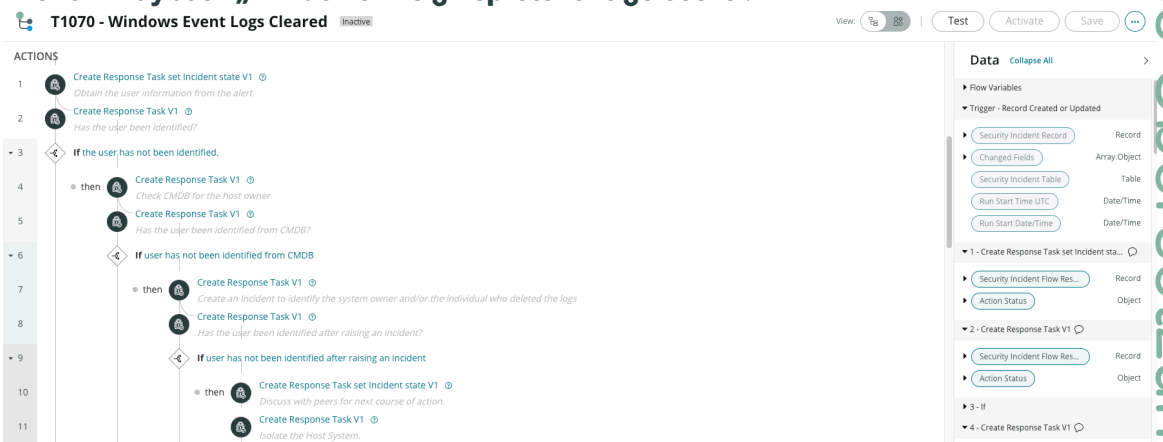
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook T1070 – Windows Events Logs Cleared (T1070 – Windows-Ereignisprotokolle gelöscht** ) aus.
3. Erstellen Sie eine Kopie des Playbook-Flows T1070 – Windows-Ereignisprotokolle gelöscht, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **T1070 – Playbook „Windows-Ereignisprotokolle gelöscht“.**

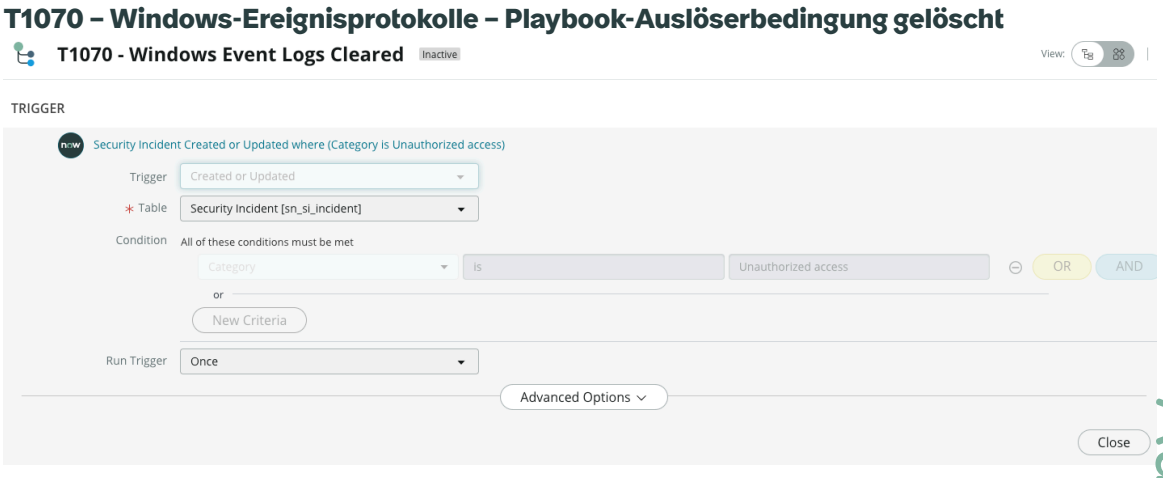
   
   

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieNicht autorisierter Zugriff**lautet.




### Verwenden Sie das Playbook T1070 – Windows Events Logs Cleared (T1070 – Windows-Ereignisprotokolle gelöscht).

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die Event-Typen nachverfolgen, bei denen der Benutzer Sicherheitsprotokolle entfernt. Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Playbook T1070 – Windows Events Logs Cleared (T1070 – Windows-Ereignisprotokolle gelöscht) verfügbar sind.

#### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

#### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, rufen Sie in Aktion 1 die Benutzerdetails aus der Warnung ab.
2. Überprüfen Sie in Aktion 2, ob der Benutzer identifiziert wurde.
3. Wenn der Benutzer in Aktion 3 nicht identifiziert wurde, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie in Aktion 4 die CMDB (Configuration Management Database) auf die Details des Hostbesitzers.

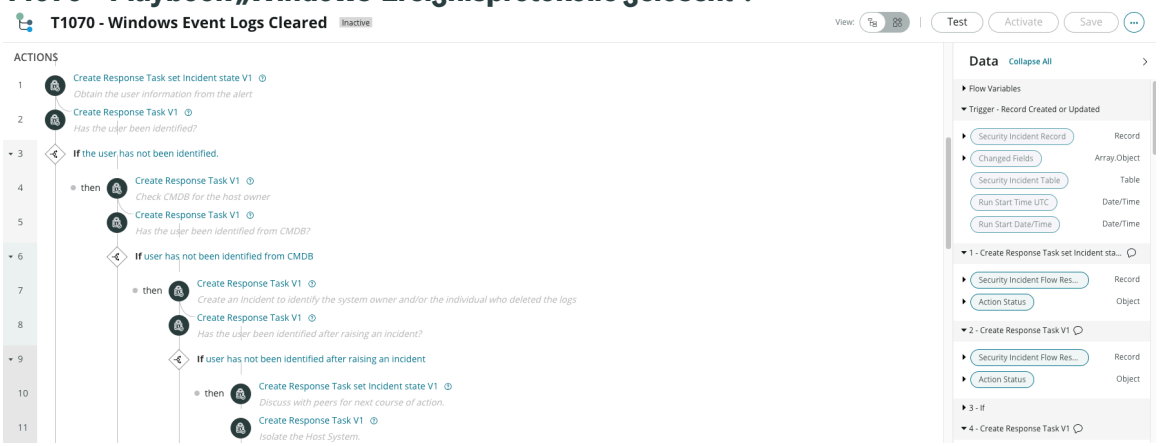
   b. Überprüfen Sie in Aktion 5, ob der Benutzer in der CMDB identifiziert wurde.

      Wenn der Benutzer in der CMDB identifiziert wurde, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**T1070 – Playbook „Windows-Ereignisprotokolle gelöscht“.**




**c.** Wenn der Benutzer in Aktion 6 nicht aus der CMDB identifiziert wurde, führen Sie die folgenden Schritte aus:

**i.** Erstellen Sie in Aktion 7 einen Incident, um den Systembesitzer und die Person zu identifizieren, die die Protokolle gelöscht hat.

**ii.** Überprüfen Sie in Aktion 8, ob der Benutzer nach dem Auslösen eines Incident identifiziert wurde oder nicht.

Wenn der Benutzer nach dem Auslösen eines Incident identifiziert wurde, wird in Aktion 8 eine manuelle Antwortaufgabe erstellt, und der Flow wird beendet.

**iii.** Wenn der Benutzer nach dem Auslösen eines Incidents nicht identifiziert wurde, führen Sie in Aktion 9 die folgenden Schritte aus:

**1.** Besprechen Sie in Aktion 10 die nächste Vorgehensweise mit Kollegen.

**2.** Isolieren Sie in Aktion 11 das Hostsystem.

**3.** Entfernen Sie in Aktion 12 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Konten.

**4.** Heben Sie in Aktion 13 die Eindämmung auf, und bringen Sie die Systeme wieder in den Betriebszustand.

**5.** Schließen Sie in Aktion 14 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

In Aktion 15 endet der Flow.

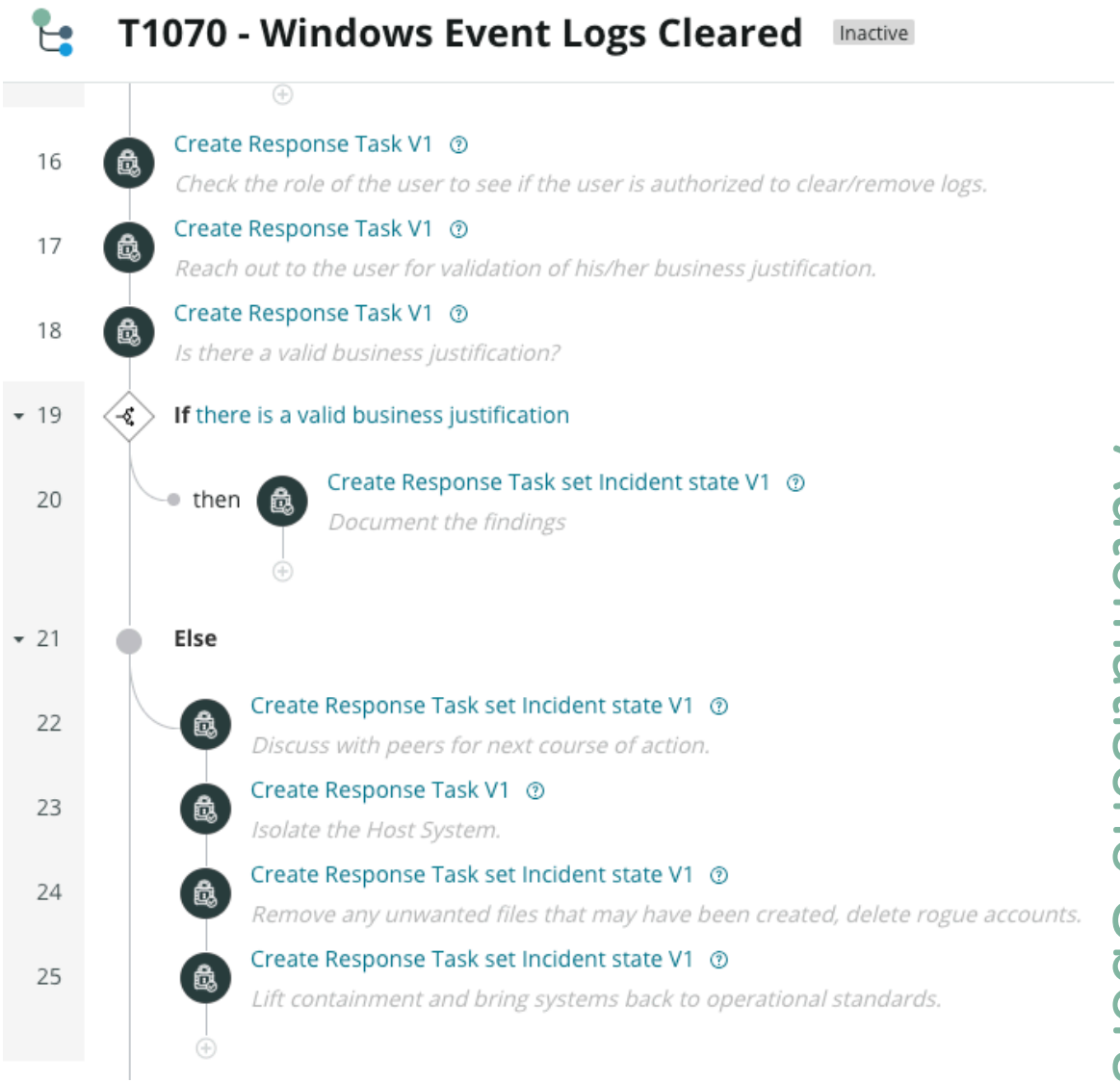
**4.** Wenn der Benutzer in Aktion 16 identifiziert wurde, überprüfen Sie die Rolle des Benutzers, um festzustellen, ob der Benutzer zum Löschen oder Entfernen von Protokollen berechtigt ist.

**5.** Wenden Sie sich in Aktion 17 an den Benutzer, um eine Validierung seiner geschäftlichen Begründung zu erhalten.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Benutzer zu kontaktieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Verwenden des Playbooks T1070 – Windows-Ereignisprotokolle gelöscht**






6. Überprüfen Sie in Aktion 18, ob eine gültige geschäftliche Begründung angegeben ist.
7. Wenn in Aktion 19 eine gültige geschäftliche Begründung angegeben wurde, dokumentieren Sie in Aktion 20 die bisherigen Ergebnisse.
   Der Flow endet.
8. Wenn in Aktion 21 keine gültige geschäftliche Begründung angegeben wurde, führen Sie die folgenden Schritte aus:

   a. Besprechen Sie in Aktion 22 die nächste Vorgehensweise mit Kollegen.

   b. Isolieren Sie in Aktion 23 das Hostsystem.

   c. Entfernen Sie in Aktion 24 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Konten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Heben Sie in Aktion 25 die Eindämmung auf, und bringen Sie die Systeme wieder in den Betriebszustand. Der Flow endet.

**9.** Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

### Playbook für OSquery der externen Adresse in der Datei /etc/hosts

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hinweisen, dass ein interner Hostname oder eine Domäne einer externen IP-Adresse im lokalen DNS (/etc/hosts) eines Linux-Servers zugewiesen wurde.

### Richten Sie die OSquery der externen Adresse im Playbook der Datei /etc/hosts ein

Führen Sie die folgenden Schritte aus, um die OSquery der externen Adresse im Playbook der Datei /etc/hosts einzurichten.

#### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

#### Prozedur

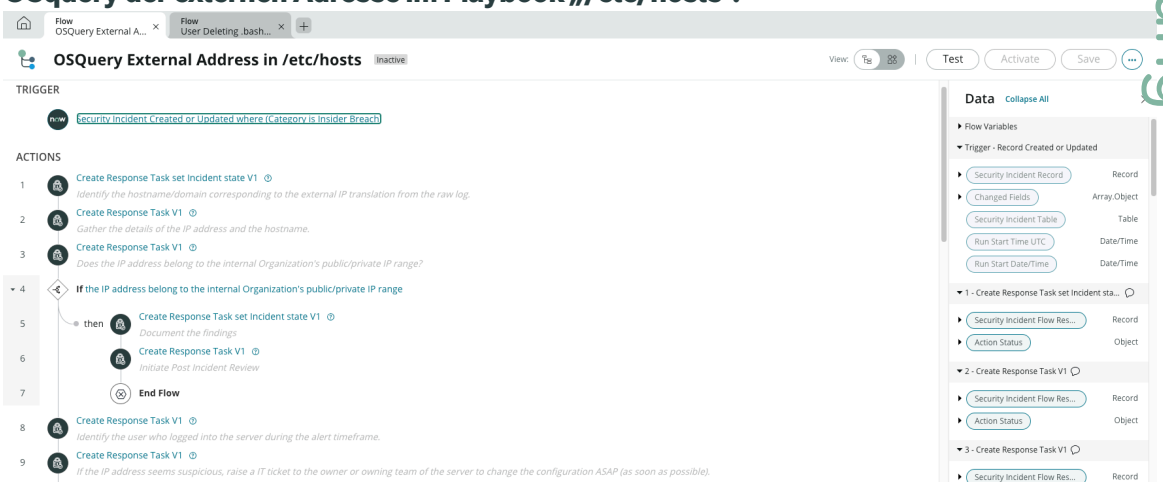
**1.** Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.

**2.** Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook OSquery External Address in / etc/hosts** aus.

**3.** Erstellen Sie eine Kopie der externen OSquery-Adresse im Playbook-Flow /etc/hosts, und nehmen Sie die erforderlichen Änderungen vor.

Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

**OSquery der externen Adresse im Playbook „/etc/hosts“.**




**4.** Aktivieren Sie die Playbooks.



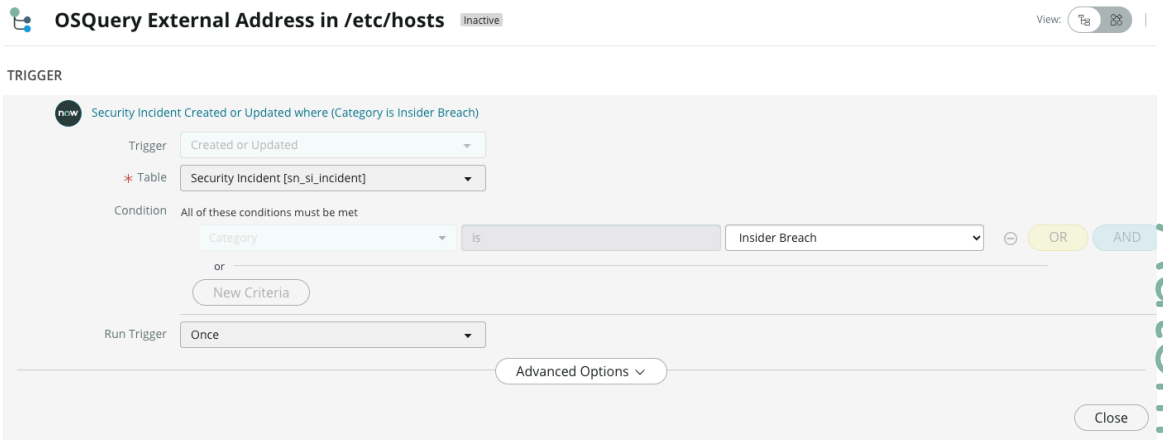
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.

**b.** Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieInsider-Verstoß**lautet.

**OSquery der externen Adresse in der Playbook-Auslöserbedingung „/etc/hosts“.**




## Verwenden Sie die OSquery of External Address im Playbook der Datei /etc/hosts

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, dass ein interner Hostname oder eine Domäne einer externen IP-Adresse im lokalen DNS (/etc/hosts) eines Linux-Servers zugewiesen wurde. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die in der OSquery der externen Adresse im Playbook der Datei /etc/hosts verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

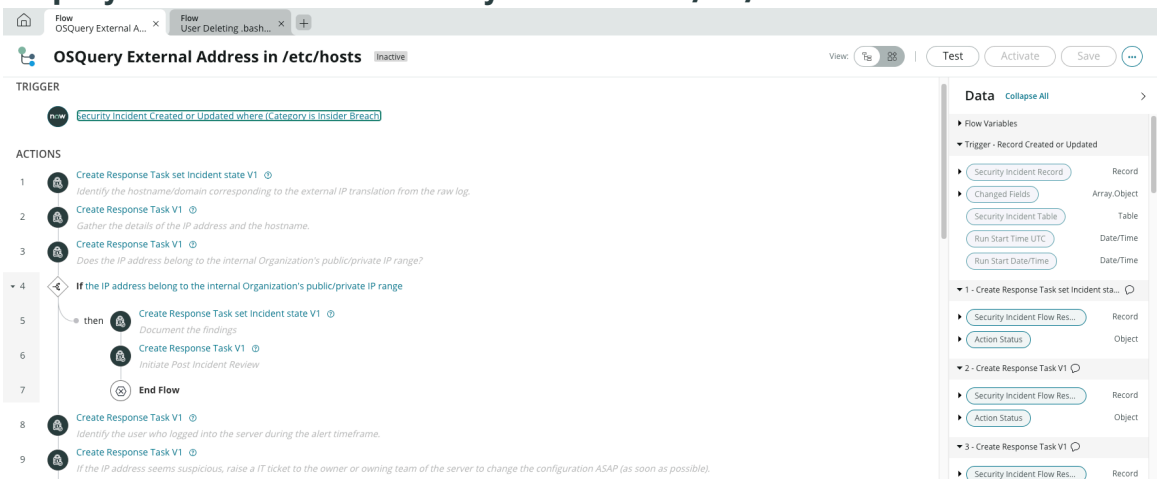
### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, identifizieren Sie in Aktion 1 den Hostnamen oder Domänennamen, der der externen IP-Übersetzung entspricht, aus dem Rohprotokoll.
2. Erfassen Sie in Aktion 2 die Details der IP-Adresse und des Hostnamens.
3. Überprüfen Sie in Aktion 3, ob diese IP-Adresse zum öffentlichen/privaten IP-Bereich der internen Organisation gehört oder nicht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### OSquery der externen Adresse im Playbook der Datei /etc/hosts




4. Wenn die IP-Adresse in Aktion 4 zum öffentlichen/privaten IP-Bereich der internen Organisation gehört, führen Sie die folgenden Schritte aus:

   a. Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 6 eine Überprüfung nach Incidents.
   In Aktion 7 endet der Flow nach der Überprüfung nach Incidents.

5. Wenn die IP-Adresse nicht zum öffentlichen/privaten IP-Bereich der internen Organisation gehört, identifizieren Sie in Aktion 8 den Benutzer, der sich während des Warnungszeitrahmens beim Server angemeldet hat.
6. Wenn die IP-Adresse in Aktion 9 verdächtig erscheint, erstellen Sie ein IT-Ticket beim Besitzer oder beim Team des Servers, um die Konfiguration so bald wie möglich zu ändern.
7. Überprüfen Sie in Aktion 10, ob vor und nach dem Hinzufügen des DNS-Eintrags schädliche Aktivitäten auf dem Server aufgetreten sind.
8. Überprüfen Sie in Aktion 11 auf Verbindungen des Servers mit der externen IP-Adresse.
9. Dokumentieren Sie in Aktion 12 die bisherigen Ergebnisse.
10. Überprüfen Sie in Aktion 13, ob die Besitzer- oder Teaminformationen verfügbar sind.
11. Wenn in Aktion 14 die Besitzer- oder Teaminformationen verfügbar sind, führen Sie die folgenden Schritte aus:

    a. Wenden Sie sich in Aktion 15 an den Besitzer oder das Team des Servers, um zu erfahren, ob sie die Aktivität erkennen.
    Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Besitzer oder das Team des Servers zu kontaktieren.

    b. Überprüfen Sie in Aktion 16, ob der Besitzer oder das Team eine gültige geschäftliche Begründung angegeben hat.

    c. Wenn der Besitzer oder das Team in Aktion 17 keine gültige geschäftliche Begründung angegeben hat, wird der Flow beendet.
    Wenn der Besitzer oder das Team jedoch eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:



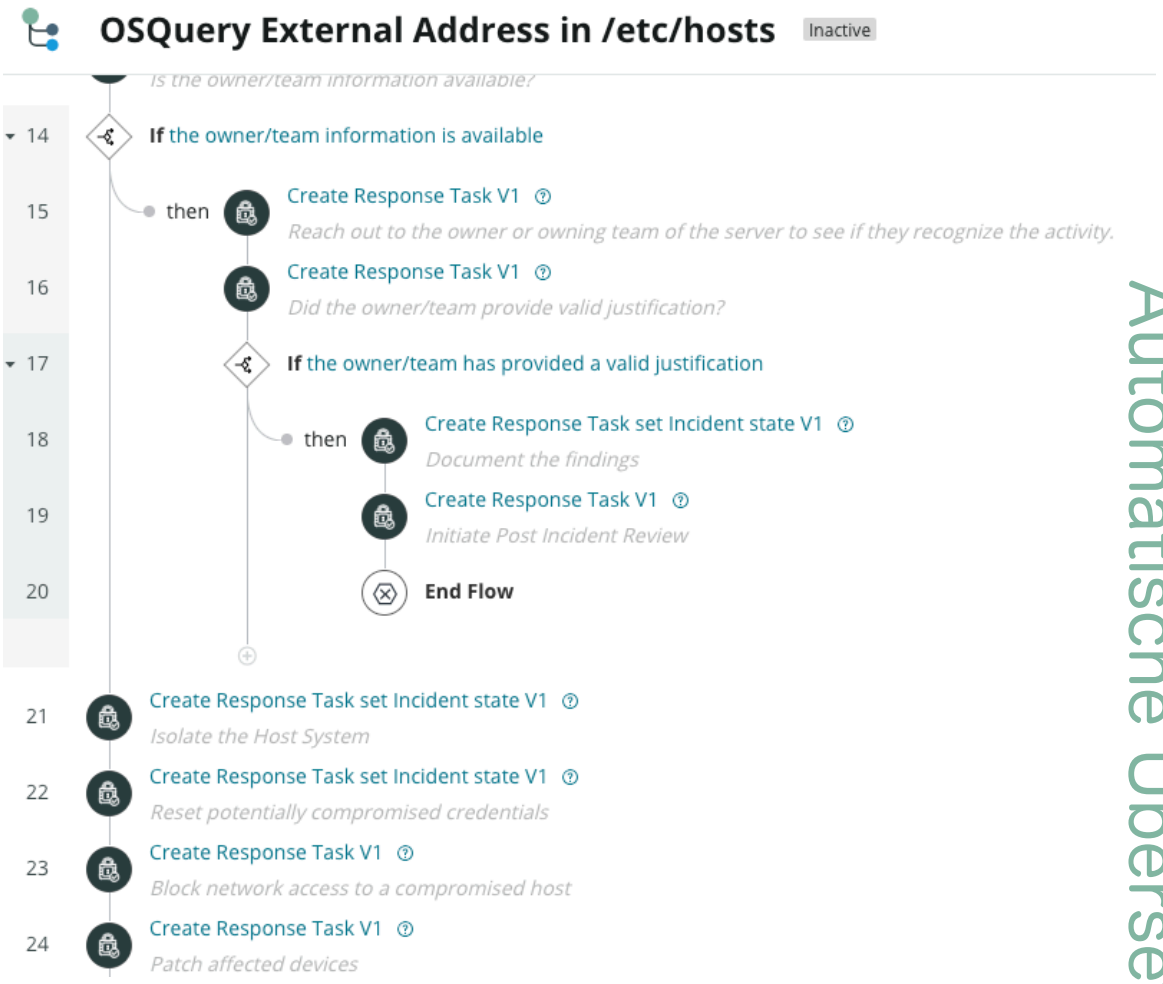
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Dokumentieren Sie in Aktion 18 die bisherigen Ergebnisse.

ii. Initiieren Sie in Aktion 19 eine Überprüfung nach Incidents.

In Aktion 20 endet der Flow nach der Überprüfung nach dem Incident.

**Verwenden der OSquery of External Address in /etc/hosts-Datei-Playbook**




**12.** Wenn in Aktion 21 keine Besitzer- oder Teaminformationen verfügbar sind, isolieren Sie das Hostsystem.

**13.** Setzen Sie in Aktion 22 die potenziell gefährdeten Anmeldeinformationen zurück.

**14.** Blockieren Sie in Aktion 23 den Netzwerkzugriff auf den gefährdeten Host.

**15.** Patchen Sie in Aktion 24 die betroffenen Geräte.

**16.** In Aktion 25 heben Sie das Containment auf und bringen die Systeme wieder in den Betriebszustand.

**17.** Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

### Playbook zum Löschen des Bash-Verlaufs durch Anwender – Cloud

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hinweisen, ob jemand versucht hat, die Bash-Verlaufsdatei (`.bash_history`) von einem Linux-Server zu entfernen.

**Hinweis:**
Sie müssen diese Warnung vorsichtig entschärfen, da sie selten ausgelöst wird und möglicherweise auf eine interne Bedrohung hinweist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie das Playbook „User Deleting Bash History“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „User Deleting Bash History“ (Benutzer löscht Bash-Verlauf) einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

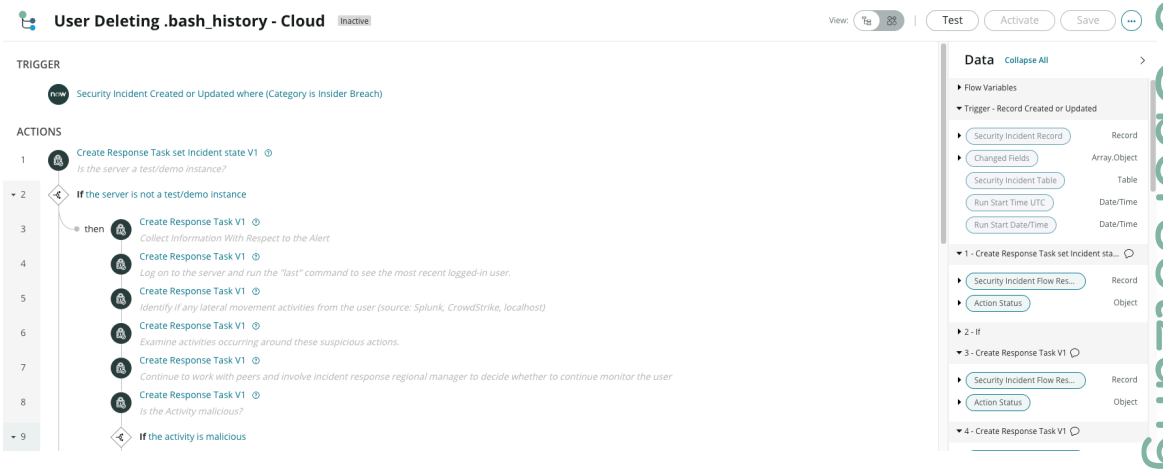
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **User Deleting .bash_history - Cloud aus**.
3. Erstellen Sie eine Kopie des Playbook-Flows „User Deleting .bash_history - Cloud“ (Benutzer löschen .bash_history – Cloud), und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **Anwender löscht Bash-Verlauf – Cloud-Playbook**

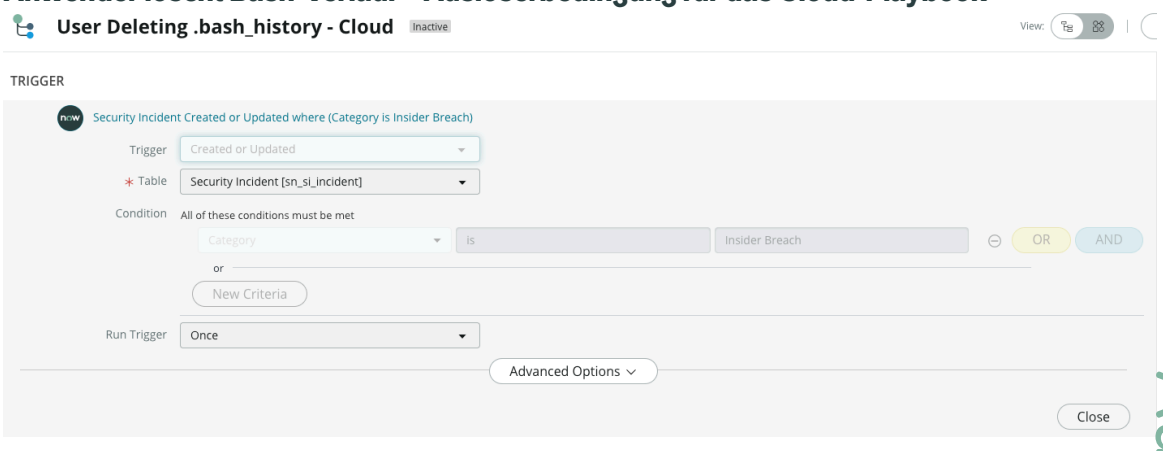
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieInsider-Verstoß**lautet.

**Anwender löscht Bash-Verlauf – Auslöserbedingung für das Cloud-Playbook**




### Verwenden Sie das Playbook „Benutzer löscht Bash-Verlauf“.

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, dass jemand versucht hat, die Bash-Verlaufsdatei von einem Linux-Server zu entfernen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook User Deleting the Bash History (`.bash_history`) verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, überprüfen Sie in Aktion 1, ob der Server eine Test- oder Demo-Instanz ist.
2. Wenn der Server in Aktion 2 keine Test- oder Demoinstanz ist, führen Sie die folgenden Schritte aus:

   a. Erfassen Sie in Aktion 3 die folgenden Informationen für die Warnung:
      - Benutzername
      - IP-Adresse
      - Böswillige Befehle, die versuchen, den Bash-Verlauf zu löschen
      - Alle vom Benutzer ausgeführten Befehle, sofern in den CrowdStrike-Protokollen verfügbar.

   b. Melden Sie sich in Aktion 4 beim Server an, und führen Sie den `letzten` Befehl aus, um den zuletzt angemeldeten Benutzer anzuzeigen.

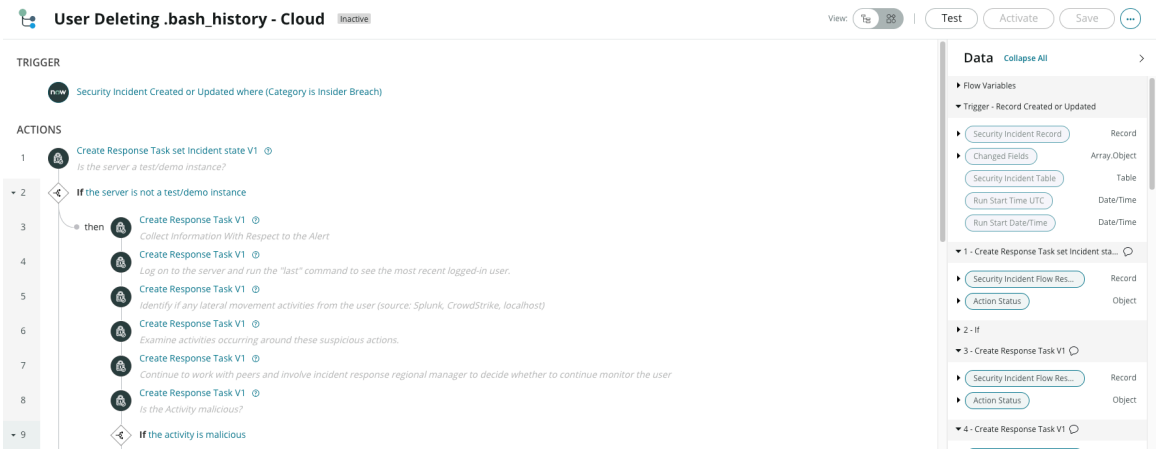
   c. Identifizieren Sie in Aktion 5, ob der Benutzer Aktivitäten im Rahmen der Seitenbewegung durchgeführt hat (Quelle: Splunk, CrowdStrike, localhost).

   d. Untersuchen Sie in Aktion 6 die Aktivitäten, die im Zusammenhang mit diesen verdächtigen Aktionen auftreten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook „Benutzer löscht Bash-Verlauf“.**




**e.** Setzen Sie in Aktion 7 die Zusammenarbeit mit Kollegen fort, und beziehen Sie den Regional Manager für Incident-Antwort in die Entscheidung ein, ob der Benutzer weiterhin überwacht werden soll.

**f.** Bestimmen Sie in Aktion 8, ob die Aktivität schädlich ist oder nicht.

**g.** Wenn die Aktivität in Aktion 9 schädlich ist, führen Sie die folgenden Schritte aus:

**i.** Wenden Sie sich in Aktion 10 während der Untersuchung an den IT-Support, und fordern Sie eine Kontosperre an.

**ii.** Stellen Sie in Aktion 11 sicher, dass die Instanz in einen normalen Zustand ohne schädliche Aktivitäten zurückgesetzt wird.

**iii.** Heben Sie in Aktion 12 das Containment auf und bringen Sie die Systeme wieder in den Betriebszustand.

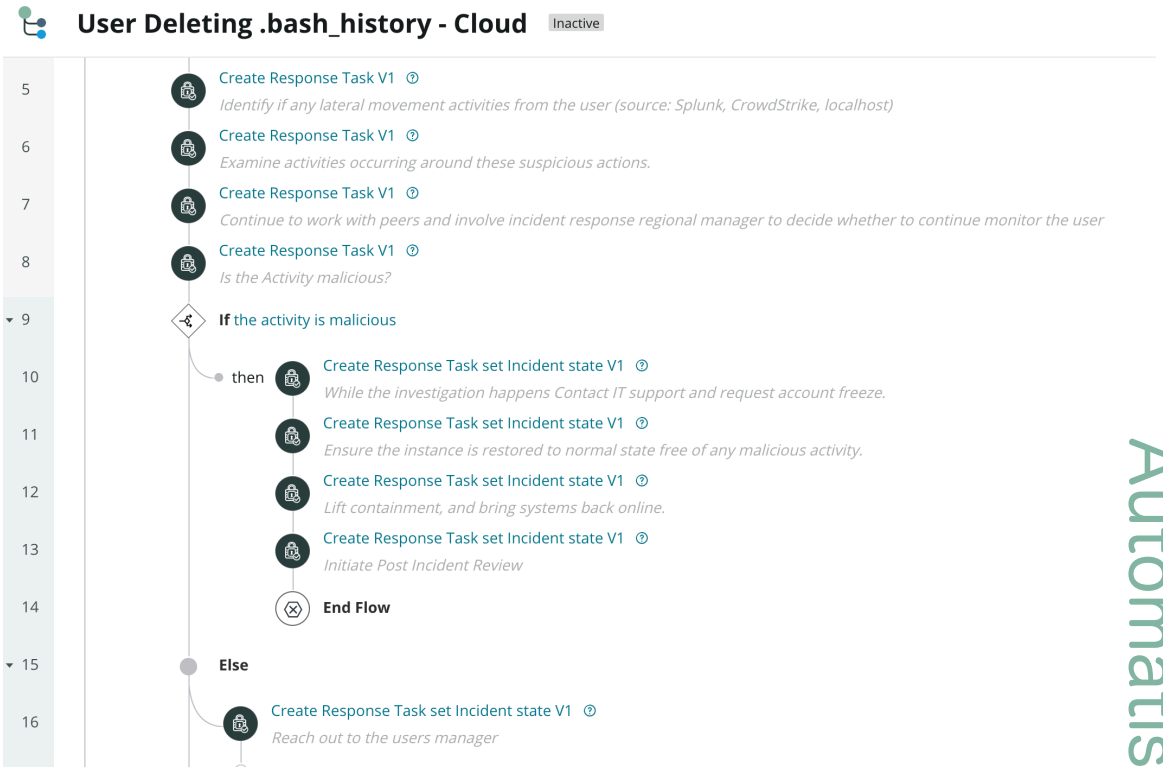
**iv.** Initiieren Sie in Aktion 13 eine Überprüfung nach Incidents.

In Aktion 14 endet der Flow nach der Überprüfung nach dem Incident.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Verwenden des Playbooks „User Deleting Bash History“ (Benutzer löscht Bash-Verlauf).**




**h.** Wenn die Aktivität in Aktion 15 nicht schädlich ist, wenden Sie sich in Aktion 16 an den Vorgesetzten des Benutzers.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Vorgesetzten des Benutzers zu kontaktieren und ihn über den empfohlenen Ansatz zu informieren.

**3.** Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.

**4.** Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

## Playbook für erfolgreiche VPN-Versuche über die Servicekonten – Unternehmen/Cloud

Dieses Playbook enthielt systematische Korrekturschritte zur Untersuchung von Incidents, die erfolgreiche Anmeldeversuche von Servicekonten über VPN nachverfolgen. Servicekonten dürfen keine Anmeldeereignisse von einem VPN aufweisen, und solche Ereignisse können Indikatoren für Brute-Force oder eine mögliche Offenlegung der Anmeldeinformationen des Kontos sein.

### Richten Sie das Playbook „Successful VPN Attempts“ (Erfolgreiche VPN-Versuche) über das Servicekonten-Playbook ein

Führen Sie die folgenden Schritte aus, um die erfolgreichen VPN-Versuche aus dem Playbook „Servicekonten“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.



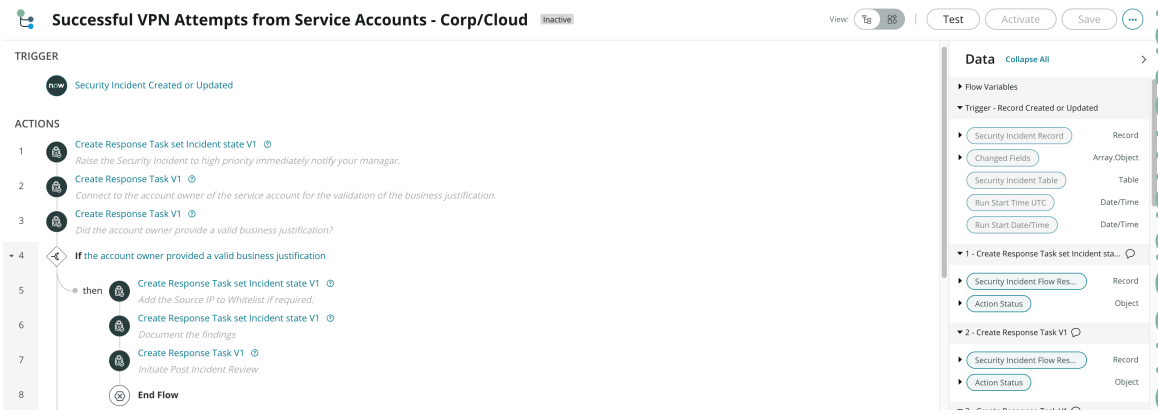
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie im Playbook „ **Servicekonten“ die Option „Successful VPN Attempts“ (Erfolgreiche VPN-Versuche) aus**.
3. Erstellen Sie eine Kopie der erfolgreichen VPN-Versuche aus dem Playbook-Flow „Servicekonten“, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

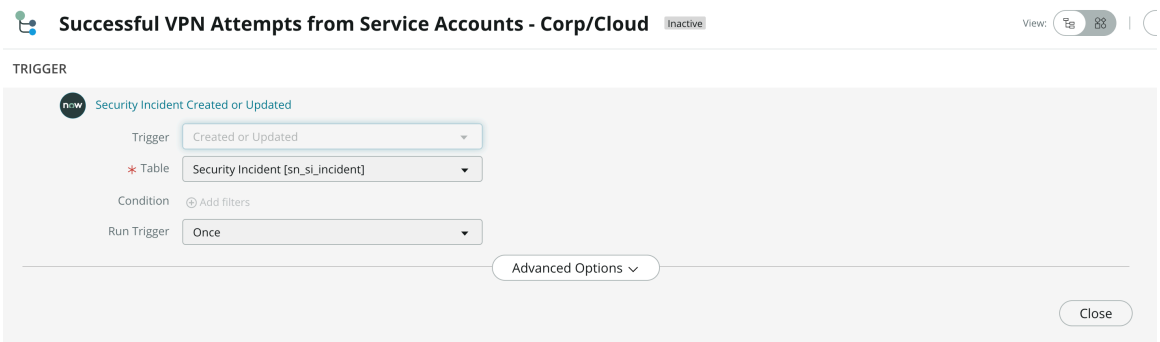
**Erfolgreiche VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/ Cloud“.**




4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird.

   Zum Beispiel, wenn die **Kategorie„Innerer Verstoß“**ist.

**Erfolgreiche VPN-Versuche aus der Playbook-Auslöserbedingung „Servicekonten – Unternehmen/Cloud“.**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden Sie „Successful VPN Attempts“ (Erfolgreiche VPN-Versuche) aus dem Playbook „Servicekonten“.

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die erfolgreiche Anmeldeversuche von Servicekonten über VPN nachverfolgen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Successful VPN Attempts from the Service Accounts“ (Successful VPN Attempts from the Service Accounts) verfügbar sind.

## Vorbereitungen

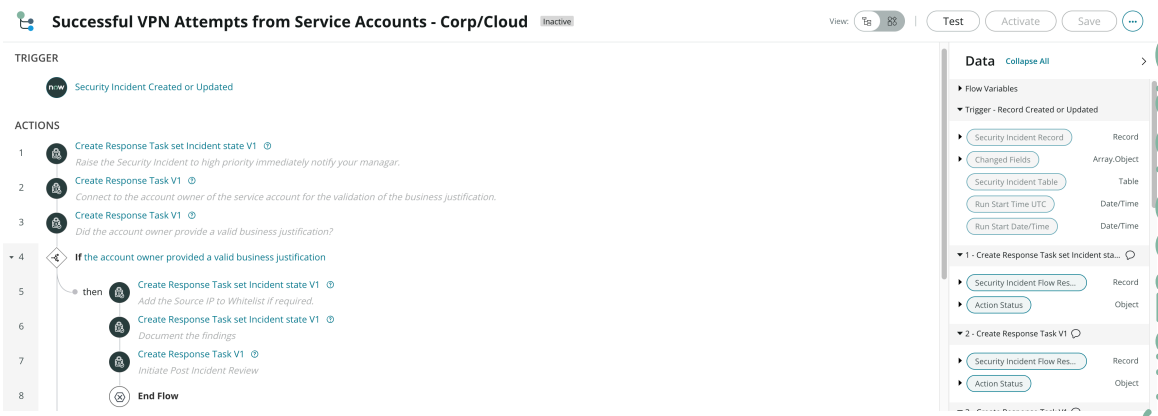
Erforderliche Rolle:

- sn_si.admin
- flow_designer

## Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, erhöhen Sie in Aktion 1 den Security Incident auf eine hohe Priorität, und benachrichtigen Sie sofort Ihren Vorgesetzten.
2. Wenden Sie sich in Aktion 2 an den Besitzer des Service-Accounts, um die geschäftliche Begründung zu validieren.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um sich an den Besitzer des Service-Accounts zu wenden und die geschäftliche Begründung zu validieren.
3. Überprüfen Sie in Aktion 3, ob der Service-Account-Besitzer eine gültige geschäftliche Begründung angegeben hat.

**Erfolgreiche VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/Cloud“.**




4. Wenn der Besitzer des Servicekontos eine gültige geschäftliche Begründung angegeben hat, führen Sie in Aktion 4 die folgenden Schritte aus:

   a. Fügen Sie in Aktion 5 die Quell-IP der Allow-Liste hinzu, falls erforderlich.

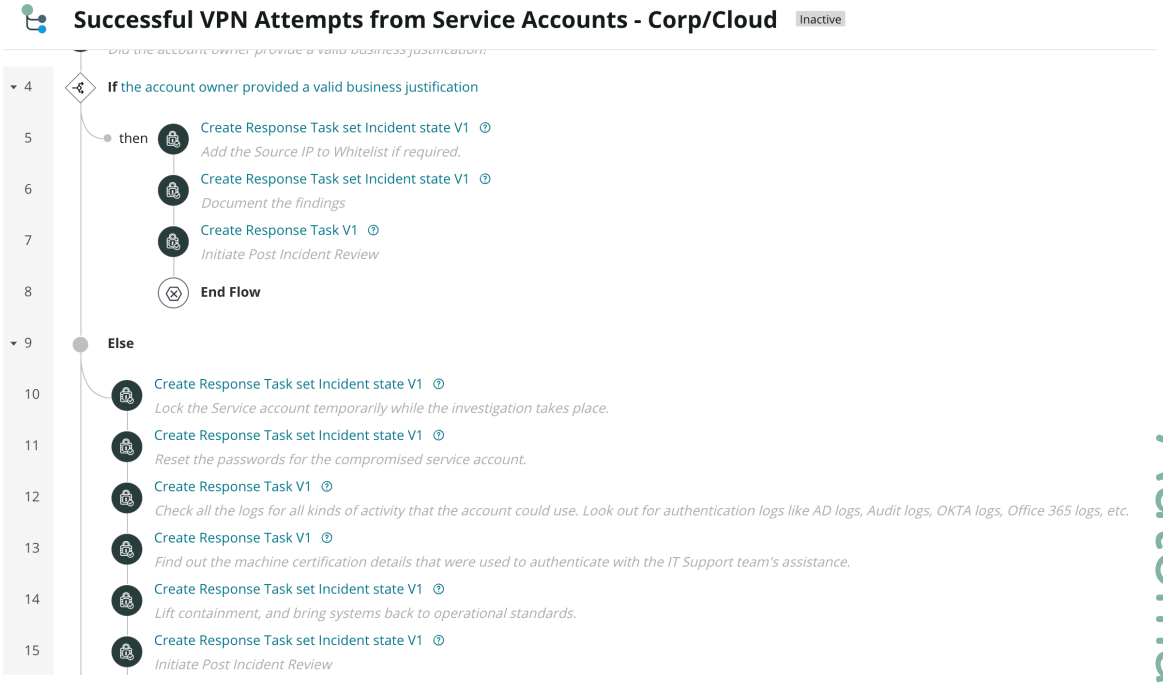
   b. Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

   c. Initiieren Sie in Aktion 7 eine Überprüfung nach Incidents.
      In Aktion 8 endet der Flow nach der Überprüfung nach Incidents.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Verwenden der erfolgreichen VPN-Versuche aus dem Playbook „Servicekonten – Unternehmen/Cloud“.**




5. Wenn der Besitzer des Servicekontos in Aktion 9 keine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

   a. Sperren Sie in Aktion 10 das Servicekonto während der Untersuchung vorübergehend.

   b. Setzen Sie in Aktion 11 die Passwörter für das gefährdete Servicekonto zurück.

   c. Überprüfen Sie in Aktion 12 die Protokolle auf alle Arten von Aktivitäten, die der Account verwenden könnte.
   Achten Sie auf Authentifizierungsprotokolle wie Active Directory-Protokolle, Audit-Protokolle, Okta-Protokolle, Office 365-Protokolle usw.

   d. Suchen Sie in Aktion 13 nach den Computer-Zertifizierungsdetails, die zur Authentifizierung mit Unterstützung des IT-Supportteams verwendet werden.

   e. Heben Sie in Aktion 14 das Containment auf und bringen Sie die Systeme wieder in den Betriebszustand.

   f. Schließen Sie in Aktion 15 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

### Playbook für versuchten Zugriff auf deaktivierte Accounts

Dieses Playbook wird ausgelöst, wenn ein Mitarbeiter, dessen Konto gekündigt, deaktiviert oder getrennt wurde, versucht, sich mit seinen Anmeldeinformationen anzumelden. Der Identitätsstatus des Benutzers in Sail Point wird im Allgemeinen am Kündigungsdatum auf „Deaktiviert“ aktualisiert.

30 Tage ab dem Kündigungsdatum ist der ideale Zeitpunkt, um in einen getrennten Status aktualisiert zu werden. Sie können Geschäftslogik in Sail Point verwenden, um die RSA-Konten zu löschen und die Active Directory (AD)-Gruppenmitgliedschaften nach 30 Tagen zu entfernen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie das Playbook „Zugriffsversuche deaktivierter Account“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Zugriffsversuche deaktivierter Account“ einzurichten.

**Vorbereitungen**
Erforderliche Rolle:

- sn_si.admin
- flow_designer

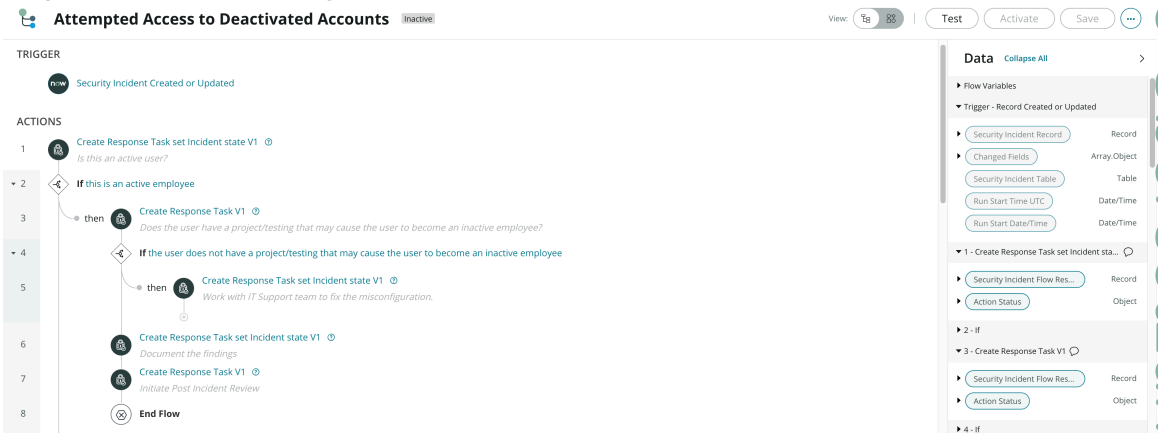
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

**Prozedur**

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Zugriffsversuch deaktiviertes Konto** “ aus.
3. Erstellen Sie eine Kopie des Playbook-Flows für Zugriffsversuche mit deaktiviertem Account, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **Playbook „Versuchter Zugriff auf deaktivierte Accounts“**

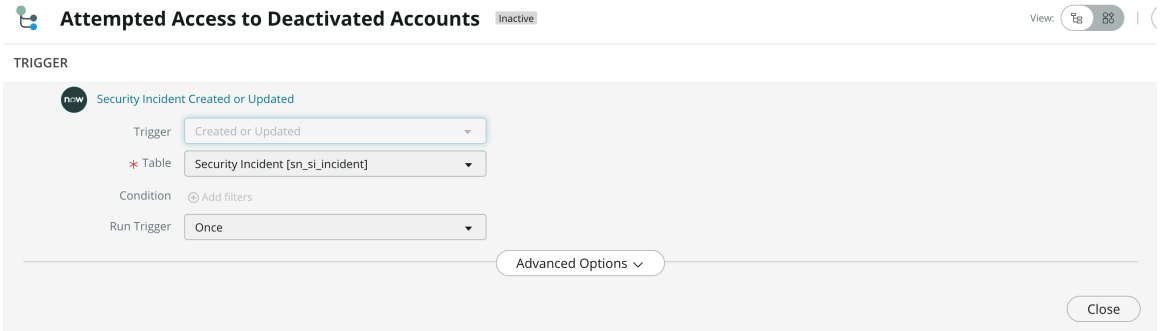
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. **Auslöserbedingung**: Dieses Playbook wird ausgelöst, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Beispiel, wenn die **Kategorie„Innerer Verstoß“**ist

**Auslöserbedingung für Playbook „Versuchter Zugriff auf deaktivierte Accounts“.**




### Verwenden Sie das Playbook „Zugriff auf deaktivierte Konten versucht“.

Verwenden Sie dieses Playbook, wenn ein Mitarbeiter, dessen Konto gekündigt, deaktiviert oder getrennt wurde, versucht, sich mit seinen Anmeldeinformationen anzumelden. Die folgenden Schritte geben Ihnen eine Vorstellung der Aktionen, Aufgaben und Subflows, die im Playbook „Zugriff auf deaktivierte Accounts“ verfügbar sind.

### Vorbereitungen

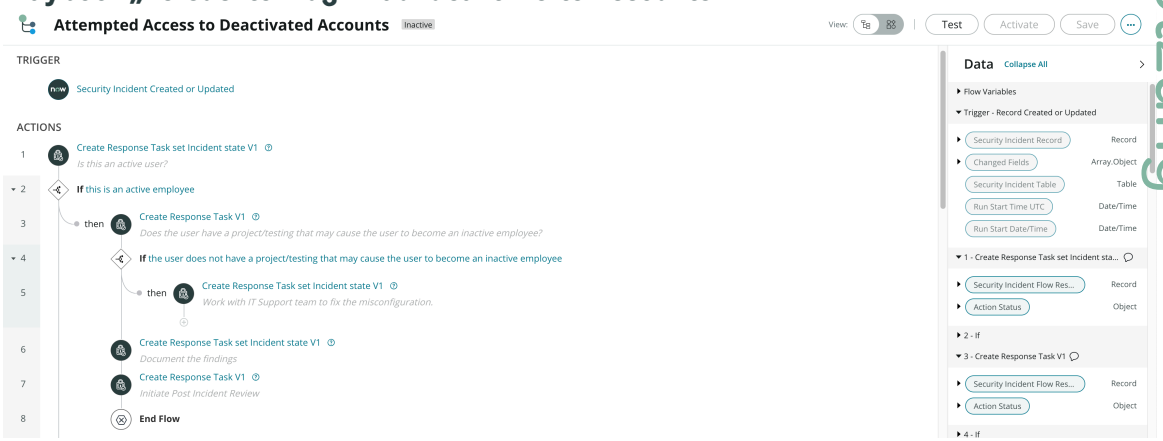
Erforderliche Rolle:

- sn_si.admin
- flow_designer

### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, überprüfen Sie in Aktion 1, ob der versuchte Zugriff auf die deaktivierten Konten von einem aktiven Benutzer durchgeführt wurde.
2. Überprüfen Sie in Aktion 2, ob der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Mitarbeiter durchgeführt wurde.

**Playbook „Versuchter Zugriff auf deaktivierte Accounts“**




3. Wenn der Zugriff auf die deaktivierten Accounts von einem aktiven Mitarbeiter versucht wurde, führen Sie die folgenden Schritte aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Überprüfen Sie in Aktion 3, ob der Benutzer ein Projekt oder einen Testfall hatte, der dazu geführt hat, dass der Benutzer ein inaktiver Mitarbeiter wurde.

**b.** Wenn der Benutzer in Aktion 4 kein Projekt oder keinen Testfall hatte, der dazu geführt hat, dass der Benutzer ein inaktiver Mitarbeiter wurde, arbeiten Sie mit dem IT-Supportteam zusammen, um die Fehlkonfiguration zu beheben.
Der Flow endet.

**c.** Wenn der Benutzer in Aktion 5 ein Projekt oder einen Testfall hatte, der dazu geführt hat, dass der Benutzer ein inaktiver Mitarbeiter wurde, führen Sie die folgenden Schritte aus:

**i.** Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

**ii.** Initiieren Sie in Aktion 7 eine Überprüfung nach Incidents.

In Aktion 8 endet der Flow nach der Überprüfung nach Incidents.

**4.** Wenn der Zugriffsversuch auf den deaktivierten Account nicht von einem aktiven Mitarbeiter durchgeführt wurde, führen Sie in Aktion 9 die folgenden Schritte aus:

**a.** Überprüfen Sie in Aktion 10, ob sich der Benutzer erfolgreich angemeldet hat.

**b.** Überprüfen Sie in Aktion 11, wann für den Mitarbeiter ein Offboarding durchgeführt wurde.

**c.** Untersuchen Sie in Aktion 12 die Events in Splunk, um die Aktivitäten des Benutzers während des Zeitraums zu untersuchen.

**d.** Ermitteln Sie in Aktion 13 basierend auf der bisherigen Untersuchung, ob der Benutzer Daten exfiltriert hat.

**e.** Wenn der Benutzer in Aktion 14 keine Daten extrahiert hat, führen Sie die folgenden Schritte aus:

**i.** In Aktion 15: Arbeiten Sie mit dem IT-Supportteam zusammen, um alle aktiven Sitzungen zu beenden und die Konten zu deaktivieren.

**ii.** Dokumentieren Sie in Aktion 16 die bisherigen Ergebnisse.

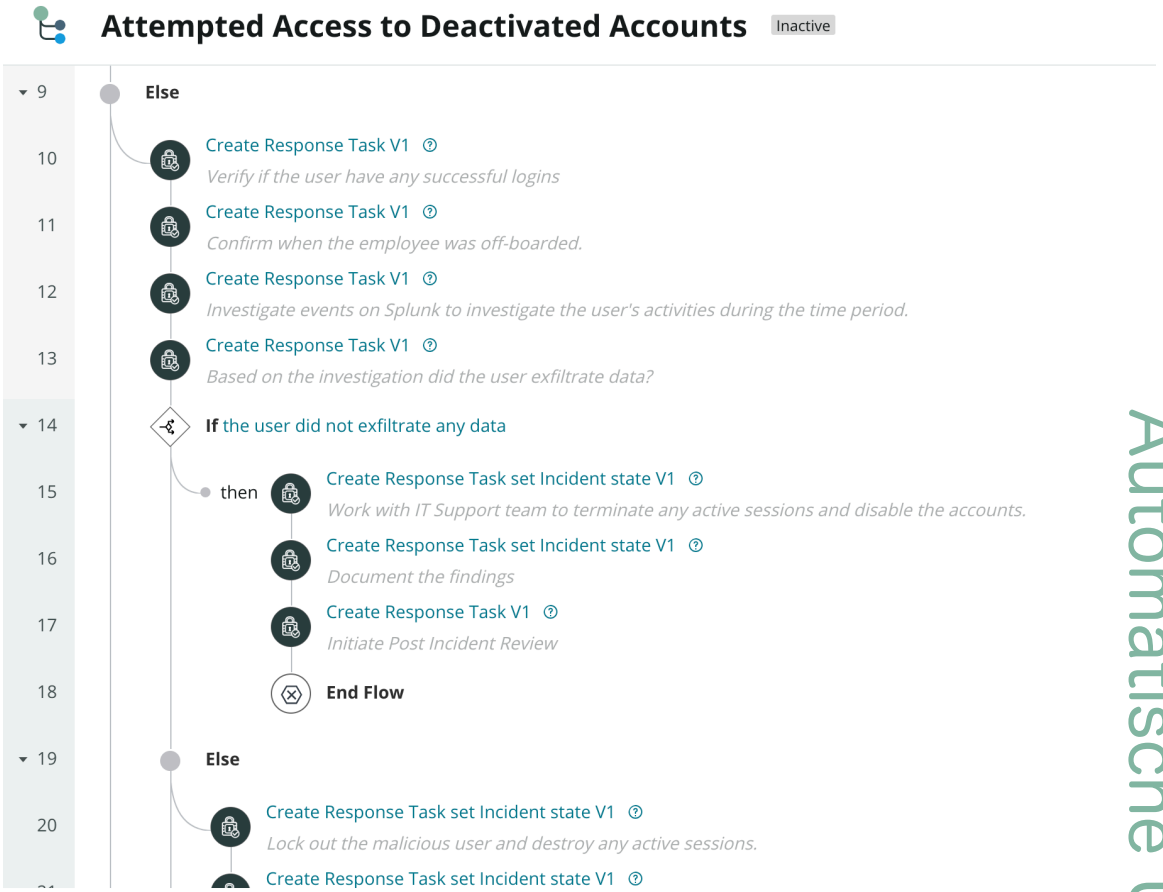
**iii.** Initiieren Sie in Aktion 17 eine Überprüfung nach Incidents.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Aktion 18 endet der Flow nach der Überprüfung nach dem Incident.

**Verwenden des Playbooks „Zugriff auf deaktivierte Konten“**




**5.** Wenn der Benutzer in Aktion 19 Daten exfiltriert hat, führen Sie die folgenden Schritte aus:

**a.** Sperren Sie in Aktion 20 den böswilligen Benutzer aus, und löschen Sie alle aktiven Sitzungen.

**b.** Arbeiten Sie in Aktion 21 mit dem IT-Supportteam zusammen, um alle Konten zu deaktivieren.

**c.** Stellen Sie in Aktion 22 sicher, dass die Ressourcen in den Normalzustand zurückversetzt und frei von böswilligen Aktivitäten sind.
Sie können bei Bedarf ein neues Image der Ressourcen erstellen.

**d.** In Aktion 23 heben Sie das Containment auf und bringen die Systeme wieder in den Betriebszustand.

**e.** Schließen Sie in Aktion 24 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

### Playbook für T1003 – Defence Evasion – Mimikatz DCShadow

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, bei denen der Verdacht besteht, dass sie durch Mimikatz DCShadow verursacht werden. DCShadow ist eine Funktion in Mimikatz, die das Verhalten eines Domänencontrollers (eines Servers, der Active Directory steuert) simuliert, um eigene Daten einzufügen und die meisten standardmäßigen Sicherheitskontrollen (einschließlich SIEMs) zu umgehen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mimikatz DCShadow hilft dem Angreifer, einen nicht autorisierten Domänencontroller (DC) einzurichten, der Teil des Active Directory (AD) wird. Nach der Registrierung kann er als rechtmäßiger DC fungieren und Schaden anrichten.

### Richten Sie das T1003 – Defence Evasion – Mimikatz DCShadow-Playbook ein

Führen Sie die folgenden Schritte aus, um das T1003 – Defence Evasion – Mimikatz DCShadow-Playbook einzurichten.

#### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

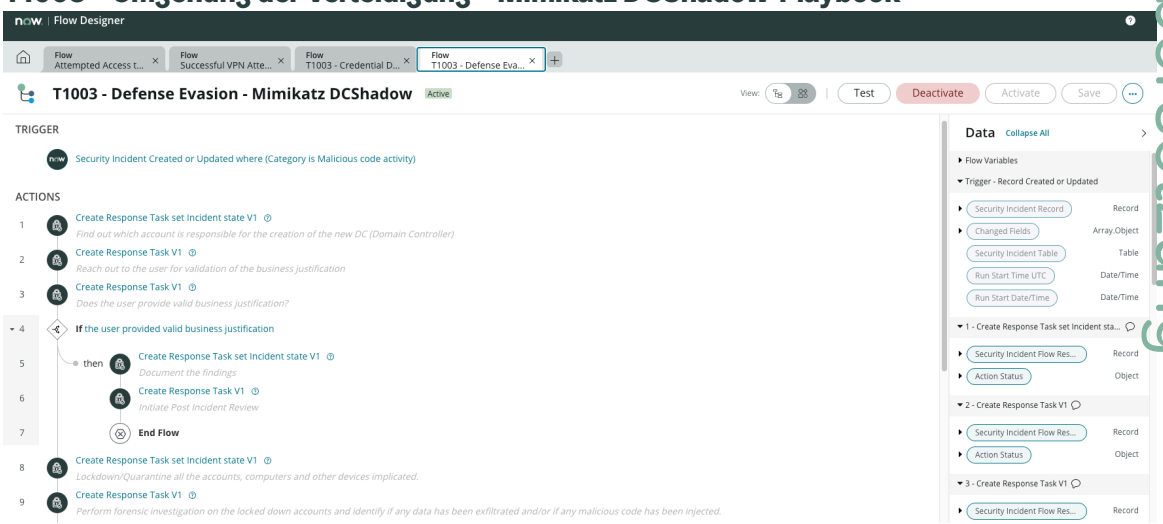
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

#### Prozedur

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook T1003 – Defence Evasion – Mimikatz DCShadow aus**.
3. Erstellen Sie eine Kopie des Playbook-Flows T1003 – Defence Evasion – Mimikatz DCShadow, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **T1003 – Umgehung der Verteidigung – Mimikatz DCShadow-Playbook**

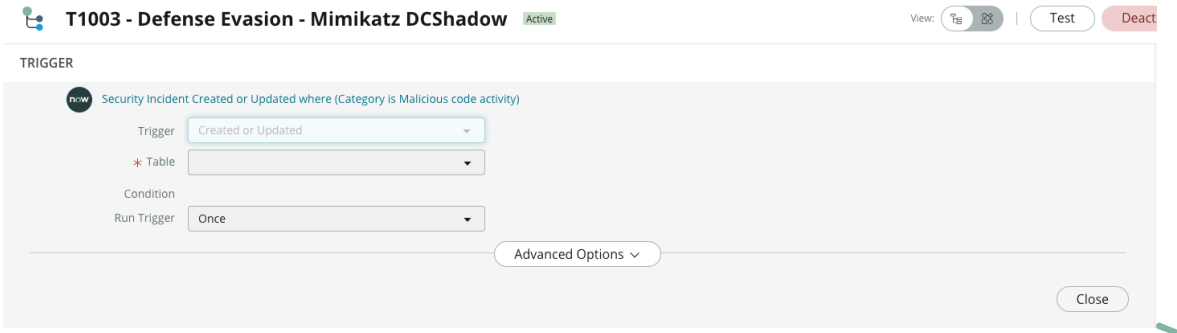
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieAktivität mit böswilligem Code**lautet.

**T1003 – Umgehung der Verteidigung – Mimikatz DCShadow-Playbook-Auslöserbedingung**




### Verwenden Sie das Playbook T1003 – Defence Evasion – Mimikatz DCShadow

Verwenden Sie dieses Playbook, um Security Incidents zu untersuchen, bei denen der Verdacht besteht, dass sie durch Mimikatz DCShadow verursacht werden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Defence Evasion – Mimikatz DCShadow verfügbar sind.

#### Vorbereitungen

Erforderliche Rolle:

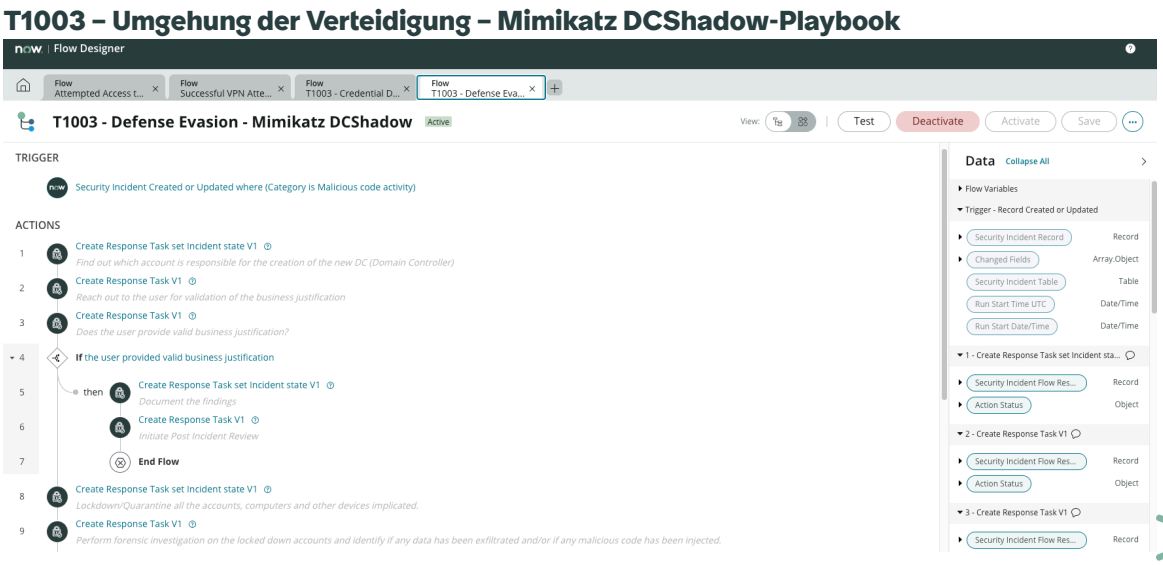
- sn_si.admin
- flow_designer

#### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, ermitteln Sie in Aktion 1, welches Konto für die Erstellung des neuen Domänencontrollers (DC) verantwortlich ist.
2. Wenden Sie sich in Aktion 2 an den Benutzer, um die geschäftliche Begründung zu validieren. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Benutzer zu kontaktieren.
3. Überprüfen Sie in Aktion 3, ob der Benutzer eine gültige geschäftliche Begründung angegeben hat.
4. Wenn der Benutzer in Aktion 4 eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:



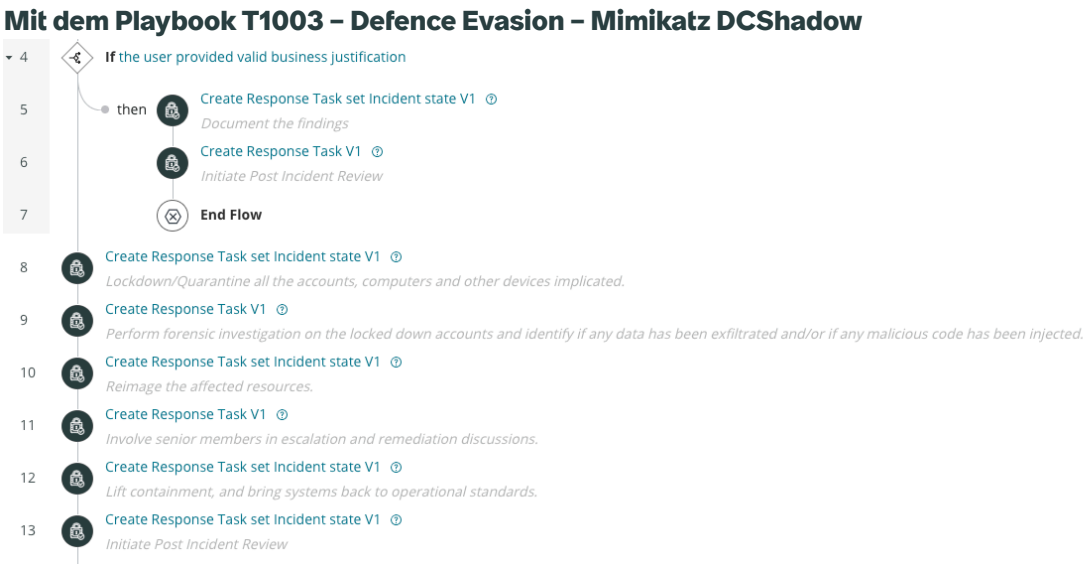
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**a.** Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

**b.** Initiieren Sie in Aktion 6 eine Überprüfung nach Incidents.
In Aktion 7 endet der Flow nach der Überprüfung nach Incidents.

**5.** Wenn der Benutzer in Aktion 8 keine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:




**a.** Sperren oder stellen Sie in Aktion 9 alle beteiligten Konten, Computer und anderen Geräte unter Quarantäne.

**b.** Führen Sie in Aktion 10 eine forensische Untersuchung der gesperrten Konten durch und stellen Sie fest, ob Daten exfiltriert oder schädlicher Code eingefügt wurde.

**c.** Führen Sie in Aktion 11 ein neues Image der betroffenen Ressourcen durch.

**d.** Heben Sie in Aktion 12 das Containment auf und bringen Sie die Systeme wieder in den Betriebszustand.

**e.** Schließen Sie in Aktion 13 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Playbook für T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, bei denen vermutet wird, dass sie durch Mimikatz DCSync verursacht werden. Dieses Playbook wird ausgelöst, wenn eine der Mimikatz-Funktionen (`lsadum::dcsync`) verwendet wird. Die Funktion wird normalerweise für angegriffene Domänencontroller (DC) verwendet.

Mimikatz ist ein beliebtes Hacking-Tool, mit dem Benutzer Befehle ausgeben können, die beim Abrufen vertraulicher Daten aus dem angegriffenen System helfen. Zu den vertraulichen Daten gehören Passwörter, deren Hashes und andere Daten.

**Hinweis:**
Dies ist eine Warnung mit hoher Genauigkeit, von der angenommen wird, dass sie selten ausgelöst wird. Wenn sie ausgelöst wird, sollten Sie sofort ein leitendes Teammitglied oder einen Manager benachrichtigen.

### Richten Sie das Playbook T1003 – Credential Dumping – Mimikatz DCsync ein

Führen Sie die folgenden Schritte aus, um das Playbook T1003 – Credential Dumping – Mimikatz DCsync einzurichten.

#### Vorbereitungen
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

#### Prozedur

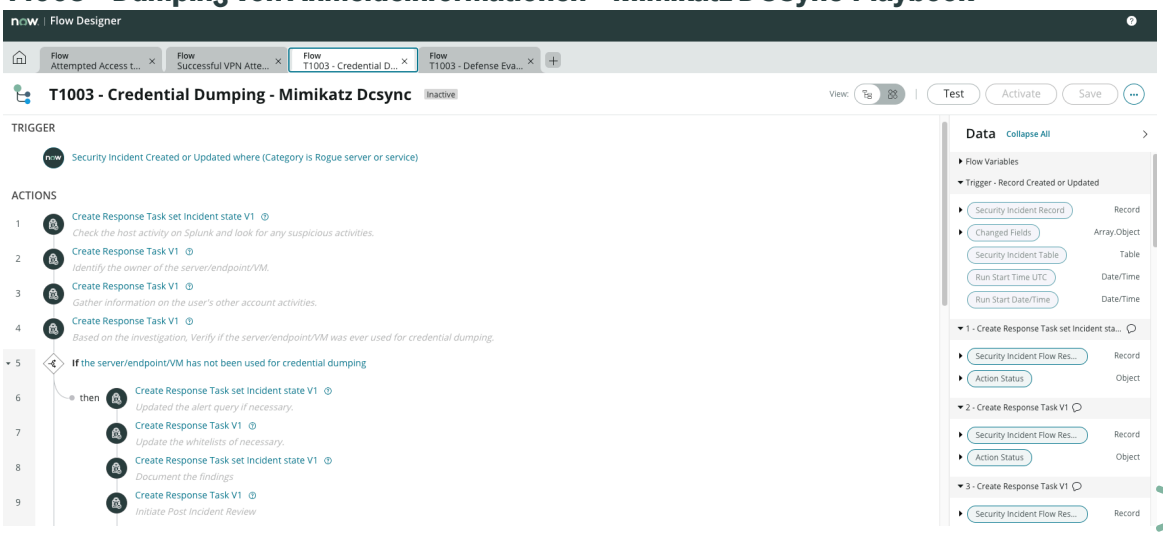
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook T1003 – Credential Dumping – Mimikatz DCsync aus**.
3. Erstellen Sie eine Kopie des Playbook-Flows T1003 – Credential Dumping – Mimikatz DCsync, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.



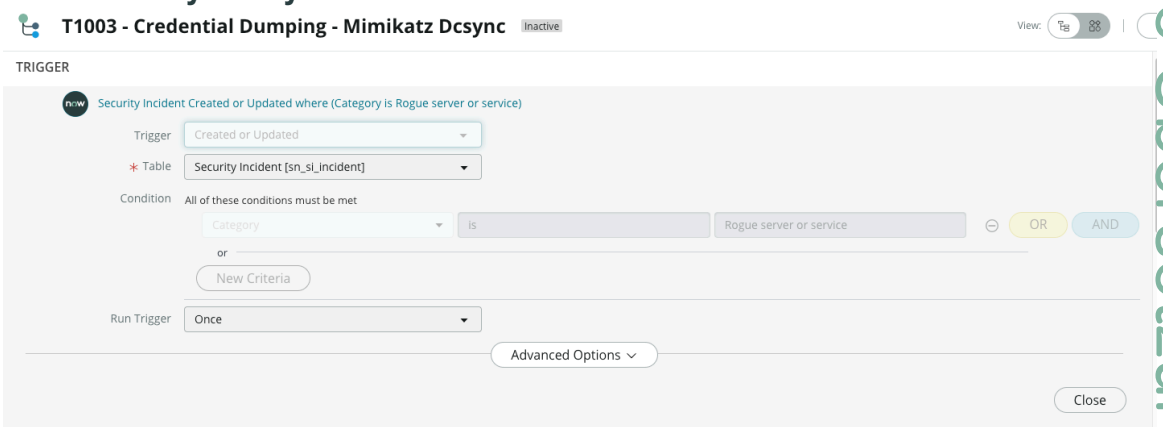
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync-Playbook




4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieRogue-Server oder**-Service lautet.

### T1003 – Dumping von Anmeldeinformationen – Auslöserbedingung für Mimikatz DCSync-Playbook




## Verwenden Sie das Playbook T1003 – Credential Dumping – Mimikatz DCsync

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, bei denen der Verdacht besteht, dass sie durch Mimikatz DCSync verursacht werden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Credential Dumping – Mimikatz DCsync verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

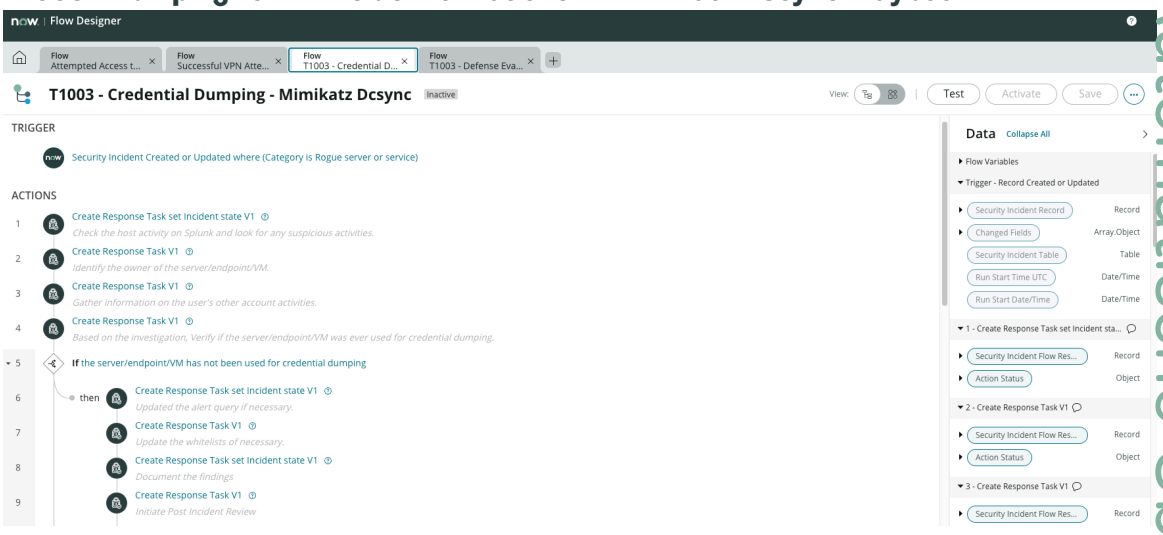


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, überprüfen Sie in Aktion 1 die Hostaktivität in Splunk, und suchen Sie nach verdächtigen Aktivitäten.
2. Identifizieren Sie in Aktion 2 den Besitzer des Servers/Endpunkts/der VM.
   Wenn der Benutzer online ist, führen Sie CrowdStrike EDR aus, um einen besseren Umfang der Systemaktivitäten zu erfassen.
3. Erfassen Sie in Aktion 3 Informationen zu den anderen Kontoaktivitäten des Benutzers.
4. Überprüfen Sie in Aktion 4 basierend auf der Untersuchung, ob der Server/Endpunkt/die VM jemals für das Dumping von Anmeldeinformationen verwendet wurde.
5. Wenn in Aktion 5 der Server/Endpunkt/die VM nicht für das Dumping von Anmeldeinformationen verwendet wurde, führen Sie die folgenden Aktionen aus:

**T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync-Playbook**




   a. Aktualisieren Sie in Aktion 6 die Warnungsabfrage, falls erforderlich.

   b. Aktualisieren Sie in Aktion 7 die Allow-Liste, falls erforderlich.

   c. Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

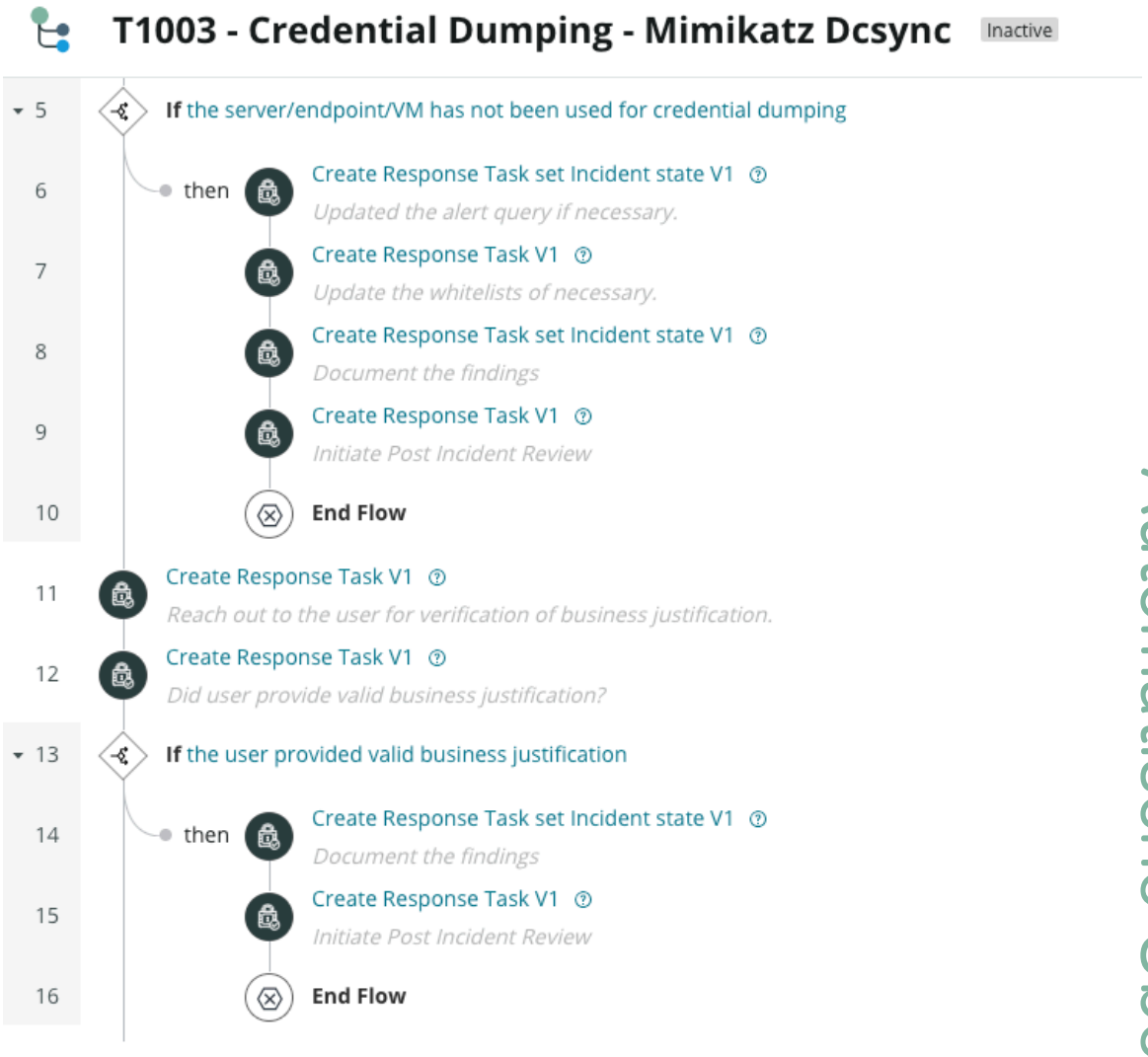
   d. Initiieren Sie in Aktion 9 eine Überprüfung nach Incidents.
   In Aktion 10 endet der Flow.

6. Wenn der Server/Endpunkt/die VM für das Dumping von Anmeldeinformationen verwendet wurde, wenden Sie sich in Aktion 11 an den Benutzer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Verwenden des Playbooks T1003 – Credential Dumping – Mimikatz DCsync**




7. Wenden Sie sich in Aktion 12 an den Benutzer, um die geschäftliche Begründung zu validieren.
8. Wenn der Benutzer in Aktion 13 eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aktionen aus:

   a. Dokumentieren Sie in Aktion 14 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 15 eine Überprüfung nach Incidents.
   In Aktion 16 endet der Flow.

9. Wenn der Benutzer keine gültige geschäftliche Begründung angegeben hat, stellen Sie das System in Aktion 17 unter Quarantäne.
10. Entfernen Sie in Aktion 18 alle unerwünschten Dateien, die möglicherweise von den nicht autorisierten Konten erstellt oder gelöscht wurden.
11. Heben Sie in Aktion 19 das Containment auf und bringen Sie die Systeme wieder in den Betriebszustand.
12. Schließen Sie in Aktion 20 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Playbook für Okta-Anwenderanmeldungsfehler von mehreren IPs

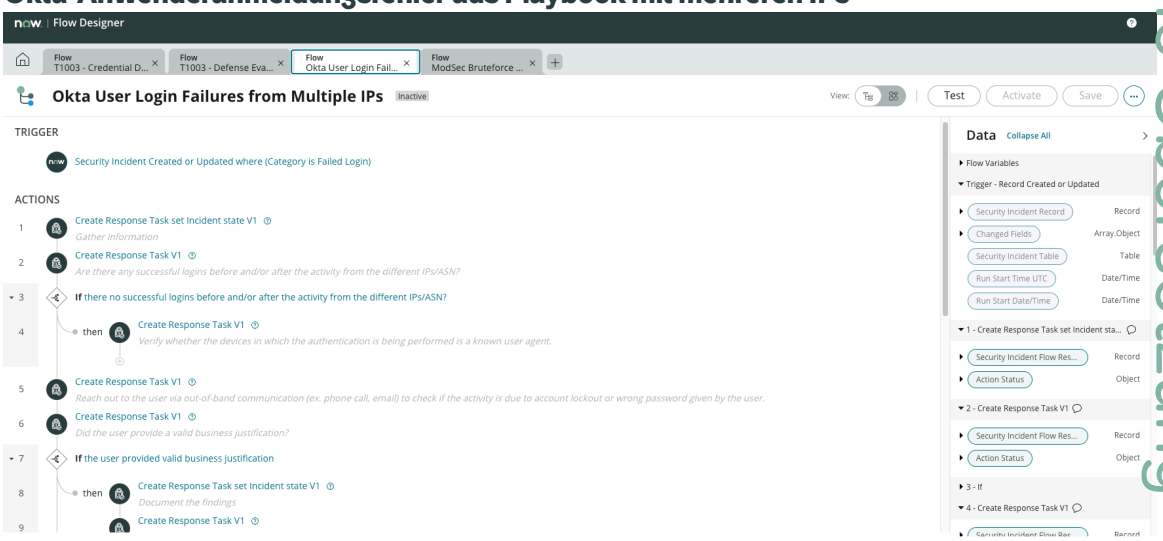
Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents für Benutzeranmeldungsfehler bei Okta.

Das Playbook „Okta-Benutzeranmeldungsfehler bei mehreren IPs“ enthält Anweisungen zur Analyse der Warnung, wenn ServiceNow-Kontofehler in Okta aus mehreren Nicht-ServiceNow-IPs erkannt werden. Die mit diesem Playbook verbundene Warnung überprüft die Okta-Protokolle. Sie löst eine Warnung aus, wenn ein Anmeldefehler für ServiceNow-Benutzer-IDs aus mehr als drei Nicht-ServiceNow-IP-Bereichen innerhalb einer Stunde auftritt.

## Erste Schritte mit dem Playbook „Okta-Anwenderanmeldungsfehler bei mehreren IPs“.

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Okta-Benutzeranmeldungsfehler“ aus „Mehrere IPs** “ aus.
3. (Optional) Sie können eine Kopie des Playbook-Flows „Okta-Benutzeranmeldungsfehler aus mehreren IPs“ erstellen und die erforderlichen Änderungen vornehmen. Um eine Kopie des Playbook-Flows zu erstellen, klicken Sie auf das Menüsymbol und wählen Sie **Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

**Okta-Anwenderanmeldungsfehler aus Playbook mit mehreren IPs**



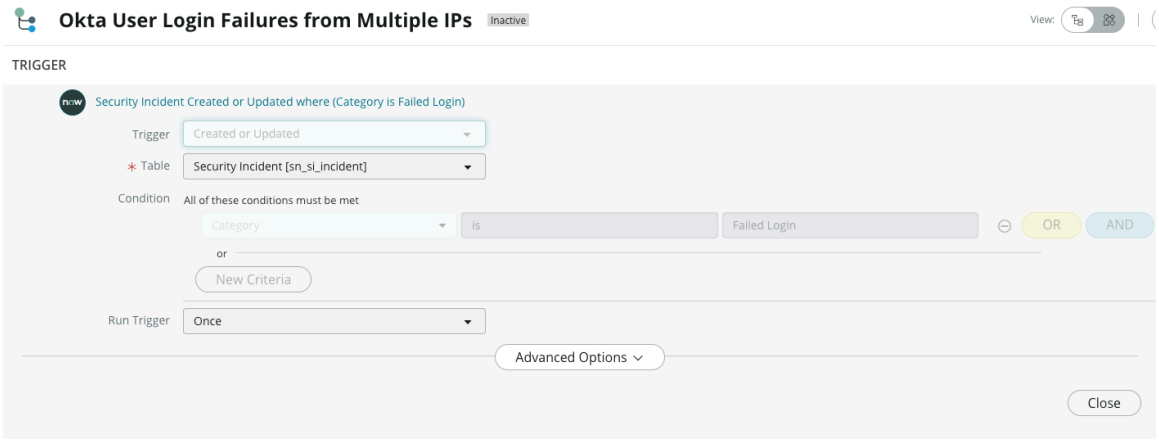

4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

**Auslöserbedingung**: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **Kategorie„Fehlgeschlagene Anmeldung**“ lautet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Playbook-Auslöserbedingung „Okta-Anwenderanmeldungsfehler aufgrund mehrerer IPs“.**




## Richten Sie das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Okta-Anwenderanmeldungsfehler aus mehreren IPs“ einzurichten.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

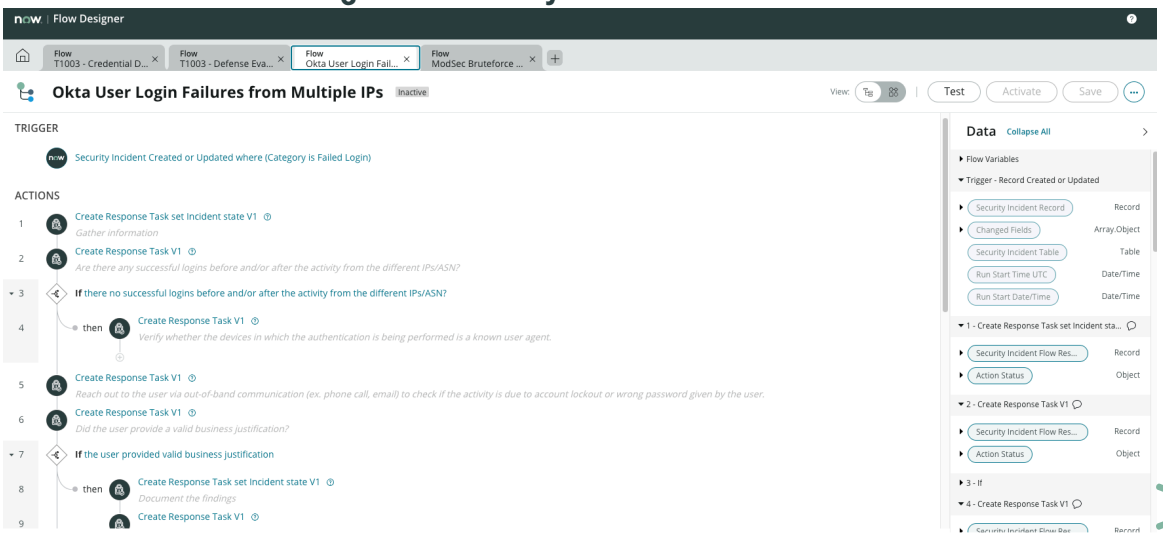
1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das Playbook **„Okta-Benutzeranmeldungsfehler“ aus „Mehrere IPs** “ aus.
3. Erstellen Sie eine Kopie des Playbook-Flows „Okta-Benutzeranmeldungsfehler aus mehreren IPs“, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.



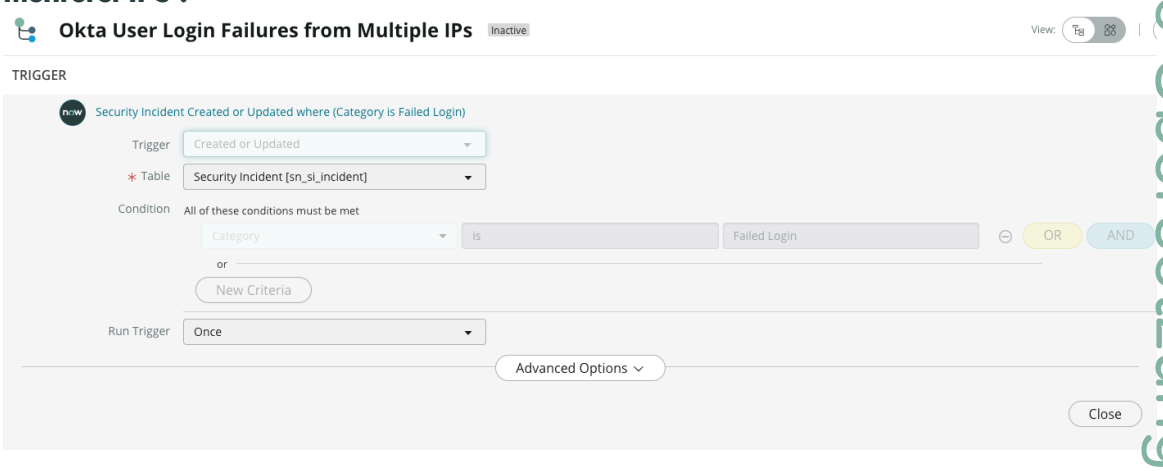
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Okta-Anwenderanmeldungsfehler aus Playbook mit mehreren IPs**




4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die **KategorieFehlgeschlagene Anmeldung**lautet.

**Playbook-Auslöserbedingung „Okta-Anwenderanmeldungsfehler aufgrund mehrerer IPs“.**




## Verwenden Sie das Playbook „Okta-Benutzeranmeldungsfehler aus mehreren IPs“.

Verwenden Sie dieses Playbook, um Security Incidents für Benutzeranmeldungsfehler bei Okta zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Okta-Benutzeranmeldungsfehler bei mehreren IPs“ verfügbar sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

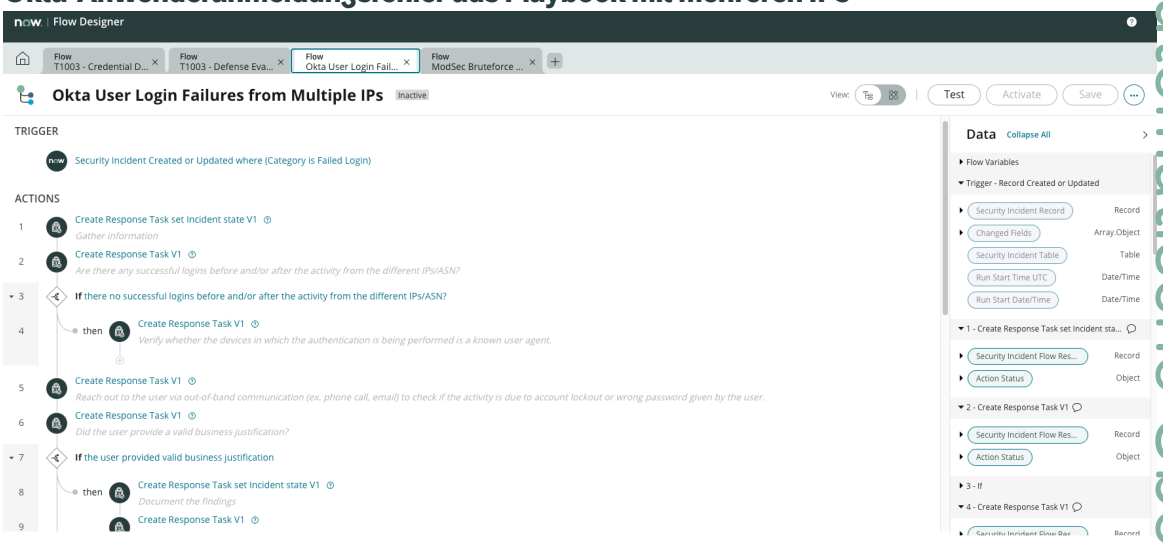


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, führen Sie in Aktion 1 die folgenden Aufgaben aus:
   - Identifizieren Sie das Zielbenutzerkonto.
   - Überprüfen Sie das IP-Subnetz, und prüfen Sie, ob alle zum selben Besitzer der autonomen Systemnummer (ASN) gehören.
2. Überprüfen Sie in Aktion 2, ob vor oder nach der Aktivität erfolgreiche Anmeldungen von den verschiedenen IPs/ASNs aufgetreten sind.
3. Wenn in Aktion 3 vor oder nach der Aktivität keine erfolgreichen Anmeldungen von den verschiedenen IPs/ASNs erfolgt sind, überprüfen Sie in Aktion 4, ob die Geräte, auf denen die Authentifizierung durchgeführt wird, bekannte Benutzer-Agents sind.
   Wenn die Geräte von bekannten Benutzeragenten authentifiziert werden, endet der Flow.

**Okta-Anwenderanmeldungsfehler aus Playbook mit mehreren IPs**

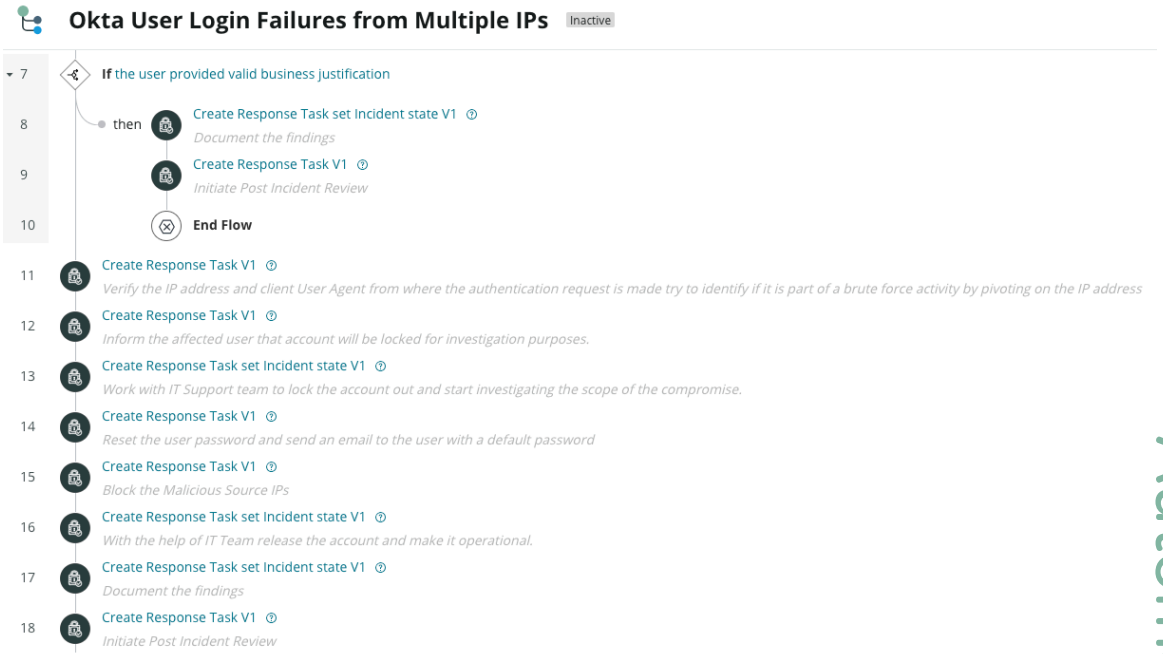



4. Wenden Sie sich in Aktion 5 basierend auf der Untersuchung an den Benutzer durch Out-of-Band-Kommunikation (z. B. Telefonanruf oder E-Mail), um zu überprüfen, ob die Aktivität auf eine Kontosperrung oder ein falsches Passwort des Benutzers zurückzuführen ist.
5. Überprüfen Sie in Aktion 6, ob der Benutzer eine gültige geschäftliche Begründung angegeben hat.
6. Wenn der Benutzer in Aktion 7 eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aufgaben aus.
   a. Erstellen Sie in Aktion 8 eine Antwortaufgabe, um die bisherigen Ergebnisse zu dokumentieren.
   b. Erstellen Sie in Aktion 9 eine Antwort, um eine Überprüfung nach Incidents zu initiieren.
      In Aktion 10 endet der Flow.
7. Überprüfen Sie in Aktion 11 die IP-Adresse und den Client-Benutzer-Agent, von dem die Authentifizierungsanforderung gestellt wird, und versuchen Sie festzustellen, ob sie Teil einer Brute-Force-Aktivität ist, indem Sie die IP-Adresse verwenden.
8. Informieren Sie den betroffenen Anwender in Aktion 12 darüber, dass der Account zu Untersuchungszwecken gesperrt wird.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Benutzer zu informieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden des Playbooks „Okta-Benutzeranmeldungsfehler aus mehreren IPs“.




9. Arbeiten Sie in Aktion 13 mit dem IT-Supportteam zusammen, um das Konto zu sperren und mit der Untersuchung des Umfangs der Gefährdung zu beginnen.
10. Setzen Sie in Aktion 14 das Benutzerpasswort zurück, und senden Sie eine E-Mail mit dem Standardpasswort an den Benutzer.
11. Blockieren Sie in Aktion 15 die schädlichen Quell-IPs.
12. In Aktion 16 erhalten Sie Hilfe vom IT-Supportteam, um den Account freizugeben und ihn wieder auf Betriebsniveau zu bringen.
13. Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.
14. Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

## Playbook für ModSec Brute Force nach IP-Burst

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents von Brute-Force-Versuchen auf den Anmeldeseiten von mehreren von ModSec erkannten IPs. Die Event-Bedingungen können in der ModSec-Richtlinie selbst festgelegt werden und lösen bei Splunk eine Warnung aus, wenn das Event bei ModSec erstellt wird.

Dieses Playbook hilft bei der Erkennung von anormalen Datenverkehrszahlen auf der Anmeldeseite. In diesem Beispiel sollten zwei aufeinanderfolgende Bursts mit mehr als 50 Treffern/Minute von einer IP-Adresse zur Anmeldeseite gelangen, was auf einen Brute-Force-Anmeldeversuch hinweist.

### Richten Sie das ModSec Brute Force by IP Burst-Playbook ein

Führen Sie die folgenden Schritte aus, um das ModSec Brute Force by IP Burst-Playbook einzurichten.

**Vorbereitungen**
Erforderliche Rolle:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

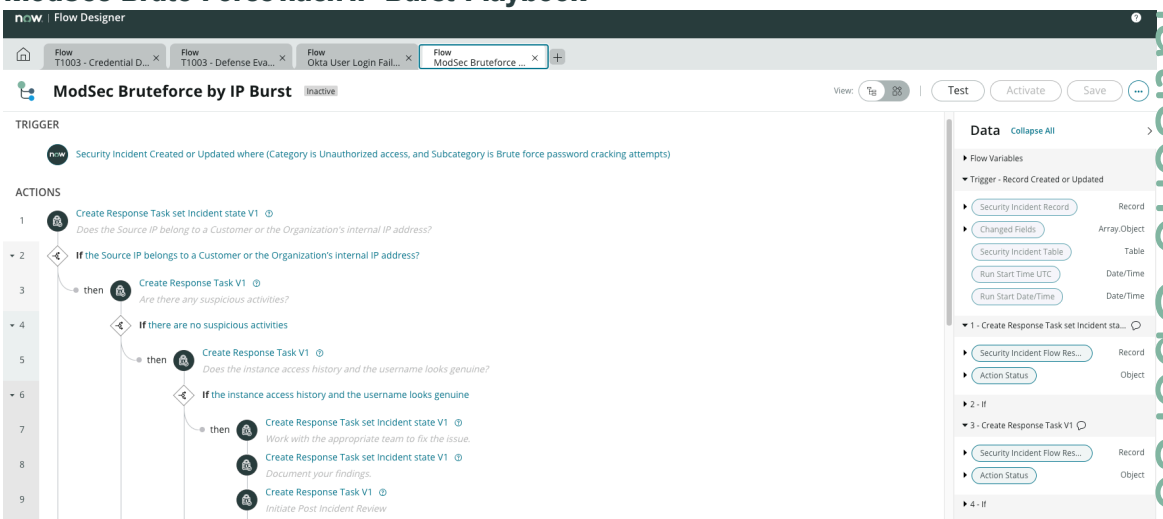
Stellen Sie sicher, dass Sie Security Operations Spoke (*sn_sec_spoke*) installiert haben.

### Prozedur

1. Melden Sie sich als Benutzer mit den Rollen sn_si.user und flow_designer an.
2. Navigieren zu **Alle** > **Flow Designer** und wählen Sie das **Playbook ModSec Bruteforce by IP Burst aus**.
3. Erstellen Sie eine Kopie des Playbook-Flows ModSec Bruteforce by IP Burst, und nehmen Sie die erforderlichen Änderungen vor.

   Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol und **dann Flow kopieren**aus. Führen Sie diesen Schritt nur aus, wenn Sie den Flow anpassen oder bestimmte Änderungen daran vornehmen möchten.

   **ModSec-Brute-Force nach IP-Burst-Playbook**



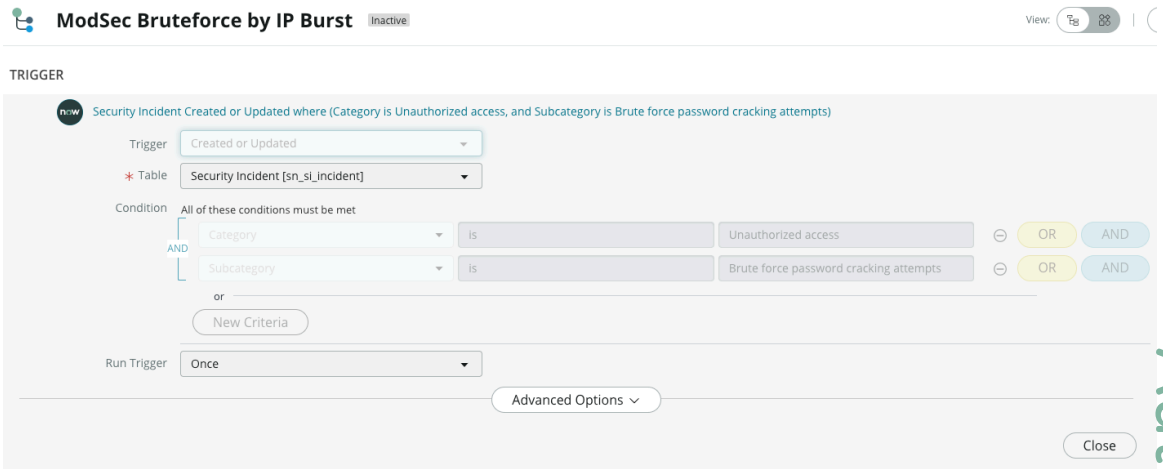

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. **Auslöserbedingung** für das Playbook: Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kategorie** ist **„Nicht autorisierter Zugriff“**.
- **Unterkategorie** ist **Brute-Force-Angriffe auf Passwörter**.

**ModSec-Brute-Force nach IP-Burst-Playbook-Auslöserbedingung**




### Verwenden Sie das ModSec Brute Force by IP Burst-Playbook

Verwenden Sie dieses Playbook, um Incidents von Brute-Force-Versuchen auf den Anmeldeseiten von mehreren von ModSec erkannten IPs zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „ModSec Brute Force by IP Burst“ verfügbar sind.

### Vorbereitungen

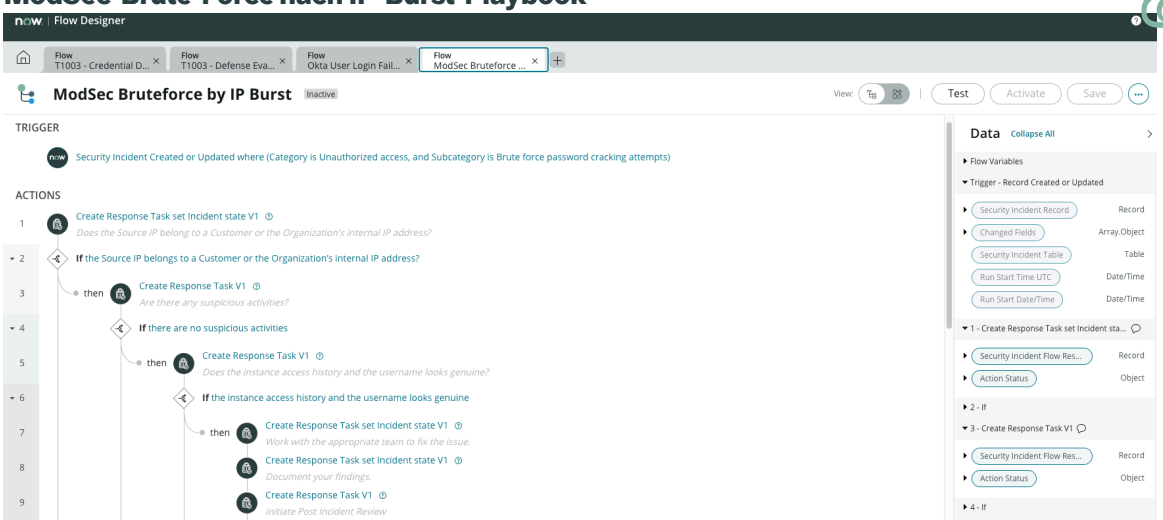
Erforderliche Rolle:

- sn_si.admin
- flow_designer

### Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, überprüfen Sie in Aktion 1, ob die Quell-IP zu einem Kunden oder zur internen IP-Adresse der Organisation (Aktion 1)gehört.
2. Wenn die Quell-IP zu einem Kunden oder zur internen IP-Adresse der Organisation gehört, führen Sie in Aktion 2 die folgenden Schritte aus:

**ModSec-Brute-Force nach IP-Burst-Playbook**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Überprüfen Sie in Aktion 3, ob verdächtige Aktivitäten aufgetreten sind.

- Überprüfen Sie die Aktivität der Quell-IP in den letzten Tagen. Wenn die IP-Adresse vernachlässigbaren Datenverkehr aufwies, weist dies auf einen tatsächlichen Angriff hin.
- Überprüfen Sie die Benutzernamen für die Anwendung. Überprüfen Sie beispielsweise, ob die Benutzernamen in alphabetischer Reihenfolge angeordnet sind.
- Suchen Sie nach beteiligten generischen Kontonamen. Zum Beispiel admin, sysadmin, root, Administrator und andere Anwendungskontonamen.

Wenn keine verdächtigen Aktivitäten vorhanden sind, wird der Flow beendet.

**b.** Wenn in Aktion 4 verdächtige Aktivitäten aufgetreten sind, überprüfen Sie in Aktion 5, ob der Instanzzugriffsverlauf und der Benutzername echt aussehen.

Überprüfen Sie die Protokolle *Appnode* auf Fehler. Es kann SAML-, SSO- oder LDAP-Fehlerereignisse geben, die auf ein Betriebsproblem zurückzuführen sein können.

Wenn der Instanzzugriffsverlauf und der Benutzername nicht korrekt aussehen, wird der Flow beendet.

**c.** Wenn in Aktion 6 der Instanzzugriffsverlauf und der Benutzername korrekt aussehen, führen Sie die folgenden Schritte aus:

**i.** Koordinieren Sie in Aktion 7 das Problem mit dem entsprechenden Team, um das Problem zu beheben.

**ii.** Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

**iii.** Schließen Sie in Aktion 9 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

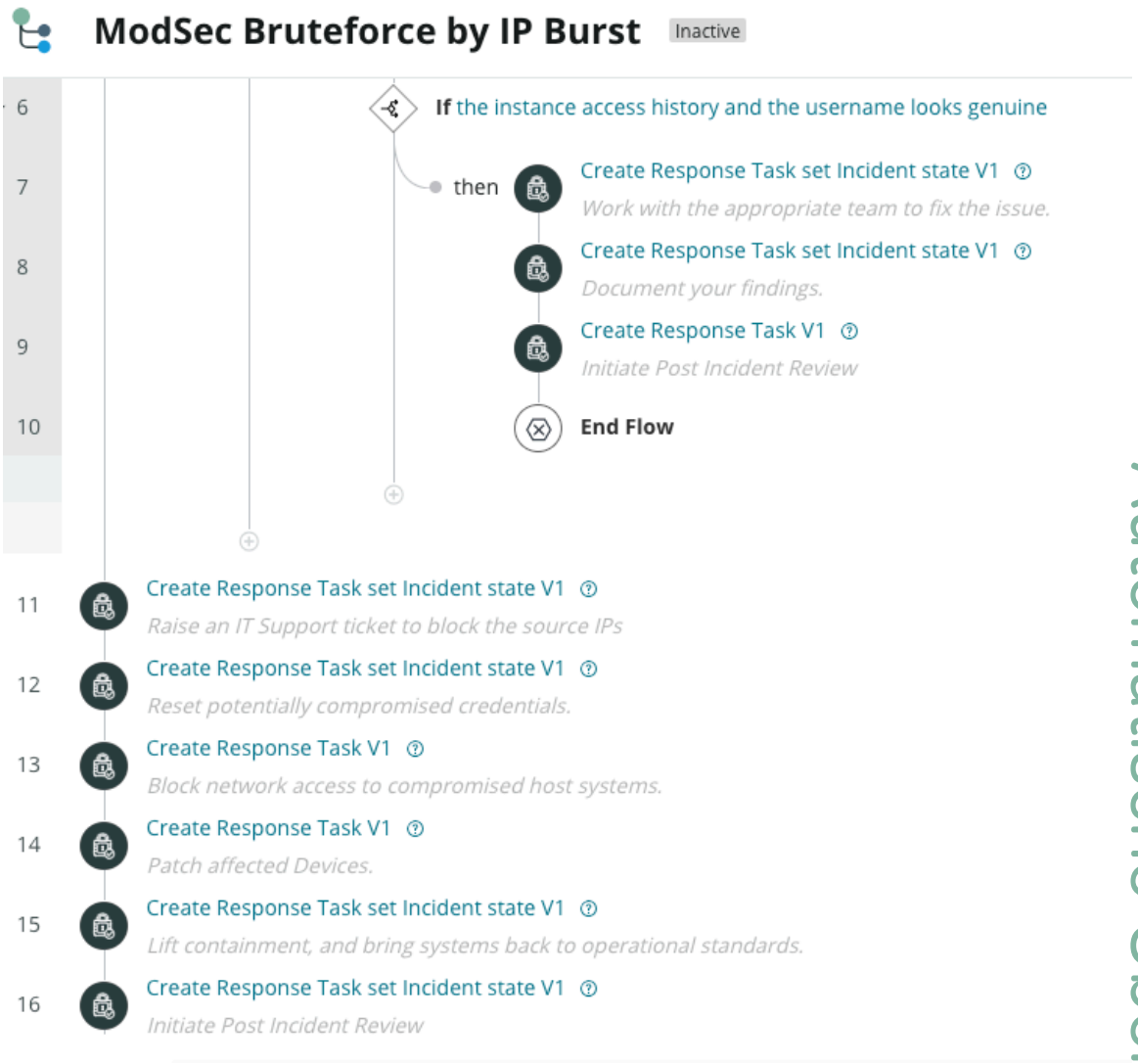
In Aktion 10 endet der Flow.

**3.** Wenn die Quell-IP nicht zu einem Kunden oder zur internen IP-Adresse der Organisation gehört, erstellen Sie in Aktion 11 ein IT-Supportticket, um die Quell-IPs zu blockieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden des ModSec Brute Force by IP Burst-Playbooks




4. Setzen Sie in Aktion 12 die potenziell gefährdeten Anmeldeinformationen zurück.
5. Blockieren Sie in Aktion 13 den Netzwerkzugriff auf gefährdete Hostsysteme.
6. Patchen Sie in Aktion 14 die betroffenen Geräte.
7. Heben Sie in Aktion 15 die Eindämmung auf, und bringen Sie die Systeme wieder in den Betriebszustand.
8. Schließen Sie in Aktion 16 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

## Security Incident Response-Playbook-Aktionen

In diesem Abschnitt werden die in der Flow Designer-Aktionsbibliothek bereitgestellten Aktionen beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktionsname | Beschreibung | Beispielszenario | |
|---|---|---|---|
| Fügen Sie dem Security Incident ein Sicherheits-Tag hinzu | Verwenden Sie diese Aktion, um mithilfe der Flow Designer-Logik automatisch ein Sicherheits-Tag hinzuzufügen. | Wenn der Flow einen IoC erkennt, kann das Tag **IoC** erkannt mit dieser Aktion automatisch hinzugefügt werden.<br><br>**Flow**: | • Eingabe: Security Incident, Sicherheits-Tag<br>• Ausgabe: nicht zutreffend |
| Fügen Sie dem Security Incident erkennbare Elemente hinzu | Verwenden Sie diese Aktion, um einem ausgewählten Security Incident erkennbare Elemente hinzuzufügen.<br>• Standardmäßig wird die Liste der erkennbaren Elemente durch das Trennzeichen Komma (,) getrennt. Dies kann jedoch geändert werden. Sie können ein anderes einzelnes Sonderzeichen als Trennzeichen angeben. Beim Hinzufügen von erkennbaren Elementen wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt.<br>• Wenn die erkennbaren Elemente dem Security Incident hinzugefügt werden, wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt.<br>• Wenn die erkennbaren Elemente hinzugefügt werden, identifiziert die Option Erkennbare Elemente der zulässigen Liste | | • Eingabe:<br>◦ Security Incident<br>◦ Erkennbare Elemente<br>◦ Trennzeichen<br>◦ Zulässige Liste erkennbarer Elemente filtern und Aktivitätsnotiz veröffentlichen<br>• Ausgabe: nicht zutreffend |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktionsname | Beschreibung | Beispielszenario | |
|---|---|---|---|
| | die erkennbaren Elemente der zulässigen Liste und fügt sie nicht der zugehörigen Liste der erkennbaren Elemente des Security Incident hinzu. Eine automatisierte Systemaktivität (Antwort) wird hinzugefügt, um anzugeben, dass diese erkennbaren Elemente entfernt wurden. | | |
| Betroffene Benutzer (zugehörige Listen) aus mehreren Security Incidents abrufen V1 | Ruft alle betroffenen Benutzer ab, die in der zugehörigen Liste „Betroffene Benutzer“ für die angegebenen Security Incidents aufgeführt sind. | Möglicherweise haben Sie übergeordnete Security Incidents mit mehreren untergeordneten Security Incidents. Verwenden Sie diese Aktion, um ein Rollup für betroffene Benutzer von allen untergeordneten Security Incidents zu den entsprechenden übergeordneten Security Incidents durchzuführen. Es wird nur ein Rollup für eindeutige betroffene Benutzer durchgeführt, und alle Duplikate werden eliminiert. | • Eingabe: Security Incidents<br>• Ausgabe:<br>◦ betroffener Benutzer<br>◦ count |
| Rufen Sie betroffene Benutzer aus mehreren Security Incidents ab | Ruft den primär betroffenen Anwender für den angegebenen Security Incident ab. Sie enthält nicht die betroffenen Benutzer aus der zugehörigen Liste „Betroffene Benutzer“. | • Senden Sie während der Untersuchung eines Phishing-Security Incident eine E-Mail an die primär betroffenen Benutzer (die den Phishing-Incident gemeldet haben), um zu bestätigen, ob einer der Benutzer auf die schädlichen Links in der Phishing-E-Mail geklickt hat. | • Eingabe: Security Incidents<br>• Ausgabe:<br>◦ betroffene Benutzer<br>◦ count |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktionsname | Beschreibung | Beispielszenario | |
|---|---|---|---|
| | | • Aktualisieren Sie den Schweregrad oder die Risikopunktzahl des übergeordneten Security Incident basierend auf der Anzahl der primär betroffenen Benutzer. | |
| Ruft betroffene Benutzer (zugehörige Liste) aus einem Security Incident ab | Ruft alle betroffenen Benutzer ab, die in der zugehörigen Liste „Betroffene Benutzer“ für einen angegebenen Security Incident aufgeführt sind. | | • Eingabe: Security Incidents<br>• Ausgabe:<br>◦ betroffene Benutzer<br>◦ count |
| Fügen Sie dem Security Incident betroffene Benutzer hinzu | Fügt alle betroffenen Benutzer einem Security Incident hinzu. | Angenommen, Sie haben einen übergeordneten Security Incident mit mehreren untergeordneten Security Incidents. Sie können diese Aktion verwenden, um ein Rollup für betroffene Benutzer aus allen untergeordneten Security Incidents zum entsprechenden übergeordneten Security Incident durchzuführen. Es wird nur ein Rollup für eindeutige betroffene Benutzer durchgeführt, und alle Duplikate werden eliminiert. | • Eingabe:<br>◦ Security Incident<br>◦ Anwender<br>• Ausgabe: nicht zutreffend |
| Ruft Konfigurationselemente der betroffenen Benutzer ab | Ruft die Konfigurationselemente (CIs) aller betroffenen Anwender ab. | In Phishing- oder Malware-Szenarien können Sie diese Aktion verwenden, um die zugehörige Liste „Betroffene Konfigurationselemente (CI)“ zu aktualisieren und die CIs zu untersuchen. Sie können dann den Schweregrad oder die Risikopunktzahl des Security Incident | • Eingabe: Benutzer<br>• Ausgabe:<br>◦ Konfigurationselemente<br>◦ count |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktionsname | Beschreibung | Beispielszenario | |
|---|---|---|---|
| | | basierend auf der Anzahl der identifizierten CIs aktualisieren. | |
| Ruft alle untergeordneten Security Incidents für einen Security Incident ab | Ruft alle untergeordneten Security Incidents ab, die sich auf einen bestimmten übergeordneten Security Incident beziehen. | Beispielszenario: Verwenden Sie diese Aktion für Folgendes:<br>• Aktualisieren Sie den Status der untergeordneten Security Incidents, wenn der Status der entsprechenden übergeordneten Security Incidents aktualisiert wird.<br>• Aktualisieren Sie den Schweregrad oder die Risikopunktzahl des Security Incident automatisch basierend auf der Anzahl der untergeordneten Security Incidents. | • Eingabe:<br>◦ Security Incident<br>◦ Incident-Status<br>• Ausgabe:<br>◦ untergeordneter Security Incident<br>◦ count |
| Konfigurationselemente für die erkennbaren Elemente abrufen (IP-Adresse eingeben) | Ruft alle Konfigurationselemente (CIs) für erkennbare Elemente vom Typ „IP-Adresse“ ab. | Eine erkennbare IP-Adresse kann einem Konfigurationselement zugeordnet werden. Zum Beispiel die IP-Adresse eines Servers. Wenn Sie diese Aktion verwenden, können Sie Informationen für den Server abrufen. | • Eingabe: IP-Adresse des erkennbaren Elements<br>• Ausgabe:<br>◦ Konfigurationselemente<br>◦ count |
| Ist erkennbares Element böswillig | Bestätigt das Vorhandensein eines oder mehrerer schädlicher erkennbarer Elemente in einem Satz von erkennbaren Elementen. | Nachdem die Bedrohungssuche abgeschlossen ist und Sie das Vorhandensein schädlicher erkennbarer Elemente identifiziert haben, können Sie den Schweregrad oder die Risikopunktzahl eines Security Incidents erhöhen. | • Eingabe: Security Incident<br>• Ausgabe: schädlich (true/false) |
| Senden Sie eine E-Mail, um die | Sendet eine E-Mail als Antwort auf eine Benutzerantwort. | Wenn ein Benutzer mehrmals versucht, sich bei einer Anwendung | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktionsname | Beschreibung | Beispielszenario | |
|---|---|---|---|
| Benutzerinteraktion zu bestätigen | | anzumelden, und dies fehlschlägt, führt dies zu einem fehlgeschlagenen Anmeldeszenario. In diesem Fall wird eine E-Mail an den Benutzer gesendet, um zu bestätigen, ob der Benutzer versucht hat, sich anzumelden. Abhängig von der Benutzerantwort (Ja oder Nein) können verschiedene Aktionen ausgeführt werden.<br><br>**Flow**: Playbook „Manuelle fehlgeschlagene Anmeldung“. | |
| Filtern Sie die erkennbaren Elemente der zulässigen Liste heraus | Verwenden Sie diese Aktion, um die Liste erkennbarer Elemente aus einem bestimmten Satz von erkennbaren Elementen zuzulassen. | Sie können bestimmte erkennbare Elemente identifizieren, die aus einer Reihe von erkennbaren Elementen ignoriert werden können. Diese erkennbaren Elemente werden bei der Lösung des Security Incident nicht berücksichtigt. | • Eingabe: Security Incident<br>• Ausgabe:<br>◦ zulässige Liste erkennbarer Elemente<br>◦ count |
| Setzen Sie das Passwort für betroffene Benutzer zurück | Verwenden Sie diese Aktion, um das Passwort für betroffene Anwender zurückzusetzen. | Wenn ein Benutzerkonto angegriffen wurde oder ein Benutzer das Zurücksetzen des Passworts anfordert, wird eine E-Mail an den Benutzer gesendet, um das Passwort zurückzusetzen.<br><br>**Flow**: Playbook „Manuelle fehlgeschlagene Anmeldung“. | |
| Ruft die Benutzergruppe für den betroffenen Benutzer ab | Ruft die Anwendergruppendetails der betroffenen Anwender ab. | Wenn in einer Organisation zwei oder mehr Benutzer Phishing-E-Mails melden, können Sie die Gruppe ermitteln, zu der sie gehören, und ermitteln, ob weitere Benutzer betroffen waren | • Eingabe: Benutzer<br>• Ausgabe:<br>◦ Benutzergruppen<br>◦ count |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Security Incident Response-Berichterstellung

Sicherheitsmanager können Problembereiche mithilfe allgemeiner grafischer Schnittstellen identifizieren.

## Greifen Sie auf Security Incident Response Explorer zu

Sie können auf das Security Incident Response Explorer-Dashboard zugreifen, um Security Incident-Aktivitäten anzuzeigen, um Problembereiche sofort zu erkennen und Probleme schnell zu lösen.

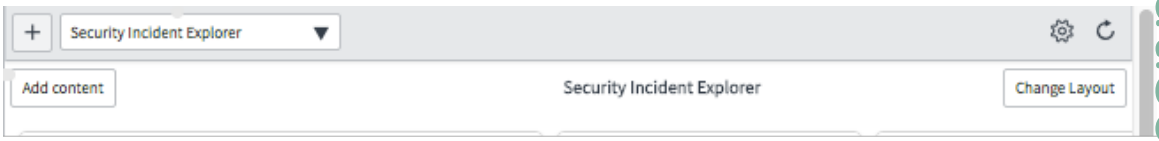
### Vorbereitungen

Erforderliche Rollen:

- sn_si.admin (zum Schreiben)
- sn_si_basic (zum Lesen)

### Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Homepage** oder navigieren Sie zu **Selfservice** > **Dashboards**.
2. Wählen Sie in der Berichtsliste Security Incident Explorer aus.

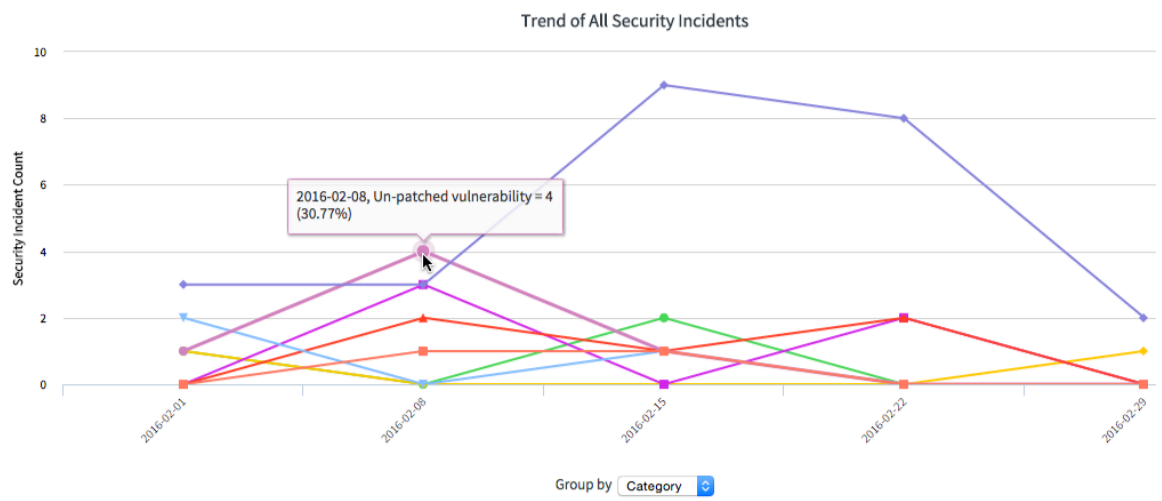



## Security Incident Response-Übersicht

Die Security Incident Response -Übersicht bietet einen Überblick über Security Incident-Aktivitäten, Trends und Berichte sowie Detailinformationen zu bestimmten Daten.

Das -Übersichtsmodul zeigt Security Incident-Informationen an, die auf die Rolle des Benutzers zugeschnitten sind. Sie können auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt, Heatmap usw.) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Siehe folgende Abbildung. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

**Trend aller Security Incidents**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Sicherheitsvorfallmanager – Übersicht

Benutzer mit den Rollen „Security Incident-Administrator“ und „Security Incident Manager“ zeigen die Security Incident Manager-Übersicht an. Sie enthält die folgenden Berichte im Basissystem.

### Security Incident Manager-Übersichtsberichte

| Name | Visuell | Beschreibung |
|---|---|---|
| Team Security Incidents mit Priorität „Kritisch“ | Einzelne Punktzahl | Die Anzahl der kritischen Security Incidents, die dem Team zugewiesen sind. |
| Team Security Incidents mit Priorität „Hoch“ | Einzelne Punktzahl | Die Anzahl der Incidents mit hohem Sicherheitsniveau, die dem Team zugewiesen sind. |
| In 24 Stunden ablaufende SLAs | Einzelne Punktzahl | Die Anzahl der SLAs, die innerhalb der nächsten 24 Stunden ablaufen. |
| Risiko vs. Schweregrad | Heatmap | Verteilung der dem Team zugewiesenen Security Incidents nach Risiko und Schweregrad. |
| Security Incidents nach CI-Klasse, letzte 3 Monate | Balkendiagramm | Anzahl der Security Incidents, die dem Team nach Konfigurationselementklasse zugewiesen sind. |
| Trend aller Security Incidents | Trend | Stellt die Anzahl der eingegangenen Security Incidents nach Kategorie oder Priorität dar. |
| Security Incidents für nicht autorisierten Zugriff | Balkendiagramm | Zeigt die Typen der Security Incident-Kategorien an, die im Laufe der Zeit eingegangen sind. |
| Durchschnittliche Zeit bis zur Eindämmung | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Eindämmung aller Security Incidents benötigt wird. |
| Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Eindämmung aller kritischen Security Incidents benötigt wird. |
| Durchschnittliche Zeit bis zur Identität | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Identifizierung aller Security Incidents benötigt wird. |

## Sicherheitsanalyst – Übersicht

Benutzer mit der Rolle „Security Incident-Analyst“ zeigen die Sicherheitsanalystenübersicht an. Sie enthält die folgenden Berichte im Basissystem.

### Sicherheitsanalysten-Übersichtsberichte

| Name | Visuell | Beschreibung |
|---|---|---|
| Meine Arbeit mit kritischer Priorität | Einzelne Punktzahl | Die Anzahl der mir zugewiesenen kritischen Security Incidents. |
| Meine Arbeit mit hoher Priorität | Einzelne Punktzahl | Die Anzahl der mir zugewiesenen Incidents mit hohem Sicherheitsniveau. |
| Meine in 24 Stunden ablaufenden SLAs | Einzelne Punktzahl | Die Anzahl der mir zugewiesenen SLAs, die innerhalb der nächsten 24 Stunden ablaufen. |
| Mir zugewiesene Security Incidents | Balkendiagramm | Mir zugewiesene Security Incidents nach Incident-Status oder -Kategorie. |
| Mir zugewiesene Arbeit nach Typ | Balkendiagramm | Sicherheitsaufgaben (Incidents, Aufgaben oder Anforderungen), die mir nach Typ oder Priorität zugewiesen wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Sicherheitsanalysten-Übersichtsberichte (Fortsetzung)

| Name | Visuell | Beschreibung |
|---|---|---|
| Mir zugewiesene Security Incidents, Anforderungen, Aufgaben | Liste | Eine Liste aller Security Incidents, Sicherheitsanforderungen und Aufgaben, die mir zugewiesen sind. |
| Security Incident-Standort | Karte | Regionaler Standort der Security Incidents |
| Anzahl | Karte | Anzahl der Security Incidents pro Region. |
| Min./Max.-Anzahl | Farbspektrumleiste | Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbbalken. |
| Prozentsatz der Anzahl | Karte | Prozentsatz der Incident-Gesamtanzahl pro Region. |

## Security Incident CISO-Übersicht mit aktivierter Security Incident Analytics

Wenn das Plugin Security Incident Analytics aktiviert ist, können Benutzer mit den Rollen „Security Incident CISO“ und „Systemadministrator“ die Security Incident CISO-Übersicht anzeigen. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

### Security Incident CISO-Übersichtsberichte (mit aktivierter Security Incident Analytics)

| Name | Visuell | Beschreibung |
|---|---|---|
| Neue Security Incidents diese Woche | Einzelne Punktzahl | Die Anzahl der neuen Security Incidents, die in der aktuellen Woche eingegangen sind. |
| Diese Woche geschlossene Security Incidents | Einzelne Punktzahl | Die Anzahl der in der aktuellen Woche geschlossenen Security Incidents. |
| Neue Security Incidents (Laufzeit: 7 Tage) | Einzelne Punktzahl | Die Anzahl der in den letzten 7 Tagen geöffneten Security Incidents. |
| Geschlossene Security Incidents (Laufzeit: 7 Tage) | Einzelne Punktzahl | Die Anzahl der in den letzten 7 Tagen geschlossenen Security Incidents. |
| Tägliche neue Security Incidents im Vergleich zu geschlossenen Security Incidents | Trend | Anzahl der neuen und geschlossenen Security Incidents im Zeitverlauf nach Tag. |
| Wöchentliche neue Security Incidents im Vergleich zu geschlossenen Security Incidents | Trend | Neue und geschlossene Security Incidents im Zeitverlauf nach Woche. |
| Lösungscode für Security Incident | Trend | Vollständige Anzahl der Abschlusscodes im Zeitverlauf. |
| Sicherheits-Incident – Geschäftsauswirkung | Verzeichnisübersicht | Business Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz. |
| Durchschnittliche Zeit bis Eindämmung (wöchentlich) | Trend | Die durchschnittliche Zeit von 7 Tagen, die benötigt wird, um einen Security Incident im Laufe der Zeit einzudämmen. |
| Durchschnittliche Zeit bis Beseitigung (wöchentlich) | Trend | Die durchschnittliche Zeit von 7 Tagen, die im Laufe der Zeit benötigt wird, um einen Security Incident zu beseitigen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Incident CISO-Übersichtsberichte (mit aktivierter Security Incident Analytics) (Fortsetzung)

| Name | Visuell | Beschreibung |
|---|---|---|
| Durchschnittliche Zeit bis Identifizierung (wöchentlich) | Trend | Die durchschnittliche Zeit von 7 Tagen, die im Laufe der Zeit benötigt wird, um einen Security Incident zu identifizieren. |
| Security Incident-Standort | Karte | Regionaler Standort der Security Incidents |
| Anzahl | Karte | Anzahl der Security Incidents pro Region. |
| Min./Max.-Anzahl | Farbspektrumleiste | Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbbalken. |
| Prozentsatz der Anzahl | Karte | Prozentsatz der Incident-Gesamtanzahl pro Region. |

## Security Incident-CISO-Übersicht ohne aktivierte Security Incident Analytics

Wenn das Plugin Security Incident Analytics nicht aktiviert ist, können Benutzer mit den Rollen „Security Incident CISO“ und „Systemadministrator“ die Security Incident CISO Reporting Übersicht anzeigen. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

### Security Incident CISO-Übersichtsberichte (ohne aktivierte Security Incident Analytics)

| Name | Visuell | Beschreibung |
|---|---|---|
| Neue Security Incidents diese Woche | Einzelne Punktzahl | Die Anzahl der neuen Security Incidents, die in der aktuellen Woche geöffnet wurden. |
| Diese Woche geschlossene Security Incidents | Einzelne Punktzahl | Die Anzahl der in der aktuellen Woche geschlossenen Security Incidents. |
| Neue Security Incidents (Laufzeit: 7 Tage) | Einzelne Punktzahl | Die Anzahl der in den letzten 7 Tagen geöffneten Security Incidents. |
| Geschlossene Security Incidents (Laufzeit: 7 Tage) | Einzelne Punktzahl | Die Anzahl der in den letzten 7 Tagen geschlossenen Security Incidents. |
| Wöchentliche neue Security Incidents | Trend | Die neuen Security Incidents, die wöchentlich geöffnet werden. |
| Wöchentliche geschlossene Security Incidents | Trend | Die Security Incidents wurden wöchentlich geschlossen. |
| Lösungscodes für Security Incident | Trend | Abschlusscodes für Security Incidents im Zeitverlauf. |
| Business Services mit Sicherheitsvorfällen – Geschäftsauswirkung | Verzeichnisübersicht | Business Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz. |
| Durchschnittliche Zeit bis zur Eindämmung | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Eindämmung aller Security Incidents benötigt wird. |
| Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Eindämmung aller kritischen Security Incidents benötigt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident CISO-Übersichtsberichte (ohne aktivierte Security Incident Analytics) (Fortsetzung)**

| Name | Visuell | Beschreibung |
|---|---|---|
| Durchschnittliche Zeit bis zur Identität | Einzelne Punktzahl | Die durchschnittliche Zeit, die zur Identifizierung aller Security Incidents benötigt wird. |

**Hinweis:**
Das Security Incident Response Basissystem enthält Performance Analytics-Lösungen zum Anzeigen vorkonfigurierter Best Practice-Dashboards. Die Dashboards enthalten wichtige Metriken für die Analyse Ihres Prozesses in Security Incident Response, z. B. neue Sicherheitsvorfälle oder das durchschnittliche Alter offener Sicherheitsvorfälle. Weitere Informationen und Installationsanweisungen finden Sie unter Security Incident Response Platform Analytics-Lösungenan.

### Security Incident-Übersicht

Die Security Incident-Zuordnung enthält Daten nach geografischem Standort. Die Weltkarte wird in jedem Bereich hervorgehoben, in dem ein Incident auftritt. Wenn das Plugin Security Incident Analytics aktiviert ist, können Sie die Security Incident-Übersicht der Übersicht Security Incident Response hinzufügen. Nachdem sie hinzugefügt wurde, können Sie die Zuordnung konfigurieren, indem Sie die Zuordnungsfilter ändern.

### Fügen Sie der Übersicht Security Incident Response eine Karte hinzu

Sie können die Karte der Übersicht Security Incident Response hinzufügen, um Security Incident-Daten nach geografischem Standort anzuzeigen. Mit einer Karte können Sie Detailinformationen zu Security Incidents nach Standort anzeigen.

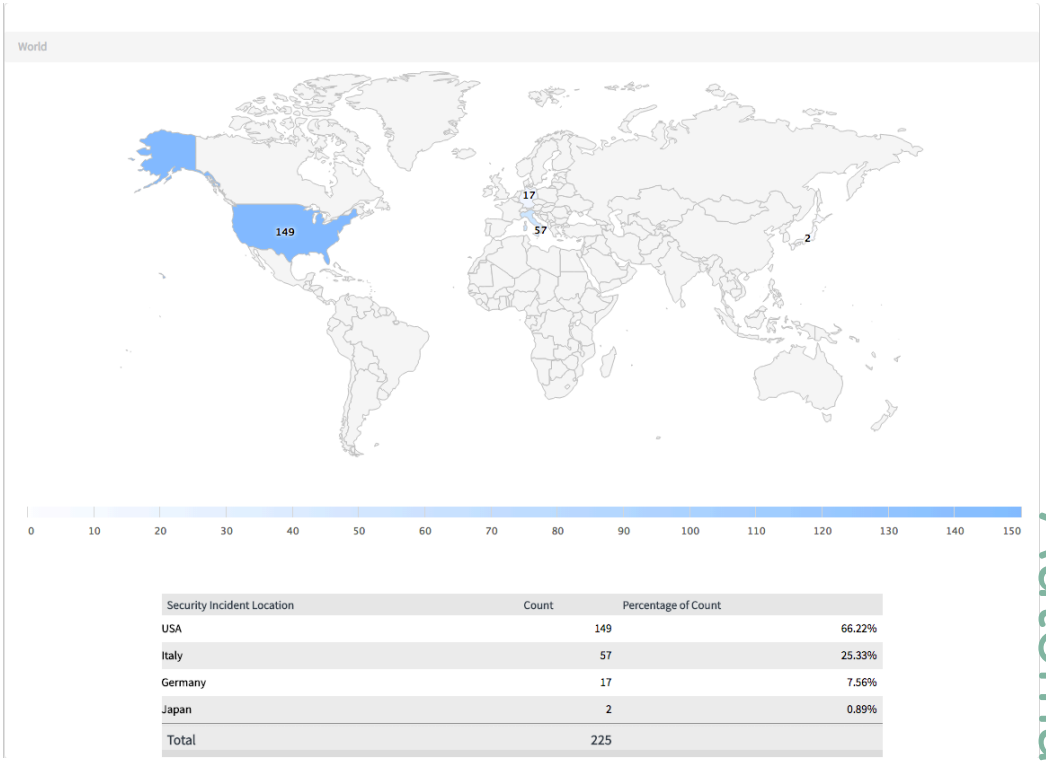
#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**.
2. Klicken Sie oben links auf der Seite auf **Inhalt** hinzufügen, um die Steuerung für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Berichte**.
4. Klicken Sie im zweiten Auswahlfeld auf **Security Incident**.
5. Klicken Sie im dritten Auswahlfeld auf **Security Incident map**(Security Incident-Übersicht).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




| Security Incident Location | Count | Percentage of Count |
|---|---|---|
| USA | 149 | 66.22% |
| Italy | 57 | 25.33% |
| Germany | 17 | 7.56% |
| Japan | 2 | 0.89% |
| Total | 225 | |

6. Klicken Sie unten auf dem Bildschirm auf die Stelle auf dem Bildschirm, die Sie dem Bericht hinzufügen möchten.
7. Schließen Sie das Feld **Inhalt** hinzufügen.

### Ändern Sie die Security Incident-Zuordnung

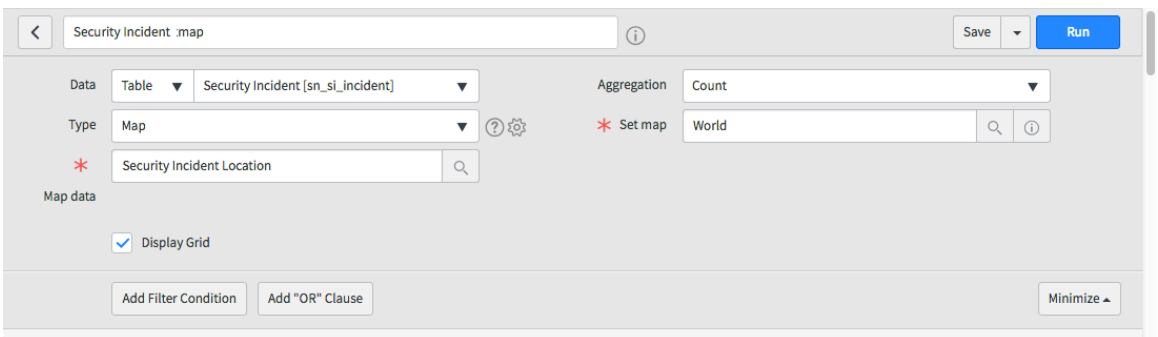
Administratoren in der globalen Domäne können mithilfe von Filtern ändern, wie in der Security Incident Map Security Incidents behandelt werden.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Berichte** > **Administration** > **Alle**.
2. Suchen Sie nach der **Security Incident-Karte**.
3. Klicken Sie **auf Bericht bearbeiten**.




4. Klicken Sie auf **Filterbedingung** hinzufügen, um Filter hinzuzufügen oder zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.


Automatische Übersetzung

5. Klicken Sie auf **Ausführen**, um die angewendeten Änderungen anzuzeigen.
6. Klicken Sie auf **Speichern**.

### Security Incident-Verzeichnisübersichten

Wenn das Plugin Security Incident Analytics aktiviert ist, können Sie die Verzeichnisübersichten „Security Incident – Serviceauswirkung“ und „Security Incident – Echtzeit“ der Security Incident Response -Übersicht hinzufügen. Nachdem sie hinzugefügt wurden, können Sie die Verzeichnisübersichten konfigurieren, indem Sie die Verzeichnisübersichtskategorien und -indikatoren ändern.

### Fügen Sie der Security Incident Response-Übersicht Verzeichnisübersichten hinzu

Verzeichnisübersichten zeigen hierarchische (baumstrukturierte) Daten als Satz verschachtelter Rechtecke an. Jede Verzweigung der Struktur erhält ein Rechteck, das dann mit kleineren Rechtecken gekachelt wird, die Unterverzweigungen darstellen. Mit Verzeichnisübersichten können Sie Informationen zu Security Incidents auf dynamische und ansprechende Weise anzeigen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**.
2. Klicken Sie oben links auf der Seite auf **Inhalt** hinzufügen, um die Steuerung für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Verzeichnisübersicht**.
4. Wählen Sie im zweiten Auswahlfeld aus der folgenden Liste die Verzeichnisübersicht aus, die Sie einfügen möchten:
   - Security Incident – Serviceauswirkung
   - Security Incident – Echtzeit
   - Security Incident – Geschäftsauswirkung
   - Signifikanz der Schwachstelle

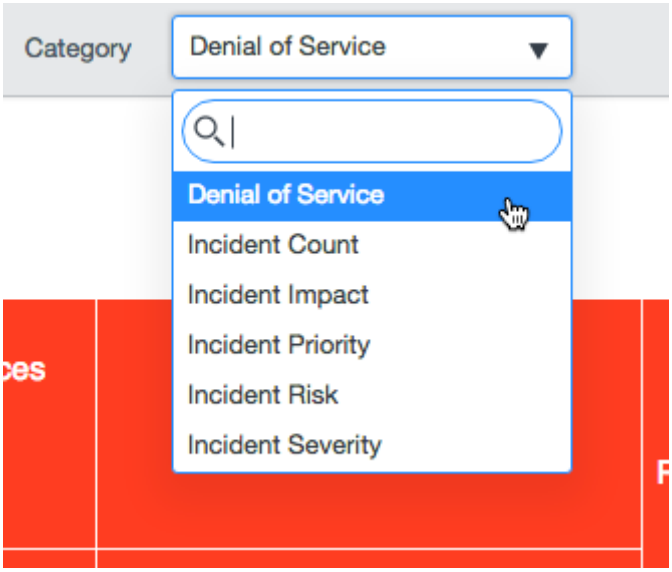
   **Hinweis:**
   Die Geschäftsauswirkungs-Treemap wird standardmäßig auf der Homepage Security Incident Response angezeigt. Für die Serviceauswirkungs- und Echtzeit-Treemaps muss das Plugin „Security Incident Analytics“ aktiviert sein.

5. Wählen Sie im dritten Auswahlfeld die Granularitätsebene der Informationen aus, die für die ausgewählte Verzeichnisübersicht abgerufen werden sollen.

   **Hinweis:**
   Wählen Sie für die Verzeichnisübersicht Security Incident - Service Impact **Security Incident** im dritten Auswahlfeld aus. Diese Auswahl stellt eine Dropdown-Liste mit mehreren Datenkategorien bereit.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie unten auf dem Bildschirm auf die Stelle auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
7. Schließen Sie das Feld **Inhalt** hinzufügen.

### Erstellen oder aktualisieren Sie eine Verzeichnisübersichtskategorie

Sie können die vordefinierten Kategorien für die Security Incident-Verzeichnisübersichten ändern oder nach Bedarf Kategorien erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Verzeichnisübersichten verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

#### Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem sind Verzeichnisübersichtskategorien wie Incident-Risiko, Denial of Service und Incident-Schweregrad enthalten. Sie können diese Kategorien ändern oder nach Bedarf weitere Kategorien definieren.

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration**, und öffnen Sie die Verzeichnisübersicht, für die Sie Kategorien konfigurieren möchten:
   - **Servicerelevanz-Berichterstellungsdefinition**
   - **Echtzeitdefinition**
2. **Wahlweise:** Ändern Sie den Namen der Verzeichnisübersicht.
   Im Basissystem lautet der Standardname für die Definition der Serviceauswirkungs-Treemap **Security Incident**. Der Standardname für die Echtzeit-Treemap-Definition lautet **Security Incident – Echtzeit**.
3. Ändern Sie den Wert der **PA-Indikatorgruppe** nicht, es sei denn, Sie verwenden eine benutzerdefinierte Verzeichnisübersicht.
4. Um die Verzeichnisübersicht zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
   Wenn Sie beispielsweise die Kategorie „Denial of Service“ im Systemauswirkungs-Dashboard deaktivieren, ist diese Verzeichnisübersicht nicht verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der zugehörigen Liste „ **Treemap-Kategorien** “ eine zu ändernde Kategorie aus, oder klicken Sie auf **Neu**, um eine neue Kategorie zu erstellen.
6. Füllen Sie die Felder aus.

**Formular „Treemap-Kategorie“**

| Feld | Beschreibung |
|---|---|
| Name | Der Name, der für die Kategorie in der Liste „ **Kategorien** “ über der Verzeichnisübersicht angezeigt wird. |
| Bestellung | Die Reihenfolge, in der die Kategorie in der Liste „ **Kategorien** “ über der Verzeichnisübersicht angezeigt wird. |
| Verzeichnisübersicht | Der Name der Verzeichnisübersicht, die diese Kategorie verwendet. |
| Farbe | Die Farbe, die für diese Kategorie in der Verzeichnisübersicht angezeigt wird. |
| Aktiv | Wählen Sie diese Option aus, um diese Kategorie zu aktivieren. |
| Beschreibung | Eine Beschreibung der Kategorie. |
| Für alle Rollen sichtbar | Wählen Sie diese Option aus, um diese Kategorie für alle Benutzer unabhängig von ihrer Rolle sichtbar zu machen. |
| Rollen | Wenn Sie die Checkbox Für **alle Rollen sichtbar** nicht aktiviert haben, wählen Sie die Rollen aus, die diese Kategorie anzeigen können. |

7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

### Erstellen oder aktualisieren Sie einen Verzeichnisübersichtsindikator

Sie können die vordefinierten Indikatoren für eine Verzeichnisübersicht ändern oder neue Indikatoren erstellen. Für jeden Indikator können Sie die Datenquelle konfigurieren und angeben, wie Listen von Security Incidents aus Verzeichnisübersichten geöffnet werden, die mit dem Indikator angezeigt werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Verzeichnisübersichten verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

#### Prozedur

1. Öffnen Sie die Verzeichnisübersichtsdefinition, für die Sie Indikatoren konfigurieren möchten.
2. **Wählen** Sie in der zugehörigen Liste Verzeichnisübersichts-Kategorien die Kategorie aus, für die Sie Indikatoren konfigurieren möchten.
3. Wählen Sie in der zugehörigen Liste „ **Treemap-Indikatoren** “ einen zu ändernden Indikator aus, oder klicken Sie auf **Neu**, um einen neuen Indikator zu erstellen.
4. Füllen Sie die Felder aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Treemap-Indikator“.**

| Feld | Beschreibung |
|---|---|
| Name | Der Name, der für den Indikator in der Liste **Indikatoren** im Serviceauswirkungs-Dashboard angezeigt wird. |
| Kurzbeschreibung | Eine Beschreibung, die für den Indikator in der Liste **Indikatoren** über der Verzeichnisübersicht angezeigt wird. |
| Ergebnisgrenzwert | Die maximal zulässige Anzahl von Ergebnissen. Die Obergrenze ist 100. |
| Ergebnisgenauigkeit | Die Anzahl der Nachkommastellen, die angezeigt werden sollen.<br>Dieses Feld wird nur für die Echtzeit-Treemap-Definition angezeigt. |
| Aktiv | Kontrollkästchen, um diesen Indikator zu aktivieren. |
| Kategorie | Der im vorherigen Bildschirm eingegebene Kategoriename. |
| Richtung | Gibt an, ob die Kachel in der Verzeichnisübersicht minimiert oder maximiert wird.<br>Dieses Feld wird nur für die Echtzeit-Treemap-Definition angezeigt. |
| Einheit | Die Maßeinheit, die für die Metrik verwendet werden soll.<br>Dieses Feld wird nur für die Echtzeitdefinition angezeigt. |
| Automatisches Aktualisierungsintervall | Wie oft die Verzeichnisübersicht aktualisiert werden soll. |
| Bestellung | Die Reihenfolge, in der der Indikator in der **Indikatorenliste** über der Verzeichnisübersicht angezeigt wird. |



5. Klicken Sie auf die Registerkarte **Datenquellenkonfiguration**, und konfigurieren Sie eine der folgenden Datenquellenoptionen für den Indikator.

6. Klicken **Sie** auf die Registerkarte Clickthrough, und geben Sie an, wie Listen von Security Incidents aus der Verzeichnisübersicht geöffnet werden sollen.
   a. Wählen Sie im Feld **Clickthrough-URL-Navigationstyp** aus, ob die Liste der Security Incidents in einem neuen Fenster, im selben Fenster oder in einem Dialogfeld geöffnet werden soll.
   b. **Wahlweise:** Ändern Sie im Feld **Clickthrough-URL-Skript** das Beispielskript bei Bedarf.
7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie einer Übersicht Schwachstellen-Bedeutungsdiagramme hinzu

Wenn das Plugin Vulnerability Response aktiviert ist, können Sie der Übersicht Diagramme zur Bedeutung von Schwachstellen und andere Visualisierungen hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Navigieren Sie zur Übersichtsseite, der Sie die Anzeige für die Signifikanz der Schwachstelle hinzufügen möchten.
2. Klicken Sie oben links auf der Seite auf **Inhalt** hinzufügen, um die Steuerung für die Widget-Auswahl zu öffnen.
3. Treffen Sie in den drei Auswahlfeldern die Auswahl abhängig von der Anzeige (Baumübersicht oder Punktzahlbericht), die Sie hinzufügen möchten:
   - Um die Strukturzuordnung für die Bedeutung der Schwachstelle hinzuzufügen, treffen Sie diese Auswahl:
     - Verzeichnisübersicht
     - Signifikanz der Schwachstelle
     - Signifikanz der Schwachstelle
   - Um den Bericht über die Signifikanzpunktzahl der Schwachstelle hinzuzufügen, treffen Sie diese Auswahl:
     - Performance Analytics
     - Punktzahl
     - Services mit Schwachstellenbedeutung
4. Klicken Sie auf die Stelle auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie das Feld **Inhalt** hinzufügen.

## Management schwerwiegender Sicherheits-Incidents

Die Anwendung ServiceNow® Management schwerwiegender Sicherheits-Incidents verfolgt den Fortschritt von Major Security Incident (MSI) von der Erkennung über die Analyse, das Vorschlagen, Hochstufen und Verknüpfen von Security Incidents bis hin zum Abschluss.

Management schwerwiegender Sicherheits-Incidents

| Erkunden | Konfigurieren | integrieren |
|---|---|---|
| Erfahren Sie, wie Analysten, Administratoren und Manager Major Security Incident Management (MSIM) verwenden. | Planen und konfigurieren Sie Ihre Implementierung | Erweitern Sie die MSIM-Fähigkeiten durch die Integration mit anderen Microsoft -Anwendungen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Verwalten | Verwenden | Statusberichte |
|---|---|---|
| Administrationsaufgaben zum Kennzeichnen von Incident-Datensätzen und zum Konfigurieren von Bezeichnungen | Datensätze zu schwerwiegenden Security Incidents über die Arbeitsbereichsverwaltung vorschlagen, heraufstufen, verknüpfen und ablehnen | Incident-bezogene Aufgaben überwachen und Prozesse durch Metriken, Trenddiagramme und Berichte verbessern |
| **Zusätzliche Fähigkeiten** | | |
| Konfigurieren Sie Informationen, um für Datensätze ein Rollup durchzuführen | | |

## Fordern Sie Apps im Store an

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Security Operations-Apps im Store anfordern

Wenn Sie ein neuer Security Operations -Kunde mit der Version Rome oder höher sind, besuchen Sie die ServiceNow Store -Website, um die verfügbaren Apps und Informationen zum Senden von Anforderungen an den Store anzuzeigen.

## Weitere Ressourcen

Besuchen Sie das Management schwerwiegender Sicherheits-Incidents Forum auf der ServiceNow Community.

## Major Security Incident Management erkunden

Erkunden Sie Management schwerwiegender Sicherheits-Incidents, um zu verstehen, wie die Anwendung in Bezug auf die Nachverfolgung kritischer Security Incidents mit hoher Priorität funktioniert, die als Bedrohung für die Organisation identifiziert werden.

In diesem Abschnitt erfahren Sie mehr über die wichtigsten Funktionen und die verschiedenen Rollen, die bei der Arbeit mit Datensätzen zu schwerwiegenden Security Incidents eine Rolle spielen. Dieser Abschnitt hilft Ihnen auch dabei, die ersten Schritte mit der Anwendung, die Voraussetzungen und Plugins zu verstehen, die für die Arbeit mit der Anwendung erforderlich sind.

### Management schwerwiegender Sicherheits-Incidents

Verfolgen und verwalten Sie verschiedene Aktivitäten, die normalerweise Teil der Lösung eines schwerwiegenden Security Incident sind, über Management schwerwiegender Sicherheits-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incidents. Über einen intuitiven Arbeitsbereich können Incident-Manager und diejenigen, die an einem Incident arbeiten, Incidents vorschlagen und zu schwerwiegenden Incidents heraufstufen, Aktivitäten zu schwerwiegenden Security Incidents nachverfolgen und problemlos mit Kollegen zusammenarbeiten.

## Übersicht

Die Funktionen für das Management schwerwiegender Security Incidents funktionieren in Verbindung mit den vorhandenen Security Incident Response-Produktfunktionen. Dies umfasst die Möglichkeit für einen Sicherheitsanalysten, einen standardmäßigen Security Incident zu einem schwerwiegenden Security Incident zu eskalieren, sodass die neuen Produktfunktionen zur Unterstützung des Korrekturprozesses verfügbar sind.

Nach der Installation von in Ihrer Instanz von ServiceNow kann ein Security Incident-Analyst:

- Schlagen Sie einen Security Incident dem Kandidaten für einen schwerwiegenden Security Incident vor, um einen Überprüfungsprozess für die Notwendigkeit der Erstellung eines schwerwiegenden Security Incident zu initiieren.
- Stufen Sie einen Security Incident direkt zu einem schwerwiegenden Security Incident hoch, ohne dass ein zusätzlicher Überprüfungsprozess erforderlich ist.
- Lehnen Sie einen Security Incident ab, der als schwerwiegender Security Incident (Major Security Incident, MSI) vorgeschlagen wird.
- Verknüpfen Sie einen Security Incident als untergeordneten Incident mit dem schwerwiegenden Security Incident (Major Security Incident, MSI), damit alle Security Incidents bearbeitet werden können.

## Schlüsselfunktionen

Major Security Incident Management (MSIM) verbessert den Korrekturprozess für schwerwiegende Security Incidents mit den folgenden Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der für die Benutzerrolle „Manager für schwerwiegende Security Incidents“ entwickelt wurde.
- Organisieren Sie Reaktionsaufgaben für mehrere „untergeordnete“ Security Incidents.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chat-Kommunikationskanälen, nachdem ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien), die sich auf den schwerwiegenden Security Incident beziehen, über eine Microsoft SharePoint -Integration.
- Chat-Channel-Manager- und Aktivitätenstrom-Komponenten zur Verwaltung der Kommunikation über mehrere Sicherheits-, IT- und Funktionsgruppen hinweg über eine Microsoft Teams -Integration.

## Arbeitsbereichskomponenten

Das Produkt Management schwerwiegender Sicherheits-Incidents enthält mehrere neue Arbeitsbereichskomponenten und Benutzeroberflächenseiten, die die wichtigsten Features und Funktionen bereitstellen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Benutzerrolle „Manager für schwerwiegende Security Incidents“ entwickelt wurde.
- Organisieren Sie Reaktionsaufgaben für mehrere untergeordnete Security Incidents.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chat-Kommunikationskanälen, nachdem ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien), die sich auf den schwerwiegenden Security Incident beziehen, über eine Microsoft SharePoint -Integration.
- Chat-Channel-Manager- und Aktivitätenstrom-Komponenten zur Verwaltung der Kommunikation über mehrere Sicherheits-, IT- und Funktionsgruppen hinweg über eine Microsoft Teams -Integration.

## Unterstützte Versionen von Major Security Incident Management

Management schwerwiegender Sicherheits-Incidents (MSIM) erfordert die Rome-Version von Now Platform®.

Diese Funktion unterstützt Microsoft Teams, einen chatzentrierten Arbeitsbereich in der Suite Microsoft Office 365. Früher war Microsoft Teams eine separate Installation der Anwendungen Microsoft Office 365.

## Unterstützte Versionen Now Platform .

Diese Funktion wird ab Rome und späteren Releases unterstützt.

Die folgenden Security Operations -Anwendungen sind die standardmäßigen Security Incident Response -Plugins, die wahrscheinlich für die meisten Benutzer installiert werden, wenn sie bereits Security Incident Response (SIR) verwenden. Wenn nicht installiert, müssen Sie über ServiceNow Storeinstallieren und aktivieren. Installieren und aktivieren Sie jeweils eine Anwendung in der angegebenen Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Incident Response: com.snc.si_dep ist das abhängige Plugin. Durch die Installation dieses Plugins werden die anderen Security Operations-Anwendungen aktiviert.
2. Security Integration Framework
3. Security Support Common
4. Security Support Common Orchestration

### Erste Schritte mit MSIM

Überprüfen Sie die folgenden Informationen, bevor Sie mit Management schwerwiegender Sicherheits-Incidentsarbeiten.

Erforderliche Rolle: sn_msi.workspace_admin.

Für eine einfache Installation und Konfiguration der Anwendung Management schwerwiegender Sicherheits-Incidents müssen Sie möglicherweise überprüfen, ob die folgenden Plugins aktiviert sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Wichtig:**
Ein Update Set (KB1289784 ) ist im Schnellstartleitfaden für Major Security Incident Management verfügbar, um Benutzern mit einer einfachen Konfiguration zu helfen. Sie müssen das Update Set importieren, nachdem Sie die Installation der Anwendung abgeschlossen haben. Befolgen Sie das Verfahren im Schnellstartleitfaden (Schritt 2) im Abschnitt „Unterstützende Dokumente“ in der MSIM-Anwendung im ServiceNow Store.

### Voraussetzung

| Aufgabe | Beschreibung |
|---|---|
| Bevor Sie mit der Anwendung beginnen, stellen Sie sicher, dass Sie über die erforderlichen abhängigen Plugins verfügen. | Installieren Sie als ersten Schritt:<br>• ServiceNow IntegrationHub-Installationsprogramm (com.glide.hub.integrations)<br>• ServiceNow® IntegrationHub Laufzeit (com.glide.hub.integration.runtime).<br>• ServiceNow® IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)<br>• ServiceNow® IntegrationHub Aktionsvorlage – Datenstrom (com.glide.hub.action_type.datastream)<br>• ServiceNow® IntegrationHub Flow Designer – Dynamische Eingaben (com.glide.hub.dynamic_inputs)<br>**Hinweis:** Wenn Sie nicht über die erforderlichen Berechtigungen für eines der aufgeführten ServiceNow® IntegrationHub -Plugins verfügen, erstellen Sie ein Support-Ticket, um die erforderlichen Anwendungen zu installieren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Zugriffsrechte für die Installation von Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke verfügen.<br>**Hinweis:** Die oben aufgeführten sind die primären abhängigen Anwendungen, um mit Management schwerwiegender Sicherheits-Incidentszu beginnen. | Stellen Sie vor der Installation von Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke sicher, dass Sie über den erforderlichen Zugriff auf die Anwendungen ServiceNow IntegrationHub verfügen.<br>**Hinweis:** Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke sind abhängige Anwendungen zu ServiceNow® IntegrationHub Anwendungen. |

### Prüfliste für das Setup von MSIM .

Bevor Sie die Anwendung ServiceNow® Management schwerwiegender Sicherheits-Incidents (MSIM) verwenden, laden Sie die Anwendung aus dem ServiceNow® Storeherunter.

Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration in der folgenden Tabelle nach.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die der Anwendung Management schwerwiegender Sicherheits-Incidents zugewiesenen Rollen werden in den folgenden Abschnitten aufgeführt. Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen.

Führen Sie die folgende Prüfliste durch die End-to-End-Schritte zur Installation und Konfiguration der Anwendung Management schwerwiegender Sicherheits-Incidents.

**Prüfliste**

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Management schwerwiegender Sicherheits-Incidents über ServiceNow® Store] installiert und aktiviert wurde. | Management schwerwiegender Sicherheits-Incidents v1.1.1 ist auf ServiceNow® Storeverfügbar.<br><br>Befolgen Sie diese Anweisungen: Herunterladen einer Anwendung aus dem ServiceNow Store. |
| Vergewissern Sie sich, dass die folgenden Anwendungen in der angegebenen Reihenfolge installiert wurden. | Die folgenden Anwendungen werden standardmäßig installiert, nachdem Sie die Anwendung Management schwerwiegender Sicherheits-Incidents in der aktuellen Release-Version der Anwendung installiert haben:<br>• File Explorer Core for Security Operations v1.1.1<br>• Microsoft SharePoint File Explorer Connector für Security Operations v1.1.1<br>• File Explorer ]-Komponente für Security Operations v1.0.0<br>• Microsoft Teams Chat Connector für Security Operations v1.0.0<br>• Chat-Core für Security Operations v1.0.0<br>• Major Security Incident Antwort v1.1.1<br>• Collab Chat EVAM-Karte für MSIM Workspace v1.0.0 (Diese Anwendung wird nur für die UI-Visualisierungen im Anwendungshintergrund für Management schwerwiegender Sicherheits-Incidents Workspace eingerichtet.)<br>• UI-Komponente des Aufgabenorganisators für Management schwerwiegender Sicherheits-Incidents workspace 1.0.0<br>• Security Incident Response v12.8.1 |
| Vergewissern Sie sich, dass die Benutzerrollen Major Security Incident zugewiesen sind. | Im Folgenden sind die Rollen aufgeführt, die während des gesamten Incident-Lebenszyklus des Korrekturprozesses Major Security Incident eine Rolle spielen: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| | • MSI-Administrator [sn_msi.workspace_admin]<br>• MSI-Manager [sn_msi.workspace_manager]<br>• MSI-Responder [sn_msi.workspace_responder<br><br>Ausführlichere Informationen zu den einzelnen Rollen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen. |
| Vergewissern Sie sich, dass Sie die Konfiguration Microsoft SharePoint v1.0.0 erfolgreich eingerichtet haben. | Microsoft SharePoint verwaltet Sites, Ordner, Dateien, Gruppen und Benutzer in Microsoft SharePoint.<br><br>Fügen Sie Microsoft SharePoint Daten zu Ihrer Instanz ServiceNow® hinzu. Dazu müssen Sie Graph- und REST-Verbindungen einrichten.<br><br>Weitere Informationen zum Einrichten der Konfiguration von REST- und Graph-Verbindungen finden Sie in der Dokumentation zuMicrosoft SharePoint-Spoke v1.1.2.<br><br>Stellen Sie eine Graph- und REST-Verbindung her, um eine Verbindung zu Ihrer Instanz [ ServiceNow® von Microsoft SharePointherzustellen. |
| Vergewissern Sie sich, dass Sie eine Microsoft SharePoint -Website erstellt haben, um eine Dokumentbibliothek zu erstellen. | Erstellen Sie bei Bedarf eine Microsoft SharePoint -Website, oder verwenden Sie eine vorhandene Website, um unsere Dokumentbibliothek zu erstellen. |
| Vergewissern Sie sich, dass Sie eine Dokumentbibliothek unter der Website Microsoft SharePoint erstellt haben. | Erstellen Sie eine dedizierte Dokumentbibliothek unter einer neuen oder vorhandenen Microsoft SharePoint -Website. |
| Stellen Sie sicher, dass die erforderlichen Berechtigungen für die Benutzer bereitgestellt und den erforderlichen Benutzergruppen in Microsoft SharePointzugewiesen werden. | Verwalten Sie den Zugriff von der Website Microsoft SharePoint auf verschiedene Benutzer und Benutzergruppen. |
| Vergewissern Sie sich, dass Sie das Laufwerk Microsoft SharePoint und die | Um die Laufwerkskonfigurationen zu überprüfen, richten Sie Microsoft SharePoint |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| erforderlichen Konfigurationseinstellungen erstellt und konfiguriert haben. | Datei-Explorer-Connector, Ordner- und Dateiaktionen und Ordnervorlagen ein:<br>• Konfigurieren Sie das Laufwerk Datei-Explorer Repository .: Erstellt eine Verbindung von Microsoft SharePoint zu Instanz ServiceNow®.<br>• Konfigurieren Sie die Einstellungen für Ordner- und Dateiaktionen: Konfigurieren und steuern Sie die einzelnen Ordner- und Dateiaktionen, die in der Datei-Explorer-Komponente angezeigt werden.<br>• Erstellen Sie Ordnervorlagen: Konfigurieren Sie, um eindeutige Ordner für verschiedene Typen schwerwiegender Security Incidents zu erstellen. |
| Vergewissern Sie sich, dass Sie erfolgreich eine Verbindung zur Microsoft Teams Chat Connector-Anwendung hergestellt haben. | Führen Sie das hier erläuterte Verfahren aus, um eine Verbindung der Microsoft Teams Chat Connector-Anwendung mit der Instanz ServiceNow® herzustellen: Stellen Sie eine MS Teams Graph-Verbindung auf her Now Platform. |
| Vergewissern Sie sich, dass Sie Microsoft Teams mit der Instanz Now Platform® konfiguriert und Konfigurationen für Verbindungen und Anmeldeinformationen erstellt haben. | Gehen Sie wie folgt vor, um die Konfiguration von ServiceNow® mit der Instanz Microsoft Teams zu überprüfen:<br>• Stellen Sie eine MS Teams Graph-Verbindung auf her Now Platform<br>• Erstellen Sie eine Chatkanalvorlage |
| Vergewissern Sie sich, dass die Konfigurationseinstellungen für „Administration schwerwiegender Security Incidents“ erfolgreich sind. | Als MSI-Administrator müssen Sie in der Lage sein:<br>• bestimmen, ob Sicherheitsanalysten den Incident vorschlagen und heraufstufen und andere Security Incidents verknüpfen können.<br>• Benachrichtigungen aktivieren oder deaktivieren, wenn ein Incident vorgeschlagen oder heraufgestuft wird. Möglichkeit zum Bearbeiten von Standardvorlagennachrichten.<br>• Konfigurieren Sie Sicherheits-Tags, die in der Benutzeroberfläche für Sicherheitsanalysten angezeigt werden, um die Incidents zu unterscheiden, die als Kandidaten für schwerwiegende |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prüfliste (Fortsetzung)

| Setupaufgabe | Beschreibung |
|---|---|
| | Security Incidents vorgeschlagen oder zu schwerwiegenden Security Incidents heraufgestuft wurden. |
| Stellen Sie sicher, dass die Einstellungen für „Administration schwerwiegender Security Incidents – Benachrichtigungen“ erfolgreich sind. | Als MSI-Administrator E-Mail-Benachrichtigungen auslösen, wenn ein Security Incident vorgeschlagen und an alle Benutzer und Gruppen gesendet wird, die für die Benachrichtigungsliste konfiguriert sind. Weitere Informationen finden Sie unter Legen Sie die Benachrichtigungseinstellungen für fest MSIM. |

## Management schwerwiegender Sicherheits-Incidents Rollen

Weisen Sie Rollen zu, um sicherzustellen, dass Benutzer alle erforderlichen Aktionen in der MSIM-Anwendung ausführen können.

### Rollen für Management schwerwiegender Incidents

| Rollentyp | Rolle | Beschreibung |
|---|---|---|
| MSI-Administrator | sn_msi.workspace_admin | Kann ich Management schwerwiegender Incidents installieren und konfigurieren und die abhängigen Anwendungen einrichten, z. B. File Explorer (FE), Microsoft Teams- und Chat-Kanal-Konfiguration, Workspace-Setup und MSI-Administration: Setup von Konfigurationen und Benachrichtigungen?<br><br>So richten Sie ein:<br><br>• Datei-Explorer (FE)-Komponente:<br>◦ Konfigurieren Sie das Datei-Repository.<br>◦ Konfigurieren Sie Datei- und Ordneraktionen, die in der Komponente „Dateiexplorer“ der Registerkarte „Zusammenarbeit“ im Arbeitsbereich „Major Security Incident Management“ bereitgestellt werden.<br>◦ Erstellen Sie die Stammordner und Unterordner, und gewähren Sie Zugriff auf die Unterordner. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Rollen für Management schwerwiegender Incidents (Fortsetzung)**

| Rollentyp | Rolle | Beschreibung |
|---|---|---|
| | | • Chat-Kanalverwaltung<br>○ Aktivieren und konfigurieren Sie Microsoft Teams, indem Sie die Verbindung Microsoft Teams ] validieren.<br>○ Chat-Teams und Chat-Kanäle erstellen, Benutzer hinzufügen und Benutzer den verschiedenen Benutzergruppen zuweisen.<br>• MSI-Administration:<br>○ Konfigurationen: Konfigurieren Sie die Aktionen von Sicherheitsanalysten, Benachrichtigungen, die gesendet werden, wenn Incidents vorgeschlagen und heraufgestuft werden, und zeigen Sie Tags für die Security Incidents an.<br>○ Benachrichtigungen: Automatisieren Sie den E-Mail-Benachrichtigungsprozess und Benutzerbenachrichtigungen, wenn ein Security Incident entweder vorgeschlagen oder als schwerwiegender Security Incident heraufgestuft wird. |
| MSI-Manager | sn_msi.workspace_manager | • Zeigen Sie den Zugriff auf die Seite mit den Konfigurationseinstellungen für die Verwaltung schwerwiegender Security Incidents an. Die Konfigurationseinstellungen können nicht geändert werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Rollen für Management schwerwiegender Incidents (Fortsetzung)**

| Rollentyp | Rolle | Beschreibung |
|---|---|---|
| | | • Zeigen Sie Incident-Datensatzdaten auf den Registerkarten **Details**, **Zusammenarbeit**und **Aufgabenorganisator** des Arbeitsbereichs Management schwerwiegender Incidents an, und bearbeiten Sie sie.<br>• Stufen Sie den Security Incident zu einem schwerwiegenden Security Incident herauf.<br>• Konfigurieren Sie Datei- und Ordneraktionen, die in der Datei-Explorer-Komponente auf der Registerkarte **Zusammenarbeit** des Arbeitsbereichs Management schwerwiegender Incidents verfügbar sind.<br>• Verknüpfung zusätzlicher Datensätze mit schwerwiegenden Security Incidents aus dem Arbeitsbereich wird aufgehoben bzw. aufgehoben. |
| MSI-Responder | sn_msi.workspace_responder | • Ansichts- und Bearbeitungszugriff (nur) auf **Details** und **Aufgaben** -Registerkarten des Arbeitsbereichs Management schwerwiegender Incidents.<br>• Verknüpfung zusätzlicher Datensätze mit schwerwiegenden Security Incidents aus dem Arbeitsbereich wird aufgehoben bzw. aufgehoben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Wird integriert Management schwerwiegender Sicherheits-Incidents

Erweitern Sie die Fähigkeiten von Management schwerwiegender Sicherheits-Incidents, und stellen Sie eine Verbindung mit der Instanz Now Platform her, indem Sie mit Anwendungen von Microsoft integrieren.

**Wichtig:**
Ein Update Set (KB1289784 ) ist im Schnellstartleitfaden für Major Security Incident Management verfügbar, um Benutzern mit einer einfachen Konfiguration zu helfen. Sie müssen das Update Set importieren, nachdem Sie die Installation der Anwendung abgeschlossen haben. Befolgen Sie das Verfahren im Schnellstartleitfaden (Schritt 2) im Abschnitt „Unterstützende Dokumente“ in der MSIM-Anwendung im ServiceNow Store.

### Richten Sie die Dokumentbibliothek Microsoft SharePoint ein

Überprüfen Sie das erforderliche Setup, das in Microsoft SharePointdurchgeführt werden muss.

#### Vorbereitungen

Vergewissern Sie sich, dass das folgende Konfigurationsverfahren abgeschlossen ist.

Erforderliche Rolle: Systemadministrator, sn_msi.workspace_admin

#### Prozedur

1. Erstellen Sie eine neue Dokumentbibliothek unter der neuen oder vorhandenen Microsoft SharePoint Site, und verwenden Sie dieselbe Site, während Sie die Konfiguration des Management schwerwiegender Sicherheits-Incidents Datei-Repositorys konfigurieren.
2. Registrieren Sie eine Anwendung bei Microsoft, um eine Verbindung herzustellen und mit Microsoft SharePointMicrosoft SharePoint über die REST-API [] zu kommunizieren.
   Durch die Registrierung der Anwendung wird eine Verbindung zwischen der App und Microsoft hergestellt. Weitere Informationen finden Sie unter Einrichten des reinen App-Zugriffs auf SharePoint im Portal docs.microsoft.com.

   Es gibt zwei Möglichkeiten, eine Anwendung bei Microsoft SharePointzu registrieren:

   a. Gewähren des Zugriffs über die Azure AD-Nur-App

   b. Gewähren des Zugriffs mit Microsoft SharePoint Nur App

   **Wichtig:**
   Das Gewähren des Zugriffs nur über die App Microsoft SharePoint ist ein älterer Ansatz, aber sehr relevant und einfach zu konfigurieren.

   Verwenden Sie die Client-ID und den geheimen Clientschlüssel, die im obigen Schritt generiert wurden, während Sie die REST-Verbindung für den Datei-Explorer-Connector Microsoft SharePoint konfigurieren.
3. Registrieren Sie eine weitere App bei Microsoft, um mit Microsoft SharePoint über Microsoft Graph APIs zu kommunizieren.
   Weitere Informationen finden Sie unter Anwendungen bei Microsoft Identity Platform registrieren
   **Registrieren Sie eine neue Anwendung in Azure mit der Now Platform-Instanz**

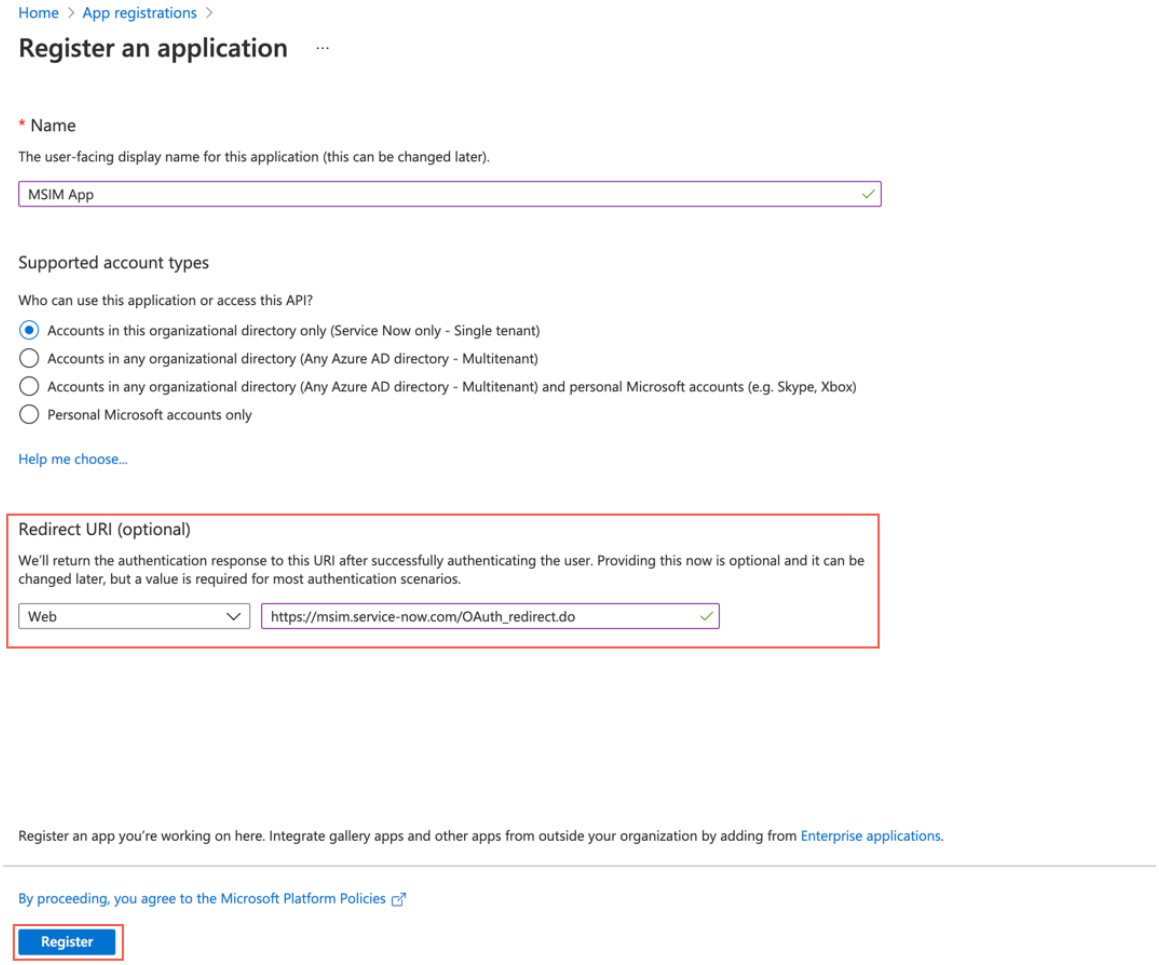
   a. Melden Sie sich mit Ihrem Konto Microsoft beim Azure- Portal an.

   b. Befolgen Sie die Anweisungen im Microsoft-Portal.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**c.** Geben Sie die Instanzumleitungs-URL Now Platform® im Feld „Zulässige Umleitungs-URL“ an. Beispiel: `msim.service-now.com/OAuth_redirect.do`




**d.** **Registrieren** die Anwendung.

**e.** Navigieren Sie zum Abschnitt **Zertifikate** und geheime Schlüssel, und erstellen Sie einen neuen geheimen Clientschlüssel.

> **Hinweis:**
> Sie können auch ein Client-Zertifikat hochladen und den generierten Fingerabdruckwert kopieren und speichern.

**f.** Kopieren und speichern Sie den generierten geheimen Clientschlüssel an einem beliebigen Ort, da er beim Konfigurieren der OAuth-Anwendungsregistrierung in der Instanz ServiceNow® erforderlich ist.

**4.** Fügen Sie unter **API-Berechtigungen**die Microsoft Graph-Berechtigung hinzu:

**a.** Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.

**b.** Wählen Sie **Microsoft Graph** aus.

**c.** Wählen Sie **Delegierte Berechtigungen aus**.

**d.** Wählen Sie in der Liste **Sites** die Berechtigung **Sites.ReadWrite.All aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Wählen Sie in der Liste **Benutzer** die Berechtigung **User.Read aus**.

f. Klicken Sie auf **Berechtigungen hinzufügen**.

5. Fügen Sie unter **API-Berechtigungen**die SharePoint-Berechtigung hinzu:

a. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.

b. Wählen Sie **SharePoint aus**.

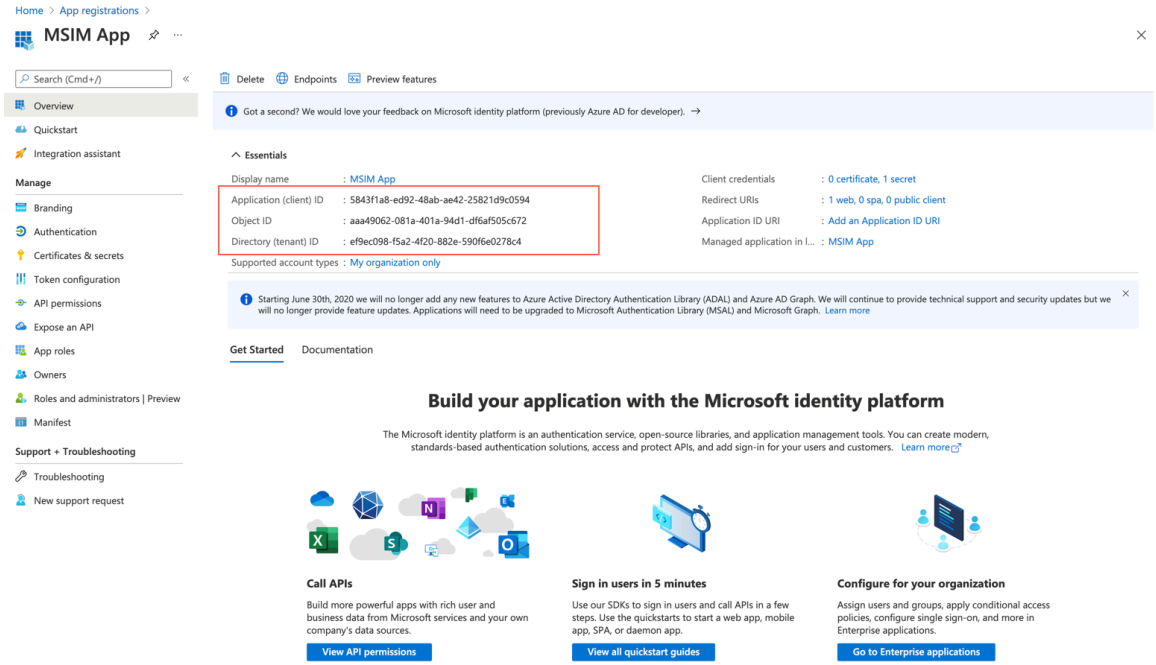
c. Wählen Sie **Anwendungsberechtigungen aus**.

d. Wählen Sie in der **Sites** -Liste die **Berechtigung Sites.FullControl.All aus**.

e. Klicken Sie auf **Berechtigungen hinzufügen**.

6. Klicken Sie nach dem Hinzufügen von Berechtigungen auf **„Administratoreinwilligung gewähren“**.

7. Verwenden Sie bei der Konfiguration der Graph-Verbindung für den Datei-Explorer-Connector Microsoft Teams dieselben Client-ID- und Client-Secret-Werte, die aus dieser Anwendungsregistrierung generiert wurden (verfügbar im Abschnitt „Übersicht“).




## Richten Sie Graph- und REST-Verbindungen in ein Now Platform

Konfigurieren Sie Graph- und REST-Verbindungen in der Instanz Now Platform für die Kommunikation mit Microsoft SharePoint.

Integrieren Sie die Instanz [ Now Platform und Microsoft SharePoint, indem Sie in Microsoft SharePoint eine benutzerdefinierte OAuth-Anwendung erstellen, um Now Platform-Anforderungen zu authentifizieren.

## Konfigurieren Sie die REST-Verbindung für MS SharePoint

Konfigurieren Sie die REST-Verbindung in der Instanz Now Platform für die Kommunikation mit Microsoft SharePoint.

### Vorbereitungen

Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Konfigurieren Sie einen neuen Mandantendatensatz, und wählen Sie **MicrosoftSharepointOnline** als Aliasdatensatz aus.
   Weitere Informationen finden Sie unter Microsoft SharePoint-Mandanten definieren.
2. So konfigurieren Sie den **MicrosoftSharepointOnline** -Alias für Verbindungen und Anmeldeinformationen: .
3. Wählen Sie den in Schritt 2 oben erstellten Mandantendatensatz wie folgt aus: **REST-Verbindung** beim Ausfüllen des Formulars **„Datei-Repository-Konfiguration** “.

## Konfigurieren Sie Graph Connection für MS SharePoint

Konfigurieren Sie die Graph-Verbindung in der Instanz Now Platform für die Kommunikation mit Microsoft SharePoint.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Informationen zum Konfigurieren des Alias für Graph-Verbindungen und -Anmeldeinformationen mit dem Client-Secret finden Sie unter .
   Führen Sie die folgenden Schritte aus, um den Alias für Graph-Verbindungen und -Anmeldeinformationen mithilfe des Client-Zertifikats zu konfigurieren.

   **Hinweis:**
   Standardmäßig werden hier in diesem Verfahren der JWT-Provider, der JWT-Schlüssel und das Zertifikat verwendet, die in der vorherigen REST-Verbindung konfiguriert wurden. Weitere Informationen finden Sie unter Konfigurieren Sie die REST-Verbindung für MS SharePoint.

   a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.

   b. Öffnen Sie den Datensatz **MicrosoftSharePointGraph**.

   c. Klicken Sie auf den zugehörigen Link **Neue Verbindung und Anmeldeinformationen erstellen**.

   d. Füllen Sie diese Details im Formular aus.

| Feld | Beschreibung |
|---|---|
| OAuth-Entitätsname | Name zur Identifizierung des OAuth-Anwendungsregistrierungsdatensatzes. |
| OAuth-Client-ID | Client-ID |
| Geheimer OAuth-Schlüssel | Sie können einen beliebigen Wert eingeben.<br>**Hinweis:**<br>Das ist nicht wichtig, da Sie die zertifikatbasierte Authentifizierung verwenden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| OAuth-Autorisierungs-URL | Autorisierungs-URL in folgendem Format: https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/authorize?response_mode=query |
| OAuth-Token-URL | Token-URL in folgendem Format: https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/token |
| Token-Sperr-URL | Token-Widerrufs-URL in folgendem Format: https://login.microsoftonline.com/<tenant-id> /oauth2/v2.0/token . |
| OAuth-Umleitungs-URL | ServiceNow Umleitungs-URL in diesem Format: https://empipaas.service-now.com/oauth_redirect.do |

**Hinweis:**
Sie können die Standardwerte entsprechend Ihren Anforderungen ändern.

e. Klicken Sie auf **OAuth-Token erstellen und abrufen**.
Eine Fehlermeldung mit der Aufforderung 401 – nicht autorisiert wird angezeigt.

f. Laden Sie das Formular neu, und öffnen Sie den Datensatz in der zugehörigen Liste **„Verbindungen** “.

g. Geben Sie den base64-codierten **Fingerabdruckwert** in das **AttributCodierter Fingerabdruckwert** im Abschnitt „Attribute“ ein.

**Hinweis:**
Der **Fingerabdruckwert** ist ein Hexadezimalwert. Sie können ein Hexadezimal-zu-Base64-Konvertierungstool (Hex in Base64) verwenden, um den **Fingerabdruckwert** in einen Base64-Wert zu codieren.

h. Navigieren zu **System-Oauth** > **Applikationsregistrierung**.

i. Öffnen Sie den Datensatz, der mit dem **OAuth-Entitätsnamen**identisch ist. Dies ist der Schritt in diesem Verfahren.

j. Ändern Sie das OAuth-API-Skript in: **OAuthUtilJWTFESPGraph**

k. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.

l. Öffnen Sie den Datensatz: **Microsoft SharePoint Graph-Anmeldeinformationen**.

m. Klicken Sie im Abschnitt „Zugehörige Links“ auf **OAuth-Token** abrufen.

2. Aktualisieren Sie den OAuth-Entitätsbereich.

a. Navigieren zu **System-Oauth** > **Applikationsregistrierung**.

b. Öffnen Sie den OAuth-Anwendungsregistrierungsdatensatz, der in Schritt 1 generiert wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**c.** Wählen Sie die zugehörige Liste **OAuth-Entitätsumfänge** aus.

**d.** Ersetzen Sie das Feld **OAuth-Anwendungsbereich** durch den folgenden Wert **offline_access** :

```
https://graph.microsoft.com/Sites.ReadWrite.All
```

**Hinweis:**
Sie können Schritt 2 ignorieren und mit dem nächsten Schritt fortfahren, wenn Sie ein Client-Zertifikat hinzufügen.

3. Konfigurieren Sie einen neuen Mandantendatensatz, und wählen Sie den Aliasdatensatz aus, wie in Schritt 1 erstellt.
Weitere Informationen finden Sie unter Microsoft SharePoint-Mandanten definieren.
4. Wählen Sie den in Schritt 3 erstellten Mandantendatensatz aus als: **Graph-Verbindung** beim Ausfüllen des Formulars „Datei-Repository-Konfiguration“.

### Stellen Sie eine MS Teams Graph-Verbindung auf her Now Platform

Integrieren Sie die Instanz Microsoft TeamsNow Platform und das Konto [], indem Sie eine Verbindung Microsoft Teams Graph herstellen.

**Vorbereitungen**
Wenn Sie möchten, können Sie dieselbe Anwendung verwenden, die Sie für SharePoint erstellt haben, um die Microsoft Teams Graph-Verbindung herzustellen.

Erforderliche Rolle: admin, Azure admin

**Registrieren Sie eine neue Anwendung in Azure für Microsoft Teams Graph-Verbindung**

**Prozedur**

1. Melden Sie sich mit Ihrem Konto Microsoft beim Azure- Portal an.
2. Navigieren zu **Azure-Services** > **Anwendungsregistrierung** > **Neue Registrierung**.
3. Geben Sie den Namen der Anwendung ein.
Beispiel: Microsoft Teams Graph.
4. Wählen Sie die entsprechende Option **Unterstützte** Kontotypen aus, die für Ihre Organisation gilt.
Wählen Sie beispielsweise die Option **Nur Accounts in diesem Organisationsverzeichnis (Nur ServiceNow – Einzelmandanten) aus**.

**Hinweis:**
Weitere Informationen zu unterstützten Kontotypen finden Sie unter Anwendungen bei Microsoft Identity Platform registrieren .

5. Wählen Sie **Webtyp** aus der Dropdown-Liste unter der Umleitungs-URL aus.
6. Geben Sie Now Platform Instanzumleitungs-URL in das Feld „Zulässige Umleitungs-URL“ ein.
Beispiel: https://<<InstanceName> >.service-now.com/oauth_redirect.do
7. Klicken Sie auf **Registrieren**, um Ihre neue Anwendung zu registrieren und sicherzustellen, dass die Seite mit dem Abschnitt „ **Übersicht** “ angezeigt wird.

### Verwenden von Zertifikaten für die Authentifizierung

Fordern Sie ein Zugriffstoken mit Zertifikatanmeldeinformationen an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

1. Sie können entweder ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgestelltes Zertifikat verwenden. Sie können ein selbstsigniertes Zertifikat erstellen, indem Sie das PowerShell-Skript ausführen (siehe Azure AD-Apps für den App-Only-Zugriff einrichten) . Das Skript generiert zwei Dateien: PFX-Datei und CER-Datei.

   **Hinweis:**
   Vergewissern Sie sich, dass Sie das Passwort kennen, das zum Verschlüsseln des privaten Schlüssels zum Generieren der PFX-Datei und der CER-Datei verwendet wird.

2. Verwenden Sie die PFX-Datei, um eine JKS-Datei (Java Key Store) zu erstellen.

   **Hinweis:**
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Generieren der JKS-Datei aus der PFX-Datei verwendet wird.

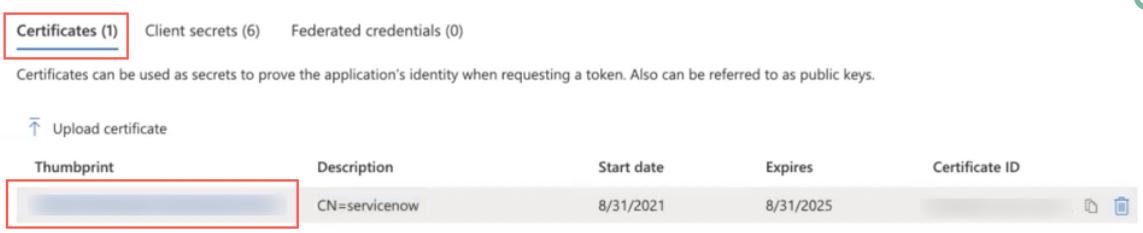
Erforderliche Rolle: admin

### Prozedur

1. Navigieren Sie im Azure AD-Portal zu **App-Registrierungen**.
2. Klicken Sie im Abschnitt „ **Verwalten** “ auf **Zertifikate und geheime** Schlüssel.
3. Klicken Sie auf der Registerkarte **Zertifikate** auf **Zertifikat hochladen**.
4. Füllen Sie diese Werte im Formular aus.

| Feld | Beschreibung |
|---|---|
| Laden Sie ein Zertifikat (öffentlichen Schlüssel) mit einem der folgenden Dateitypen hoch: .cer, .pem, .crt | .CER-Datei, die Sie mit dem PowerShell-Skript generiert haben. |
| Beschreibung | Beschreibung des Zertifikats |

5. Klicken Sie auf **Hinzufügen**.
   Das Zertifikat wird hochgeladen, und seine Details werden auf der Registerkarte **Zertifikate** angezeigt.
6. Kopieren Sie den **Fingerabdruckwert** des hochgeladenen Zertifikats.
   Der **Fingerabdruckwert** ist ein Hexadezimalwert.




7. Codieren Sie den **Fingerabdruckwert** in einen Base64-Wert, und notieren Sie den Wert zur späteren Verwendung.

   **Hinweis:**
   Sie können ein Konvertierungstool Hexadezimal in Base64 (Hex in Base64) verwenden, um den **Fingerabdruckwert** in einen Base64-Wert zu codieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Hängen Sie ein Java Key Store-Zertifikat für MS Teams an

Aktivieren Sie die Authentifizierung des JWT Bearer Grant-Tokens, indem Sie ein gültiges JKS-Zertifikat (Java Key Store) anhängen.

#### Vorbereitungen

Melden Sie sich bei Ihrer ServiceNow-Instanz an, um das folgende Verfahren auszuführen.

- Gültiges Java Key Store-Zertifikat
- Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Systemdefinition** > **Zertifikate**.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector-Zertifikat**.
   Stellen Sie sicher, dass Sie nur den Standarddatensatz **Microsoft Teams Connector-Zertifikat** verwenden.
3. Geben Sie das der JKS-Datei zugeordnete Passwort in das Feld **Schlüsselspeicher-Passwort ein**.
4. Klicken Sie auf das Anhangsymbol ( ), und hängen Sie das generierte JKS-Zertifikat an.
   Weitere Informationen finden Sie unter .
5. Klicken Sie **auf Speicher/Zertifikate validieren**.
6. Klicken Sie auf **Aktualisieren**.

### Konfigurieren Sie den JWT-Signierschlüssel für MS Teams

Erstellen Sie einen JWT-Signierschlüssel (JSON Web Token), um ihn Ihrem Java Key Store-Zertifikat zuzuweisen.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Schlüssel**.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector JWT**.
3. Geben Sie das Passwort ein, das zum Verschlüsseln des privaten Schlüssels zum Generieren der PFX-Datei und der **.CER**-Datei in Signaturschlüsselpasswort verwendet wird.
4. Klicken Sie auf **Aktualisieren**.

### Konfigurieren Sie den JWT-Provider für MS Teams

Fügen Sie Ihrer ServiceNow-Instanz einen JSON Web Token (JWT)-Provider hinzu.

#### Vorbereitungen

- Kopieren und notieren Sie den Wert der **Anwendungs-ID (Client)** und der **Verzeichnis** -ID (Mandant) der Anwendung, die Sie im Azure-Portal registriert haben.

- Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Anbieter**.
2. Öffnen Sie den Datensatz **MS Teams Connector JWT Provider**.
3. Geben Sie Werte für **iss**, **sub**und **aud** in die zugehörige Liste Standardansprüche ein.

| Feld | Wert |
|---|---|
| aud | Microsoft Online-URL in folgendem Format: https://login.microsoftonline.com/<tenant-id> / oauth2/token . Ersetzen<tenant-id> mit dem Wert Verzeichnis-ID (Mandant) Ihrer Anwendung im Azure-Portal registriert wurde. |
| ist | **Anwendungs-ID (Client)** der Anwendung, die Sie im Azure-Portal registriert haben |
| Sub | **Anwendungs-ID (Client)** der Anwendung, die Sie im Azure-Portal registriert haben |

4. Klicken Sie auf **Aktualisieren**.

#### Stellen Sie mithilfe von Zertifikaten eine Verbindung her

Stellen Sie mithilfe von Zertifikaten eine Verbindung zwischen der neu erstellten Microsoft Teams Graph-Anwendung her.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Öffnen **Sie Microsoft Teams-Spoke**.
3. Ändern Sie den **Feldwert Konfigurationsvorlage: MSIM Microsoft Teams ConnectorAuthorization Code Template** (Vorlage für Autorisierungscode für MSIM Microsoft Teams), und speichern Sie das Formular.

   **Hinweis:**
   Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Neue Verbindung und Anmeldeinformationen**erstellen.
5. Klicken **Sie auf Oauth-Token erstellen und abrufen**.
   Eine Fehlermeldung mit der Aufforderung 401 – nicht autorisiert wird angezeigt.
6. Laden Sie das Formular neu, und öffnen Sie den Datensatz in der zugehörigen Liste „Verbindungen“.
7. Geben Sie den Base64-codierten **Fingerabdruckwert** in das **AttributCodierter Fingerabdruck des Zertifikats** im Abschnitt Attribute ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Der Fingerabdruckwert ist ein Hexadezimalwert. Sie können ein Hexadezimal-zu-Base64-Konvertierungstool (Hex in Base64) verwenden, um den Fingerabdruckwert in einen Base64-Wert zu codieren.

8. Navigieren zu **System-OAuth** > **Applikationsregistrierung**
9. Öffnen **Sie den Datensatz „MSIM Microsoft Teams Connector-Autorisierungscode“**.
10. Ändern Sie das OAuth-API-Skript: **OAuthUtilJWTMSTeamsConnector**.
11. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Berechtigungen**.
12. Öffnen Sie den Datensatz **MSIM Microsoft Teams Connector-Anmeldeinformationen**.
13. Klicken Sie unter Zugehörige Links auf **OAuth-Token abrufen**.
    Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (13) | | | | |
| Channel.Create | Delegated | Create channels | Yes | Granted for Service Now |
| Channel.Delete.All | Delegated | Delete channels | Yes | Granted for Service Now |
| Channel.ReadBasic.All | Delegated | Read the names and descriptions of channels | No | Granted for Service Now |
| ChannelMember.ReadWrite.All | Delegated | Add and remove members from channels | Yes | Granted for Service Now |
| ChannelMessage.Read.All | Delegated | Read user channel messages | Yes | Granted for Service Now |
| ChannelSettings.ReadWrite.All | Delegated | Read and write the names, descriptions, and settings of ch... | Yes | Granted for Service Now |
| offline_access | Delegated | Maintain access to data you have given it access to | No | Granted for Service Now |
| openid | Delegated | Sign users in | No | Granted for Service Now |
| Team.Create | Delegated | Create teams | No | Granted for Service Now |
| TeamMember.ReadWrite.All | Delegated | Add and remove members from teams | Yes | Granted for Service Now |
| TeamSettings.ReadWrite.All | Delegated | Read and change teams' settings | Yes | Granted for Service Now |
| User.Read | Delegated | Sign in and read user profile | No | Granted for Service Now |
| User.Read.All | Delegated | Read all users' full profiles | Yes | Granted for Service Now |

Automatische Übersetzung

### Geheimer Clientschlüsselwert wird verwendet

Verwenden Sie den Wert des geheimen Clientschlüssels, um den Registrierungsdatensatz der Graph-Anwendung zu konfigurieren.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Prozedur

1. Navigieren Sie im Azure AD-Portal zu **App-Registrierungen**.
2. Klicken Sie im Abschnitt „ **Verwalten** “ auf **Zertifikate und geheime** Schlüssel.
3. Klicken Sie auf **New client secret** (Neuer geheimer Clientschlüssel).
4. Kopieren Sie den erstellten geheimen Clientschlüssel aus dem Feld **Wert**, und notieren Sie ihn.

### Stellen Sie eine Verbindung mit dem geheimen Clientschlüssel her

Stellen Sie eine Verbindung zwischen der neu erstellten Microsoft Teams Graph-Anwendung und der Instanz Now Platform her.

#### Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Öffnen **Sie Microsoft Teams-Spoke**.
3. Ändern Sie den **Feldwert Konfigurationsvorlage: MSIM Microsoft Teams ConnectorAuthorization Code Template** (Vorlage für Autorisierungscode für MSIM Microsoft Teams), und speichern Sie das Formular.

   **Hinweis:**
   Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Neue Verbindung und Anmeldeinformationen**erstellen.

5. Klicken **Sie auf Oauth-Token erstellen und abrufen**.
   Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (13) | | | | |
| Channel.Create | Delegated | Create channels | Yes | Granted for Service Now |
| Channel.Delete.All | Delegated | Delete channels | Yes | Granted for Service Now |
| Channel.ReadBasic.All | Delegated | Read the names and descriptions of channels | No | Granted for Service Now |
| ChannelMember.ReadWrite.All | Delegated | Add and remove members from channels | Yes | Granted for Service Now |
| ChannelMessage.Read.All | Delegated | Read user channel messages | Yes | Granted for Service Now |
| ChannelSettings.ReadWrite.All | Delegated | Read and write the names, descriptions, and settings of ch... | Yes | Granted for Service Now |
| offline_access | Delegated | Maintain access to data you have given it access to | No | Granted for Service Now |
| openid | Delegated | Sign users in | No | Granted for Service Now |
| Team.Create | Delegated | Create teams | No | Granted for Service Now |
| TeamMember.ReadWrite.All | Delegated | Add and remove members from teams | Yes | Granted for Service Now |
| TeamSettings.ReadWrite.All | Delegated | Read and change teams' settings | Yes | Granted for Service Now |
| User.Read | Delegated | Sign in and read user profile | No | Granted for Service Now |
| User.Read.All | Delegated | Read all users' full profiles | Yes | Granted for Service Now |

Automatische Übersetzung

## Aktivieren Sie den MS Teams-Chat-Connector für den Spoke-Benutzer von MS Teams Graph

Wenn Sie bereits Benutzer von sind, befolgen Sie das Verfahren in diesem Abschnitt, um den Microsoft Teams-Chat-Connector zu aktivieren.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

**Wenn Sie bereits Microsoft Teams Graph Spoke-Benutzer sind, führen Sie die folgenden Schritte aus:**

- Navigieren Sie zu Ihrer registrierten Anwendung im Azure-Portal, das von Microsoft Teams Graph Spoke verwendet wird.
- Navigieren Sie zum Abschnitt **API-Berechtigungen**, um die erforderlichen API-Berechtigungen zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
- Wählen Sie **Microsoft Graph** aus.
- Um die Anwendung Microsoft Teams Connector zu verwenden, müssen Sie Ihrer Anwendung zwei weitere delegierte Berechtigungen aus dem Azure-Portal hinzufügen: „ChannelMember.ReadWrite.All“ und „TeamMember.ReadWrite.All“.
- Nachdem Sie die oben genannten erforderlichen Berechtigungen hinzugefügt haben, klicken Sie auf **„Administratoreinwilligung erteilen“**.

**Konfigurieren Sie MS Teams in der Now Platform-Instanz für einen vorhandenen Benutzer:**

- Navigieren Sie zu Aliasse für **Verbindungen und Anmeldeinformationen**.
- Wählen Sie den **Microsoft Teams-Spoke** -Datensatz aus, wie in der folgenden Abbildung dargestellt.
- Wählen Sie den Anmeldeinformationsdatensatz aus, der der Microsoft Teams-Spoke zugeordnet ist.
- Klicken **Sie auf OAuth-Token abrufen**. Eine Bestätigungsmeldung zeigt an, dass das OAuth-Aktualisierungstoken verfügbar ist.

Als vorhandener Benutzer haben Sie jetzt die Integration der Microsoft Teams-Chat-Connector-Anwendung mit der Microsoft Teams Graph API abgeschlossen.

### Management schwerwiegender Sicherheits-Incidents Integration einer Telefonkonferenz

Mit der Integration von Management schwerwiegender Sicherheits-Incidents Telefonkonferenzen können Sie mit Ihren Kunden und Kollegen zusammenarbeiten, um Kundenprobleme mithilfe der Video- und Bildschirmfreigabeoptionen in Microsoft Teams, Cisco Webexoder Zoom in der MSIM-Anwendung zu lösen.

Mit der Management schwerwiegender Sicherheits-Incidents -Telefonkonferenzintegration können Sie den Konferenzkommunikationskanal in den Kommunikationskanal Notify integrieren, indem Sie ein Microsoft Teams-, Cisco Webex- oder Zoom -Meeting direkt über die Anwendung Management schwerwiegender Sicherheits-Incidents ] verwalten und initiieren.

Als MSI-Manager können Sie die MSIM-Telefonkonferenzintegration verwenden, um Microsoft Teams-, Cisco Webex - oder Zoom -Meetings zu initiieren. Integrieren Sie die Telefonkonferenz Management schwerwiegender Sicherheits-Incidents mit externen Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen und schwerwiegende Security Incidents zu beheben.

## Schlüsselfunktionen

Die Integration der Major Security Incident Management-Telefonkonferenz bietet die folgenden wichtigen Funktionen:

- MSI-Manager können eine Microsoft Teams-, Cisco Webex- oder Zoom -Telefonkonferenz direkt aus dem schwerwiegenden Security Incident initiieren.
- Laden Sie zusätzliche Teilnehmer zum Anruf ein.
- Zeigen Sie Anrufaufzeichnungen und Chatdetails an.
- Sendet Einladungen an Teilnehmer per E-Mail und Microsoft Teams Chat.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konferenzanruf starten

Starten Sie eine Telefonkonferenz über eine Aufgabe oder einen wichtigen Sicherheitsvorfall, indem Sie einen oder mehrere Benutzer zur Teilnahme an der Telefonkonferenz einladen. Die Telefonkonferenz beginnt nur, wenn mindestens zwei Teilnehmer beitreten.

## Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Vergewissern Sie sich, dass Sie die folgenden Schritte in der Instanz ServiceNow® durchgeführt haben:

- Das Plugin Notify (com.snc.notify) ist installiert und aktiviert.
- Die App Notify UI Components for Configurable Workspaces ist installiert.
- Das Visual Task Board-Plugin (com.devsnc.snb_vtb) ist installiert und aktiviert.

Weitere Informationen finden Sie unter IntegrationHub anfordern .

## Warum und wann dieser Vorgang ausgeführt wird

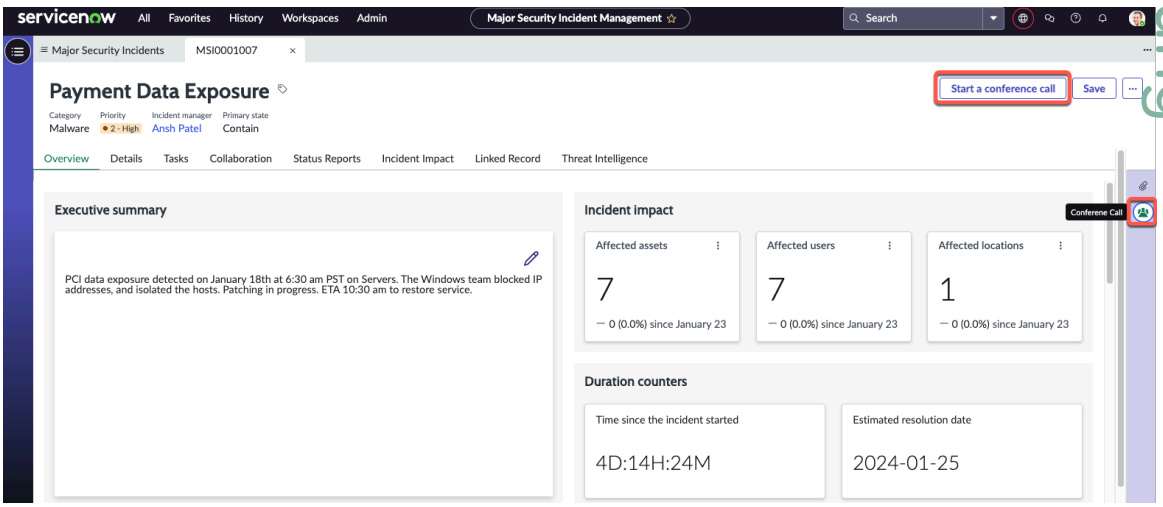
Zu den Anrufteilnehmern können gehören:

- Benutzer, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das auswählen und das +-Symbol auswählen.
   Das Popup Telefonkonferenz starten wird angezeigt.

**MSIM-Telefonkonferenz**




5. Wählen Sie im Feld Konferenzbrücke eine **Konferenzbrücke aus, über** die Sie eine Verbindung herstellen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

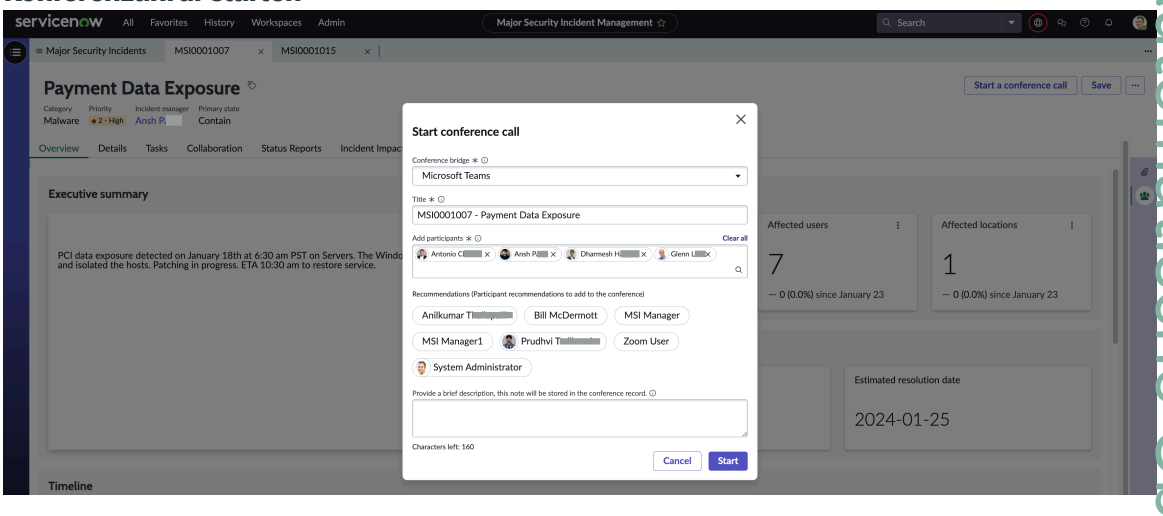
Zum Beispiel Microsoft Team, Zoom oder Cisco Webex.

6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Telefonkonferenz beschreibt.
7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der Liste „ **Empfehlungen** “ auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.

   Der Benutzer (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle dem schwerwiegenden Security Incident zugeordneten Benutzer sind standardmäßig in der Liste **„Empfehlungen** “ verfügbar.

   **Hinweis:**
   Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

**Konferenzanruf starten**




8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Start der Telefonkonferenz ein.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Starten**.
   Die Telefonkonferenz beginnt in der ausgewählten Konferenzbrücke. Alle Teilnehmer werden per E-Mail benachrichtigt, und sie werden auch über die jeweilige ausgewählte Konferenzbrücke benachrichtigt.
10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz teilzunehmen.
    Die Teilnehmer können den Link aus der E-Mail-Benachrichtigung oder die Benachrichtigung von der ausgewählten Konferenzbrücke verwenden, um dem Anruf beizutreten.
11. Öffnen Sie den zugeordneten schwerwiegenden Security Incident, um die Details der Telefonkonferenz anzuzeigen.
    Wenn der letzte Teilnehmer die Konferenz verlässt, wird die Konferenzschaltung beendet, oder wählen Sie **Anruf** beenden, um die Konferenzschaltung zu beenden.

### Einer Telefonkonferenz Teilnehmer hinzufügen

Fügen Sie einer Telefonkonferenz mithilfe der Suchoption im Popup **Telefonkonferenz starten** Teilnehmer hinzu, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen. Sie können Teilnehmer auch hinzufügen, indem Sie die Teilnehmer aus der Liste „Empfehlungen“ auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

## Warum und wann dieser Vorgang ausgeführt wird

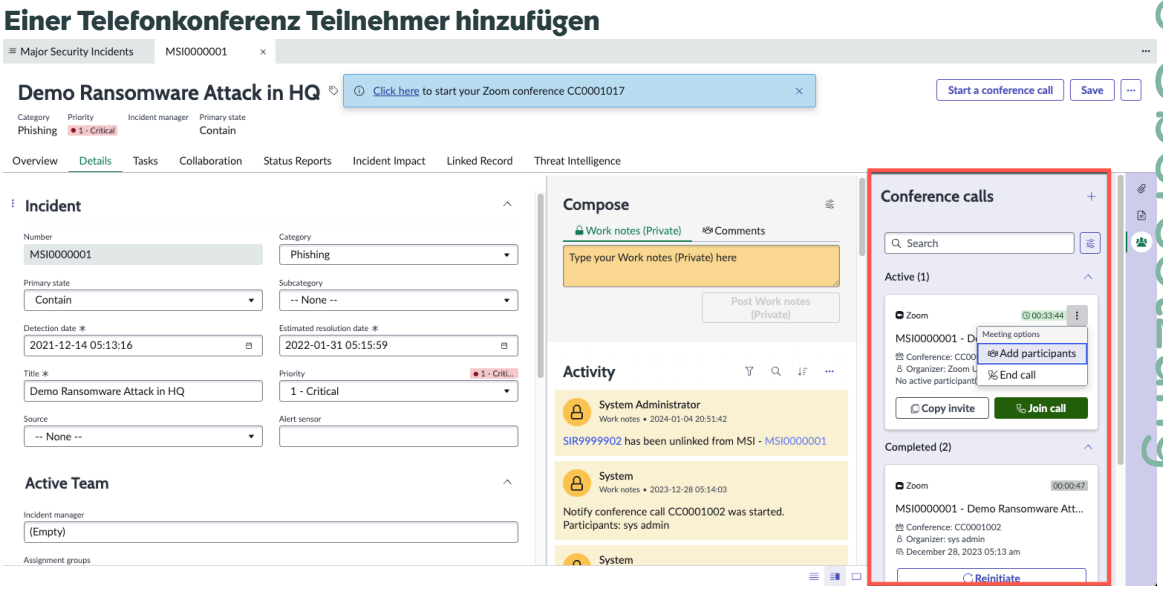
Der Benutzer (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle dem schwerwiegenden Security Incident zugeordneten Benutzer sind standardmäßig in der Liste „Empfehlungen“ verfügbar.

Zu den Anrufteilnehmern können gehören:

- Benutzer, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im rechten Kontextmenü das Symbol „ “ aus, um die Details der Telefonkonferenzen anzuzeigen.
   Dies umfasst Details wie den Namen der Konferenzbrücke, den Namen des Organisators, Datum, Uhrzeit, Dauer des Anrufs sowie aktive und inaktive Teilnehmer.
4. Wählen Sie neben der aktiven Telefonkonferenz und dann die Option **Teilnehmer** hinzufügen aus.




5. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der Liste „ **Empfehlungen** “ auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.
6. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Start der Telefonkonferenz an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Teilnehmer werden per E-Mail benachrichtigt, und sie werden auch über die jeweilige ausgewählte Konferenzbrücke benachrichtigt. Die Teilnehmer können den Link aus der E-Mail-Benachrichtigung oder die Benachrichtigung von der ausgewählten Konferenzbrücke verwenden, um dem Anruf beizutreten.

7. Alternativ können Sie Teilnehmer hinzufügen, indem Sie im Abschnitt „Telefonkonferenzen“ im rechten Kontextmenü die Option **Einladung kopieren** auswählen und die Einladung für die erforderlichen Teilnehmer freigeben.

### Schalten Sie Teilnehmer in einer Telefonkonferenz stumm

Als MSI-Manager oder Host einer Telefonkonferenz haben Sie die Möglichkeit, einen bestimmten Teilnehmer oder alle Teilnehmer der Telefonkonferenz stummzuschalten.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

Vergewissern Sie sich vor Beginn dieses Verfahrens, dass eine aktive Telefonkonferenz mit einem oder mehreren Teilnehmern stattfindet.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im rechten Kontextmenü das Symbol „ “ aus, um die Details der Telefonkonferenzen anzuzeigen.
4. Wählen Sie auf der aktiven Konferenzbrücke An **Anruf teilnehmen** aus.
5. Nachdem Sie der Telefonkonferenz beigetreten sind, wählen Sie einen Teilnehmer aus, den Sie stummschalten möchten, und wählen Sie auf der Konferenzbrücke die Option **Stumm**.
6. Um alle Teilnehmer der Telefonkonferenz stummzuschalten, wählen Sie **Teilnehmer** in den Besprechungssteuerungen und **dann Alle**stummschalten aus.

### Zeigen Sie die Details der Telefonkonferenz an

Telefonkonferenzen werden als Systemaktivitäten im Abschnitt „Aktivität“ des schwerwiegenden Security Incidents und auch in der zugehörigen Liste „Telefonkonferenzen“ aufgeführt. Sie können Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs sowie aktive und inaktive Teilnehmer anzeigen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

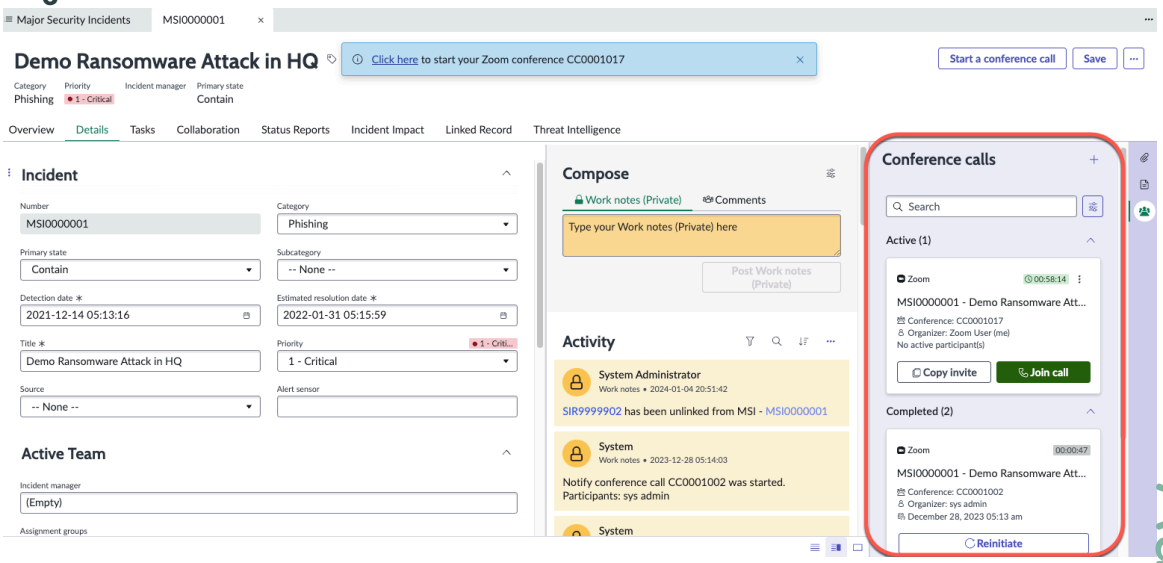
#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie im rechten Kontextmenü das Symbol „ “ aus, um die Details der Telefonkonferenzen anzuzeigen.
   Dies umfasst Details wie den Namen der Konferenzbrücke, den Namen des Organisators, Datum, Uhrzeit, Dauer des Anrufs sowie aktive und inaktive Teilnehmer.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie die Details der Telefonkonferenz an




4. Sie können die Suchoption verwenden, um nach einer bestimmten Telefonkonferenz zu suchen. Es kann mehrere Anrufe für denselben schwerwiegenden Security Incident geben.
5. Um einer Telefonkonferenz Teilnehmer hinzuzufügen, wählen Sie ⋮ neben der aktiven Telefonkonferenz und dann die Option **Teilnehmer** hinzufügen aus.
6. Sie können Teilnehmer auch hinzufügen, indem Sie die Option **Einladung kopieren** verwenden und den Link für die erforderlichen Teilnehmer freigeben.
7. Um an einer Telefonkonferenz teilzunehmen, navigieren Sie zum Abschnitt Aktiv, und wählen Sie die Option An **Anruf** teilnehmen für die gewünschte Telefonkonferenz aus.
8. Um eine Telefonkonferenz zu beenden, wählen Sie ⋮ neben der aktiven Telefonkonferenz und dann die Option **Anruf** beenden aus.
9. Um eine Telefonkonferenz neu zu starten, navigieren Sie zum Abschnitt „Abgeschlossen“ und wählen Sie die Option **Erneut initiieren** für die erforderliche Telefonkonferenz aus.

## Integrieren Sie MSIM-Telefonkonferenzen mit Microsoft Teams

Mit der Telefonkonferenz Microsoft Teams -Integration können Sie eine Microsoft Teams Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren.

## Schlüsselfunktionen

- Starten und beenden Sie Microsoft Teams Telefonkonferenzen direkt aus schwerwiegenden Security Incidents oder einer Aufgabe aus der Workbench für schwerwiegende Security.
- Verwalten Sie eine Microsoft Teams Telefonkonferenz, indem Sie Teilnehmer hinzufügen oder entfernen.

## Voraussetzungen

Vergewissern Sie sich, dass Sie die folgenden IntegrationHub -Plugins in Ihrer Instanz von ServiceNow installiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Notify Plugin „“ (com.snc.notify)
- Microsoft Teams Kommunikations-Speichen-Plugin (sn_msteams_com_spk).
- Plugin „Azure Active Directory User Mapping“ (sn_now_azure).
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

## Konfiguration

- Informationen zum Konfigurieren der MSIM-Telefonkonferenz Microsoft Teams -Integration mit der vorkonfigurierten App finden Sie unter Integrate Notify connector pre-published app with Microsoft Teams .
- Informationen zum Konfigurieren der MSIM-Telefonkonferenz Microsoft Teams -Integration mit der selbst konfigurierten App finden Sie unter Integrating Notify connector self-configured app with Microsoft Teams .

### Verwenden Sie die Integration von MSIM-Telefonkonferenzen Microsoft Teams .

Die folgenden Schritte zeigen Ihnen, wie Sie eine Microsoft Teams Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren können.

### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

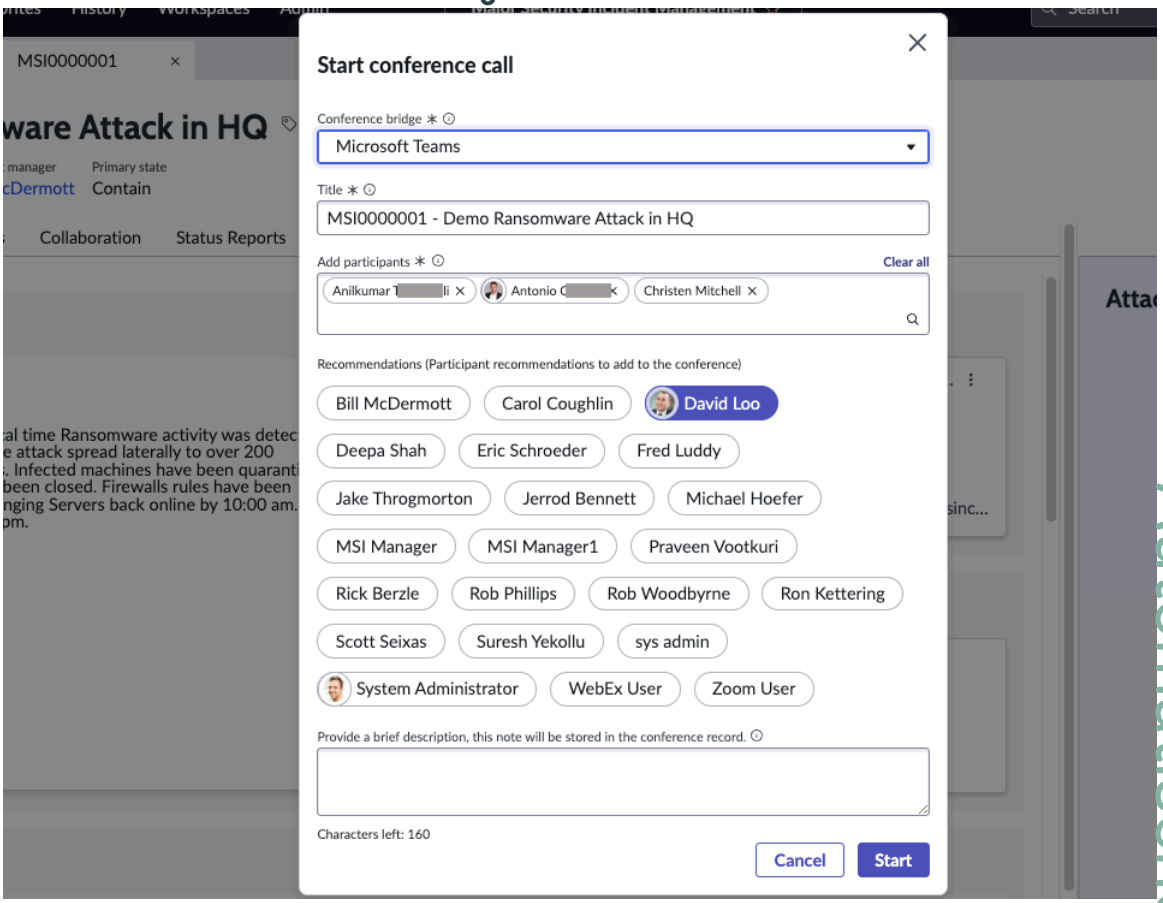
### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das auswählen und das +-Symbol auswählen.
   Das Popup Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Microsoft Teams** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Microsoft Teams-Telefonkonferenz beschreibt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verwenden der Microsoft Teams-Integration für Telefonkonferenzen




7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Microsoft Teams-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der Liste „ **Empfehlungen** “ auswählen, die Teilnehmerempfehlungen für die Microsoft Teams-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Microsoft Teams-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle dem schwerwiegenden Security Incident zugeordneten Benutzer sind standardmäßig in der Liste **„Empfehlungen** “ verfügbar.

   **Hinweis:**
   Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Start der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.

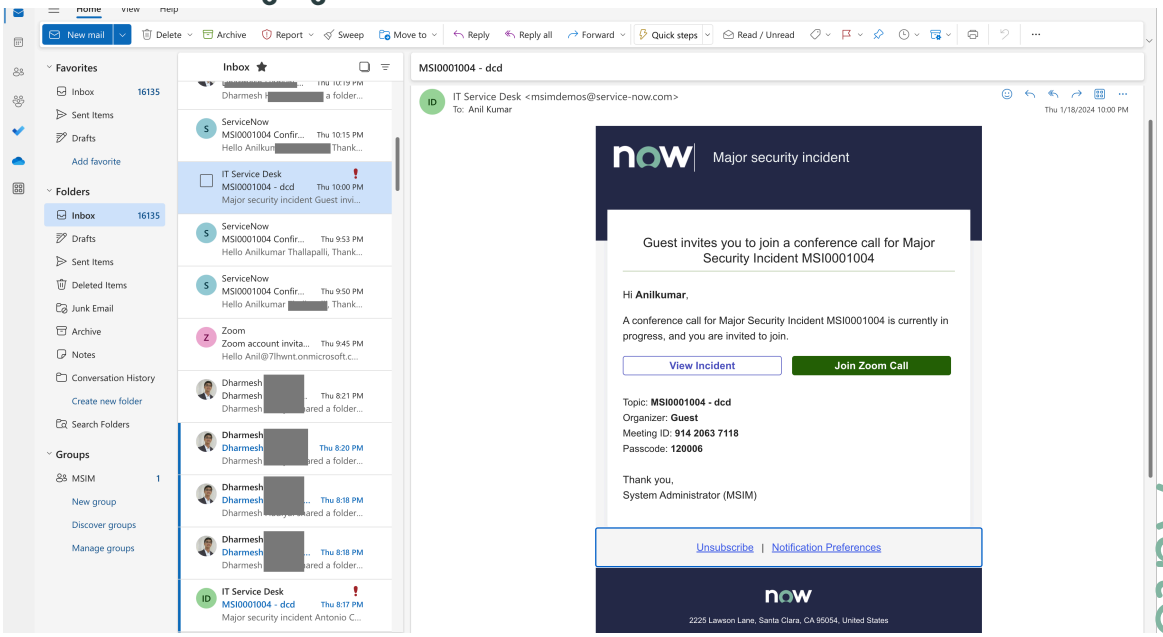
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Starten**.
   Die Telefonkonferenz wird in der Microsoft Teams-App gestartet. Alle Teilnehmer werden per E-Mail von der MSIM-App benachrichtigt, und die andere Benachrichtigung wird über einen Bot in der Microsoft Teams-App gesendet.

10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Microsoft Teams-App teilzunehmen.
    Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Microsoft Teams-App verwenden, um dem Anruf beizutreten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**E-Mail-Benachrichtigung**




11. Öffnen Sie den zugeordneten schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie **Anruf** beenden im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

### Integrieren Sie MSIM-Telefonkonferenzen mit Zoom

Mit der Telefonkonferenz Zoom -Integration können Sie eine Zoom Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren.

## Schlüsselfunktionen

- Starten und beenden Sie Zoom -Meetings direkt aus einem Aufgabendatensatz, z. B. einem schwerwiegenden Security Incident oder einem Change, oder sogar aus der Workbench für schwerwiegende Incidents.
- Verwalten Sie Zoom Besprechungen, indem Sie Teilnehmer hinzufügen oder entfernen.
- Verfolgen und melden Sie Besprechungsdetails wie Besprechungsdauer und Teilnehmer zur weiteren Analyse.

## Voraussetzungen

Vergewissern Sie sich, dass Sie die folgenden IntegrationHub -Plugins in Ihrer Instanz von ServiceNow installiert haben.

- Notify Plugin „“ (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Konfiguration

Informationen zur Konfiguration der MSIM-Telefonkonferenz Zoom -Integration mit dem Kommunikationskanal Notify finden Sie unter Configure Notify Zoom connector in Notify .

### Verwenden Sie die Integration von MSIM-Telefonkonferenzen Zoom .

Die folgenden Schritte zeigen Ihnen, wie Sie eine Zoom Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren können.

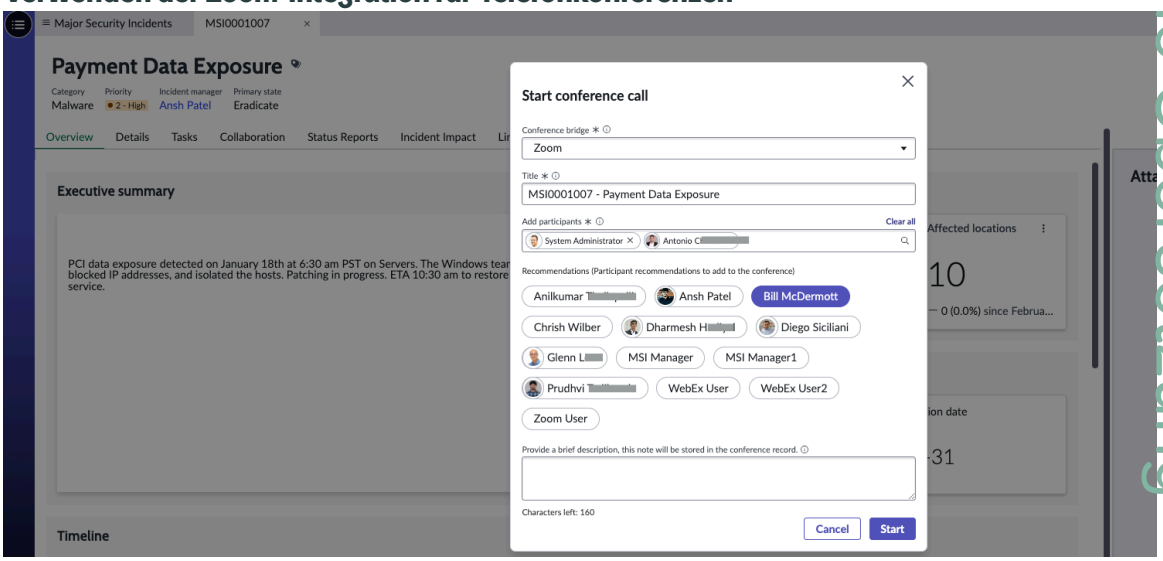
### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ einen schwerwiegenden Security Incident aus.
3. Klicken Sie auf die Aktion **Telefonkonferenz starten**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü auf das klicken und das +-Symbol auswählen.
   Das Popup Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Zoom** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel ein, der den Grund für die Zoom-Telefonkonferenz beschreibt.

**Verwenden der Zoom-Integration für Telefonkonferenzen**




7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Zoom-Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der Liste „ **Empfehlungen** “ auswählen, die Teilnehmerempfehlungen für die Zoom-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Zoom-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle dem schwerwiegenden Security Incident zugeordneten Benutzer sind standardmäßig in der Liste **„Empfehlungen** “ verfügbar.

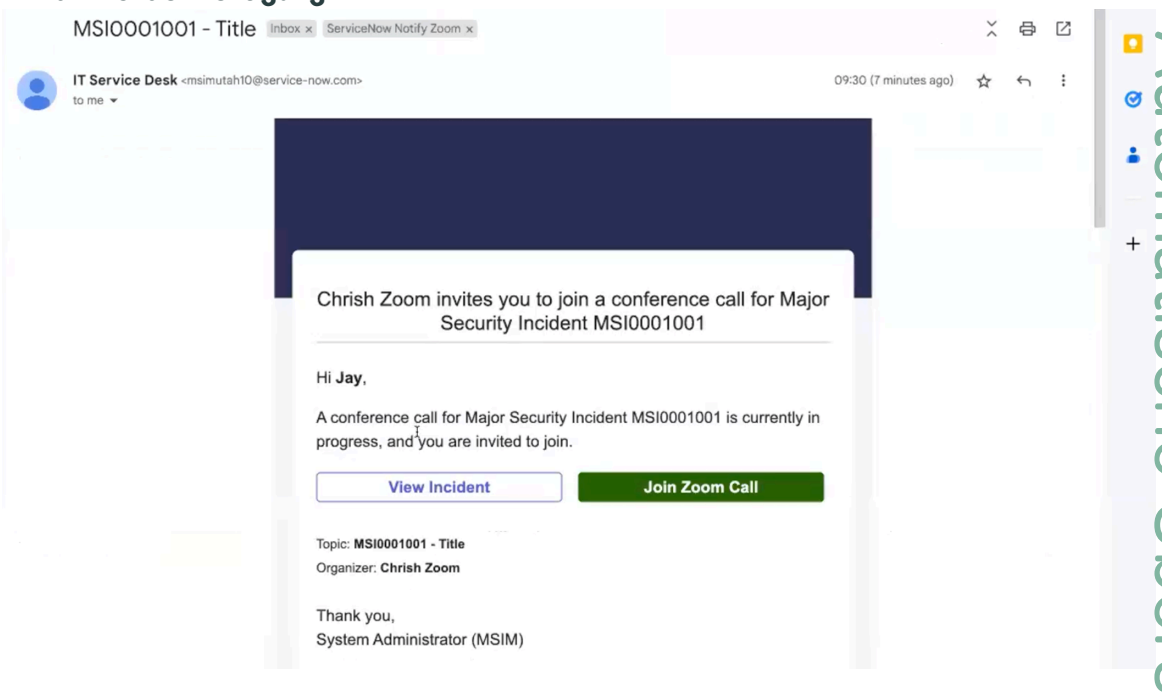
**Hinweis:**
Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Start der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, klicken Sie auf **Starten**.
   Die Telefonkonferenz beginnt in der Zoom-App. Alle Teilnehmer werden durch zwei E-Mails benachrichtigt, eine E-Mail wird von der MSIM-App an die Teilnehmer gesendet und die andere E-Mail wird von der Zoom-Konferenzbrücke gesendet.
10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Zoom-App teilzunehmen.
    Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Zoom-App verwenden, um dem Anruf beizutreten.

**E-Mail-Benachrichtigung**




11. Öffnen Sie den zugeordneten schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie **Anruf** beenden im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incident verfügbar.

### Integrieren Sie MSIM-Telefonkonferenzen mit Cisco Webex

Mit der MSIM-Telefonkonferenz Cisco Webex -Integration können Sie eine Cisco Webex Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Schlüsselfunktionen

- Starten und beenden Sie Cisco Webex -Meetings direkt aus schwerwiegenden Security Incidents.
- Verwalten Sie eine Cisco Webex Besprechung, indem Sie Teilnehmer hinzufügen oder entfernen.

## Voraussetzungen

Vergewissern Sie sich, dass Sie die folgenden IntegrationHub -Plugins in Ihrer Instanz von ServiceNow installiert haben.

- Notify Plugin „“ (com.snc.notify)
- Notify Cisco Webex -Connector (sn_notify_webex)
- Cisco Webex Teams-Spoke (sn_cisco_teams_spk)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

## Konfiguration

Informationen zur Konfiguration der MSIM-Telefonkonferenz Cisco Webex -Integration mit dem Kommunikationskanal Notify finden Sie unter Configure Notify Cisco Webex Connector .

### Verwenden Sie die Integration von Telefonkonferenzen Cisco Webex .

Die folgenden Schritte zeigen Ihnen, wie Sie eine Cisco Webex Telefonkonferenz direkt aus einem schwerwiegenden Security Incident verwalten und initiieren können.

**Vorbereitungen**
Erforderliche Rolle: sn_msi.workspace_manager

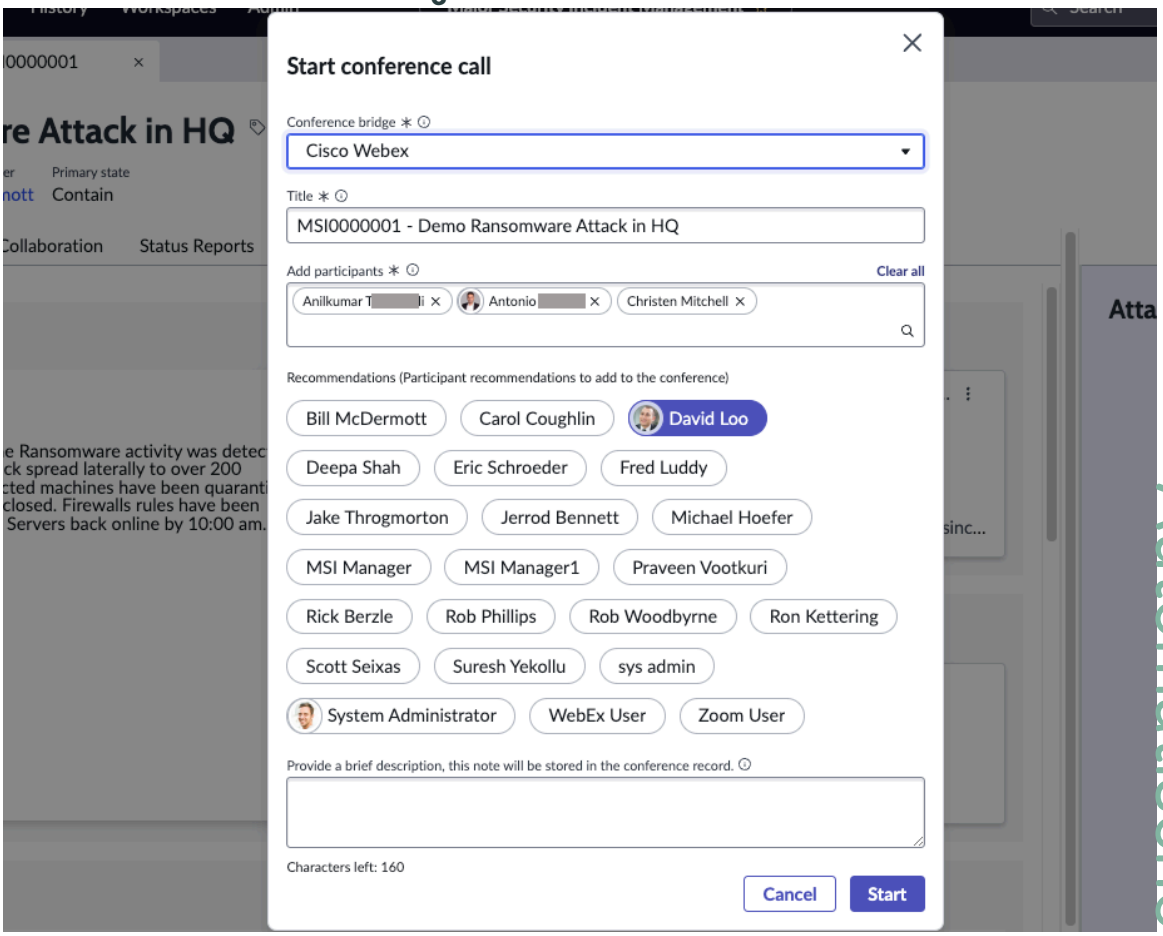
**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**.
2. Wählen Sie in der Liste „Schwerwiegender Security Incident“ einen schwerwiegenden Security Incident aus.
3. Wählen Sie die Aktion **Telefonkonferenz starten aus**.
4. Sie können eine Telefonkonferenz auch starten, indem Sie im rechten Kontextmenü das auswählen und das +-Symbol auswählen.
   Das Popup Telefonkonferenz starten wird angezeigt.
5. Wählen Sie **Cisco Webex** als Konferenzbrücke aus, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel ein, der den Grund für die Cisco Webex-Telefonkonferenz beschreibt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verwenden der Cisco Webex-Integration für Telefonkonferenzen




7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Cisco Webex-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen, oder die Teilnehmer aus der Liste „ **Empfehlungen** “ auswählen, die Teilnehmerempfehlungen für die Cisco Webex-Telefonkonferenz enthält.

   Der Benutzer (Host), der die Cisco Webex-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle dem schwerwiegenden Security Incident zugeordneten Benutzer sind standardmäßig in der Liste **„Empfehlungen** “ verfügbar.

   **Hinweis:**
   Stellen Sie sicher, dass die von Ihnen ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Start der Telefonkonferenz ein.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.

9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie **Starten**.
   Die Telefonkonferenz beginnt in der Cisco Webex-App. Alle Teilnehmer werden durch zwei E-Mails benachrichtigt, eine E-Mail wird von der MSIM-App an die Teilnehmer gesendet und die andere E-Mail wird von der Cisco Webex-Konferenzbrücke gesendet.

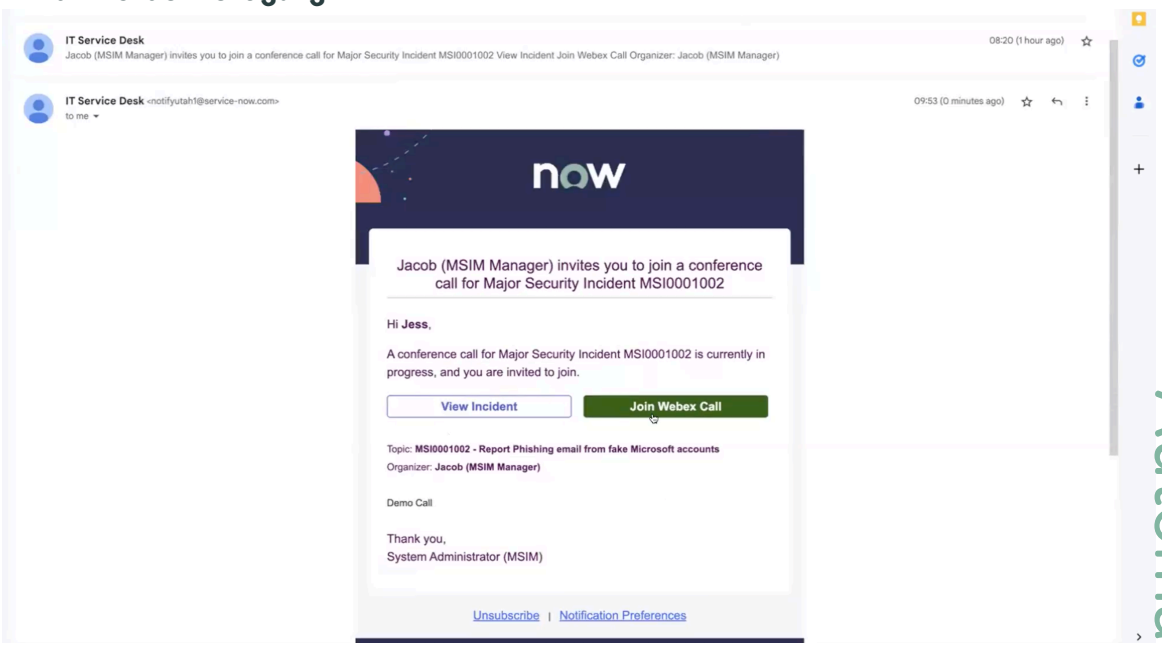
10. Wählen Sie die Option **Hier klicken** über dem schwerwiegenden Security Incident aus, um an der Telefonkonferenz in der Cisco Webex-App teilzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Cisco Webex-App verwenden, um dem Anruf beizutreten.

**E-Mail-Benachrichtigung**




11. Öffnen Sie den zugeordneten schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Details der Telefonkonferenz anzuzeigen.

    Wenn der letzte Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie **Anruf** beenden im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incident verfügbar.

## Management schwerwiegender Sicherheits-Incidents konfigurieren

Installieren und konfigurieren Sie die Anwendung Management schwerwiegender Sicherheits-Incidents.

In diesem Abschnitt erfahren Sie, wie Sie die erforderlichen Konfigurationen für die Arbeit mit Major Security Incident -Datensätzen durch Integration mit anderen externen Microsoft -Anwendungen einrichten, um Verbindungen mit der Instanz ServiceNow ] herzustellen.

### Konfigurieren Sie die Datei-Explorer-Komponente

Die Datei-Explorer-Arbeitsbereichskomponente organisiert und verfolgt die Sammlung von Artefakten (Dateien), die sich auf einen schwerwiegenden Security Incident beziehen. Es unterstützt die Integration mit Dateihosting-Providern von Drittanbietern wie Microsoft SharePoint im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents.

- File Explorer Komponente: Stellt eine grafische Benutzeroberfläche zum Anzeigen des Dateisystems bereit und ermöglicht Benutzern das Ausführen von Dateivorgängen.
- File Explorer Core: Stellt eine Abstraktionsebene bereit, die es der Datei-Explorer-Komponente ermöglicht, das Dateisystem anzuzeigen und verschiedene Dateivorgänge

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auszuführen, ohne etwas über den zugrunde liegenden Connector zu wissen, der für die Kommunikation mit externen Repositorys verwendet wird.

- File Explorer Microsoft SharePoint Connector-Anwendung: Stellt die Implementierungsmodule bereit, die zum Verfolgen und Abrufen von Dateien/Ordner-Metadaten aus einer Microsoft SharePoint -Dokumentbibliothek und zum Ausführen von Dateivorgängen erforderlich sind.

Die Komponente File Explorer Core stellt eine Basisinfrastruktur bereit, die für die verschiedenen Connector-Anwendungen für die Dateifreigabe erforderlich ist, um die Verbindungseigenschaften zu definieren.

Sie müssen das Datei-Repository-Laufwerk und den Datei-Repository-Provider installieren und konfigurieren, indem Sie die Verbindungseigenschaften hinzufügen, um die Dateimetadaten von einem Datei-Hosting-Provider-Speicherort abzurufen.

Für diese aktuelle Version von File Explorerumfassen diese Anweisungen das Konfigurieren und Abonnieren einer Datei -Metadaten, z. B. Microsoft SharePoint Datei- und Ordneraktualisierungen, Dateivorgänge und Protokollierung von Dateiaktivitäten. Eine bestimmte Microsoft SharePoint Dokumentbibliothek und die zugehörige Laufwerkskonfiguration sind erforderlich, um einzelne Ordner zu erstellen, die für einen schwerwiegenden Security Incident spezifisch sind.

File Explorer ermöglicht auch Connector-Anwendungen wie Microsoft SharePoint. Sie können dieses Beispiel verwenden, um die Implementierungen von Dateivorgängen wie zu konfigurieren **Herunterladen** oder **Umbenennen** Ordner- und Dateiaktionen werden in der Datei-Explorer-Arbeitsbereichskomponente aktiviert. Diese Aktionen werden mit den integrierten Flow Designer-Subflows aktiviert und ausgeführt. Weitere Informationen finden Sie unter Einstellungen für Ordner- und Dateiaktionen.

File Explorer Konfiguration umfasst das folgende Setup:

- Konfigurieren Sie das Laufwerk Datei-Explorer Repository .
- Konfigurieren Sie die Einstellungen für Ordner- und Dateiaktionen
- Erstellen Sie Ordnervorlagen

### Erste Schritte mit dem Datei-Explorer

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Komponente File Explorer arbeiten.

Überprüfen Sie die folgenden Informationen, bevor Sie die Verbindung mit Microsoft SharePointherstellen, Ordner- und Dateiaktionen erstellen und Ordnervorlagen für die Datei-Explorer-Komponente erstellen.

#### Voraussetzungen

| Name | Beschreibung |
|---|---|
| Microsoft SharePoint -Spoke, Version 2.0.2 für ServiceNow® IntegrationHub. | Verwenden Sie die Plugin-ID **sn_sp_spoke**, um die Spoke Microsoft SharePoint zu suchen und zu installieren.<br>Durch die Installation dieses Plugins werden Flows und Aktionen zur Automatisierung der Zusammenarbeit, der Dokumentverwaltung |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Voraussetzungen (Fortsetzung)**

| Name | Beschreibung |
|---|---|
| | und der Benutzerzugriffsrechte in Microsoft SharePointbereitgestellt . |
| Datei-Explorer-Komponente v1.1.0 | Verwenden Sie die Plugin-ID **sn_file_explorer**, um die Datei-Explorer-Komponente v1.1.0 zu suchen und zu installieren<br>Durch die Installation dieses Plugins wird eine grafische Benutzeroberfläche zum Durchsuchen des Dateisystems bereitgestellt, die im Datei-Explorer-Core verfügbar ist. |
| File Explorer Core for Security Operations v1.1.1 | Verwenden Sie die **sn_fe-** Plugin-ID, um den Datei-Explorer-Core zu suchen und zu installieren.<br>Durch die Installation dieses Plugins wird eine Basisinfrastruktur für die Integration mit jedem Dateihosting-Provider einer Drittpartei bereitgestellt. |
| Microsoft SharePoint Datei-Explorer-Connector für Security Operations v1.1.1 | Verwenden Sie die Plugin-ID **sn_fe_sharepoint**, um Microsoft SharePoint File Explorer Connector zu suchen und zu installieren.<br>Durch die Installation dieses Plugins werden Microsoft SharePoint Dateien/Ordner mit dem Datei-Explorer verwaltet. |

### Konfigurieren Sie das Laufwerk Datei-Explorer Repository .

Der Connector Microsoft SharePoint bietet verschiedene Funktionen, die in den Datei-Explorer-Funktionen von Microsoft SharePoint implementiert werden können, indem die Dateimetadaten verwaltet und nachverfolgt werden.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Schwerwiegender Security Incident** > **Dateiexplorer** > **Datei-Repository-Konfiguration**.
2. Füllen Sie die folgenden Felder wie in der folgenden Tabelle beschrieben aus:

| Feldname | Feldbeschreibung |
|---|---|
| Name | Name des Datei-Repository-Datensatzes, der die Verwendung angibt. Beispiel: MSIM. |
| Anbieter | Name des Providers, bei dem es sich um den Drittanbieter-Dateihosting-Repository-Provider handelt. Beispiel:Microsoft SharePoint |



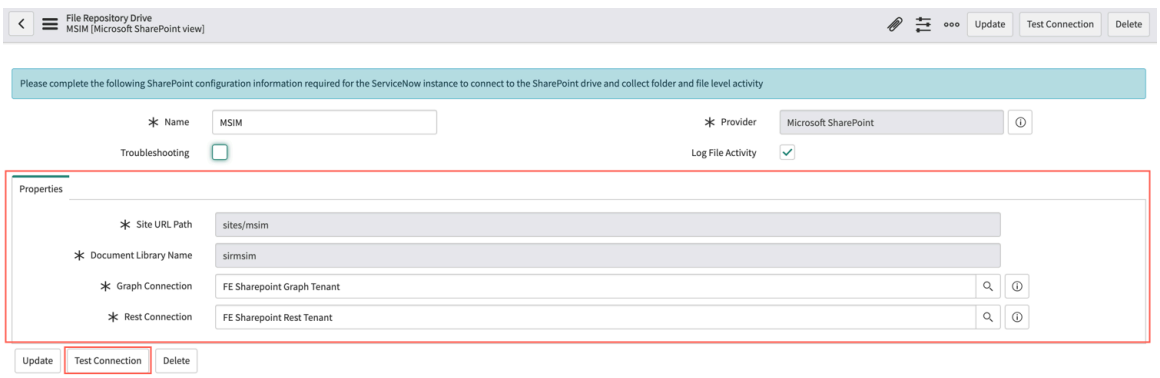
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feldname | Feldbeschreibung |
|---|---|
| **Eigenschaften** | |
| Website-URL-Pfad | Geben Sie eine Microsoft SharePoint URL mit einem bestimmten Website-Pfad ein.<br><br>Geben Sie nur den relativen Pfad zur Website an. Eine vollständige Website-URL ist möglicherweise nicht erforderlich. Beispiel: Sites/MSIM. |
| Name der Dokumentbibliothek | Erstellen Sie eine Dokumentbibliothek unter der Website Microsoft SharePoint, und geben Sie hier denselben Namen für die Dokumentbibliothek an.<br><br>Dies wäre dieselbe Dokumentbibliothek, die Sie im Setup von Microsoft SharePoint Connector Drive erstellt haben. |
| Graph-Verbindung | Wählen Sie den Mandantendatensatz des Datei-Explorer-Diagramms aus.<br><br>Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke. |
| REST-Verbindung | Wählen Sie den Datensatz des Datei-Explorer-REST-Mandanten aus.<br><br>Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke. |

3. Wählen Sie **Speichern**.
4. Klicken **Verbindung testen** Registerkarte, um die Verbindung zu testen und die Konfigurationseigenschaften des Datei-Repository-Laufwerks zu validieren.

> **Hinweis:**
> Stellen Sie vor dem **Aktivieren** des Datei-Repositorys sicher, dass die entsprechende Dokumentbibliothek unter Microsoft SharePoint keine Ordner- oder Dateidaten enthält.

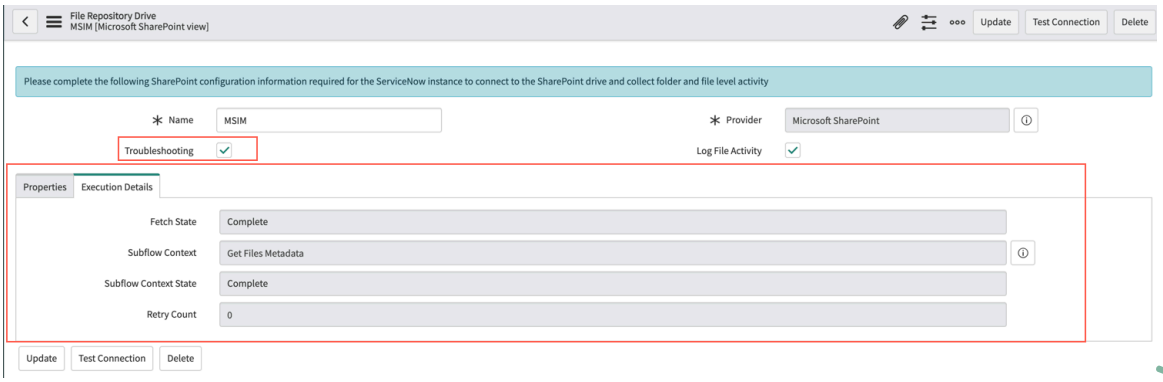
5. Klicken Sie auf **Aktivieren**, um das Datei-Repository zu aktivieren.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Aktivieren Sie das Kontrollkästchen **Problembehandlung**, um die **Ausführungsdetails** des Datei-Repositorys zu überprüfen, und überprüfen Sie die **Status abrufen** ist abgeschlossen, und stellen Sie sicher, dass Microsoft SharePoint Laufwerksabonnements erstellt wurde und der Status „Abgeschlossen“ ist.




**Hinweis:**
Mit der Schaltfläche **Verbindung testen** kann entweder der MSI-Administrator oder der MSI-Manager nur die Konfiguration des Datei-Repository validieren.

### Konfigurieren Sie die Einstellungen für Ordner- und Dateiaktionen

Ckonfigurieren die Ordner- und Dateiaktionen, die über die Datei-Explorer-Komponente im Arbeitsbereich „Major Security Incident Management“ aktiviert werden sollen, mithilfe der Setup-Seite „Ordner- und Dateiaktionseinstellungen“. Als MSI-Administrator können Sie die einzelnen Ordner- und Dateiaktionen steuern, die in der Datei-Explorer-Komponente angezeigt werden.

### Vorbereitungen

Im Folgenden sind die implementierten Dateivorgangsfunktionen in der Datei-Explorer-Komponente mit dem Flow Designer [ ServiceNow® aufgeführt:

#### Funktionen für Dateivorgänge

| Dateivorgang | Beschreibung |
|---|---|
| Öffnen Sie in Microsoft SharePoint | Öffnet eine neue Browserregisterkarte, um die Dateiansicht der Dokumentbibliothek Microsoft SharePoint anzuzeigen |
| Ordner erstellen | Möglichkeit zum Erstellen zusätzlicher Ad-hoc-Ordner, nachdem ein schwerwiegender Security Incident erstellt wurde. |
| Ordner umbenennen | Möglichkeit zum Umbenennen der erstellten Ordner. |
| Datei verschieben | Ermöglicht das Verschieben von Dateien zwischen Ordnern in der Datei-Explorer-Komponente des Arbeitsbereichs, was zu einer Verschiebung von Dateien in führt Microsoft SharePoint |
| Suchen Sie Datei | Zeigt den Ordnerspeicherort bei Verwendung von an **Letzte** -Ansicht des Dateiexplorers. |
| Datei löschen | Löschen Sie die Datei. |
| Ordner löschen | Löschen Sie den Ordner. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Funktionen für Dateivorgänge (Fortsetzung)**

| Dateivorgang | Beschreibung |
|---|---|
| Datei herunterladen | Lädt die Datei auf der vorhandenen Browserregisterkarte des MSIM-Arbeitsbereichs herunter, um sie schnell anzuzeigen. |
| Benennen Sie die Datei um | Benennt die Datei um. |

**Hinweis:**

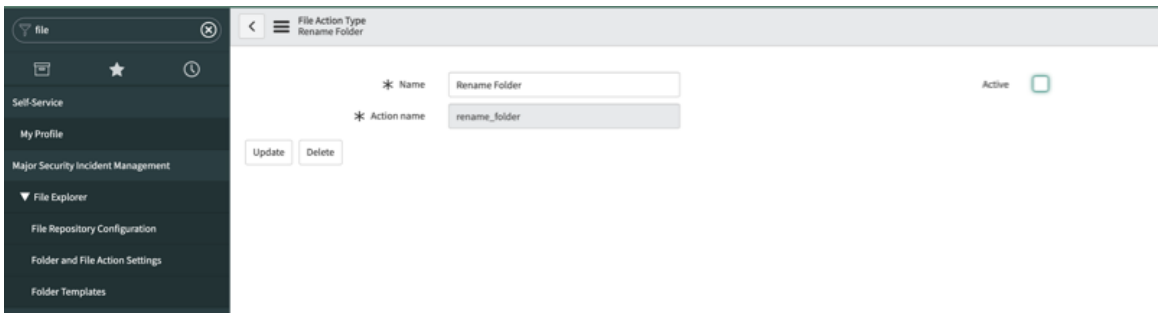
1. Alle aufgelisteten Aktionen sind derzeit standardmäßig aktiviert. Sie müssen die bearbeiten **Dateiaktionseinstellungen** wenn bestimmte Aktionen nicht angezeigt werden sollen. Alle Einstellungen gelten derzeit für alle Benutzer global, , was bedeutet, dass Aktionen für eine Teilmenge der Benutzer mit einer bestimmten Rolle nicht aktiviert werden können.
2. **Anwenderzugriff widerrufen** und **Berechtigungen hinzufügen** -Aktionen sind systembezogene Aktionen. Es wird empfohlen, diese Dateiaktionen nicht zu ändern.

Das folgende Beispielverfahren beschreibt eine der Dateivorgänge-Fähigkeitenies , um bestimmte Ordner- und Dateiaktionen während der Konfiguration des Datei-Explorer-Repositorys zu deaktivieren. Dieses Verfahren gilt für alle anderen Aktionen, die möglicherweise bearbeitet werden müssen:

Erforderliche Rolle: sn_msi.workspace_admin

### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Einstellungen für Ordner- und Dateiaktionen**.
2. Wählen Sie den gewünschten Datensatz aus, um die Ordner- bzw. Dateiaktion zu aktivieren oder zu deaktivieren.
3. Deaktivieren Sie . **Aktiv** Kontrollkästchen zum Deaktivieren der Ordner- und Dateiaktion.

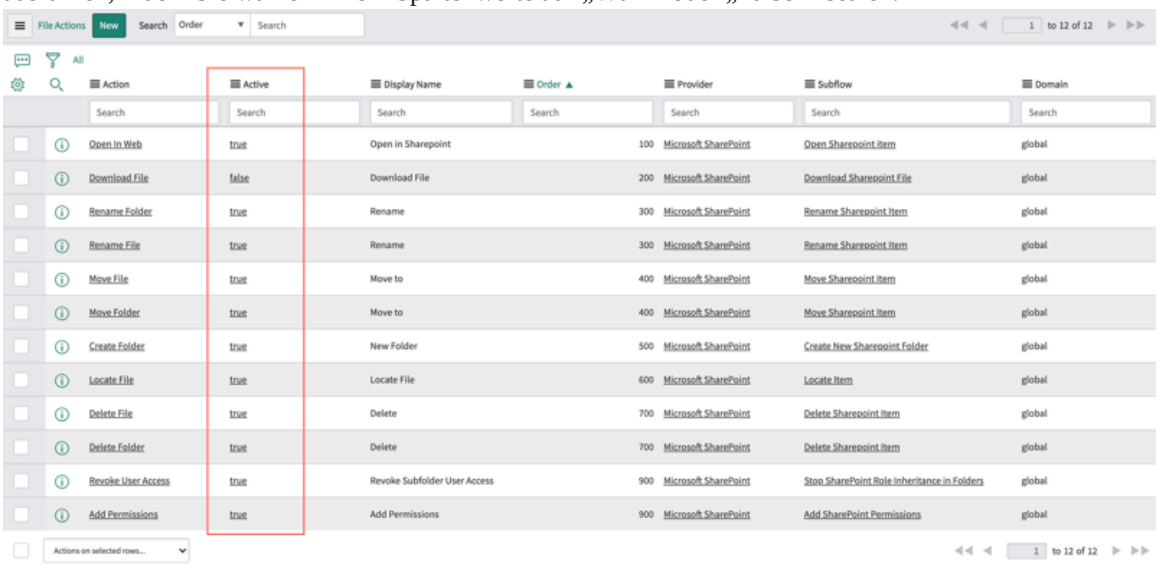




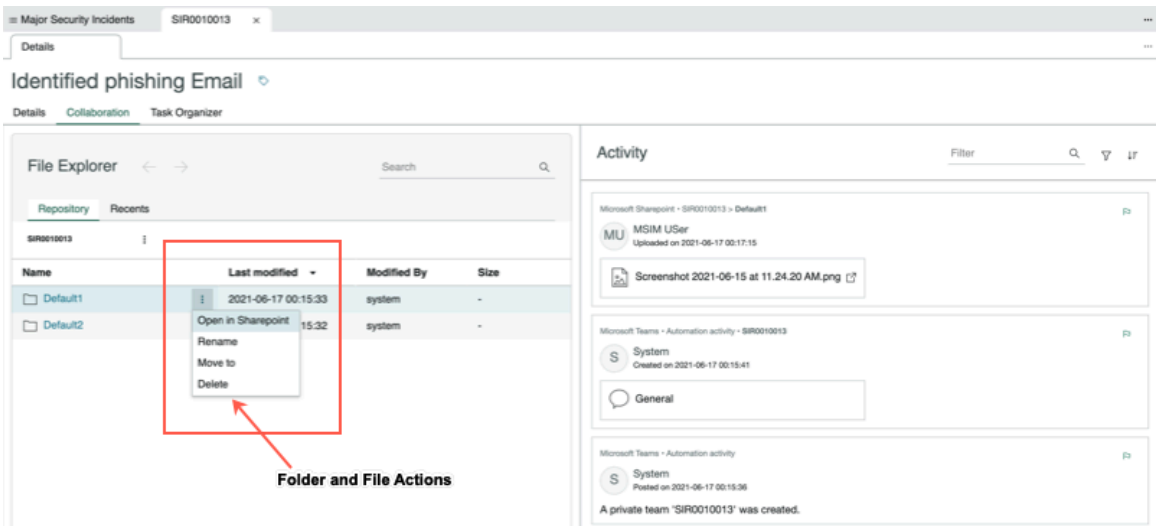

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Aktualisieren Sie** den Laufwerksdatensatz.

**Hinweis:**
Sie können die Dateiaktion auch direkt aus der Liste der angezeigten Dateivorgänge ausführen, indem Sie wählen **Aktiv** Spaltenwerte auf „Wahr“ oder „Falsch“ setzen.




Wenn die ausgeführte Dateiaktion deaktiviert ist, wird die Aktion nicht im angezeigt **Kollaborationen** Registerkarte des **Management schwerwiegender Sicherheits-Incidents** Arbeitsbereich.




## Erstellen Sie Ordnervorlagen

Verwenden Sie Ordnervorlagen, um automatisch eindeutige Ordner für verschiedene Typen schwerwiegender Security Incidents zu erstellen. Die Ordnervorlagen in der Datei-Explorer-Komponente werden verwendet, um eine Basisordnerstruktur für den Security Incident in Microsoft SharePointzu erstellen.

### Vorbereitungen

Als MSI-Administrator definieren Sie die anfängliche Ordnerstruktur, die für die Zusammenarbeit zwischen verschiedenen Incident-Beantworter-Gruppen erforderlich ist, und weisen die entsprechenden Zugriffsberechtigungen auf einer Unterordnerebene zu. Mehrere Konfigurationen können für verschiedene Major Security Incident -Typen erstellt werden, indem ein Bedingungsgenerator für bestimmte Major Security Incident -Feldwerte



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet wird. Dies umfasst den Zugriff für verschiedene Benutzer und Benutzergruppen auf jeder Unterordnerebene.

**Hinweis:**
Diese Ordnervorlagen werden von allen schwerwiegenden Security Incidents verwendet, die die im Bedingungsgenerator angegebenen Bedingungen erfüllen. Es wird empfohlen, Incident-Feldvariablen zu verwenden, z. B. die Incident-Nummer oder -Kategorie, um eindeutige Stammordnernamen zu erstellen, die einen Satz von Unterordnern mit gemeinsamen Ordnernamen für einen schwerwiegenden Security Incident von ähnlichen Ordnern mit diesen Namen unterscheiden, die Teil von sind einen anderen schwerwiegenden Security Incident.

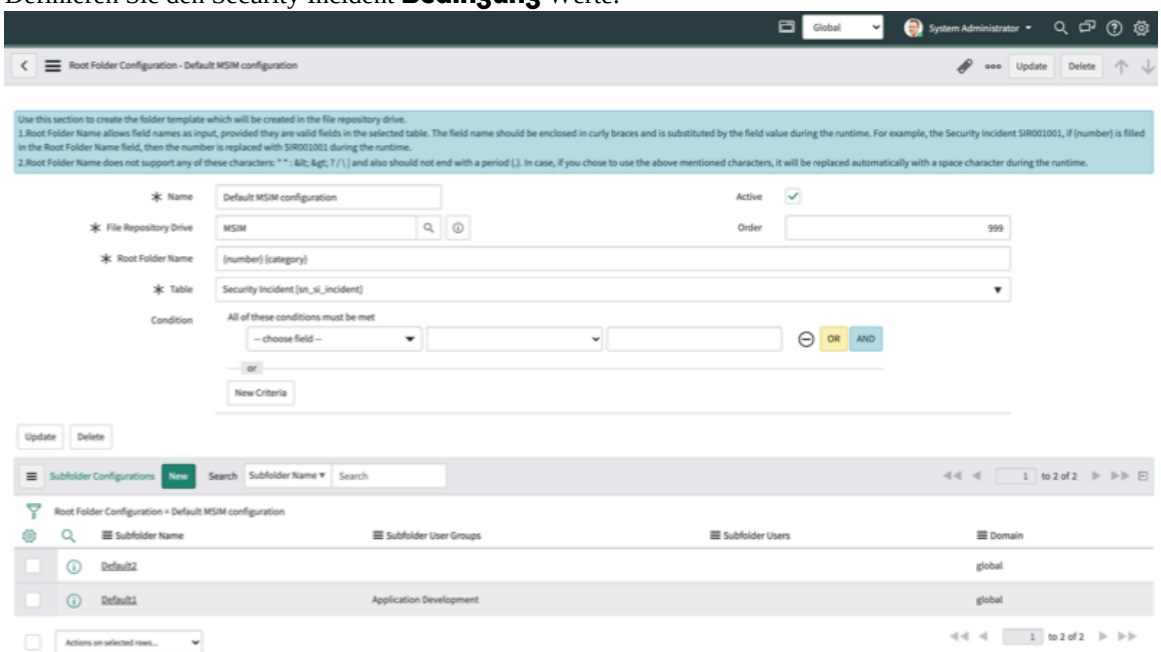
Die definierte Ordnervorlagenkonfiguration wird nur dann auf den schwerwiegenden Security Incident angewendet, wenn die Bedingung erfüllt ist.

**Hinweis:**
Eine Basissystemkonfiguration (ohne Unterordner) wird auf alle Security Incidents angewendet. Sie können diese Standardkonfiguration entweder bearbeiten, um bestimmte Unterordner einzubeziehen, oder eine neue Konfiguration basierend auf einem bestimmten Satz von Feldwerten für schwerwiegende Security Incidents erstellen. Beispiel: Kategorie = Aktivität des schädlichen Codes.

Erforderliche Rolle: sn_msi.workspace_admin

### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Ordnervorlagen**.
2. Klicken **Neu** für Stammordnerkonfiguration.
3. Füllen Sie die Felder im Formular aus.
4. Definieren Sie den Security Incident **Bedingung** Werte.

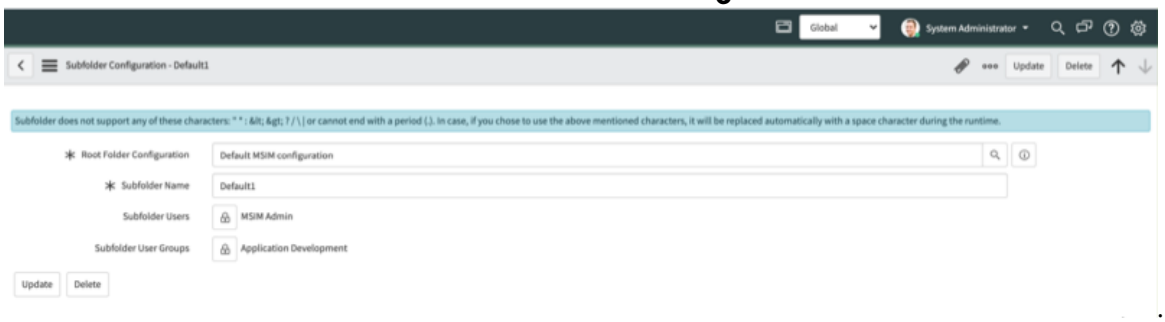



5. **Aktualisieren** Datensatz.
   Die Unterordner werden mit den definierten Werten erstellt.
6. Klicken Sie auf den gewünschten **Unterordner**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie keinen Unterordner mit einem entsprechenden Namen erstellen, werden die Namen der Unterordner als erstellt **Standard** in der **Unterordnerkonfigurationen** Abschnitt.




Dieselbe Ordnerstruktur wird automatisch in Microsoft SharePoint mit denselben Zugriffsberechtigungen erstellt, die auf der konfiguriert sind **Ordnervorlagen** Seite.

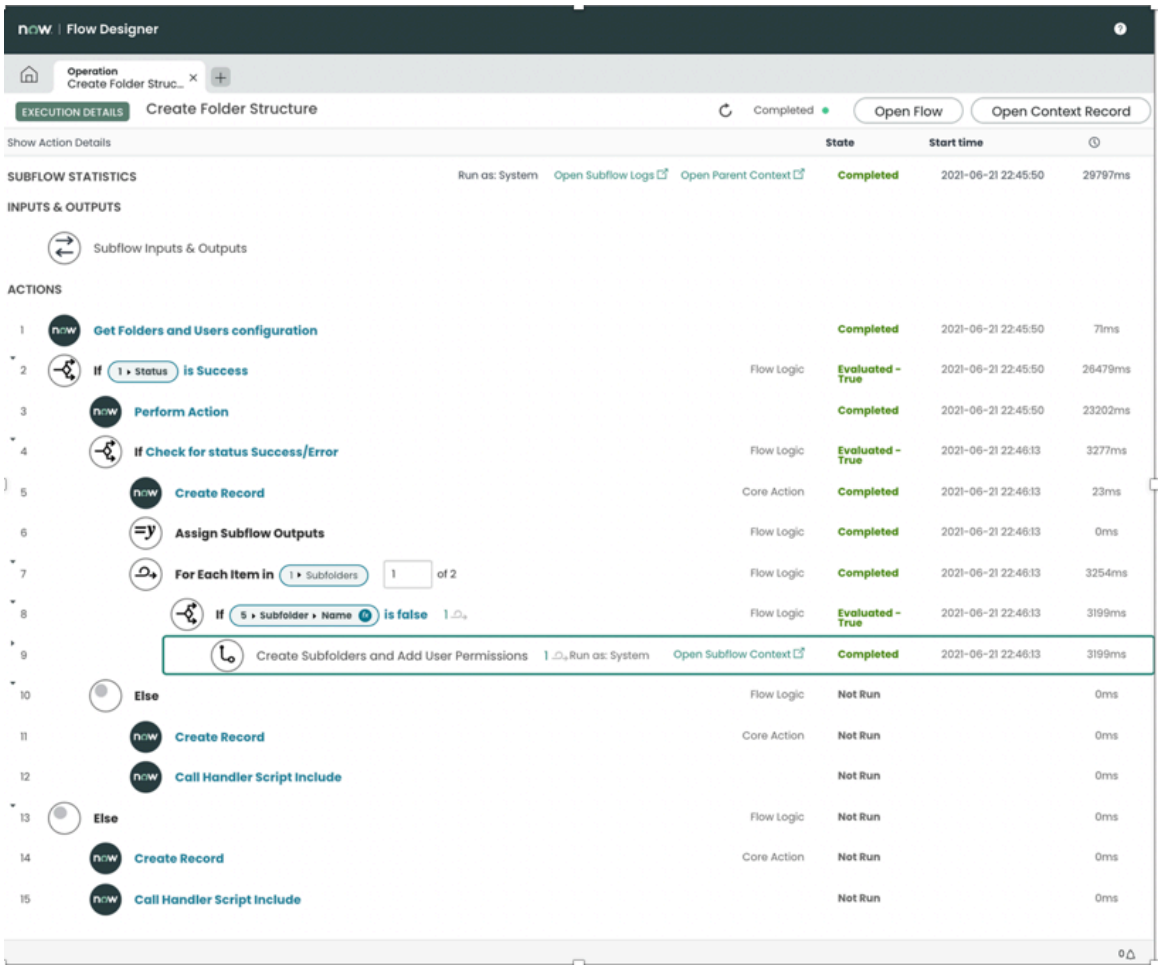
## Hinweis:

- **Stammordnername** lässt Feldvariablennamen als Eingabe zu, sofern es sich um gültige Felder in der ausgewählten Tabelle handelt. Der Feldname muss in geschweifte Klammern eingeschlossen sein und wird während der Laufzeit der Flow-Ausführung durch den Feldwert ersetzt. Beispiel: Security Incident SIR001001. Wenn die Variable {number} im Feld Stammordnername konfiguriert ist, wird die Nummer zur Laufzeit durch **SIR001001** ersetzt.
- **Stammordnername** unterstützt keines der folgenden Zeichen: " * : < > ? / \ | und darf auch nicht mit einem Punkt (.) enden. Wenn Sie die oben genannten Zeichen verwenden, werden sie zur Laufzeit automatisch durch ein Leerzeichen ersetzt.
- Wenn der Name des **Stammordners** und des Unterordners das definierte Limit (256 Zeichen) überschreitet, wird der **Ordnername** abgeschnitten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie die Ausführung des Subflows „Ordnerstruktur erstellen“ zur Laufzeit:




### File Explorer Aktivitätenstrom in Workspace

Verwenden Sie den Datei-Explorer im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents, um die Ordner und Dateien in der Reihenfolge anzuzeigen, in der sie in der Dokumentbibliothek Microsoft SharePoint erstellt wurden.

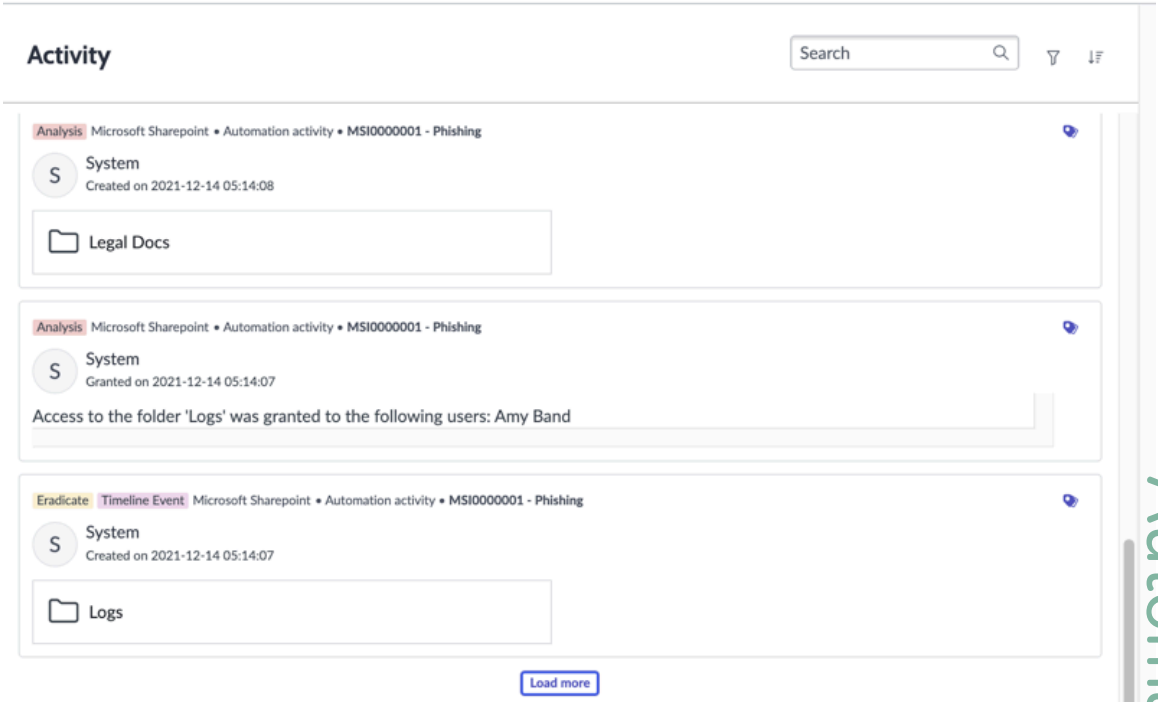
Der Aktivitätenstrom listet alle Automatisierungsaktivitätsveröffentlichungen auf, wenn während der Auflösung von Major Security Incident Ordner- und Dateiaktivitäten oder Protokolle auftreten. Die Aktivitätenstromstruktur ist im gleichen Format wie die Bibliothek Microsoft SharePoint ausgerichtet, die die erstellten Ordner und die Benutzer oder Benutzergruppen anzeigt, die diesen Ordnern zugewiesen wurden.

Der Aktivitätenstrom ermöglicht es Arbeitsbereichsmanagern und anderen Benutzern oder Benutzergruppen, effektiv zu kommunizieren und zusammenzuarbeiten, die Aktivitäten aufzulisten, die für Microsoft SharePoint Ordner und Dateien ausgeführt wurden, den Status des Incident zu überwachen, Notizen zu veröffentlichen oder zusätzliche Kommentare hinzuzufügen haben im Incident-Datensatz. Die Arbeitsbereichsmanager



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können basierend auf der zuletzt aktualisierten Aktivität fortfahren und




arbeiten.

### File Explorer-Problembehandlung

Der Abschnitt zur Fehlerbehebung kann Ihnen helfen, einige der technischen Probleme zu beheben, die beim Einrichten der Komponente File Explorer auftreten können.

Im folgenden Abschnitt finden Sie Details zu regelmäßigen Aufgaben, Systemeigenschaften und File Explorer Flow Designer-Subflows.

### Geplante Aufgaben für File Explorer

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen von Microsoft SharePointzu verarbeiten, die Dateimetadaten in der Instanz ServiceNow zu erfassen und die Datei-Repository-Abonnements nach einem wiederkehrenden Zeitplan zu verlängern.

Geplante Aufgaben sind automatisierte Aufgaben, die im Hintergrund ausgeführt werden, um:

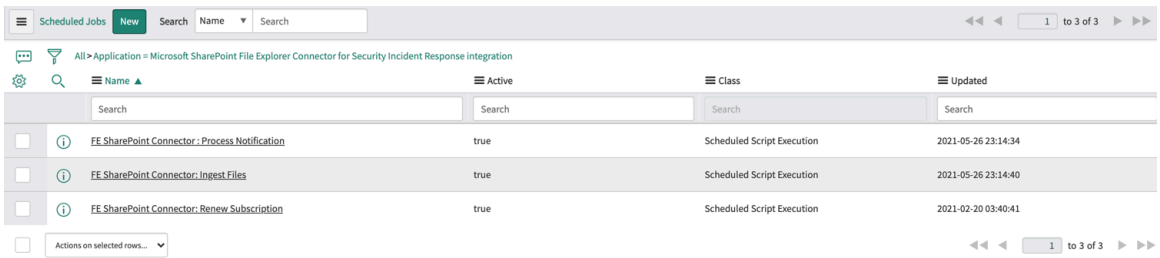
- verarbeitet die Benachrichtigungen von Microsoft Microsoft SharePoint.
- erfasst die Dateimetadaten in der Instanz Now Platform.
- Erneuern Sie das Abonnement mit der Dokumentbibliothek Microsoft SharePoint, um Benachrichtigungen zu erhalten.

| Auftrag | Beschreibung |
|---|---|
| Microsoft SharePoint File Explorer Connector: Benachrichtigung verarbeiten | Wird alle 30 Sekunden ausgeführt und ist für das Lesen der Benachrichtigungen verantwortlich, die auf Änderungen an der abonnierten Dokumentbibliothek hinweisen und den Status der Laufwerke (sn_fe_file_repo_drive) als ausstehend markieren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Auftrag | Beschreibung |
|---|---|
| Microsoft SharePoint File Explorer Connector: Dateien erfassen | Wird alle 30 Sekunden ausgeführt und ist in erster Linie für die Verarbeitung der Laufwerke (sn_fe_file_repo_drive) verantwortlich, die sich im Status „Ausstehend“ befinden, und ruft die Delta-Dateiänderungen aus der konfigurierten Microsoft SharePoint Dokumentbibliothek seit dem letzten Abruf ab. |
| Microsoft SharePoint File Explorer: Abonnement verlängern | Wird alle 10 Minuten ausgeführt und ist für die Verlängerung des Abonnements der Microsoft SharePoint Dokumentbibliothek einen Tag vor dem Ablaufdatum verantwortlich. Normalerweise laufen diese Abonnements in 30 Tagen ab. |




### Verfügbare Datei-Explorer-Systemeigenschaften

Im Folgenden finden Sie die verfügbaren Microsoft SharePoint Datei-Explorer-Connector-Systemeigenschaften.

#### Systemeigenschaften

| Eigenschaftsname | Beschreibung |
|---|---|
| sn_fe_sharepoint.max_retry_count | Steuert die Häufigkeit der Versuche, die die Connector-Anwendung Microsoft SharePoint unternommen hat, um das ausgefallene Laufwerk abzurufen oder das ausgefallene Abonnement zu verlängern. Der Standardhäufigkeitswert ist auf 50 festgelegt. |
| sn_fe_sharepoint.retry_after_seconds | Zeitintervall zwischen jedem Versuch, das ausgefallene Laufwerk abzurufen oder das Abonnement zu verlängern. Der Standardwert ist auf 900 Sekunden oder 15 Minuten festgelegt. |
| sn_fe_sharepoint.max_subscription_expiration_time | Maximaler Abonnementablaufzeitraum in Tagen für Microsoft SharePoint. Der Standardablaufzeitraum ist auf 30 Tage festgelegt. |

### File Explorer Flow Designer-Subflows

Im Folgenden finden Sie die Flow Designer-Subflows, die mit dem Connector Microsoft SharePoint File Explorer installiert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Subflows

| Name | Beschreibung |
|---|---|
| Fügen Sie Microsoft SharePoint Berechtigungen hinzu | Erteilt bestimmten Benutzern die Berechtigung zum Bearbeiten eines bestimmten Ordners. |
| Erstellen Sie ein Laufwerksabonnement | Abonniert mit einer konfigurierten Microsoft SharePoint Dokumentbibliothek, um Benachrichtigungen über Aktualisierungen in der Dokumentbibliothek zu erhalten. |
| Erstellen Sie einen neuen Microsoft SharePoint Ordner | Erstellt einen neuen Microsoft SharePoint -Ordner unter einem gegebenen übergeordneten Ordner. |
| Löschen Sie das Element Microsoft SharePoint . | Löscht Microsoft SharePoint Dateien und Ordner. |
| Laden Sie die Datei Microsoft SharePoint herunter | Gibt die Download-URL von Microsoft SharePoint Dateien zurück |
| Ruft Datei-Metadaten ab | Abonniert und ruft die Änderungen aus der Microsoft SharePoint Dokumentbibliothek ab. |
| Verschieben Sie das Element Microsoft SharePoint . | Verschiebt die Microsoft SharePoint Dateien/Ordner in den Zielordner |
| Öffnen Sie das Element Microsoft SharePoint . | Gibt die Web-URL der Datei/des Ordners Microsoft SharePoint zurück, die in einem Browser geöffnet werden soll. |
| Verlängern Sie das Laufwerksabonnement | Verlängert das Abonnement mit Microsoft SharePoint Dokumentbibliothek. |
| Erstellen Sie eine Ordnerstruktur | Entspricht den Konfigurationen der Ordnervorlage und erstellt die Ordnerstruktur in der Dokumentbibliothek Microsoft SharePoint. |

## Microsoft Teams konfigurieren

Einfache Integration und Zusammenarbeit mit Microsoft Teams, um Major Security Incident aufzulösen, um Chataktivitäten für die Zusammenarbeit anzuzeigen und zu filtern.

Das Konfigurieren und Abonnieren einer Microsoft Teams -Chatumgebung, das Abrufen von Chatkonversationen aus bestimmten Kanälen und das Archivieren des Teams und der zugehörigen Kanäle sind Teil des Incident-Abschlussprozesses. Eine bestimmte Microsoft Teams -Umgebung und die zugehörige Microsoft Teams Graph -API-Konfiguration sind erforderlich, um einzelne Kanäle zu erstellen, die für einen Major Security Incidentspezifisch sind.

Um Microsoft Teams zu konfigurieren, aktivieren Sie Teams als Chat-Anbieter. Sie können dann Chatkanäle für die verschiedenen Stakeholder und Gruppen erstellen, die über Aktivitäten kommunizieren, und Chatkonversationen nachverfolgen, um Major Security Incidentzu lösen. Die Konfiguration der Microsoft Teams- und Microsoft Graph-API umfasst:

- Stellen Sie eine MS Teams Graph-Verbindung auf her Now Platform
- Aktivieren Sie MS Teams als Chat-Anbieter
- Erstellen Sie eine Chatkanalvorlage
- Chat-Nachrichtenaktivität anzeigen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erste Schritte mit Microsoft Teams

Überprüfen Sie die folgenden Informationen, bevor Sie mit Microsoft Teams als Connector-Anwendung arbeiten.

Stellen Sie sicher, dass die folgenden Plugins installiert sind, bevor Sie mit dem Einrichten, Aktivieren und Validieren von Microsoft Teams -Setup-Verbindungen beginnen.

#### Benötigte Plugins

| Name | Beschreibung |
|---|---|
| Chat-Integration mit Security Incident Management | Verwenden Sie die Plugin-ID **sn_chat_collab_core**, um Microsoft Teams Chat zu suchen und zu installieren.<br>Durch die Installation dieses Plugins können Sie die Chataktivität für Anwendungen von Drittanbietern wie Microsoft Teams (oder Slack und andere Chatanwendungen von Drittanbietern) nachverfolgen. |
| Microsoft Teams-Chat-Connector für Security Incident Management | Verwenden Sie die Plugin-ID **sn_ms_teams_connector**, um Microsoft Teams Chat Connector für Major Security Incident Management zu suchen und zu installieren.<br>Durch die Installation dieses Plugins können Sie die Chataktivitäten mit der für Microsoft Teamsspezifischen Zusammenarbeitskomponente nachverfolgen. |
| Microsoft Teams Diagramm-Spoke | Durch die Installation dieses Plugins wird eine Graph-Spoke-Verbindung mit Microsoft Teamshergestellt. Weitere Informationen finden Sie unter Microsoft Teams Graph-Spoke |

### Aktivieren Sie MS Teams als Chat-Anbieter

Aktivieren Sie Microsoft Teams, indem Sie die Verbindung Microsoft Teams ] validieren.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Sobald die Verbindung aktiviert und validiert wurde, wird eine Informationsmeldung angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde. Sie können die Kanalkonfiguration ändern, indem Sie Benutzer hinzufügen und entfernen und möglicherweise weitere Kanäle hinzufügen oder vorhandene Kanäle umbenennen.

#### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfiguration des Chat-Providers**.
2. Wählen Sie **den Microsoft Teams-Datensatz aus**.
3. Klicken Sie **auf Verbindung validieren**.
   Eine Bestätigungsmeldung zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.
4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um den Provider-Datensatz zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Bestätigungsmeldung zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.

5. **Speichern Sie** das Formular, nachdem Sie die Chat-Provider-Konfiguration aktiviert haben.
   Damit wird die Verbindung zwischen Microsoft Teams und Now Platform Instanz erfolgreich hergestellt.

### Erstellen Sie eine Chatkanalvorlage

Konfigurieren Sie Chat-Teams und Kanalvorlagen, um Chat-Teams und Kanäle für die Zusammenarbeit zu erstellen, die Chat-Konversationen nachzuverfolgen und diesen Chat-Kanälen Benutzer und Benutzergruppen hinzuzufügen. Diese Kanalvorlagen werden in Microsoft Teams erstellt, wenn ein schwerwiegender Security Incident heraufgestuft wird.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

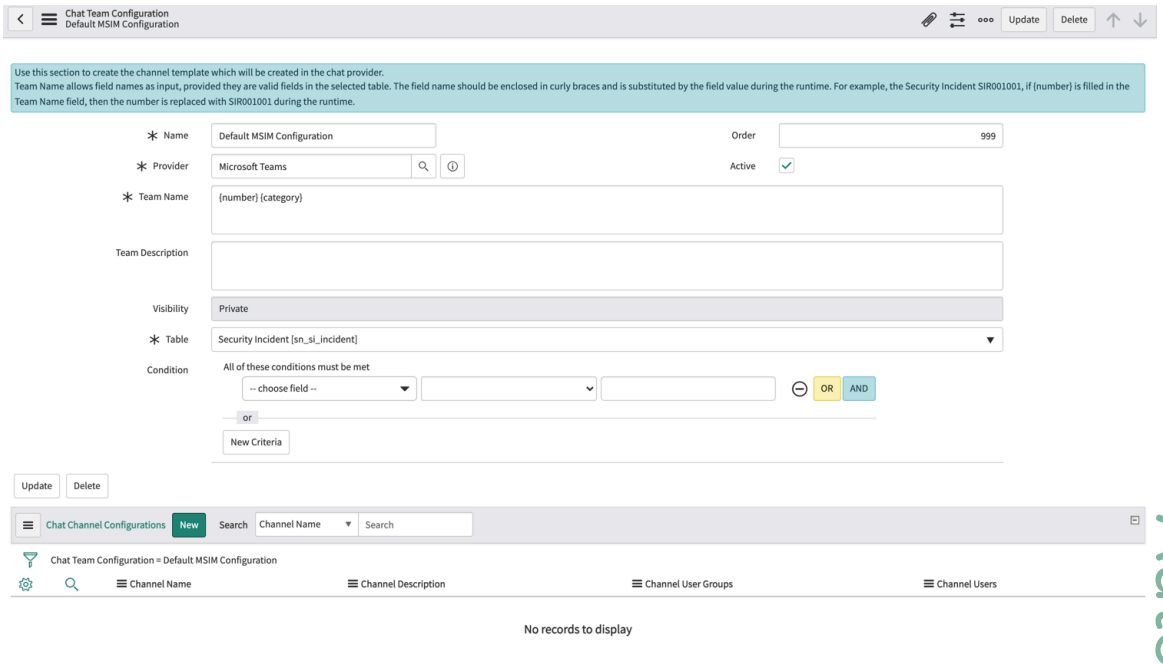
1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Kanalvorlagen**.
2. Klicken Sie im Formularheader des Formulars „Chat-Kanalkonfiguration“ auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Chat-Team-Konfiguration“.**

| Feld | Beschreibung |
|---|---|
| Name | Name des Ordners. |
| Anbieter | Microsoft Teams |
| Teamname | Name für das Team, z. B. im Format {number}-{category}.<br>**Hinweis:** Der hier angegebene Teamname wird für alle Datensätze zu schwerwiegenden Security Incidents verwendet. Um sicherzustellen, dass der tatsächliche Microsoft-Teamname in der MS Teams-Anwendung angezeigt wird und einen eindeutigen Namenswert für verschiedene schwerwiegende Security Incidents hat, wird empfohlen, einen eindeutigen Incident-Feldwert zu verwenden, z. B. die Incident-Nummer – {number}. Wie im Screenshot-Beispiel gezeigt, würden {number}, gefolgt von einem Trennzeichen '-' und die Feldvariable {category} eine eindeutige Nummer und Beschreibung des schwerwiegenden Security Incidents bereitstellen, für den Microsoft Teams erstellt wird, z. B. {number}. – {category}. |
| Teambeschreibung | Optionale Beschreibung des Teams. |
| Tabelle | Schwerwiegender Security Incident (sn_msi_incident). |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Klicken Sie auf **Absenden**.
5. Navigieren Sie zum Abschnitt Chat-Kanalkonfiguration.
6. Klicken **Neu** , um eine neue Chat-Kanalkonfiguration zu erstellen.
7. Geben Sie ein **Konfiguration des Chat-Teams** und **Kanalname**.

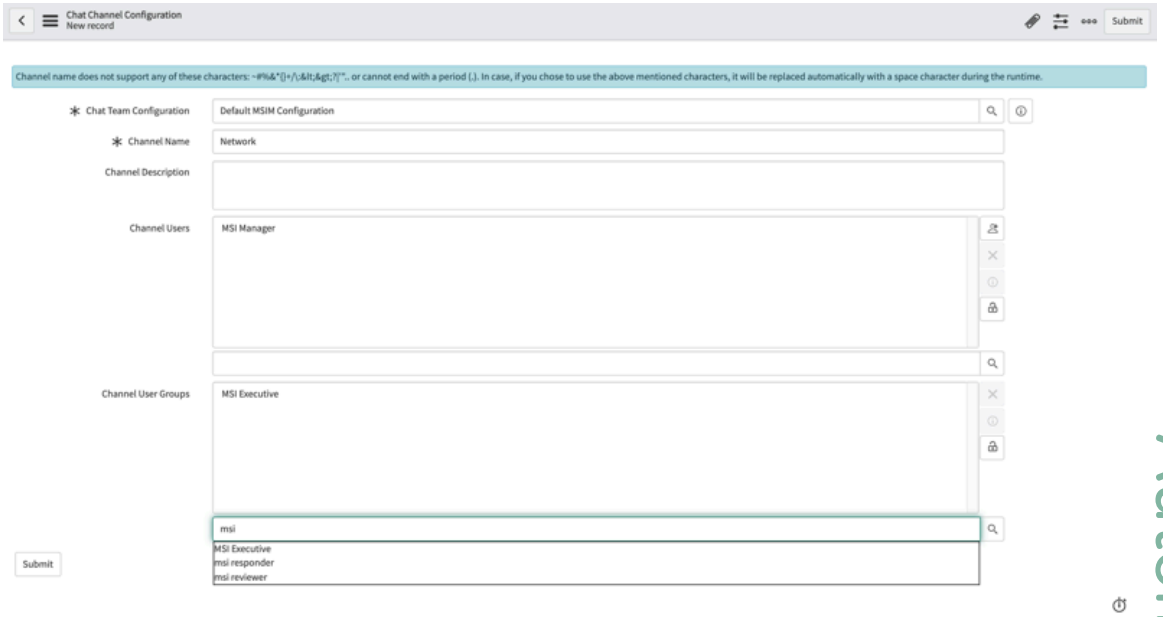
   **Hinweis:**
   Der neue Kanal, den Sie hier erstellt haben, ist auch Ihr Kanalname in Microsoft Teams. Sie können nach demselben Kanal suchen und Ihre Konversationen hinzufügen.

8. Fügen Sie die Systemeigenschaft **Kanalanwender** und **Kanalanwendergruppen** aus der Nachschlageliste.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**9. Absenden** Der neue Chatkanal-Konfigurationsdatensatz.




## Ergebnisse

Der Chatkanal wird jetzt erstellt, und die Benutzer werden diesen Chatkanalgruppen zugewiesen. Sie können die Collaboration Chat-Aktivitäten sowohl in Microsoft Teams als auch im Collaboration-Aktivitätenstrom des MSIM-Arbeitsbereichs mit der organisierten Chatkanal-Hierarchiestruktur anzeigen, wie in der Konfiguration des Chat-Kanalanbieters konfiguriert.

### Chat-Nachrichtenaktivität anzeigen

Chat-Nachrichtenaktivitäten werden aufgezeichnet und auf der Registerkarte Zusammenarbeit des Major Security Incident Management-Arbeitsbereichs angezeigt.

Die Chatnachrichtenaktivität umfasst alle Chatkonversationen, die zwischen den Teilnehmern und verschiedenen Benutzergruppen stattgefunden haben.

### Problembehandlung für MS Teams-Chat-Connector für MSIM

Weitere Informationen zu geplanten Aufgaben, Systemeigenschaften und Microsoft Teams Flow Designer-Subflows finden Sie im Abschnitt zur Problembehandlung für den Microsoft Teams-Chat-Connector.

Überprüfen Sie auf jeden Fall, ob die Chat-Nachrichten für die Zusammenarbeit in Microsoft Team und im Aktivitätenstrom für die externe Zusammenarbeit des MSIM-Arbeitsbereichs veröffentlicht werden.

### Geplante Aufgaben für Microsoft Teams

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen aus dem Chat-Connector von Microsoft Teams zu verarbeiten und die Microsoft Teams-Abonnements nach einem wiederkehrenden Zeitplan zu verlängern.

Erforderliche Rolle: admin.

- **MS Teams-Chat-Connector: Benachrichtigung verarbeiten**

  Für jedes Chatnachrichtenereignis wird eine Benachrichtigung empfangen, die die Ressourcen-ID und die Benachrichtigung enthält, die in einer Tabelle gespeichert werden. Eine regelmäßige Aufgabe wird alle 30 Sekunden ausgeführt, um unverarbeitete

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungen auszuwählen und die Microsoft Teams-API abzufragen, um den tatsächlichen Nachrichteninhalt abzurufen, der in einer anderen Tabelle gespeichert wird.

- **MS Teams-Chat-Connector: Abonnements verlängern**

  Für jeden Kanal innerhalb des Teams werden Abonnements erstellt, um über die erstellten, aktualisierten und gelöschten Events benachrichtigt zu werden. Dieses Abonnement ist nur für 60 Minuten aktiv. Die Abonnements werden alle 25 Minuten über die regelmäßige Aufgabe „Microsoft Teams Connector: Verlängerungsbenachrichtigung“ verlängert.

### Microsoft Teams Chat Connector – Funktionaler Flow

Sehen Sie sich diesen Abschnitt an, um die Microsoft Teams zugehörigen Flow Designer-Subflows zu verstehen, die zur Verwaltung der Erstellung von Chat-Kanälen und des Benutzerzugriffs bei schwerwiegenden Security Incidents verwendet werden.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

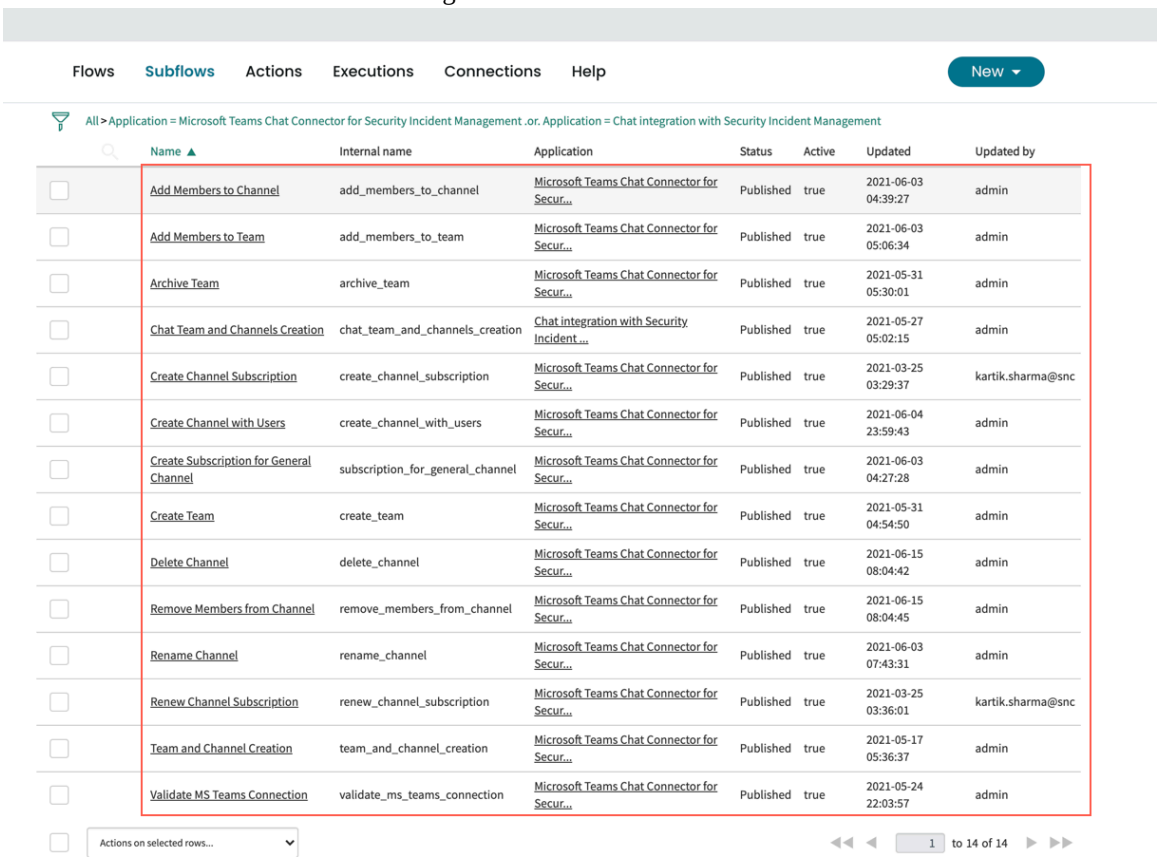
#### Prozedur

1. Navigieren zu **Alle** > **Flow Designer**.
2. Mitglieder zu Kanal hinzufügen
3. Fügen Sie dem Team Mitglieder hinzu
4. Team archivieren
5. Erstellung von Chat-Teams und Kanälen
6. Erstellen Sie ein Kanalabonnement
7. Erstellen Sie einen Kanal mit Anwendern
8. Erstellen Sie ein Abonnement für den allgemeinen Kanal
9. Team erstellen
10. Kanal löschen
11. Entfernen Sie Mitglieder aus dem Kanal
12. Benennen Sie Kanal um
13. Verlängern Sie das Kanalabonnement
14. Team- und Kanalerstellung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Validieren Sie die MS Teams-Verbindung




## Management schwerwiegender Sicherheits-Incidents – Administration

Planen und konfigurieren Sie Ihre Management schwerwiegender Sicherheits-Incidents -Implementierung.

Sie können die folgenden Aspekte der Verwaltung von Management schwerwiegender Sicherheits-Incidents konfigurieren:

### Ermöglichen Sie das Vorschlagen, Heraufstufen und Verknüpfen von schwerwiegenden Security Incidents

Ermöglichen Sie Benutzern, Incidents als schwerwiegende Security Incidents vorzuschlagen oder heraufzustufen. Verfolgen Sie alle Incidents im Zusammenhang mit einem schwerwiegenden Security Incident einfach nach, indem Sie die Verknüpfung von Security Incidents mit dem übergeordneten oder untergeordneten Incident ermöglichen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Ermöglichen Sie Benutzern, einen Security Incident zu einem schwerwiegenden Security Incident vorzuschlagen, indem Sie im Abschnitt „SIR/VR Workspace Actions“ (SIR/VR-Arbeitsbereichsaktionen) das Kontrollkästchen **Schwerwiegenden Security Incident** vorschlagen aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ermöglichen Sie Benutzern, einen Security Incident zu einem schwerwiegenden Security Incident heraufzustufen, indem Sie das Kontrollkästchen **Zu schwerwiegendem Security Incident** heraufstufen aktivieren.
4. Aktivieren Sie die Verknüpfung eines Security Incident mit einem schwerwiegenden Security Incident, damit sie zusammen nachverfolgt werden können, indem Sie das Kontrollkästchen Mit schwerwiegendem **Security Incident** verknüpfen aktivieren.
5. Wählen Sie **Aktualisieren**.

### Markieren Sie Security Incidents als schwerwiegende Security Incidents

Markieren oder kennzeichnen Sie die Security Incidents oder angreifbaren Datensätze für einen schwerwiegenden Security Incident, wenn der Incident vorgeschlagen oder heraufgestuft wird. Wenn ein Security Incident vorgeschlagen wird, wird der Incident-Datensatz als Kandidat für schwerwiegenden Security Incident bezeichnet. Wenn eine Sicherheit heraufgestuft wird, wird der Incident-Datensatz als schwerwiegender Security Incident mit dem Status „Akzeptiert“ bezeichnet.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Aktivieren Sie das Kontrollkästchen Bezeichnungen **anzeigen**, um den vorgeschlagenen Incident-Kandidaten als schwerwiegenden Security Incident zu kennzeichnen, indem Sie das **Suchfeld Bezeichnungsname – Als Kandidaten vorschlagen** auswählen und im Abschnitt „Bezeichnungen des **SIR/VR-Arbeitsbereichs** “ die Option Kandidat für schwerwiegenden Security Incident auswählen.
3. Aktivieren Sie das Kontrollkästchen Bezeichnungen **anzeigen**, um den heraufgestuften Incident-Kandidaten als schwerwiegenden Security Incident zu kennzeichnen, indem Sie das **Suchfeld Bezeichnungsname – Heraufstufung zu schwerwiegendem Security Incident** auswählen und im Abschnitt **SIR/VR Workspace Labels** (SIR/VR-Arbeitsbereich) die Option Schwerwiegender Security Incident auswählen.
4. Wählen Sie **Aktualisieren**.

### Konfigurieren Sie Bezeichnungen für schwerwiegende Security Incidents

Konfigurieren Sie Bezeichnungen in Major Security Incident Management, um benutzerdefinierte Bezeichnungen zu erstellen und die externen Zusammenarbeitsaktivitäten und -aufgaben im Aktivitätenstrom zu filtern. Die verschiedenen Arten von implementierten Bezeichnungen sind Statusbezeichnungen und Zeitleistenbezeichnungen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Aktivieren Sie das Kontrollkästchen Bezeichnungen **anzeigen**, um die Bezeichnung verschiedener Incident-Status wie „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“, „Überprüfen“,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Zeitleistenereignis“ im Abschnitt „Bezeichnungen des **MSIM-Arbeitsbereichs“ (Anzeige für Zusammenarbeitsaktivitäten und -aufgaben)** zu aktivieren.

3. Wählen Sie **Aktualisieren**.

### Konfigurieren Sie Bezeichnungen für schwerwiegende Security Incidents

Konfigurieren Sie verschiedene Arten von Bezeichnungen, um die Incident-Status besser zu filtern und anzugeben. Bezeichnungen für schwerwiegende Security Incidents bieten die Flexibilität, die Zusammenarbeitsaktivitäten und -aufgaben der Incident-Datensätze zu kennzeichnen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

Sie können die Bezeichnungen mithilfe des Bezeichnungssymbols aktivieren oder deaktivieren, das im Abschnitt „Aktivitätenstrom“ des Abschnitts „Zusammenarbeit und Aufgabenorganisator“ des MSIM-Arbeitsbereichs verfügbar ist.

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **MSI-Bezeichnungen**.
2. Klicken Sie auf **Neu**, um eine neue Bezeichnung zu erstellen.
3. **Füllen** Sie das Formular mit **Bezeichnungsname**und Bezeichnungsfarbe aus.
4. Klicken Sie auf Bezeichnung **erstellen**.
5. OOTB, im Folgenden sind die konfigurierten Bezeichnungen für jeden Incident-Status aufgeführt. Sie können den Namen oder die Farbe der Bezeichnung nicht ändern:
   - Analyse
   - Beinhalten
   - Beseitigen
   - Prüfen
   - Wiederherstellen
   - Zeitleistenereignis

**Hinweis:**
Sie können die benutzerdefinierten Bezeichnungen und ihre Eigenschaften ändern.

### Legen Sie die Benachrichtigungseinstellungen für fest MSIM

Automatisieren Sie den E-Mail-Benachrichtigungsprozess, und benachrichtigen Sie die Benutzer, wenn ein Security Incident entweder vorgeschlagen oder zu einem Kandidaten für einen schwerwiegenden Security Incident hochgestuft wird.

Erforderliche Rolle: sn_msi.workspace_admin.

Die Benachrichtigungen werden nur ausgelöst, wenn ein Security Incident vorgeschlagen und an alle Benutzer und Gruppen gesendet wird, die für die Benachrichtigungsliste konfiguriert sind. Standardmäßig wird die E-Mail-Benachrichtigung von dem Benutzer empfangen, der den Security Incident als Kandidaten für einen schwerwiegenden Security Incident vorgeschlagen hat.

**Benachrichtigung: Security Incident vorgeschlagen (SI) als schwerwiegender Security Incident (MSI)**



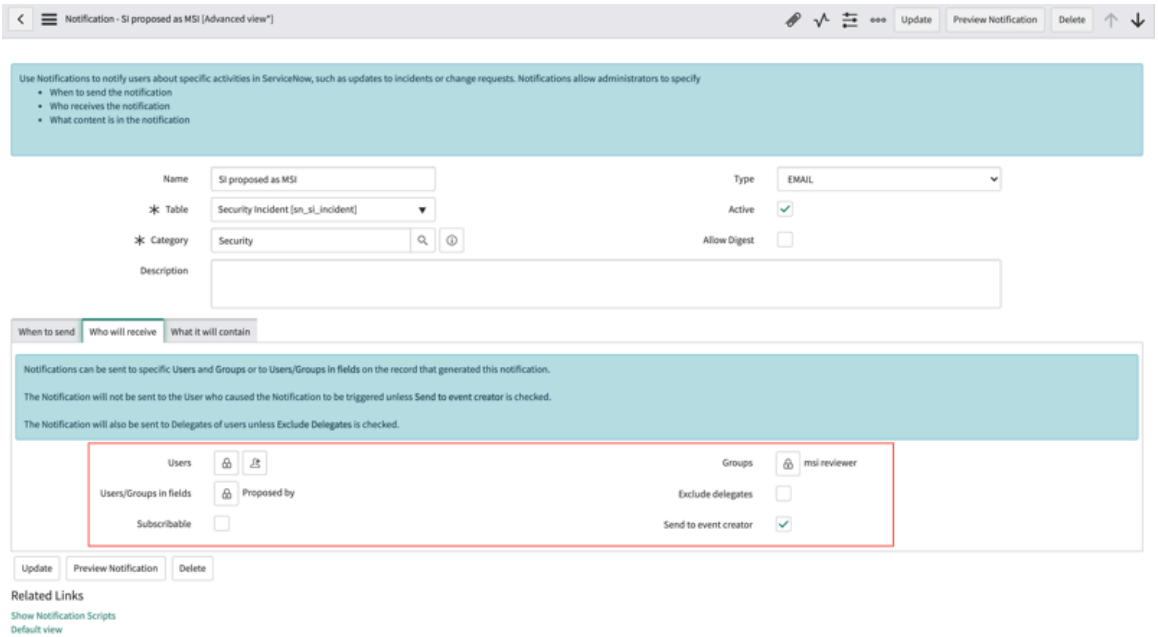
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wer erhält:

- Standardmäßig ist **MSI-Überprüfer** Gruppenname wird erstellt, und jeder Benutzer, der dieser Gruppe hinzugefügt wird, darf ein sein **MSIM-Manager** und die Benutzer, die sich in dieser Gruppe befinden, erhalten die Benachrichtigungs-E-Mails.
- Jeder bestimmte Benutzer, der hinzugefügt wird **Anwender** Die Liste erhält auch die Benachrichtigungs-E-Mails.

Was darin enthalten sein wird:

Wenn Sie den E-Mail-Inhalt ändern möchten, z. B. den E-Mail-Text, der den Betreff oder den Nachrichten-HTML-Code enthält, müssen Sie über die Systemadministrator-Rolle verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.




**Benachrichtigung: Security Incident heraufgestuft (SI) als schwerwiegender Security Incident (MSI)**

Diese Benachrichtigung wird ausgelöst, wenn ein Security Incident hochgestuft wird und wenn der Datei-Explorer und die Basisstruktur Microsoft Teams erstellt werden. Standardmäßig wird diese Benachrichtigung von dem Benutzer empfangen, der den Security Incident zu einem schwerwiegenden Security Incident heraufgestuft hat.

**Empfänger**

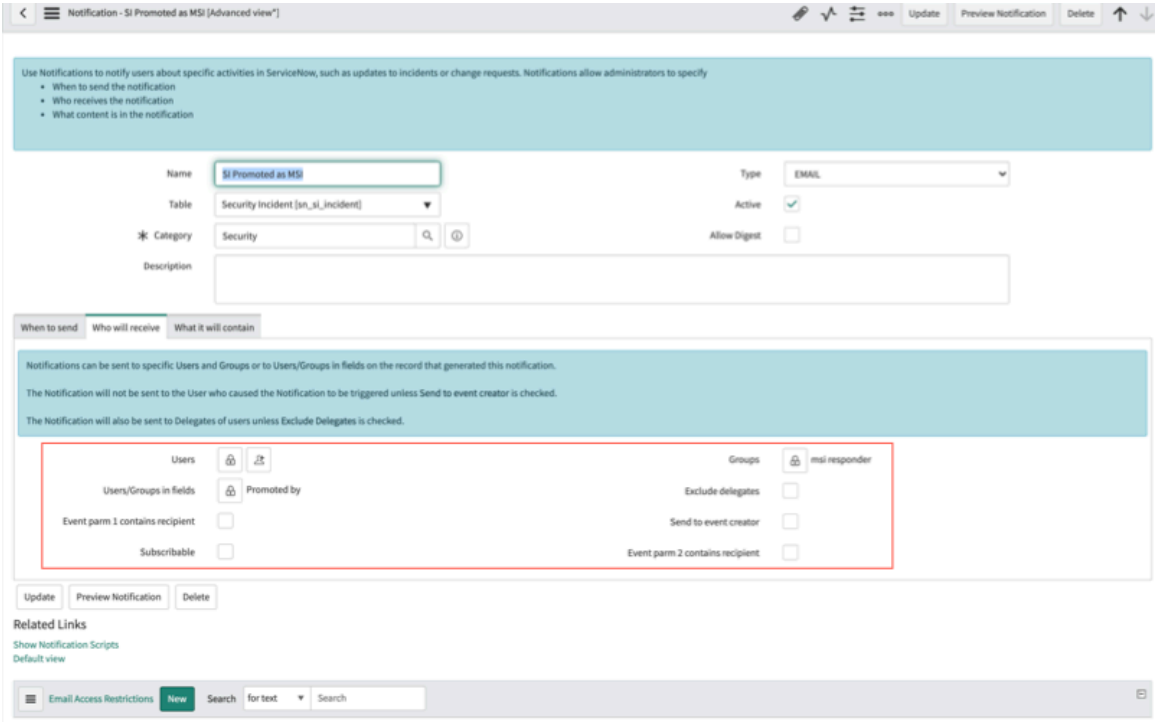
- Standardmäßig ist eine **Gruppe** nach Name **MSI-Responder** wird erstellt, und jeder Benutzer, der dieser Gruppe hinzugefügt wird, hat die Berechtigung **MSIM-Responder** Rolle und alle Benutzer, die sich in dieser Gruppe befinden, erhalten die Benachrichtigungs-E-Mail.
- Jeder bestimmte Benutzer, der hinzugefügt wird **Anwender** Die Liste erhält auch die Benachrichtigungs-E-Mails.

**Was enthalten sein wird**

Wenn Sie den E-Mail-Inhalt ändern möchten, z. B. den E-Mail-Text, einschließlich Betreff oder Nachrichten-HTML, müssen Sie über die Systemadministrator-Rolle verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Konfigurieren Sie MSI-Abschlussaktivitäten

Richten Sie Aktionen ein, die automatisch ausgeführt werden, wenn ein schwerwiegender Security Incident geschlossen wird. Erhöhen Sie die Sicherheit, indem Sie Ordner mit Lösungsinformationen automatisch archivieren und den Zugriff darauf entfernen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**.
2. Archivieren Sie Chatkommunikation im Zusammenhang mit der Lösung des Incident, indem Sie im Abschnitt „Automatisierte Abschlussaktionen“ das Kontrollkästchen **Zusammenarbeitskanäle archivieren** aktivieren.
3. Entfernen Sie Ordner, die Material im Zusammenhang mit der Lösung des Incident enthalten, indem Sie das Kontrollkästchen **Ordner für Zusammenarbeit entfernen aktivieren**.
4. Wählen Sie **Aktualisieren**.

## Management schwerwiegender Sicherheits-Incidents-Arbeitsbereich

Management schwerwiegender Sicherheits-Incidents bietet einen dedizierten Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für Major Security Incident -Manager entwickelt wurde.

Einfache Zusammenarbeit bei Aktivitäten, die zur Lösung schwerwiegender Security Incidents beitragen, indem Sie Dateien und Ordner freigeben und anzeigen, Incident-Aufgaben anzeigen und aktualisieren und über dedizierte Chatkanäle mit den an dem Incident arbeitenden Personen kommunizieren.

Major Security Incident Management (MSIM) bietet einen Mechanismus zum Nachverfolgen und Beheben schwerwiegender Security Incidents. MSIM arbeitet mit den vorhandenen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produktfunktionen von Security Incident und Vulnerability Response zusammen und verbessert den Korrekturprozess für schwerwiegende Security Incidents mit den folgenden Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Benutzerrolle „Manager für schwerwiegende Security Incidents“ entwickelt wurde.
- Organisieren Sie Aufgaben zur Reaktion auf schwerwiegende Security Incidents, einschließlich Aufgaben, die für verknüpfte Security Incidents und Schwachstellengruppen nachverfolgt werden.
- Automatisieren Sie die Erstellung von Ordnern für die Zusammenarbeit und Chat-Kommunikationskanäle, sobald ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über eine Microsoft SharePoint -Integration.
- Chat-Channel-Manager- und Aktivitätenstrom-Komponenten zur Verwaltung der Kommunikation über mehrere Sicherheits-, IT- und Funktionsgruppen hinweg über eine Microsoft Teams -Integration.
- Zusammenfassende Berichte zu Auswirkungs- und Fortschrittsmetriken für schwerwiegende Security Incidents, einschließlich Rollup der betroffenen Assets, Benutzer, Standorte und Teamressourcen sowie Zeitleisten wichtiger Incident-Meilensteine.

Verwenden Sie den MSIM-Arbeitsbereich, um schwerwiegende Security Incidents nachzuverfolgen und zu beheben:

1. Zeigen Sie die Trenddiagramme und den Fortschritt des schwerwiegenden Security Incident an.
2. Verfolgen und organisieren Sie Microsoft SharePoint-Dateiaktivitäten über den MSIM-Arbeitsbereich.
3. Verfolgen und organisieren Sie Microsoft Teams-Chataktivitäten über den MSIM-Arbeitsbereich.
4. Zeigen Sie Incident-Details über den MSIM-Arbeitsbereich an, und aktualisieren Sie sie.
5. Filtern Sie Zusammenarbeitsaktivitäten im Aktivitätenstrom des MSIM-Arbeitsbereichs.

## Arbeiten mit Management schwerwiegender Sicherheits-Incidents

Manager können den Arbeitsbereich Management schwerwiegender Sicherheits-Incidents verwenden, um die vorgeschlagenen, heraufgestuften, verknüpften und abgelehnten Incident-Datensätze anzuzeigen und die zugehörigen Aktivitäten nachzuverfolgen.

### Incident-Datensätze vorschlagen, heraufstufen und verknüpfen

Schlagen Sie Security Incidents als schwerwiegende Security Incidents vor oder stufen Sie sie herauf, wenn Incidents als kritische Bedrohung für die Organisation identifiziert werden.

Sobald „Major Security Incident Management“ in Ihrer Instanz von ServiceNow installiert ist, können Sie den Übergang von Security Incidents zu schwerwiegenden Incidents wie folgt handhaben:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schlagen Sie einen Security Incident dem Kandidaten für einen schwerwiegenden Security Incident vor, um einen Überprüfungsprozess zu initiieren.
- Stufen Sie einen Security Incident ohne Überprüfungsprozess direkt zu einem schwerwiegenden Security Incident hoch.
- Lehnen Sie einen Security Incident ab, der als schwerwiegender Security Incident vorgeschlagen wurde.

Sie können einen Security Incident auch als untergeordneten Incident mit dem schwerwiegenden Security Incident verknüpfen, sodass alle zugehörigen Security Incidents gemeinsam nachverfolgt werden können.

### Vorschlagen als Major Security Incident

Schlagen Sie einen Security Incident für einen schwerwiegenden Security Incident vor.

#### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie als schwerwiegenden Security Incident vorschlagen möchten.
3. Wählen Sie das Symbol „Zusätzliche Aktionen“ und **dann Schwerwiegenden Security Incident vorschlagen aus**.
4. Füllen Sie im Dialogfeld „Schwerwiegenden Security Incident vorschlagen“ die Felder aus.
   a. **Erkennungsdatum**: Datum, an dem der schwerwiegende Security Incident erstmals erstellt oder vorgeschlagen wurde
   b. **Begründung**: Geben Sie die Begründung für das Vorschlagen des Incident an.
   c. **Potenzielle Auswirkung**: Geben Sie die Auswirkung des Incident an.
5. Wählen **Sie Vorschlagen aus**.

#### Ergebnisse

Der Incident wird vorgeschlagen, und die folgenden Aktionen werden ausgeführt:

- Im Security Incident-Datensatz wird eine Überprüfungsbannernachricht angezeigt, und das definierte Tag Major Security Incident wird angezeigt.
- Der Datensatz wird in der zugehörigen Liste „Schwerwiegender Security Incident“ im Incident-Datensatz mit dem Status „Vorgeschlagen“ und in der Liste der Kandidaten für den MSIM-Arbeitsbereich angezeigt.
- Der Abschnitt „Aktivität“ im MSIM-Arbeitsbereich zeigt, dass vorgeschlagen wurde, den Security Incident zu einem schwerwiegenden Security Incident heraufzustufen.
- Eine Nachricht wird an die Personen in der definierten Benachrichtigungsliste gesendet, die einen Link zum Incident-Datensatz und die Registerkarte „Details“ für den Incident enthält.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Hochstufen zu Major Security Incident

Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident herauf, oder lehnen Sie heraufgestufte Vorschläge über den Management schwerwiegender Sicherheits-Incidents (MSIM)-Arbeitsbereich ab.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSIM-Arbeitsbereich**.
2. Wählen Sie in der Liste „Schwerwiegende Security Incidents“ die Option **Kandidaten**aus.
3. Wählen Sie im Formular „Security Incidents“ den zur Heraufstufung vorgeschlagenen Incident aus.
4. **Wahlweise:** Überprüfen Sie die Details des Security Incident im Abschnitt „Details“, oder zeigen Sie erweiterte Details im Incident-Datensatz auf einer separaten Registerkarte an, indem Sie auf **Weitere Details**anzeigen klicken.
5. Entweder den Security Incident heraufstufen oder den Heraufstufungsvorschlag ablehnen.
   - Um den Incident **hochzustufen, klicken Sie auf Zu schwerwiegendem Security Incident heraufstufen**.
   - Um den Heraufstufungsvorschlag abzulehnen, klicken Sie auf **Als schwerwiegenden Security Incident**ablehnen.
6. Wählen Sie **Speichern**.

#### Ergebnisse

- Wenn Sie den Heraufstufungsvorschlag abgelehnt haben, wird der Incident nicht heraufgestuft, und der Incident-Eintrag wird auf die Registerkarte „Abgelehnt“ verschoben.
- Wenn Sie den Incident heraufgestuft haben, wird der Incident-Eintrag auf die Registerkarte Offen verschoben, und im Sicherheitsdatensatz wird ein Tag angezeigt, das angibt, dass es sich um einen schwerwiegenden Security Incident handelt.
- Die Entscheidung wird im Abschnitt „Aktivität“ des MSIM-Arbeitsbereichs aufgelistet.

Sobald ein Incident heraufgestuft wurde, wird die Standardkonfiguration angewendet.

- Eine Ordnerstruktur wird basierend auf der Ordnervorlagenkonfiguration erstellt.
- Chatkanäle werden basierend auf der Kanalkonfiguration erstellt.
- Eine E-Mail-Nachricht wird an die angegebenen Benutzer gesendet. Die Standardbenachrichtigung enthält einen Link zu dem schwerwiegenden Security Incident und Details zum Incident. Die festgelegten Benutzer haben jetzt auch Zugriff auf die Zusammenarbeitsressourcen, sodass die Benachrichtigung auch den Namen des Microsoft-Teams und einen Link zu Microsoft SharePoint-Ordnern im Zusammenhang mit dem Incident enthält.

### Link zu Major Security Incident

Verknüpfen Sie Security Incidents mit einem schwerwiegenden Security Incident.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie mit dem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie das Symbol „ **Zusätzliche Aktionen** “ und dann Mit schwerwiegendem **Security Incident verknüpfen aus**.
4. Wählen Sie den schwerwiegenden Security Incident aus, zu dem Sie eine Verknüpfung herstellen möchten.
   a. Wählen Sie im Dialogfeld das Symbol Nachschlagen mit Liste aus.
   b. Wählen Sie den schwerwiegenden Security Incident aus, zu dem Sie eine Verknüpfung herstellen möchten.
   c. Wählen Sie **OK**.
5. Wählen **Sie Vorschlagen aus**.

### Ergebnisse

Der Vorschlag wird übermittelt, und die folgenden Aktionen werden ausgeführt:

- Im Security Incident-Datensatz wird eine Überprüfungsbannernachricht angezeigt, und das definierte Tag Major Security Incident wird neben dem Feld **Sicherheits-Tag auswählen** angezeigt.
- Auf der Registerkarte **Details** für den schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidentsenthält die Dropdown-Liste für Datensatznummern beide Incidents.
- Der Datensatz wird in der zugehörigen Liste „Schwerwiegender Security Incident“ des Incident-Datensatzes mit dem Status „Vorgeschlagen“ angezeigt.
- Eine Nachricht wird an die Personen in der definierten Benachrichtigungsliste gesendet, die einen Link zum Incident-Datensatz und die Registerkarte „Details“ für den Incident enthält.
- Der Abschnitt „ **Aktivität** “ im MSIM-Arbeitsbereich zeigt, dass der Security Incident dem schwerwiegenden Security Incident mit einem Link als untergeordneter Security Incident hinzugefügt wurde.

## Verwenden der MSI-Listenansicht im MSIM-Arbeitsbereich

Mit der Listenansicht im MSIM-Arbeitsbereich können Sie vorgeschlagene, heraufgestufte und abgelehnte schwerwiegende Security Incidents anzeigen.

### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

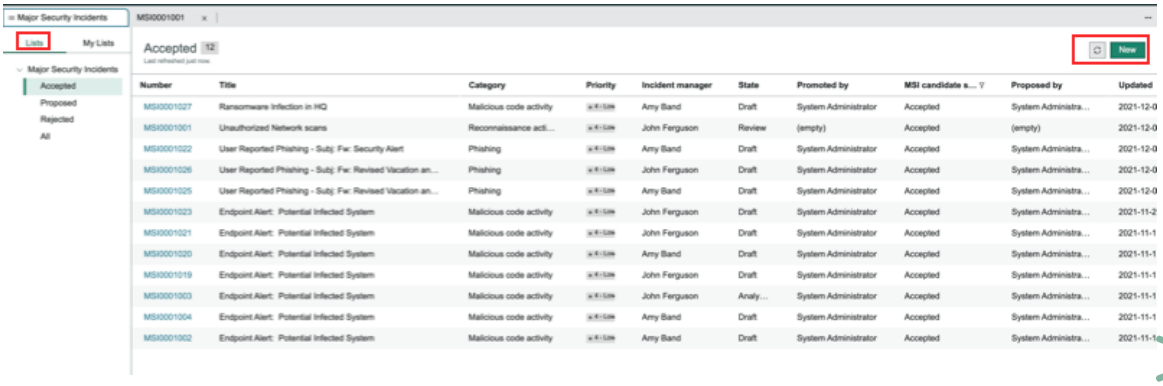
Sie können neue Incidents auch über die Schaltfläche **Neu** in der oberen rechten Ecke des Arbeitsbereichs erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Reaktion auf schwerwiegende Security Incidents** > **MSIM-Arbeitsbereich**.
2. Klicken Sie auf das Listensymbol, um die Listenansicht anzuzeigen.




3. Klicken Sie auf **Meine Listen**, um eine eigene Liste mit schwerwiegenden Security Incidents zu erstellen.
4. In der folgenden Tabelle erfahren Sie, was Sie in der Listenansicht tun können:

| Aufgabe | Beschreibung |
|---|---|
| Meine Listen | Erstellen Sie neue MSI-Datensatzlisten, und zeigen Sie die von Ihnen erstellten Listen an. |
| Legen Sie Filter für eine Spalte in einer Liste fest | Wählen Sie eine Spalte aus, und erweitern Sie das Menü mit vertikalen Punkten, um Optionen anzuzeigen, mit denen die Daten in der Spalte weiter gefiltert werden. |
| Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab | Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine der folgenden Optionen auswählen:<br>○ Übereinstimmungen anzeigen: Zeigt nur Elemente an, die dem ausgewählten Element in der Spalte entsprechen.<br>○ Herausfiltern: Filtert die Elemente aus der Spalte heraus, die dem ausgewählten Element in der jeweiligen Spalte entsprechen. |
| Liste neu laden | Aktualisieren Sie die Listen, und zeigen Sie die vollständigen Listen an, die aktualisiert wurden. |
| Neu | Erstellen Sie einen neuen MSI-Datensatz. |

### Zeigen Sie Major Security Incident Trenddiagramme an

Die Bereitstellung aktueller zusammenfassender Berichte über die Auswirkungen und den Fortschritt schwerwiegender Security Incidents ist ein wichtiger Aspekt bei der Verwaltung schwerwiegender Security Incidents im neuen Arbeitsbereich.

Die Registerkarte **Übersicht** enthält die relevanten Metriken zum Verwalten des Umfangs und des Fortschritts des Incident, einschließlich der Zusammenfassung der betroffenen Assets, Benutzer, Standorte und Teamressourcen sowie der Zeitleiste der wichtigen Incident-Meilensteine.

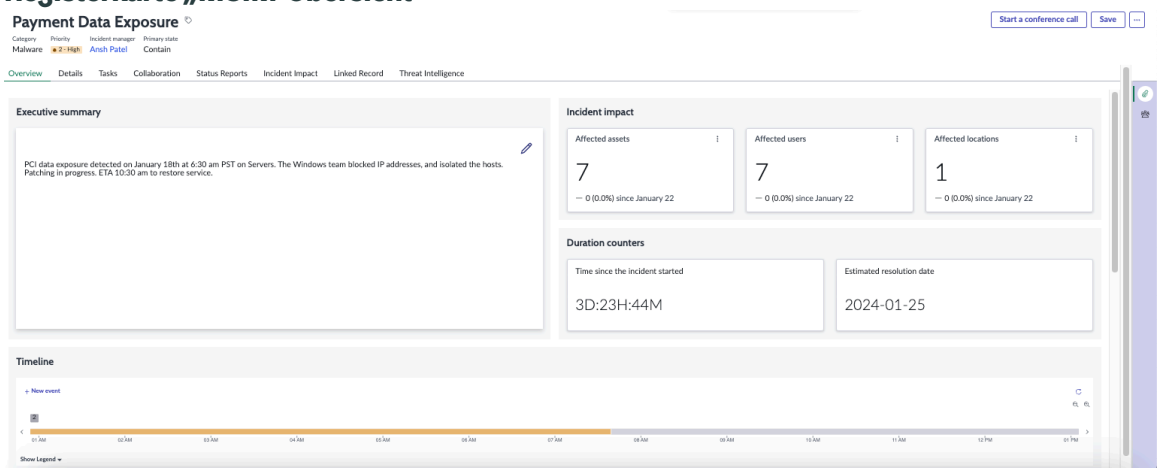
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zeitleiste bietet eine horizontale Ansicht der wichtigsten Ereignisse und Meilensteine, die im Rahmen der Lösung eines bestimmten schwerwiegenden Security Incidents aufgetreten sind. Die Zeitleistenkomponente wird über allen Registerkarten des Major Security Incident Management-Arbeitsbereichs angezeigt und kann nach Bedarf reduziert und erweitert werden. Die dargestellten Ereignisdaten werden jedes Mal aktualisiert, wenn festgelegte Meilensteinereignisse oder Meilensteine hinzugefügt oder aktualisiert werden.

Jedes Event oder jeder Meilenstein wird mit einer anderen Option für den Zeitleisten-Event-Typ angegeben, um die Anzahl und den Typ der Events oder Meilensteine zu identifizieren. Zum Beispiel NOW-Datensatzaktualisierungen, Aufgaben, Zusammenarbeitsaktivitäten. Darüber hinaus wird der Zeitraum für die verschiedenen schwerwiegenden Security Incident-Status automatisch nachverfolgt und anhand farbcodierter Bereiche angezeigt, die zusammen mit der Dauer jedes Incident-Status angezeigt werden.

**Registerkarte „MSIM-Übersicht“**




Sie können die Anzeige bestimmter Event-Typen für Zeitleistenindikatoren und Zeitleistenbereiche mithilfe der Filter-Umschaltflächen aktivieren oder deaktivieren.

In der folgenden Tabelle finden Sie zusätzliche Funktionen, die mit der Zeitleistenkomponente verfügbar sind.

**Zusätzliche Funktionen der Zeitleistenkomponente**

| Aufgabe | Beschreibung |
|---|---|
| Neues Ereignis | Erstellt neue benutzerdefinierte Events und ordnet diese Events dem MSI-Datensatz zu. Dies hilft bei der Erstellung von Ereignissen für vergangene und zukünftige Daten, die andernfalls möglicherweise nicht über eine gekennzeichnete Aufgabe, Datensatzstatusänderung oder gekennzeichnete Zusammenarbeitsaktivität erfasst würden, die standardmäßig auf der Zeitleiste angezeigt wird. |
| Zurücksetzen | Setzt alle Vergrößern/Verkleinern oder Filter zurück, die auf die Zeitleiste angewendet wurden, sodass die Standardansicht bereitgestellt wird. |
| Zeitleistenindikatoren | Listet die verschiedenen Arten von Events auf, z. B. Änderungen am Now Record-Feld, Beschriftete Aufgaben, Beschriftete Zusammenarbeitsaktivitäten und Sonstige (benutzerdefiniert), zusammen mit den Symbolen und der Gesamtzahl der Events, die in |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

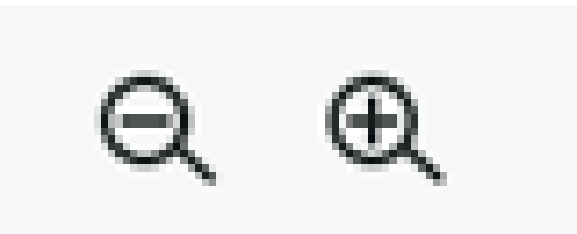
**Zusätzliche Funktionen der Zeitleistenkomponente (Fortsetzung)**

| Aufgabe | Beschreibung |
|---|---|
| | Bezug auf jeden Event-Typ-Indikator aufgetreten sind.<br>Mit dem Schieberegler können Sie alle Events für einen bestimmten Event-Typ aktivieren oder deaktivieren. |
| Legende anzeigen | Wählen Sie diese Option aus, um die Dropdown-Legende mit verschiedenen Arten von Zeitleistenindikatoren anzuzeigen. |
| Fortschrittsbalken der Zeitleiste | Zeigt den Gesamtfortschritt des Incident über festgelegte Zeitleistenereignisse oder Meilensteine an, die innerhalb der verschiedenen angezeigten Zeitleistenbereiche aufgetreten sind. |
| Zeitachsenbereiche | Zeigt verschiedene Incident-Statustypen und -Dauer an, während der Incident während des gesamten Lebenszyklus eines schwerwiegenden Security Incident voranschreitet.<br>Aktivieren oder deaktivieren Sie ein bestimmtes Event basierend auf dem Incident-Status. |

**Führen Sie die folgenden Schritte aus, um ein neues Event zu erstellen:**

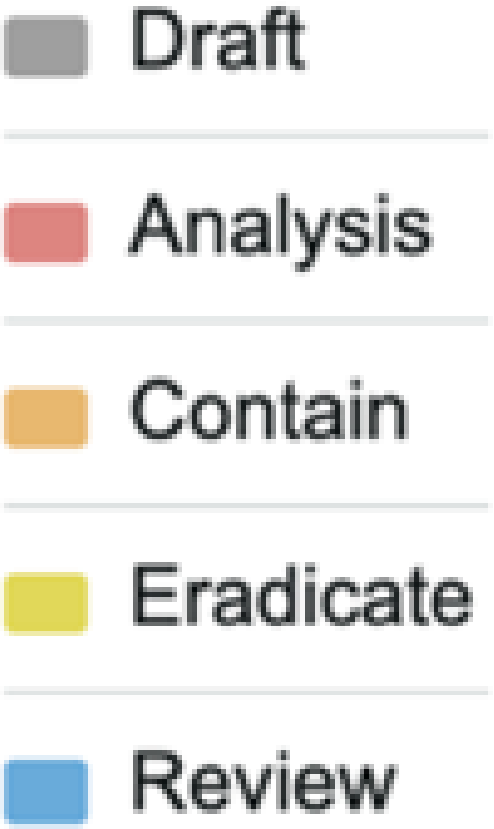
1. Wählen Sie im Abschnitt Zeitleiste der Registerkarte Übersicht die Option aus **Neues Ereignis**.
2. Geben Sie im Popup-Fenster Neues Zeitleisten-Event hinzufügen den **Event-Titel**, den **Event-Zeitstempel**und den **Event**-Text an.
3. Auswahlvorgang **Erstellen**.

In der folgenden Tabelle werden die in der Zeitleistenkomponente verwendeten Symbole beschrieben.

| Aktion | Beschreibung |
|---|---|
|  | Vergrößern oder verkleinern Sie die Fortschrittsleiste der Zeitleiste, einschließlich der Anzeige einzelner Events, wenn Zahlen angezeigt werden, um mehrere Events in unmittelbarer Nähe darzustellen. |
| | Die Now Record-Schlüssel-Events, die automatisch während einer neuen MSI-Datensatzerstellung oder einer Änderung des Heraufstufungsstatus, einer Änderung des Erkennungsdatums, eines geschätzten Lösungsdatums und anderer wichtiger Datensatz-Feldwertänderungen erstellt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aktion | Beschreibung |
| --- | --- |
| | Das Aufgabenereignis enthält Details, wenn eine Aufgabe auf der Registerkarte „Aufgabenorganisator“ des Arbeitsbereichs mit der Bezeichnung oder dem Tag der Zeitleiste gekennzeichnet wurde. |
| | Die anderen benutzerdefinierten Ereignisse oder Meilensteine. |
| | Das Zusammenarbeitsereignis enthält Details, wenn bestimmte Chats oder Zusammenarbeitsaktivitäten vorhanden sind, die auf der Registerkarte „Zusammenarbeit“ des Arbeitsbereichs mit der Zeitleistenbezeichnung oder dem Tag gekennzeichnet wurden. |
|  | Die Zeitleistendauer für die verschiedenen Incident-Status des MSI-Datensatzes. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

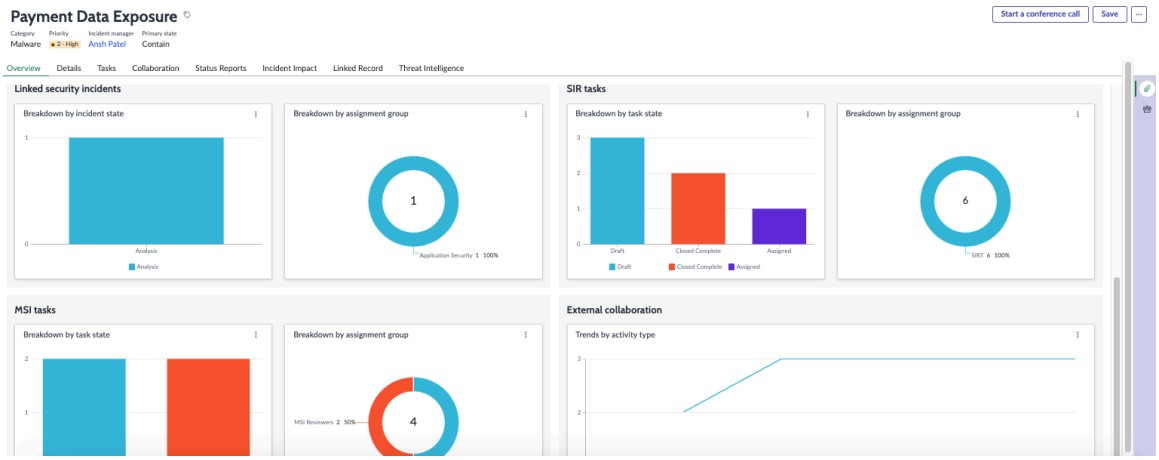
### Zeigen Sie Major Security Incident Auswirkungsmetriken an

Zeigen Sie die Fortschrittsmetriken für die Auswirkungen schwerwiegender Security Incidents als Balkendiagramme und Diagramme an.

Zusätzlich zu den Visualisierungen der Incident-Zeitleiste und des Fortschrittstrenddiagramms bietet die **Übersicht** Die Registerkarte „“ enthält relevante Auswirkungsmetriken, um den sich ändernden Umfang des Incident zu verwalten, einschließlich Rollup der betroffenen Assets, Benutzer, Standorte und Teamressourcen.

Die in den Visualisierungskomponenten angezeigten Anzahlen basieren auf aktiven Aufgaben in verknüpften SIR-Incidents (Security Incident Response). Wenn Aufgaben geöffnet und geschlossen werden, ändern sich diese Anzahlen in Bezug auf Art und Umfang der verbleibenden Aktivitäten, die für den schwerwiegenden Security Incident geplant sind, um die in den Visualisierungskomponenten des Trenddiagramms angezeigten Trends darzustellen.

**Registerkarte „MSIM-Übersicht“**




In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie über den ausführen können **Übersicht** Abschnitt:

#### Übersichts-UI-Abschnitte

| Titel | Beschreibung |
|---|---|
| **Incident Impact** | Diese Komponenten zeigen die betroffenen Ressourcen basierend auf einem Rollup aller aktiven Aufgaben und verknüpften Incidents mit identifizierten Assets, Benutzern, Standorten und zugewiesenen Teammitgliedern an. Die betroffenen Ressourcen sind:<br>• Betroffene Assets<br>• Betroffene Benutzer<br>• Betroffene Standorte<br>• Indikatoren<br>• Erkennbare Elemente<br><br>Wenn Sie auf die Zahlenwerte klicken, können Sie Detailinformationen anzeigen und zu den betroffenen Assets, Benutzern |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Übersichts-UI-Abschnitte (Fortsetzung)**

| Titel | Beschreibung |
|---|---|
| | und Standortdetails navigieren und die zugehörigen Aufgaben auf der Registerkarte „ **Incident-Auswirkung** “ des Arbeitsbereichs anzeigen.<br><br>Basierend auf dem ausgewählten Link zum Incident-Auswirkungstyp werden die zugehörigen Incident-Details wie Aufgabentyp und seine Beschreibung, Zuweisungsgruppe und Incident-Status im angezeigt **Incident Impact** Registerkarte des MSIM-Arbeitsbereichs. |
| **Zeit** | Zeigt den Zeitraum als Gesamtzahl der Tage ab dem Zeitpunkt an, zu dem der schwerwiegende Security Incident aktiv ist.<br><br>Die Zeit wird basierend auf berechnet **Erkennungsdatum** eingegeben in **Details** Registerkarte des Arbeitsbereichs.<br><br>Das Erkennungsdatum wird häufig anfänglich erfasst, wenn der schwerwiegende Security Incident zuerst erstellt oder vorgeschlagen wurde. Immer wenn dieses Datum geändert wird, wird die Uhrzeit automatisch berechnet, aktualisiert und im Format Tage: Stunden: Minuten angezeigt, z. B. 20T: 13H: 58M.<br><br>**Geschätztes Lösungsdatum**: Das Datum, bis zu dem das Incident-Lösungsdatum geschätzt wird. Dieses Datum wird häufig anfänglich erfasst, wenn der schwerwiegende Security Incident zuerst erstellt oder heraufgestuft wurde.<br><br>Das Datum wird basierend auf dem im angegebenen geschätzten Datum aktualisiert **Details** Registerkarte des Arbeitsbereichs.<br><br>Wenn das geschätzte Datum im Abschnitt „Details“ nicht angegeben ist, wird in diesem Abschnitt „Bindestrich“ ohne Datumswert angezeigt. |
| **Aktives Team** | Zeigt die verschiedenen Reaktionsteams und Teammitglieder aus jedem Team an, die aktiv an dem schwerwiegenden Security Incident und den zugehörigen Aufgaben arbeiten.<br><br>**Aktives Team** Trend: Zeigt das Trenddiagramm jedes Teams und seiner |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Übersichts-UI-Abschnitte (Fortsetzung)

| Titel | Beschreibung |
|---|---|
| | Teammitglieder an, die in regelmäßigen Abständen aktiv an dem schwerwiegenden Security Incident und zugehörigen Aufgaben arbeiten.<br><br>**Hinweis:**<br>Zeigen Sie die zugewiesenen aktiven Gruppen aus dem an **Details** Registerkarte des Arbeitsbereichs. |
| **Verknüpfte SIR-Incidents** | **Nach Incident-Status**: Zeigen Sie die Verteilung verknüpfter Security Incidents basierend auf einem Incident-Status an, z. B. „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“ oder „Überprüfen“.<br><br>**Trends nach Incident-Status**: Gibt in der Trendansicht weiter an, wie sich die Anzahl der verknüpften Incidents basierend auf dem Incident-Status entwickelt.<br><br>Wenn Sie die einzelnen Incident-Statuslinks auswählen, können Sie zu den verknüpften Security Incident-Details direkt im navigieren und sie anzeigen **Verknüpfter SI/VI** Registerkarte des Arbeitsbereichs.<br><br>Dieser Abschnitt wird automatisch aktualisiert, wenn Änderungen an den zugrunde liegenden Incidents auftreten. |
| **Antwortaufgaben** | Zeigt die aktiven Aufgaben an, die über SIR-Incidents mit dem MSI-Datensatz verknüpft sind.<br><br>• **Nach Aufgabenstatus**: Zeigen Sie die Incident-Antwortaufgaben basierend auf dem Incident-Status an, z. B. „Entwurf“, „Zugewiesen“, „In Bearbeitung“, „Abgeschlossen“. Dieses Verteilungsdiagramm ermöglicht eine weitere Verteilungsaufgliederung nach Zuweisungsgruppen. Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie eine gefilterte Liste nach Incident-Aufgabenstatus im anzeigen **Aufgaben** Registerkarte des Arbeitsbereichs. In der gefilterten Ansicht können Sie einzelne Aufgabendetails anzeigen und aktualisieren.<br><br>• **In Bearbeitung befindliche Aufgaben nach Incident-Statusbezeichnung**: Zeigt aktive Aufgaben und Gruppen basierend auf der Incident-Statusbezeichnung an, die in den Komponenten des Aufgabenorganisators |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Übersichts-UI-Abschnitte (Fortsetzung)**

| Titel | Beschreibung |
|---|---|
| | angewendet werden muss. Diese Standardbezeichnungen enthalten Werte wie „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“ oder „Überprüfen“, um die Art der betreffenden Aufgabe anzugeben.<br>• **Überfällig**: Zeigt die Security Incident Response-Aufgaben an, die aktiv sind und deren Fälligkeitsdatum überschritten wurden.<br><br>Sie können die Details aller überfälligen Aufgaben anzeigen, indem Sie die Gesamtanzahl der überfälligen Aufgaben auswählen und automatisch zur Registerkarte Aufgaben navigieren lassen.<br><br>• **Trends nach Aufgabenstatus**: Fortschrittstrend von in Bearbeitung befindlichen und geschlossenen Antwortaufgaben über die Incident-Dauer anzeigen.<br><br>**Hinweis:**<br>Das Trenddiagramm ruft die neuesten Daten basierend auf der geplanten Aufgabe ab. Sie können das Zeitintervall für den Datenabruf nach Bedarf konfigurieren oder ändern. |
| **MSI-Aufgaben** | Zeigt insgesamt aktive Aufgaben an, die direkt im MSI-Datensatz erstellt wurden (und dies sind keine verknüpften Antwortaufgaben):<br><br>**Nach Aufgabenstatus:** Zeigen Sie die erstellten Aufgaben des schwerwiegenden Security Incident, die zugewiesenen Aufgaben und die zugehörigen Informationen an.<br><br>Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie eine gefilterte Liste nach Incident-Aufgabenstatus im anzeigen **Aufgaben** Registerkarte des Arbeitsbereichs. In der gefilterten Ansicht können einzelne Aufgabendetails angezeigt und aktualisiert werden. |
| **Externe Zusammenarbeit** | Zeigt die Zusammenarbeitsaktivitäten für alle gekennzeichneten Zusammenarbeitsaktivitäten aus dem Aktivitätenstrom für Zusammenarbeit an: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Übersichts-UI-Abschnitte (Fortsetzung)**

| Titel | Beschreibung |
|---|---|
| | • **Nach Incident-Statusbezeichnung:**Zeigen Sie auf der Registerkarte „ **Zusammenarbeit** “ des Arbeitsbereichs die Daten zu Zusammenarbeitsaktivitäten bei Incidents an, die mit den Dateien und Ordnern Microsoft Teams und Microsoft SharePoint koordiniert und mit Incident-Statusbezeichnungen wie „Analyse“, „Eindämmen“, „Beseitigen“ oder „Wiederherstellen“ gekennzeichnet sind.<br>• **Trends nach Aktivitätstyp**: Zeigen Sie das Trenddiagramm für die Anzahl der Microsoft Teams - und Microsoft SharePoint -Datei- und -Ordneraktivitäten über die Incident-Dauer an. |

### Aktualisieren Sie die Details Major Security Incident .

Spezifische Details im Zusammenhang mit schwerwiegenden Security Incidents anzeigen und aktualisieren, z. B. Details zu Incident-Datensätzen, aktive Teamteilnehmer und das entsprechende Aktivitätsprotokoll.

Alle zugehörigen Details des schwerwiegenden Security Incident werden mit verschiedenen Formularabschnitten auf der Registerkarte „ **Details** “ des Arbeitsbereichs angezeigt. Zeigt Details wie Incident-Datensatzdetails, aktive Teamteilnehmer und das entsprechende Aktivitätsprotokoll an. Sie können auch die verknüpften SIR-Incidents, Datensatzdetails der Schwachstellengruppe und eine Möglichkeit anzeigen, eine Aktivitätsveröffentlichung an alle verknüpften Incident-Datensätze zu übertragen.

Die Registerkarte „Details“ enthält hauptsächlich:

1. Formularfelder für schwerwiegende Security Incidents und Incident-bezogene UI-Abschnitte.
2. Aktivitätenstrom

Die folgende Tabelle enthält die Details der Formularfelder für schwerwiegende Security Incidents:

**Formularabschnitte für schwerwiegenden Security Incident**

| Feld | Beschreibung |
|---|---|
| **Incident** | |
| Nummer | Nummer des schwerwiegenden Security Incidents |
| Primärer Status | Primärer Status des schwerwiegenden Security Incidents |
| Erkennungsdatum | Das Datum, an dem der schwerwiegende Security Incident zuerst erstellt oder vorgeschlagen wurde. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formularabschnitte für schwerwiegenden Security Incident (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | Wenn Sie das Erkennungsdatum auf der Registerkarte Details ändern, werden Datum und Uhrzeit der MSI automatisch berechnet, aktualisiert und im angezeigt **Zeit** > **Zeit seit Beginn des Incidents** Abschnitt „ **Übersicht** “ des Arbeitsbereichs. |
| Titel | Titel des schwerwiegenden Security Incidents |
| Quelle | Quelle des schwerwiegenden Security Incidents. |
| Kategorie | Kategorie des schwerwiegenden Security Incidents. |
| Unterkategorie | Unterkategorietyp des schwerwiegenden Security Incidents. |
| Geschätztes Lösungsdatum | Das Datum, bis zu dem die Auflösung des Incident-Lösungsdatums geschätzt wird. Das geschätzte Datum ist das Datum, an dem der schwerwiegende Security Incident zuerst erstellt oder heraufgestuft wurde. |
| Priorität | Gibt die Priorität des schwerwiegenden Security Incident an. |
| **Aktives Team** | |
| Incident-Manager | Name des Incident-Managers. |
| Zuweisungsgruppen | Gibt die verschiedenen Reaktionsteams und Teammitglieder jedes Teams an, die aktiv an dem schwerwiegenden Security Incident arbeiten. |
| **Kandidat** | |
| MSI-Kandidatenstatus | Gibt den Status des Kandidaten für schwerwiegenden Security Incident an, z. B. vorgeschlagen oder heraufgestuft. Wenn der Incident heraufgestuft wird, wird der Status als Akzeptiert angezeigt. |
| Hochgestuft durch | Benutzer, der den schwerwiegenden Security Incident heraufgestuft hat. |
| Hochgestuft | Datum, an dem der schwerwiegende Security Incident heraufgestuft wurde |
| Begründung | Begründung des schwerwiegenden Security Incidents. |
| Potenzieller Impact | Gibt die potenziellen Auswirkungen und den Schweregrad des schwerwiegenden Security Incident an. |
| **Beschränkung** | |
| Einschränkung erzwingen | Wählen Sie diese Option aus, um Einschränkungen für bestimmte schwerwiegende Security Incident-Einschränkungen durchzusetzen. Sie können Einschränkungen erzwingen, um den Anzeige- oder Änderungszugriff auf bestimmte Benutzer oder Gruppen zu beschränken. Weitere Informationen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formularabschnitte für schwerwiegenden Security Incident (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | finden Sie unter Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents |
| Zulässige Mitglieder | Liste der Benutzer, die auf den schwerwiegenden Security Incident zugreifen können. |
| Zulässige Gruppen | Liste der Gruppen, die auf den schwerwiegenden Security Incident zugreifen können |
| **Andere Aktionen** | |
| Anhang | Alle Anhänge im Zusammenhang mit dem schwerwiegenden Security Incident<br><br>**Wählen Sie** Option zum Hinzufügen von Anhängen zum Incident aus. |
| Telefonkonferenz | Verwenden Sie Telefonkonferenzen mit externen Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen und schwerwiegende Security Incidents zu beheben. Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Integration einer Telefonkonferenz |

**Aktivität**:

Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügte Aktivität oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

**Hinweis:**
Klicken Sie auf den Link **Weitere** Details anzeigen, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, die diesem schwerwiegenden Security Incident zugeordnet sind.

Legen Sie Ihre Einstellungen fest, um die zugehörigen Aktivitäten anzuzeigen, z. B.:

1. **Filter**: Klicken Sie auf das Symbol **„Filtersätze** “, um Filter festzulegen.

   Legen Sie Filter fest, um die Aktivitätskonversationen anzuzeigen, z. B. Aktivitäten, die in den Arbeitsnotizen, E-Mails, der Zeitleiste und zusätzlichen Kommentaren hinzugefügt wurden.

2. **Gekennzeichnet**: Klicken Sie auf das Symbol **„Gekennzeichnet“**, um die Aktivitäten zu kennzeichnen.

   Markieren Sie alle wichtigen Aktivitätskonversationen, damit Sie sie bei Bedarf schnell erneut aufrufen können.

### Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents

Legen Sie fest, wer schwerwiegende Security Incidents anzeigen oder ändern kann, die vertrauliche Informationen enthalten. Sie können Einschränkungen für schwerwiegende Security Incidents erzwingen, um zu bestimmen, wer Zugriff auf die Anzeige oder Änderung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bestimmter Datensätze schwerwiegender Security Incidents und zugehöriger Listen hat, und den Lese- oder Schreibzugriff auf bestimmte Benutzer oder Gruppen beschränken.

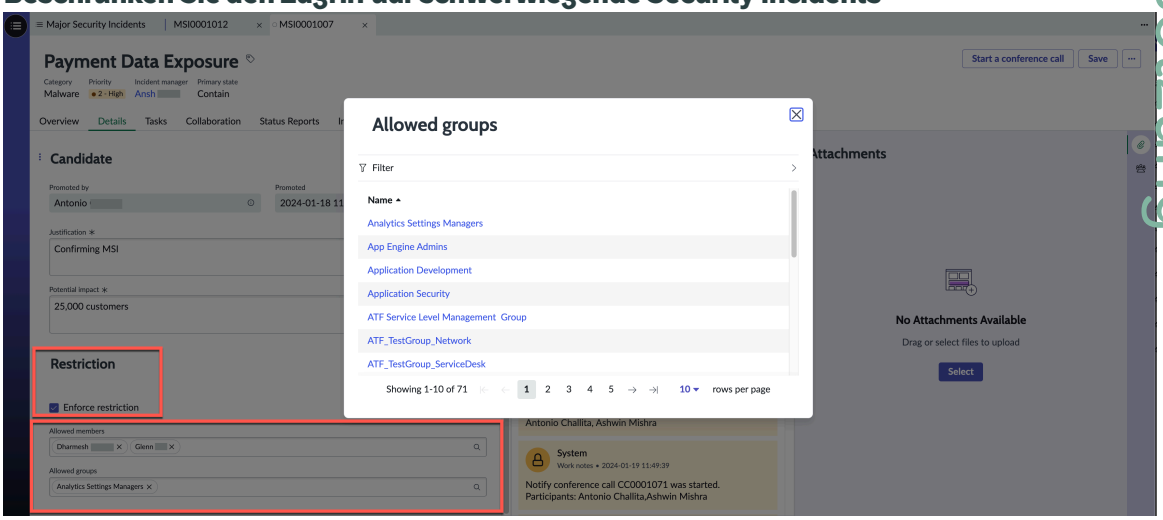
### Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

### Warum und wann dieser Vorgang ausgeführt wird
Mit Einschränkungen für schwerwiegende Security Incidents können Sie verhindern, dass alle Benutzer oder Gruppen in einer bestimmten Organisation auf kritische schwerwiegende Security Incidents zugreifen oder diese ändern. Mit diesen Einschränkungen können Sie die schwerwiegenden Security Incidents, die ein Benutzer oder eine Gruppe anzeigen oder ändern kann, granularer steuern. Sie können eine Einschränkung für schwerwiegende Security Incidents erzwingen, indem Sie das **Kontrollkästchen Einschränkung** erzwingen aktivieren und die Benutzer oder Gruppen auswählen, die den jeweiligen schwerwiegenden Security Incident anzeigen oder ändern dürfen.

Nachdem Sie die Beschränkung für schwerwiegende Security Incidents oder zugehörige Listen für bestimmte Benutzer oder Gruppen erzwungen haben, können alle verbleibenden Benutzer oder Gruppen in Ihrer Organisation diese schwerwiegenden Security Incidents oder zugehörigen Listen nicht mehr anzeigen oder ändern.

### Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Details** aus.
5. Scrollen Sie nach unten, und wählen Sie den Abschnitt **Einschränkung** aus.
6. Aktivieren Sie das **Kontrollkästchen Einschränkung erzwingen**, um die Einschränkung des schwerwiegenden Security Incident zu aktivieren.

**Beschränken Sie den Zugriff auf schwerwiegende Security Incidents**




7. Wählen Sie im Feld Zulässige Mitglieder die Benutzer aus, die den schwerwiegenden Security Incident mit der Suchoption anzeigen oder ändern können.
8. Wählen Sie im Feld Zulässige Gruppen die Gruppen aus, die den schwerwiegenden Security Incident mithilfe der Suchoption anzeigen oder ändern können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Nachdem das **Kontrollkästchen Einschränkung erzwingen** für den schwerwiegenden Security Incident aktiviert wurde, haben nur sn_msi.workspace_manager und zulässige Mitglieder oder Gruppen Zugriff, um den schwerwiegenden Security Incident anzuzeigen oder zu ändern.

9. Wählen Sie **Speichern**.

### Verknüpfen Sie zusätzliche Datensätze mit Major Security Incident

Verwenden Sie im Arbeitsbereich die Funktion zum Verknüpfen von Datensätzen, um zugehörige Security Incident-Datensätze und deren untergeordnete Security Incidents, Korrekturaufgaben aus Vulnerability Response und Sicherheitsfälle aus Threat Intelligence mit einem Major Security Incident (MSI)-Datensatz zu verknüpfen.

#### Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager und sn_msi.workspace_responder

#### Prozedur

1. Navigieren zu **Reaktion auf schwerwiegende Security Incidents** > **MSIM-Arbeitsbereich**.
2. Navigieren Sie zur **Listenansicht**, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie auf **Akzeptiert**, um die heraufgestuften Datensätze zu schwerwiegenden Security Incidents auszuwählen.
4. Wählen Sie aus der Liste der heraufgestuften Datensätze den Incident-Datensatz aus, der verknüpft werden muss und sich nicht im Status „Geschlossen“ befindet.
5. Klicken Sie auf die Registerkarte **Verknüpfte Datensätze**.
   Eine Dropdown-Liste wird bereitgestellt, um andere verknüpfte Datensatztabellen auszuwählen.
   Im Abschnitt „Verknüpfte Datensätze“ werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft wurden.
6. Wählen Sie in der Liste die gewünschte Tabellenansicht aus, z. B. „Security Incidents“, „Korrekturaufgaben“ (angreifbare Elemente) oder „Sicherheitsfall“.
   Basierend auf der Datensatztabellenansicht Ihres Auswahltyps werden die verknüpften Datensätze angezeigt, die mit den Datensätzen zu schwerwiegenden Security Incidents verknüpft sind.
7. Verknüpfen Sie einen Datensatz, der nicht mit einem MSI-Datensatz verknüpft ist und sich im Status „ **Offen** “ befindet, indem Sie den Datensatz auswählen und oben rechts auf der Seite auf **Datensatz** verknüpfen klicken.

   **Hinweis:**
   Sie können einen Incident-Datensatz nicht mit einem MSI-Datensatz verknüpfen, wenn er sich im Status „ **Geschlossen** “ befindet.

8. Wählen Sie den zu verknüpfenden Datensatz aus, und **klicken**Sie auf Verknüpfen.
   Eine Bestätigungsmeldung zeigt an, dass der Datensatz erfolgreich verknüpft wurde und der Rollup der zugehörigen Datensätze im Hintergrund verarbeitet wird.

   **Hinweis:**
   Nachdem ein Datensatz verknüpft wurde, wird die Listenansicht automatisch aktualisiert und listet die aktualisierte Liste der Incident-Datensätze auf.

#### Zugehörige Informationen

Heben Sie die Verknüpfung von Datensätzen mit auf Major Security Incident



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Heben Sie die Verknüpfung von Datensätzen mit auf Major Security Incident

Heben Sie im Arbeitsbereich „Major Security Incident Management“ die Verknüpfung der Datensätze zu schwerwiegenden Security Incidents mit dem Abschnitt „Verknüpfte Datensätze“ auf.

## Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager und sn_msi.workspace_responder

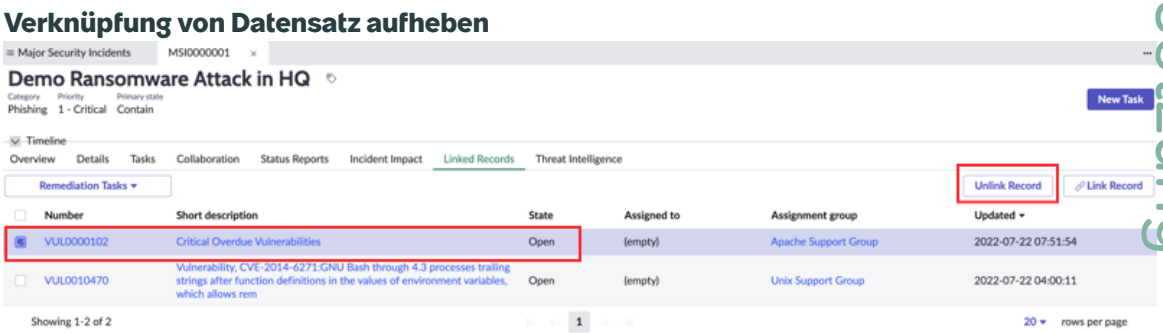
**Hinweis:**

Sie können die Verknüpfung nur für einen einzelnen Datensatz aufheben. Nachdem Sie die Verknüpfung mit einem Datensatz aufgehoben haben, werden die zugehörigen Rollup-Informationen aus den Abschnitten „Incident-Auswirkung“ und „Threat Intelligence“ im Arbeitsbereich entfernt, und die Aktion kann nicht rückgängig gemacht werden.

Weitere Informationen zu Rollup-Datensätzen finden Sie unter Rollup-Framework für MSIM.

## Prozedur

1. Navigieren zu **Reaktion auf schwerwiegende Security Incidents** > **MSIM-Arbeitsbereich**.
2. Navigieren Sie zur **Listenansicht**, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie auf **Akzeptiert**, um die heraufgestuften Datensätze zu schwerwiegenden Security Incidents auszuwählen.
4. Klicken Sie auf die Registerkarte **Verknüpfte Datensätze**.
   In diesem Abschnitt werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft sind.
5. Wählen Sie die gewünschte Tabellenansicht aus, z. B. Security Incidents, Korrekturaufgaben (angreifbare Elemente) oder Sicherheitsfall.
6. Wählen Sie den Datensatz aus, dessen Verknüpfung Sie aufheben möchten, in der Listenansicht der Datensätze.
7. Klicken Sie **auf Verknüpfung aufheben**.

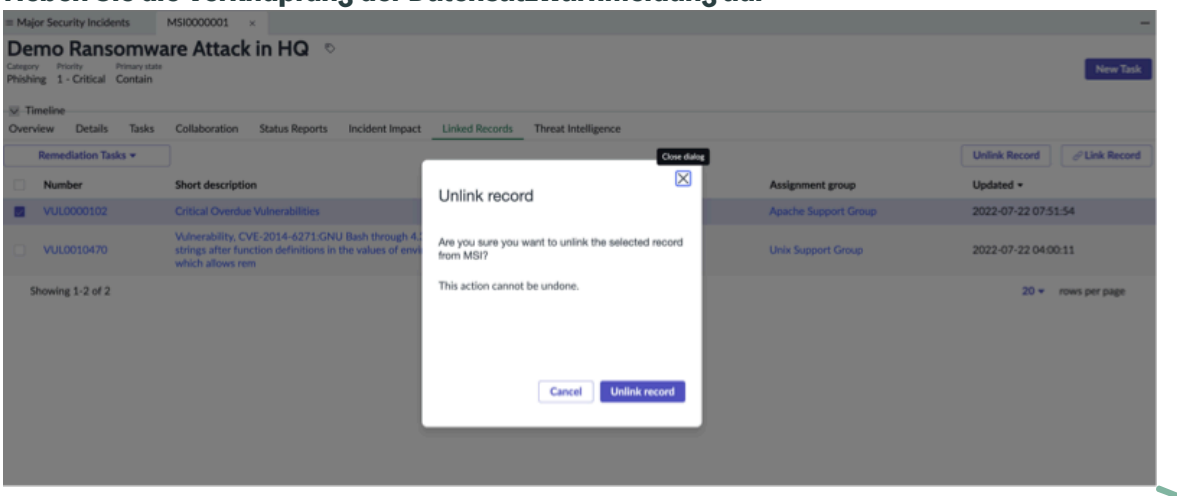



8. Eine Warnmeldung wird angezeigt, in der Sie gefragt werden, ob Sie die Verknüpfung des ausgewählten Datensatzes mit MSI aufheben möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Heben Sie die Verknüpfung der Datensatzwarnmeldung auf




9. Klicken Sie **auf Verknüpfung aufheben**.
   Die Verknüpfung des Datensatzes wird aufgehoben, und sobald die Verknüpfung aufgehoben ist, können die Änderungen nicht rückgängig gemacht werden. Die Listenansicht der verknüpften Datensätze wird nach dem Aufheben der Verknüpfung aktualisiert.

**Zugehörige Informationen**

Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents

## Verwalten Sie Aufgaben in einem Major Security Incident

Auf der Registerkarte Aufgabe können Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, im MSIM-Arbeitsbereich nachverfolgen und verwalten. Sie können die verschiedenen Aufgaben mit dem standardmäßigen Visual Task Board (Kanban-Ansicht) oder der Listenansicht anzeigen.

sn_msi.workspace_manager kann auf der Registerkarte Aufgaben:

- Eine Aufgabe erstellen
- Aufgaben ändern
- Aufgaben anzeigen und sich selbst oder anderen zuweisen
- Löschen Sie Aufgaben

**Hinweis:**
Stellen Sie sicher, dass Sie die App **„MSIM VTB Task Card: 1.0.1v“** nach der Installation der MSIM-App separat installiert haben.

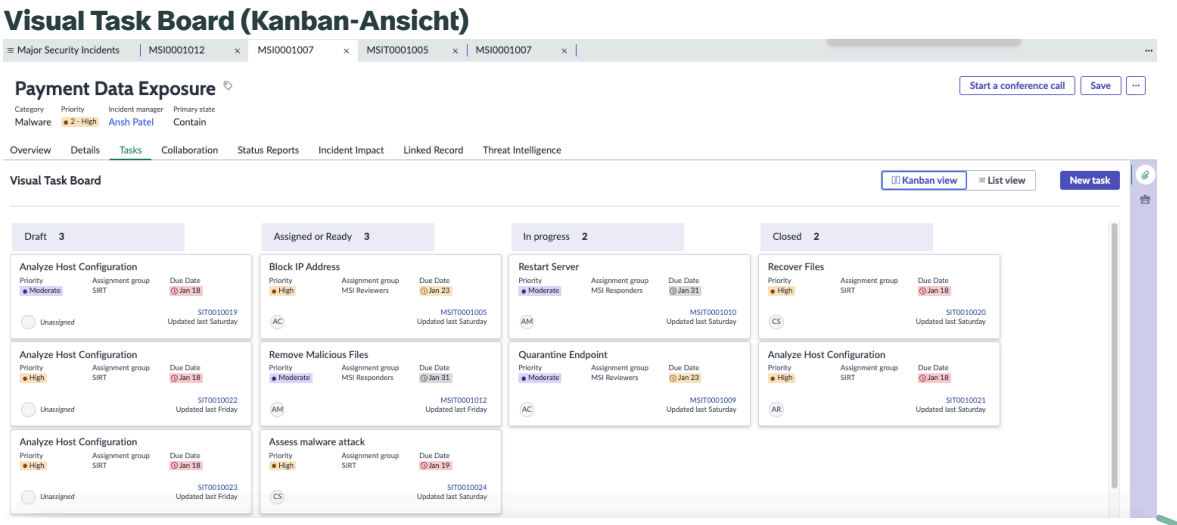
Auf der Registerkarte Aufgaben werden die Details aller Aufgaben angezeigt, die einem schwerwiegenden Security Incident zugeordnet sind. Die Registerkarte Aufgabe unterstützt zwei Ansichten:

- **Visual Task Board (Kanban-Ansicht)**:

  Zeigen Sie mehrere Aufgabendatensätze an, und aktualisieren Sie sie, die als Karten auf dem Visual Task Board angezeigt werden, die basierend auf dem Status der Aufgaben im schwerwiegenden Security Incident zwischen Spuren verschoben werden können.

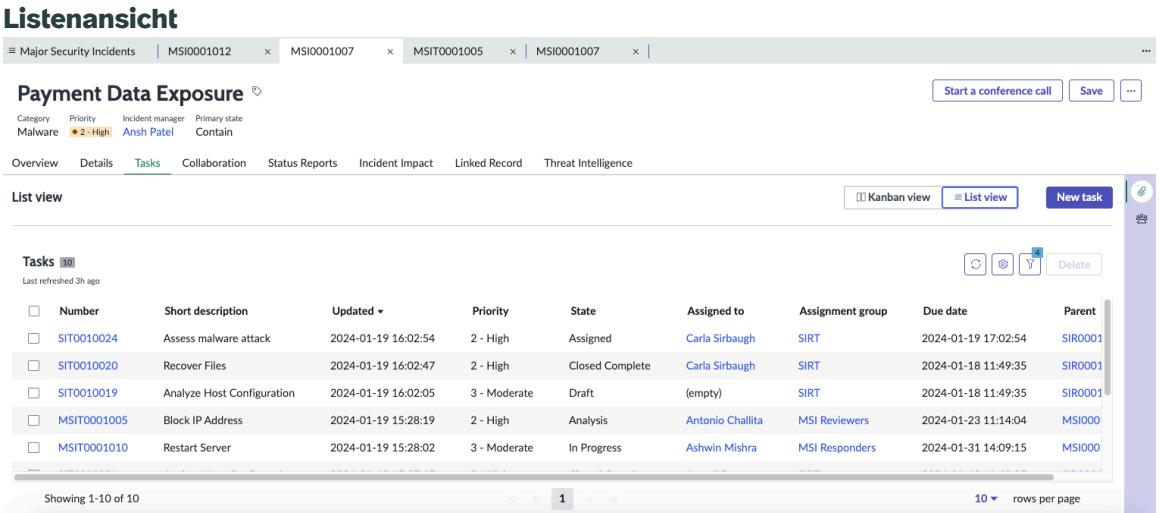
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- **Listenansicht**:

  Zeigen Sie mehrere Aufgabendatensätze mit in Form von Listen an, und aktualisieren Sie sie. Mit diesen Listenkategorien und Filtern können Sie die Aufgaben, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen, schnell finden und nachverfolgen.




Die gekennzeichneten Aktivitäten werden zusammengefasst und im Abschnitt „Übersicht“ des schwerwiegenden Security Incident angezeigt. Im Abschnitt „Übersicht“ ist ein Trenddiagramm verfügbar, um den Status der konsolidierten Aufgabenaktivitäten anzuzeigen.

### Verwalten Sie Aufgaben mit Visual Task Board

Verfolgen und verwalten Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, mithilfe des visuellen Taskboards (Kanban-Ansicht).

Sie können das visuelle Taskboard verwenden, um die Karten je nach Status der Aufgaben Schritt für Schritt zwischen Spuren wie „Entwurf“, „Zugewiesen“ oder „Bereit“, „In Bearbeitung“ und „Geschlossen“ zu verschieben. Ein Aktivitätenstrom auf der Tafel zeigt die letzten Aktivitäten an, um Aufgabenänderungen einfach nachzuverfolgen. Sie können Aufgabenkarten aus jeder Tabelle hinzufügen, die Aufgabe erweitert, um Updates



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schnell nachzuverfolgen und schwerwiegende Security Incidents direkt über die Tafel zu bearbeiten.

## Erstellen Sie eine Aufgabe mit Visual Task Board

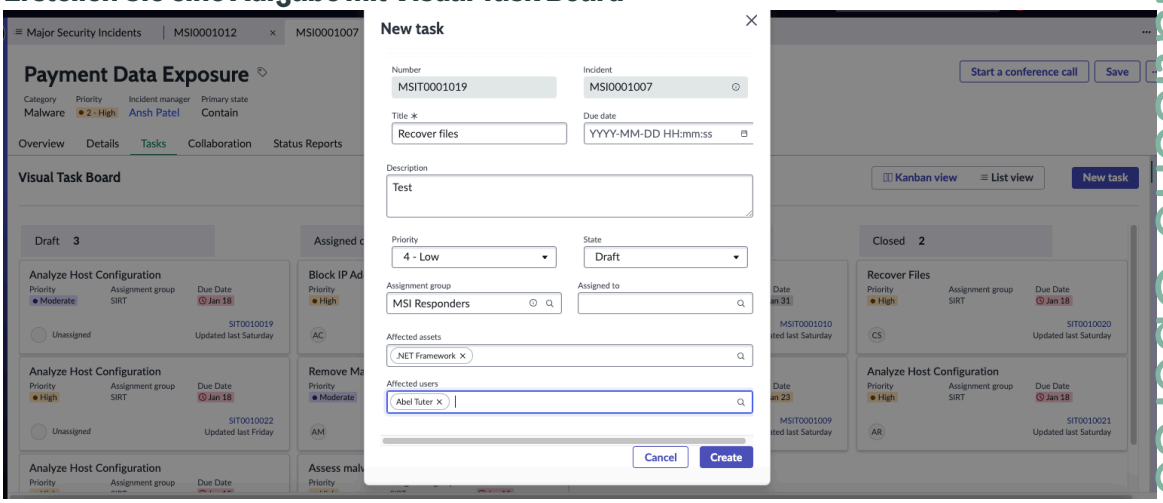
Erforderliche Rolle: sn_msi.workspace_manager.

**Hinweis:**
Stellen Sie sicher, dass Sie die App **„MSIM VTB Task Card: 1.0.1v“** nach der Installation der MSIM-App separat installiert haben.

MSI-Manager können eine Aufgabe im Visual Task Board mit den folgenden Schritten erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wechseln Sie zur Registerkarte **Aufgaben**.

**Erstellen Sie eine Aufgabe mit Visual Task Board**




5. Wählen Sie die **Kanban-Ansicht**und dann **Neue Aufgabe**aus.
6. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden. |
| Incident | Nummer des schwerwiegenden Security Incidents Dieses Feld kann nicht bearbeitet werden. |
| Titel | Geben Sie einen Namen für die Aufgabe an. |
| Fälligkeitsdatum | Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie ein Datum mit der Option **Kalender** aus, und geben Sie die Uhrzeit im Abschnitt **Zeit** auswählen an. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beschreibung | Geben Sie eine eindeutige Beschreibung für die Aufgabe an. |
| Priorität | Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein:<br>○ **Keine**<br>○ **1 – kritisch**<br>○ **2 - Hoch**<br>○ **3 – Mittel**<br>○ **4 – Niedrig**<br>○ **5: Planung** |
| Status | Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein:<br>○ **Entwurf**<br>○ **Analyse**<br>○ **In Bearbeitung**<br>○ **Geschlossen**<br>Der Standardstatus ist **Entwurf**. |
| Zuweisungsgruppe | Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen. |
| Zugewiesen an | Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll. |
| Betroffene Assets | Wählen Sie mithilfe der Suchoption die betroffenen Assets nach der Aufgabe aus. |
| Betroffene Benutzer | Wählen Sie mithilfe der Suchoption die betroffenen Benutzer nach Aufgabe aus. |

7. Wählen **Sie Erstellen** aus, um die Aufgabe zu erstellen.

## Zeigen Sie eine Aufgabe mit Visual Task Board an und ändern Sie sie

Erforderliche Rolle: sn_msi.workspace_manager.

**Hinweis:**
Stellen Sie sicher, dass Sie die App **„MSIM VTB Task Card: 1.0.1v“** nach der Installation der MSIM-App separat installiert haben.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen von den MSI-Respondern anzeigen und eine Aufgabe im visuellen Taskboard mit den folgenden Schritten ändern:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wechseln Sie zur Registerkarte **Aufgaben** und wählen Sie die **Kanban-Ansicht aus**.
5. Wählen Sie die gewünschte Aufgabenkarte in einer der Spuren aus, um die Details der Aufgabe anzuzeigen.

   Die Aufgabenkarte kann sich in einer der folgenden Spuren befinden: „Entwurf“, „Zugewiesen“ oder „Bereit“, „In Bearbeitung“ oder „Geschlossen“.
6. Im Abschnitt „Aufgabeninformationen“ können Sie die folgenden Details ändern:

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden. |
| Incident | Nummer des schwerwiegenden Security Incidents Dieses Feld kann nicht bearbeitet werden. |
| Titel | Geben Sie einen Namen für die Aufgabe an. |
| Fälligkeitsdatum | Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie ein Datum mit der Option **Kalender** aus, und geben Sie die Uhrzeit im Abschnitt **Zeit** auswählen an. |
| Beschreibung | Geben Sie eine eindeutige Beschreibung für die Aufgabe an. |
| Priorität | Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein:<br>○ **Keine**<br>○ **1 – kritisch**<br>○ **2 - Hoch**<br>○ **3 – Mittel**<br>○ **4 – Niedrig**<br>○ **5: Planung** |
| Status | Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein:<br>○ **Entwurf**<br>○ **Analyse**<br>○ **In Bearbeitung**<br>○ **Geschlossen**<br>Der Standardstatus ist **Entwurf**. |
| Zuweisungsgruppe | Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen. |
| Zugewiesen an | Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll. |
| Betroffene Assets | Wählen Sie mithilfe der Suchoption die betroffenen Assets nach der Aufgabe aus. |



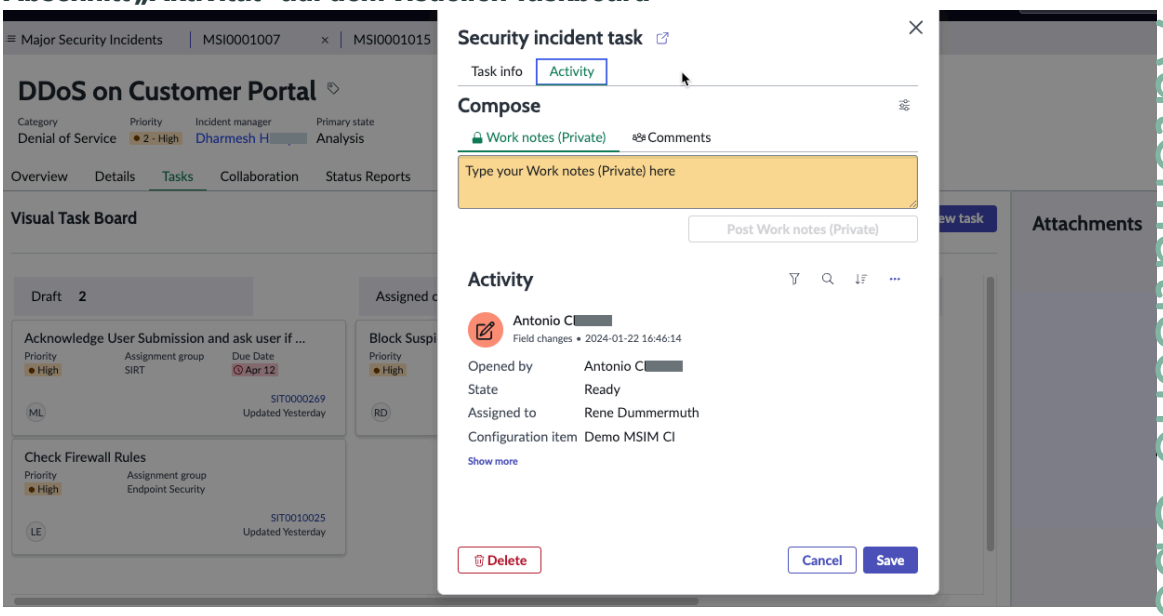
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Betroffene Benutzer | Wählen Sie mithilfe der Suchoption die betroffenen Benutzer nach Aufgabe aus. |

7. Wählen Sie den Abschnitt „ **Aktivität** “ aus, um die Aktivitätsdetails aus den MSI-Respondern anzuzeigen.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügte Aktivität oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

**Abschnitt „Aktivität“ auf dem visuellen Taskboard**




**Hinweis:**
Klicken Sie auf den Link **Weitere** Details anzeigen, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

8. Wählen **Sie Speichern** aus, um die Aufgabeninformationen zu aktualisieren.

   Die Aufgabeninformationen werden sofort aktualisiert.

## Löschen Sie eine Aufgabe mit Visual Task Board

Erforderliche Rolle: sn_msi.workspace_manager.

**Hinweis:**
Stellen Sie sicher, dass Sie die App **„MSIM VTB Task Card: 1.0.1v“** nach der Installation der MSIM-App separat installiert haben.

MSI-Manager können Aufgaben im visuellen Taskboard mit den folgenden Schritten löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wechseln Sie zur Registerkarte **Aufgaben** und wählen Sie die **Kanban-Ansicht aus**
5. Wählen Sie die Aufgabenkarte aus, die Sie löschen möchten.
6. Wählen Sie im Popup-Fenster „Aufgabe für schwerwiegenden Security Incident“ die Option **Löschen** aus.

   Das Popup-Fenster Aufgabe löschen wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.
7. Wählen Sie **Löschen**.

### Verwalten Sie Aufgaben in der Listenansicht

Verfolgen und verwalten Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, in der Listenansicht.

Die Listenansicht zeigt die Details aller Aufgaben an, die dem schwerwiegenden Security Incident zugeordnet sind, z. B. Aufgabennummer, Priorität, aktueller Status, Zugewiesen an, Zugewiesene Gruppe. Mit diesen Listenkategorien und Filtern können Sie die erforderlichen Aufgaben, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen, schnell finden und nachverfolgen.

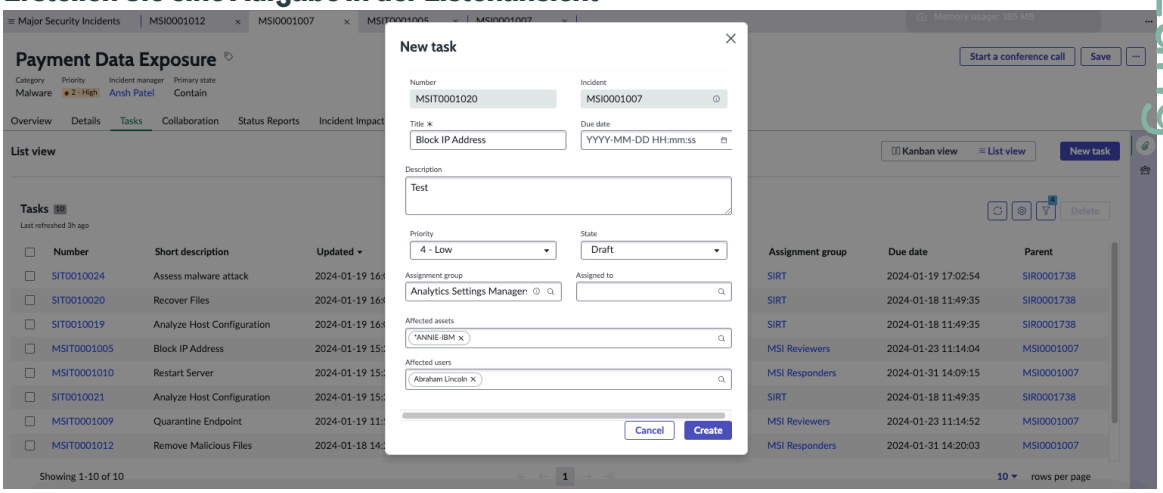
## Erstellen Sie eine Aufgabe in der Listenansicht

Erforderliche Rolle: sn_msi.workspace_manager.

MSI-Manager können mit den folgenden Schritten eine Aufgabe in der Listenansicht erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wechseln Sie zur Registerkarte **Aufgaben**.

### Erstellen Sie eine Aufgabe in der Listenansicht




5. Wählen Sie **Listenansicht**und dann **Neue Aufgabe**aus.
6. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden. |
| Incident | Nummer des schwerwiegenden Security Incidents Dieses Feld kann nicht bearbeitet werden. |
| Titel | Geben Sie einen Namen für die Aufgabe an. |
| Fälligkeitsdatum | Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie ein Datum mit der Option **Kalender** aus, und geben Sie die Uhrzeit im Abschnitt **Zeit** auswählen an. |
| Beschreibung | Geben Sie eine eindeutige Beschreibung für die Aufgabe an. |
| Priorität | Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein:<br>○ **Keine**<br>○ **1 – kritisch**<br>○ **2 - Hoch**<br>○ **3 – Mittel**<br>○ **4 – Niedrig**<br>○ **5: Planung** |
| Status | Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein:<br>○ **Entwurf**<br>○ **Analyse**<br>○ **In Bearbeitung**<br>○ **Geschlossen**<br>Der Standardstatus ist **Entwurf**. |
| Zuweisungsgruppe | Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen. |
| Zugewiesen an | Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll. |
| Betroffene Assets | Wählen Sie mithilfe der Suchoption die betroffenen Assets nach der Aufgabe aus. |
| Betroffene Benutzer | Wählen Sie mithilfe der Suchoption die betroffenen Benutzer nach Aufgabe aus. |



7. Wählen **Sie Erstellen** aus, um die Aufgabe zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zeigen Sie eine Aufgabe in der Listenansicht an, und ändern Sie sie

Erforderliche Rolle: sn_msi.workspace_manager.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen aus den MSI-Respondern anzeigen und eine Aufgabe in der Listenansicht mit den folgenden Schritten ändern

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wechseln Sie zur Registerkarte **Aufgaben** und wählen Sie **Listenansicht aus**.
5. Wählen Sie die gewünschte Aufgabe in der Listenansicht aus, um die Details der Aufgabe anzuzeigen.
6. Im Abschnitt „Aufgabeninformationen“ können Sie die folgenden Details ändern:

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Nummer, die automatisch für die ausgewählte Aufgabe generiert wird. Dieses Feld kann nicht bearbeitet werden. |
| Incident | Nummer des schwerwiegenden Security Incidents Dieses Feld kann nicht bearbeitet werden. |
| Titel | Geben Sie einen Namen für die Aufgabe an. |
| Fälligkeitsdatum | Wählen Sie ein Fälligkeitsdatum und eine Uhrzeit für den Abschluss der Aufgabe aus. Wählen Sie ein Datum mit der Option **Kalender** aus, und geben Sie die Uhrzeit im Abschnitt **Zeit** auswählen an. |
| Beschreibung | Geben Sie eine eindeutige Beschreibung für die Aufgabe an. |
| Priorität | Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einer der folgenden Werte sein:<br>○ **Keine**<br>○ **1 – kritisch**<br>○ **2 - Hoch**<br>○ **3 – Mittel**<br>○ **4 – Niedrig**<br>○ **5: Planung** |
| Status | Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein:<br>○ **Entwurf**<br>○ **Analyse**<br>○ **In Bearbeitung**<br>○ **Geschlossen** |



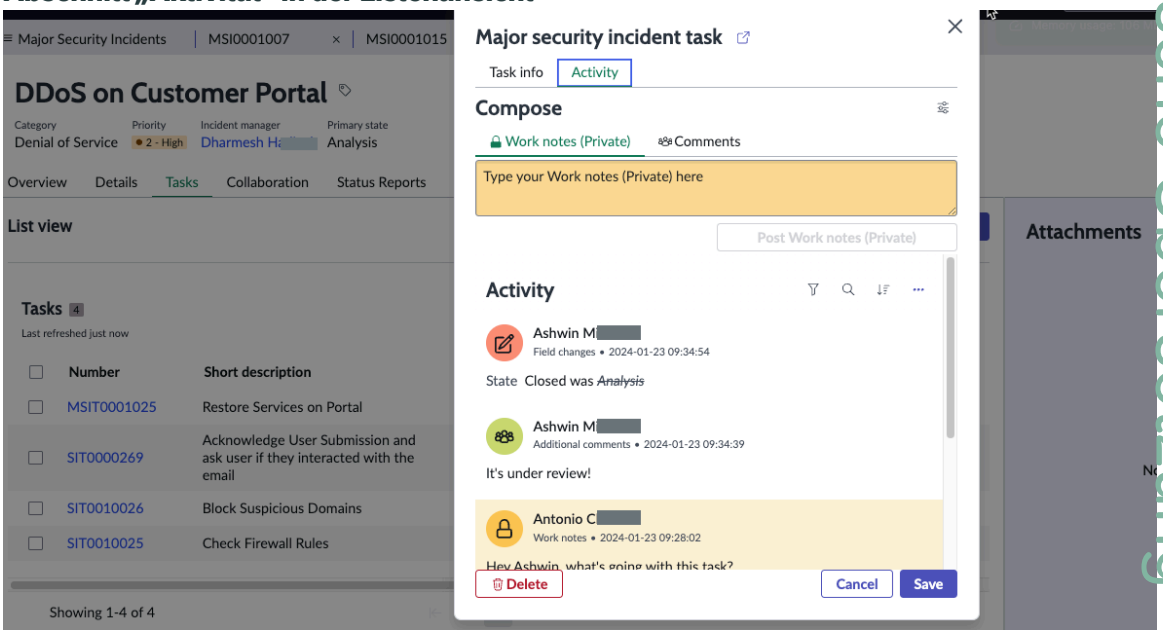
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Der Standardstatus ist **Entwurf**. |
| Zuweisungsgruppe | Wählen Sie mithilfe der Suchoption eine Zuweisungsgruppe des Benutzers aus, um die Aufgabe zuzuweisen. |
| Zugewiesen an | Wählen Sie mithilfe der Suchoption den Benutzer aus, dem die Aufgabe zugewiesen werden soll. |
| Betroffene Assets | Wählen Sie mithilfe der Suchoption die betroffenen Assets nach der Aufgabe aus. |
| Betroffene Benutzer | Wählen Sie mithilfe der Suchoption die betroffenen Benutzer nach Aufgabe aus. |

7. Wählen Sie den Abschnitt „ **Aktivität** “ aus, um die Aktivitätsdetails aus den MSI-Respondern anzuzeigen.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und bei Bedarf zusätzliche Kommentare im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügte Aktivität oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

**Abschnitt „Aktivität“ in der Listenansicht**




**Hinweis:**
Klicken Sie auf den Link **Weitere** Details anzeigen, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

8. Wählen **Sie Speichern** aus, um die Aufgabeninformationen zu aktualisieren.

   Die Aufgabeninformationen werden sofort aktualisiert.

9. In der Listenansicht können Sie auch die folgenden Aktionen ausführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. **Klicken** Sie auf das Symbol Aktualisieren, um die Liste der Aufgaben in der Listenansicht zu aktualisieren.

b. Klicken Sie auf das Symbol **Einstellungen**, und verwenden Sie die Option **Spalten bearbeiten**, um die Liste der Spalten zu ändern, die in der Listenansicht angezeigt werden. Verwenden Sie die Option **Breiten** zurücksetzen, um die Breiten der Spalten zurückzusetzen.

### Löschen Sie eine Aufgabe in der Listenansicht

Erforderliche Rolle: sn_msi.workspace_manager.

MSI-Manager können Aufgaben in der Listenansicht wie folgt löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wechseln Sie zur Registerkarte **Aufgaben**.
5. Wählen Sie **Listenansicht aus**.
6. Wählen Sie eine Aufgabe, die Sie löschen möchten, aus der Liste aus.
7. Wählen Sie im Popup-Fenster „Aufgabe für schwerwiegenden Security Incident“ die Option **Löschen** aus.

   Das Popup-Fenster Aufgabe löschen wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.
8. Wählen Sie **Löschen**.

#### Verfolgen Sie die Zusammenarbeitsaktivität über den Arbeitsbereich MSIM .

Verfolgen Sie Chat- und Dateiaktivitäten im Zusammenhang mit der Lösung schwerwiegender Security Incidents über den MSIM-Arbeitsbereich nach.

Aktivitäten werden mithilfe von Chat- und Microsoft TeamsMicrosoft SharePoint -Dateien und -Ordnern koordiniert und dann über Integrationen an Major Security Incident zurückgesendet.

Sobald Microsoft Teams und Microsoft SharePoint in Management schwerwiegender Sicherheits-Incidentsintegriert sind, können Sie den Arbeitsbereich MSIM verwenden, um die Zusammenarbeit zwischen Benutzern der Reaktion auf Incidents und anderen Gruppen, die zur Lösung eines schwerwiegenden Security Incidents beitragen, nachzuverfolgen. Alle Aktualisierungen an Zusammenarbeitsordnern und -dateien in Microsoft SharePoint werden mit dem MSIM -Arbeitsbereich File Explorer synchronisiert und auch in den Komponenten des Aktivitätenstroms angezeigt.

Wenn ein Security Incident zu einem schwerwiegenden Security Incident heraufgestuft wird:

1. Eine Ordnerstruktur wird in Microsoft SharePoint basierend auf der Ordnervorlagenkonfiguration erstellt. Dieselbe Ordnerstruktur wird in der Komponente File Explorer des Arbeitsbereichs angezeigt.
2. Ein Team mit mehreren Kanälen wird unter der Anwendung Microsoft Teams erstellt und in der Chat-Management-Komponente des Arbeitsbereichs angezeigt.

Erforderliche Rolle: sn_msi.workspace_manager.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Interagieren Sie mit Dateien und Ordnern

Der Dateiexplorer zeigt das Dateisystem an, sodass Sie Dateien und Ordner im Zusammenhang mit der Lösung des Incident anzeigen und mit ihnen interagieren können.

Zeigt die Datei und die Ordner an, die in Microsoft SharePoint für einen bestimmten Security Incident erfasst werden. Diese Ordner werden automatisch in Microsoft SharePoint für diesen schwerwiegenden Security Incident erstellt. Sie können diese standardmäßig erstellten Ordner bei Bedarf zum Hochladen von unterstützenden Dateien verwenden. Sie können diese Dateien und Ordner nach Bedarf umbenennen, verschieben oder löschen.

Außerdem wird jedes Mal, wenn Sie eine Datei in einen der Ordner hochladen, die Aktivität, die diesen Ordnern entspricht, automatisch den Datei-Explorer-Ordnern auf der Registerkarte „Zusammenarbeit“ zugeordnet, und die Aktivität wird aufgezeichnet und im Abschnitt „Aktivität“ des Major Security Incident Management angezeigt Arbeitsbereich

**Hinweis:**
Auf der Registerkarte **Zusammenarbeit** wird der Incident-Datensatz mit einer eindeutigen Incident-Nummer und Incident-Kategorie an die übergeordnete Datei im SharePoint angehängt.

1. **Repository-Ansicht**: Listet die Dateien und Ordner auf, die in Microsoft SharePoint für diesen bestimmten Security Incident aufgeführt sind. Für jede Datei oder jeden Ordner werden in der Repository-Ansicht Name, Geändert von, Zuletzt geändert und Größe angezeigt.

**Ansicht „Repository“.**

| Feld | Beschreibung |
|---|---|
| In SharePoint öffnen | Wählen Sie diese Option aus, die neben Ihrem schwerwiegenden Security Incident verfügbar ist. Klicken Sie auf den Link, um die Ordnerstruktur in Microsoft SharePoint auszuwählen und anzuzeigen. |
| Neuer Ordner | Wählen Sie diese Option aus, um nach Bedarf einen neuen Ordner zu erstellen. Nachdem Sie einen neuen Ordner erstellt haben, wird standardmäßig derselbe neue Ordner erstellt und in Ihrem Microsoft SharePoint zugeordnet. |

2. **Letzte**: Zeigt alle aktuellen Aktivitätsprotokolle an. Diese Protokolle enthalten sowohl Ihre SharePoint- als auch Ihre Datei-Explorer-Aktivitäten. Die letzten Aktivitäten sind normalerweise Ihre unterstützenden Dateien, die den übergeordneten Ordner enthalten.

   Im Folgenden finden Sie das Verfahren zum **Suchen der Protokolldatei:**

   **a.** Wählen Sie die entsprechende Datei aus, um die Details anzuzeigen.

   **b.** Klicken Sie **auf Datei suchen**.

**Hinweis:**
Die Navigation und die Details der übergeordneten Datei und der übergeordneten Ordner werden im Abschnitt **„Letzte Listenansicht** “ angezeigt. Sie können dieselbe Datei in Ihrem SharePoint öffnen. Immer wenn Sie die zugehörigen Protokolldateien oder Aktivitäten hochladen, werden alle diese Dateien und Aktivitäten sowohl in SharePoint als auch im Datei-Explorer angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwaltet Kommunikation über Chatkanäle

Der Chat-Channel-Manager zeigt die Microsoft Teams mit mehreren Kanälen an, die in der Microsoft Teams-Anwendung basierend auf einer Konfigurationsvorlage erstellt wurden.

Diese konfigurierten Kanäle werden zusammen mit den ihnen zugewiesenen Benutzern und Benutzergruppen in der Chat-Management-Komponente angezeigt. Sie können auch neue Kanäle erstellen. Gemäß der Konfiguration der Kanalvorlagen werden das Team und die Kanäle in Microsoft Teams erstellt.

#### Erstellen Sie neue Chatkanäle

1. Navigieren zu **Chatkanalmanager** > **Neuen Kanal erstellen** auf der Registerkarte Zusammenarbeit.
2. Fügen Sie einen neuen **Kanalnamen**und eine **Beschreibung hinzu**, und wählen Sie die **Mitglieder** des Kanals aus.
3. Klicken Sie auf **Erstellen**.

**Hinweis:**
Im Abschnitt „MS Teams-Kanäle“ der MS Teams-Anwendung wird ein neuer Kanaldatensatz erstellt, und derselbe Datensatz wird in MSIM angezeigt.

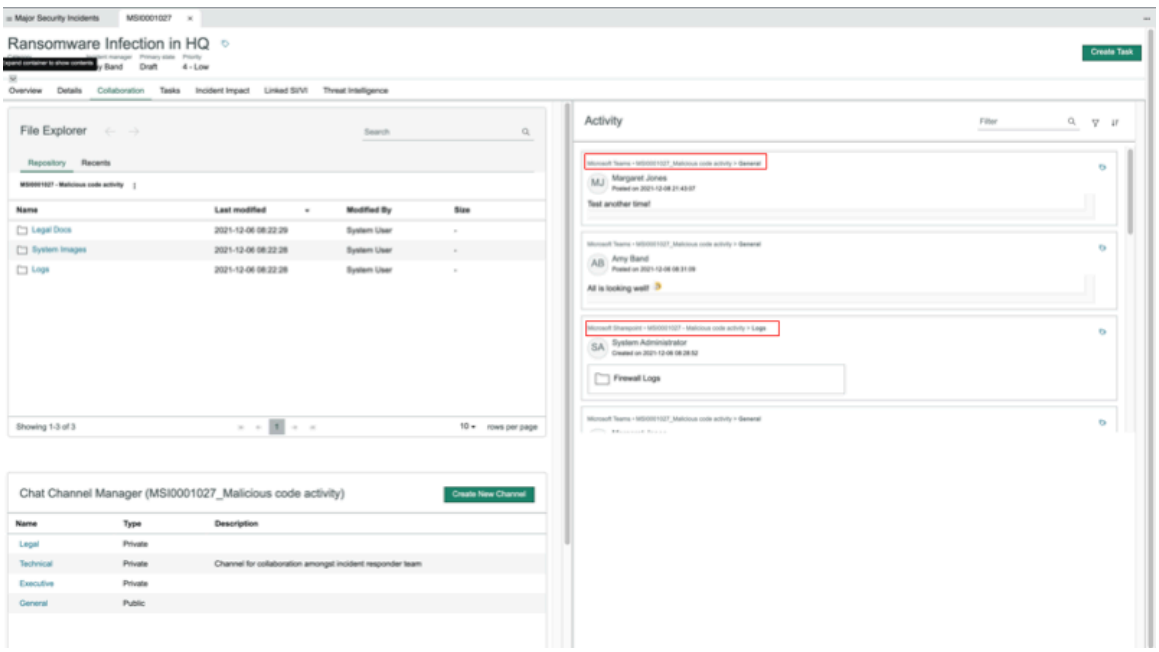
### Aktivitätenstrom-Konversationen verwalten

Zeigt alle Aktivitäten, Protokolle und Status an, die für Microsoft SharePoint, den Datei-Explorer und Microsoft Teamsausgeführt wurden.

Wenn Sie eine bestimmte Aktivität anzeigen oder die Details der Zusammenarbeitsaktivität durchsuchen möchten, die zwischen verschiedenen Dateien und Ordnern sowie in Microsoft Teams interagiert wurde, können Sie die Filterfunktion verwenden, die oben rechts im Abschnitt „Aktivitätenstrom“ angezeigt wird, und die gewünschte suchen Aktivitätsdetails.

Mit „Major Security Incident Management“ freigegebene Ordner und Chatkonversationen werden als Breadcrumbs mit der folgenden Struktur angezeigt:

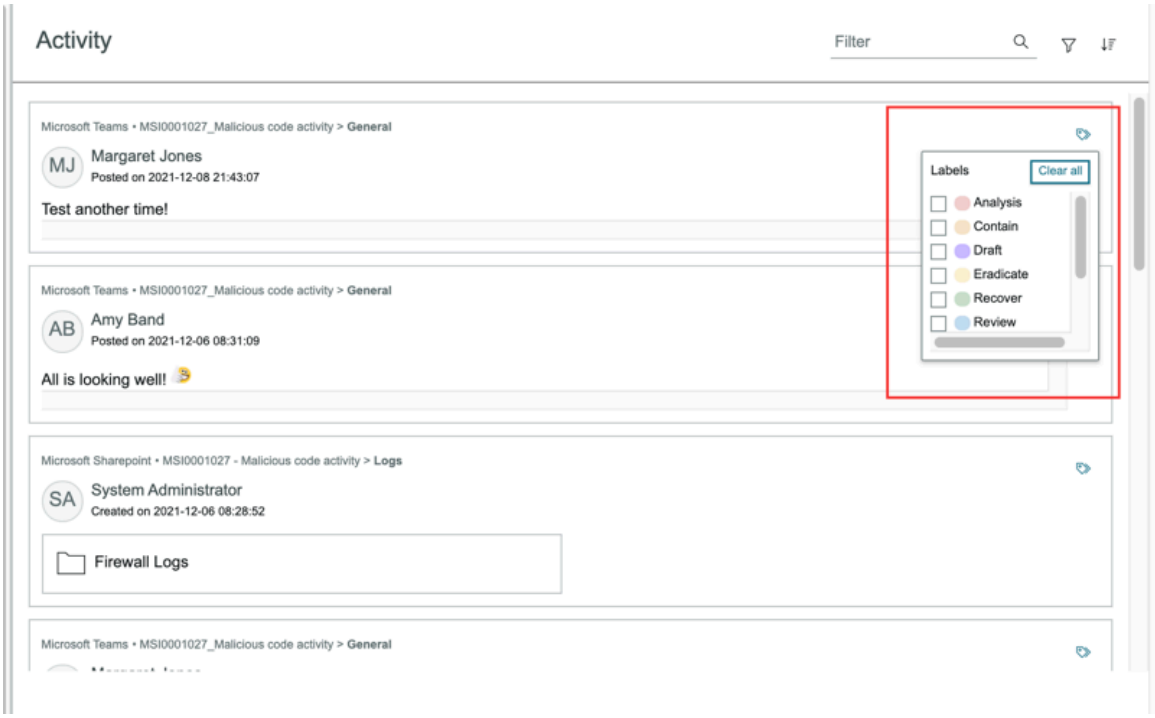
-Connector-Anwendungsname<incident number – category ><folder name> ).




**Beschriften Sie die Aktivitäten**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. **Klicken** Sie auf das Bezeichnungssymbol.
2. Aktivieren Sie das entsprechende Kontrollkästchen für die Incident-Aktivitätsbezeichnung (siehe Screenshot unten).




3. Die gekennzeichneten Aktivitäten sind farbcodiert und werden im Abschnitt „ **Externe Zusammenarbeit** “ des Arbeitsbereichs als Fortschrittstrenddiagramm dargestellt.

### Erstellen und verteilen Sie MSIM Statusberichte

Als Major Security Incident -Manager können Sie die verschiedenen Statusberichte erstellen und in verschiedenen Intervallen an verschiedene Stakeholder verteilen, basierend auf der konfigurierten Berichtsvorlage oder einem vorherigen Statusbericht während der Lösung eines schwerwiegenden Security Incidents.

**Vorbereitungen**
Erforderliche Rolle: sn_msi.workspace_manager

Sie können eine Vorschau der zuvor konfigurierten Datenelemente des Zusammenfassungsberichts anzeigen, zusätzlichen Text oder eine Zusammenfassung hinzufügen, einzelne Berichtskomponenten nach Bedarf entfernen und die Richtigkeit und Vollständigkeit des Berichts überprüfen, bevor Sie ihn an verschiedene Stakeholder verteilen.

Erstellen Sie die Statusberichte, indem Sie die gewünschte Berichtsvorlage auswählen, die ursprünglich auf der Setup-Seite für MSI-Berichtsvorlagen konfiguriert wurde.

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**.
2. Wählen Sie die **Listenansicht** aus.
3. Wählen Sie den jeweiligen heraufgestuften MSI-Datensatz aus.

Automatische Übersetzung

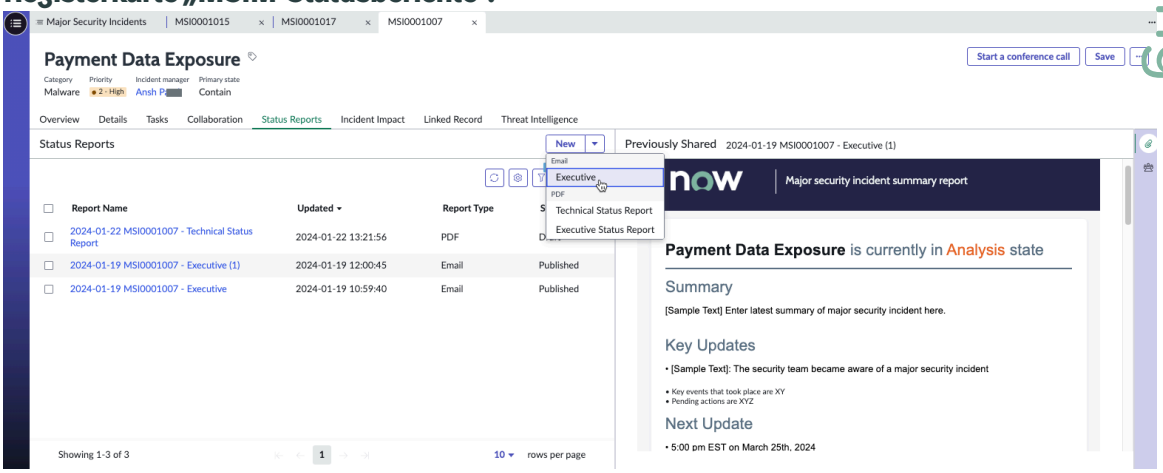
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wechseln Sie zur Registerkarte **Statusberichte**.
   Die Registerkarte „Statusberichte“ enthält drei verschiedene Arten von Unterabschnitten, wie unten dargestellt.

| Feld | Beschreibung |
|---|---|
| Berichtname | Name der Statusberichtsvorlage.<br>**Hinweis:**<br>In der Ansicht „Statusberichte“ werden die vorhandenen vordefinierten Berichtsvorlagen aufgelistet, die als Teil des Basissystems für die betreffende Persona verfügbar sind. Zum Beispiel Statusberichte für Führungskräfte per E-Mail (für Mobilgeräte geeignet), technische Statusberichte und Statusberichte für Führungskräfte als PDFs. |
| Aktualisiert | Das Datum, an dem die Berichtsvorlage zuletzt aktualisiert wurde. |
| Berichtstyp | Typ des Statusberichts. Der Statusbericht kann einen der folgenden Typen aufweisen:<br>○ PDF<br>○ E-Mail |
| Status | Status der Statusberichte. Die Statusberichte können einen der folgenden Status aufweisen:<br>○ Entwurf<br>○ In der Warteschlange<br>○ Veröffentlicht |

5. Wählen Sie den Typ des Statusberichts aus, den Sie anzeigen möchten, oder wählen Sie **Neu**, um einen Statusbericht zu erstellen.

**Registerkarte „MSIM-Statusberichte“.**




6. Wählen Sie einen der folgenden Statusberichttypen aus der Liste aus.

Automatische Übersetzung

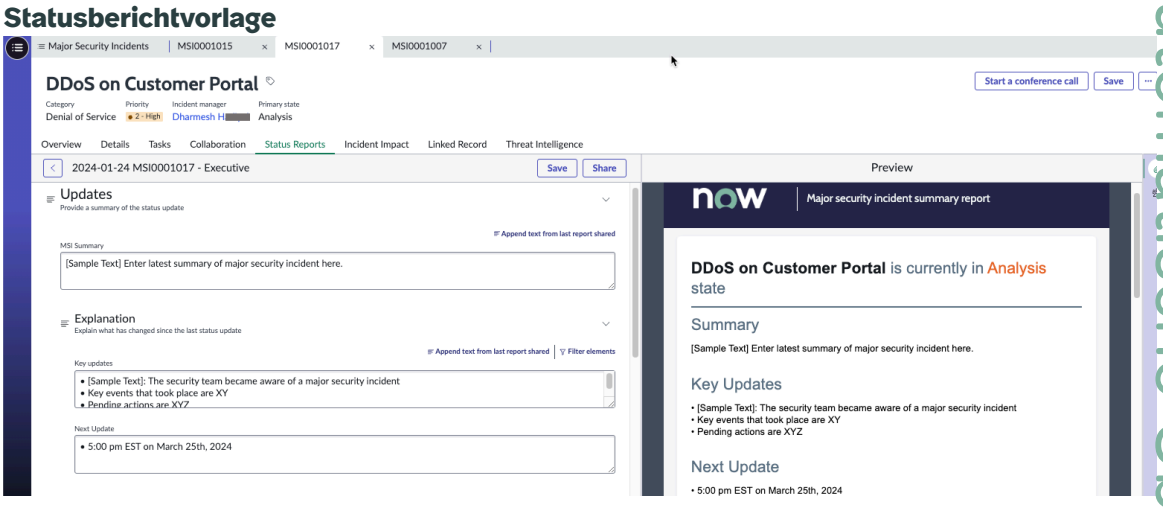
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- E-Mail-Statusberichte für **Führungskräfte**, die für Mobilgeräte geeignet sind.
- **Technischer Statusbericht (** PDF).
- **Statusbericht für Führungskräfte (** PDF).

**Hinweis:**
Wenn Sie eine beliebige Berichtsvorlage auswählen, wird die Vorschau des ausgewählten Berichts sofort im rechten Bereich generiert. Sie können den ausgewählten Statusbericht des MSI anzeigen.

7. Füllen Sie in der Vorlage „E-Mail-Statusbericht für Führungskräfte“ die Abschnitte mit den Details des Statusberichts aus.

**Hinweis:**
Die Optionen, die Sie im Abschnitt „Statusberichte“ ausgewählt haben, sind die gleichen Optionen, die im Vorschaubericht gerendert werden.

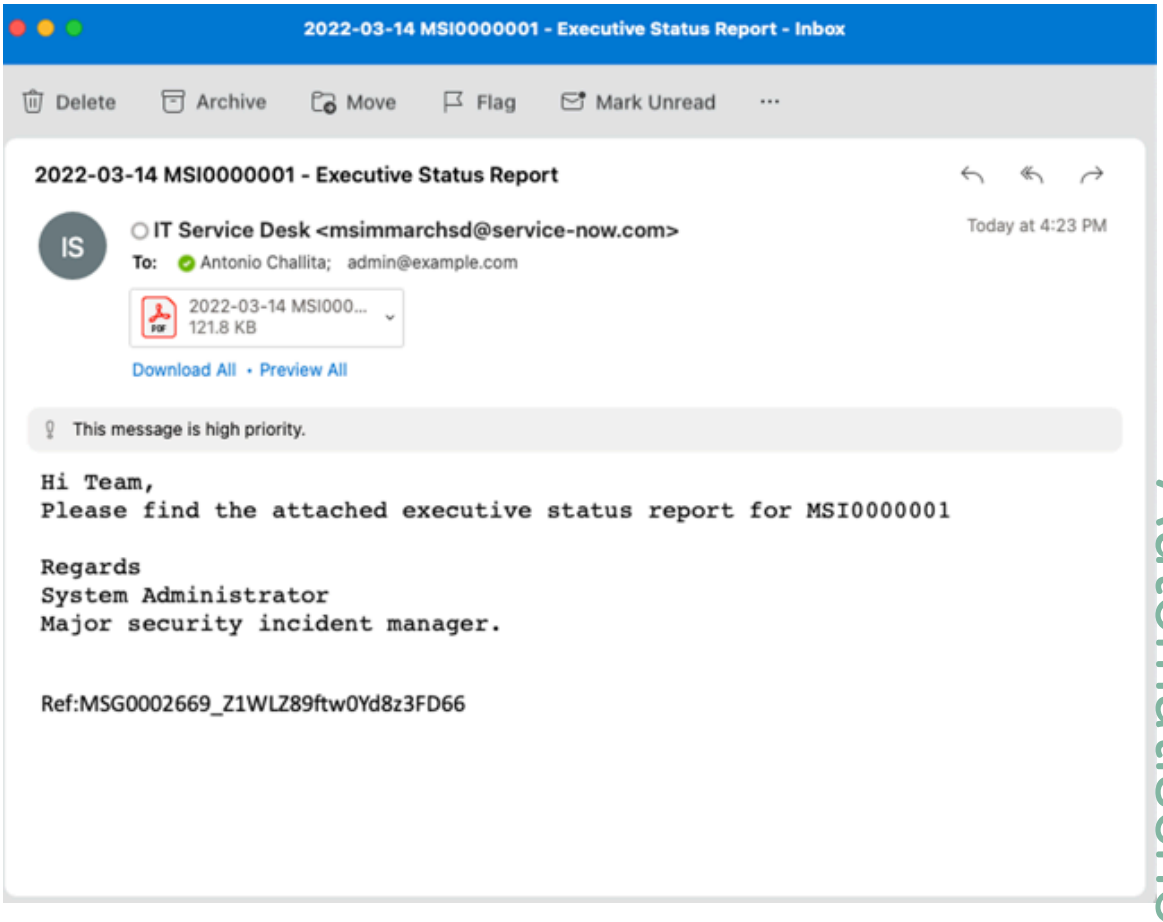



8. Wählen **Sie Speichern** aus, um die Aktualisierungen zu speichern, die Sie am Statusbericht vorgenommen haben.
9. Wählen Sie **Freigeben** aus, um den Bericht für die verschiedenen Stakeholder freizugeben.
   Das Dialogfeld „Bericht freigeben“ wird angezeigt.
10. Füllen Sie die Felder **Empfänger**, **Betreff**und **Text** nach Bedarf aus.
11. Wählen Sie E- **Mail-Bericht aus**.
    Eine E-Mail mit dem angehängten PDF-Statusbericht wird erfolgreich zur Überprüfung an den betroffenen Empfänger gesendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Statusbericht – E-Mail**




12. Sie können auch die folgenden Aktionen auf der Registerkarte Statusberichte ausführen:
    a. Verwenden Sie die **Aktion** Aktualisieren in der Ansicht „Statusberichte“, um die Liste der Statusberichte zu aktualisieren.
    b. Verwenden Sie die Aktion **Listenaktionen** in der Ansicht „Statusberichte“, um Spalten zu bearbeiten oder die Breiten der Statusberichtliste zurückzusetzen.
    c. Verwenden Sie die Aktion **Filter** in der Ansicht „Statusberichte“, um die Statusberichte basierend auf bestimmten Bedingungen zu filtern.

**Zugehörige Informationen**

Konfigurieren Sie Major Security Incident Statusberichte

## MSIM Statusberichte werden verwaltet

Statusberichte bieten vorkonfigurierte Trenddiagramme mit umsetzbaren Datenvisualisierungen, um Sicherheitsvorgänge zu verbessern und die Lösungszeitleiste, die Anzahl überfälliger Aufgaben und den Status jeder zugewiesenen Aufgabe zu messen und zu analysieren.

### Konfigurieren Sie Major Security Incident Statusberichte

Konfigurieren Sie Berichte zu schwerwiegenden Security Incidents, um die Berichte während des gesamten Lebenszyklus des Korrekturprozesses für Datensätze zu schwerwiegenden Security Incidents entsprechend Ihren geschäftlichen Anforderungen einzurichten und herunterzuladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Berichtsvorlagen mit einem bestimmten Format und Layout erstellen und diese Berichte mit der Funktion „Statusberichte“ des Management schwerwiegender Sicherheits-Incidents -Arbeitsbereichs an Ihre spezifischen Anforderungen anpassen.

Benutzer mit der Rolle „sn_msi.workspace_manager“ können die Berichtsvorlagen erstellen und konfigurieren, die den Typ der Berichtsinformationen beschreiben, die zum Generieren aller Statusberichte verwendet werden können, die für bestimmte Benutzer freigegeben werden können, z. B. für Stakeholder und Rechtsabteilungen Vorlagen für die Datensätze zu schwerwiegenden Security Incidents.

Um Ihre MSI-Statusberichte anzupassen, müssen Sie zuerst die Berichtsvorlagen mit **Berichtsvorlagen**einrichten. Mithilfe von Berichtsvorlagen können Sie die Berichtsvorlagentypen erstellen, die Berichtskomponenten für diese Berichtsvorlagen definieren, zusätzliche Informationen hinzufügen, visualisierte Daten erstellen, um Umfang und Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzufügen und die Statusberichte generieren.

Im Folgenden werden die Standardfelder beschrieben, die in allen Berichtsvorlagentypen bereitgestellt werden. Sie können die Berichtsvorlage basierend auf Ihren Anforderungen mithilfe von Abschnitten, Unterabschnitten und deren Elementen konfigurieren und formatieren:

**Komponenten des Statusberichts**

| Komponententyp | Beschreibung |
|---|---|
| Berichtstitel | Titel des Berichtstyps. Das Standardformat des Berichtstyps lautet beispielsweise: {MSI-Nummer} - {Executive Stakeholder-Bericht}, dargestellt als MSI0001001: Executive Stakeholder-Bericht. |
| Name | Zeigt den Namen des Benutzers an, der den Bericht im Abschnitt „Statusberichte“ des Arbeitsbereichs „Major Security Incident Management“ generiert hat. |
| Zusammenfassung | Zeigt eine kurze Zusammenfassung des Berichts an. |
| Datum | Zeigt das Datum an, an dem der Bericht für den betroffenen Empfänger freigegeben wurde. |
| Fortschritt | Zeigt die Umfangs- und Fortschrittsmetriken an, z. B. die verknüpften SIR-Incidents, Antwortaufgaben, Ergänzungsaufgaben, externe Zusammenarbeit, Zeitleistenkomponenten und aktuelle Zeitleistenereignisse. |
| Herausforderungen | In diesem Abschnitt wird eine kurze Beschreibung der Herausforderungen angezeigt, die mit dem Korrekturprozess für schwerwiegende Security Incidents verbunden sind. |
| Nächste Schritte | In diesem Abschnitt wird eine kurze Beschreibung der nächsten Schritte zur Behebung schwerwiegender Security Incidents angezeigt. Beispielsweise erhalten Sie im Unterabschnitt „Aktives Team“ im Bericht zu Stakeholdern für Führungskräfte die Informationen zum nächsten Schritt der Teamzuweisung, die an der weiteren Analyse des Datensatzes für schwerwiegende Security Incidents beteiligt ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Komponenten des Statusberichts (Fortsetzung)**

| Komponententyp | Beschreibung |
|---|---|
| Andere Anpassungen | Die Berichtsvorlage bietet Ihnen auch die Möglichkeit, das Logo hochzuladen und die Kopf- und Fußzeilen im Bericht anzupassen. |

Im Folgenden sind die Arten von Berichtskategorien aufgeführt, die eingerichtet und angezeigt werden können:

- E-Mail-Adresse der**Geschäftsführung**
- **Technischer Statusbericht (** PDF).
- **Statusbericht für Führungskräfte (** PDF).

Die oben genannten Berichte sind konfiguriert und für den Benutzer verfügbar, um den Bericht im Arbeitsbereich „Major Security Incident Management“ auszuwählen, anzuzeigen und zu generieren.

## Für Mobilgeräte optimierte Statusberichte für Führungskräfte – E-Mail

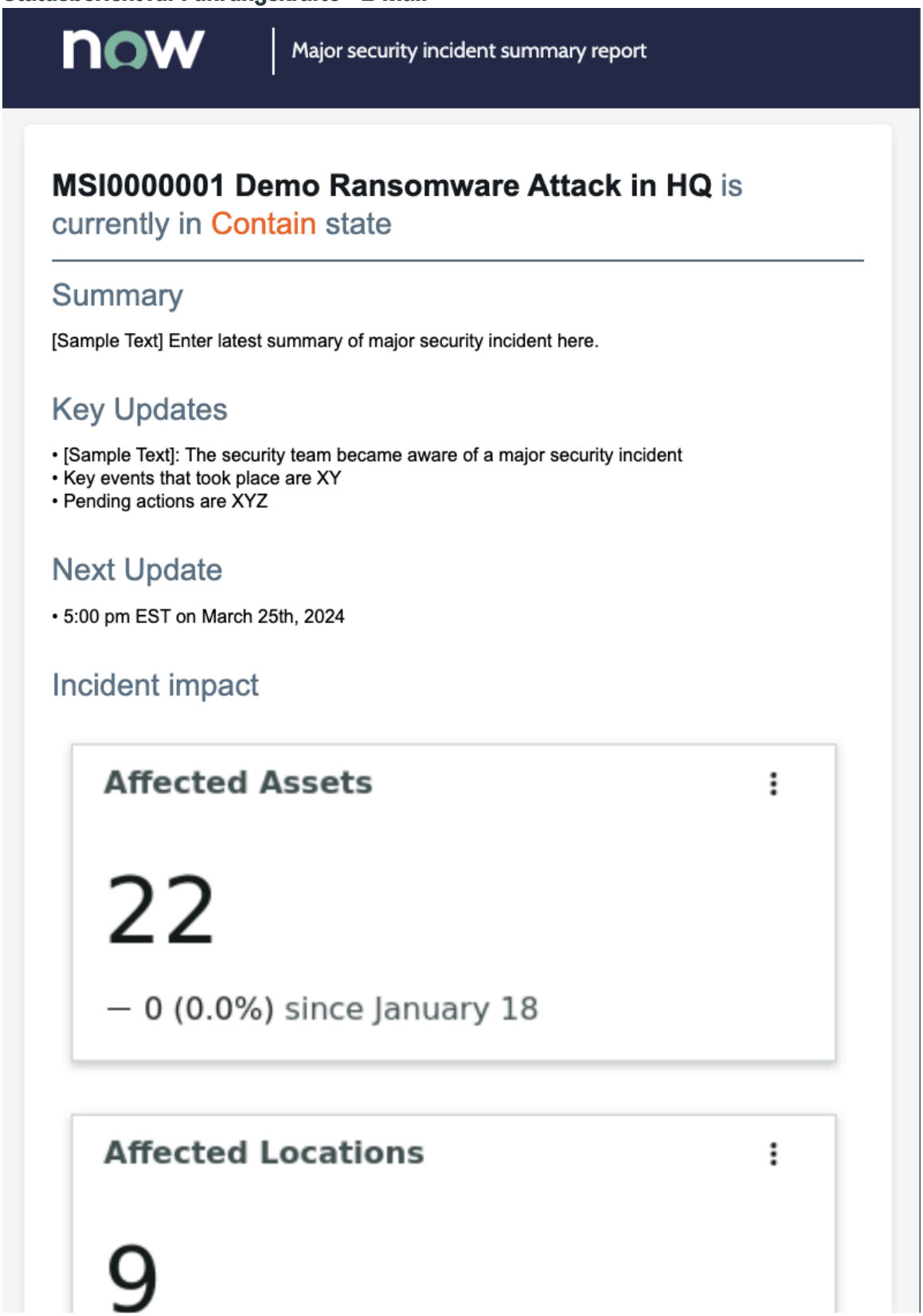
„Statusberichte für Führungskräfte – E-Mail“ sind für Mobilgeräte optimierte Statusberichte, die im E-Mail-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, eine Spalte für die MSI-Dauer, den Umfang/die Auswirkung des Incident, aktive Teammetriken, Fortschrittsmetriken und Zeitleistenkomponenten, z. B. die letzten Zeitleistenereignisse für den jeweiligen Datensatz eines schwerwiegenden Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Nachfolgend wird ein Beispiel für einen E-Mail-Statusbericht für Führungskräfte angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Statusbericht für Führungskräfte – E-Mail**




Automatische Übersetzung

## Statusberichte für Führungskräfte – PDF

„Statusberichte für Führungskräfte – PDF“ sind Statusberichte, die im PDF-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, eine Spalte für die MSI-Dauer, den Umfang/die Auswirkung des Incident, aktive Teammetriken,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortschrittsmetriken und Zeitleistenkomponenten, z. B. die letzten Zeitleistenereignisse für den jeweiligen Datensatz eines schwerwiegenden Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Nachfolgend wird ein Beispiel für einen Executive Report als Referenz angezeigt.

**Statusbericht für Führungskräfte (PDF).**

MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

**Overview**

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

**Progress**

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

**Challenges**

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

**Scope**

Affected Assets 22 — 0 (0.0%) since January 18
Affected Locations 9 — 0 (0.0%) since January 18
Affected users 45 — 0 (0.0%) since January 18

Figure 1. Incident Impact

**Progress**

By incident state — Analysis, Contain, Recover
Trends by incident state — Analysis, Contain, Recover, Eradicate, Review

Figure 2. Linked Security Incidents

In progress tasks by incident state label — Eradicate 1 17%, Analysis 2 33%, Contain 1 17%, Recover 2 33%, 6

Figure 3. Response Tasks

## Technische Statusberichte – PDF

„Technische Statusberichte – PDF“ sind Statusberichte, die im PDF-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, eine MSI-Dauerspalte, Incident-Umfang/-Auswirkung, aktive Teammetriken, Fortschrittsmetriken und Zeitleistenkomponenten, z. B. die letzten Zeitleisten-Events für diesen bestimmten Datensatz eines schwerwiegenden Security Incidents, beschriftet mit Aufgabenaktualisierungen und beschrifteten Aktivitäten. basierend auf der

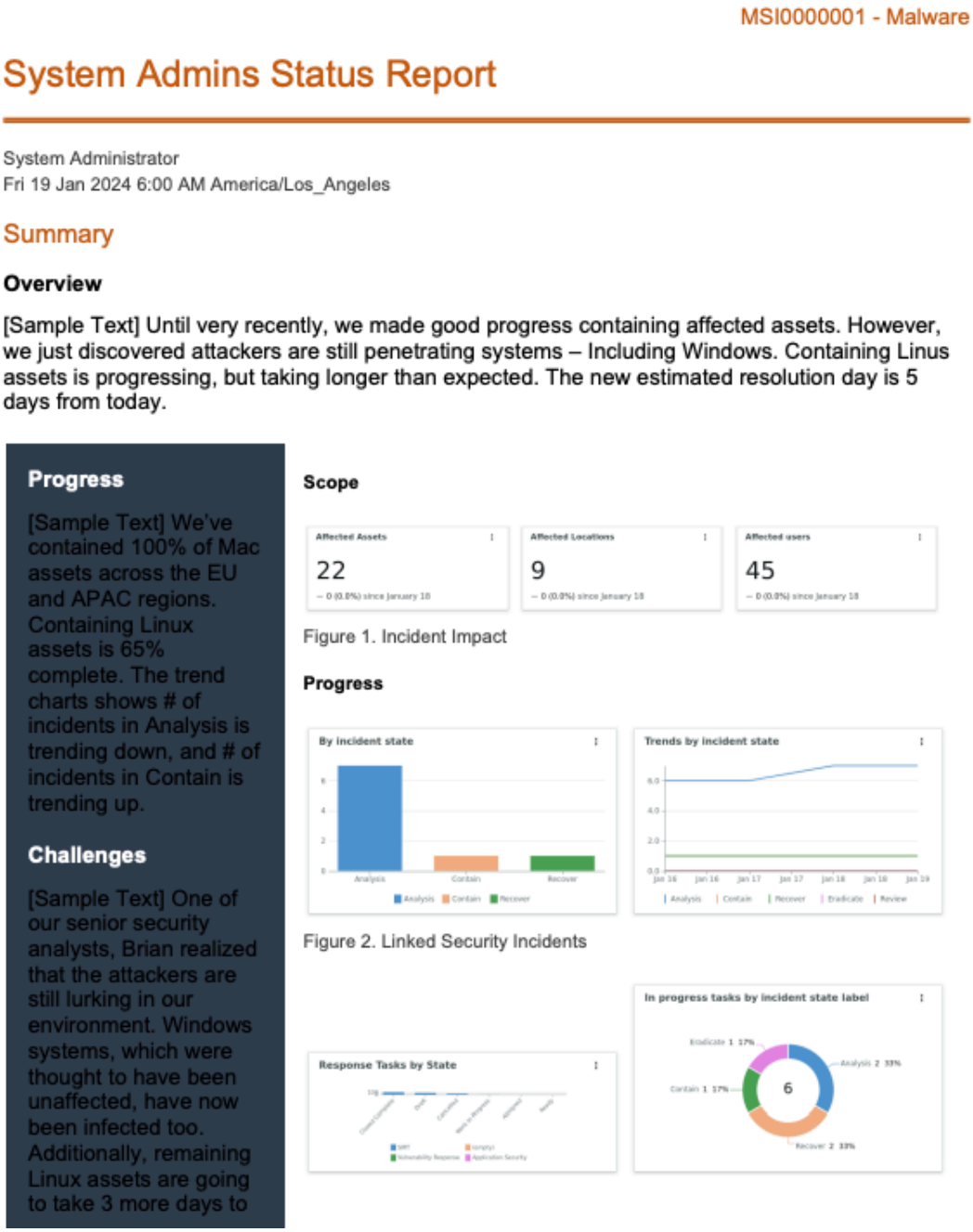


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisungsgruppe und der ausgewählten Tag-Bezeichnung seit der Generierung des letzten Statusberichts sowie zusätzlichen Informationen wie Incident-Auswirkung und verknüpfte Incidents.

Passen Sie die Berichtsvorlage an und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Ein technischer Beispielbericht, der die zusätzlichen Informationen anzeigt, z. B. die Incident-Auswirkung, ist unten als Referenz abgebildet, und der verbleibende Teil der Berichtsinformationen ähnelt den Executive Reports.

**Technischer Statusbericht – PDF**



MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

**Overview**

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

**Progress**

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

**Challenges**

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

**Scope**

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

**Progress**

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

Die Berichtsvorlagenabschnitte enthalten verschiedene Unterabschnitte, die beschreiben, wie Sie die Berichtsunterabschnitte und ihre Elemente erstellen können, z. B.:

1. Branding: Fügen Sie Ihren Berichtsvorlagen Branding hinzu
2. Vorlagenskripts: Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Verwenden Sie Visualisierungen in Berichtsvorlagen
4. Verwenden Sie Berichtslisten in Berichtsvorlagen

### Erstellen Sie eine Berichtsvorlage

Erstellen Sie verschiedene Berichtsvorlagen, die auf schwerwiegende Security Incidents angewendet werden können, und generieren Sie einen Statusbericht. Sie können der Berichtsvorlage standardmäßige und benutzerdefinierte Felder des Formulars „Major Security Incident Response“ hinzufügen, die Dot-Walk-fähig sind. Darüber hinaus können Sie den Bericht basierend auf Ihren Anforderungen mithilfe von Abschnitten, Unterabschnitten und deren Elementen formatieren und konfigurieren.

#### Vorbereitungen

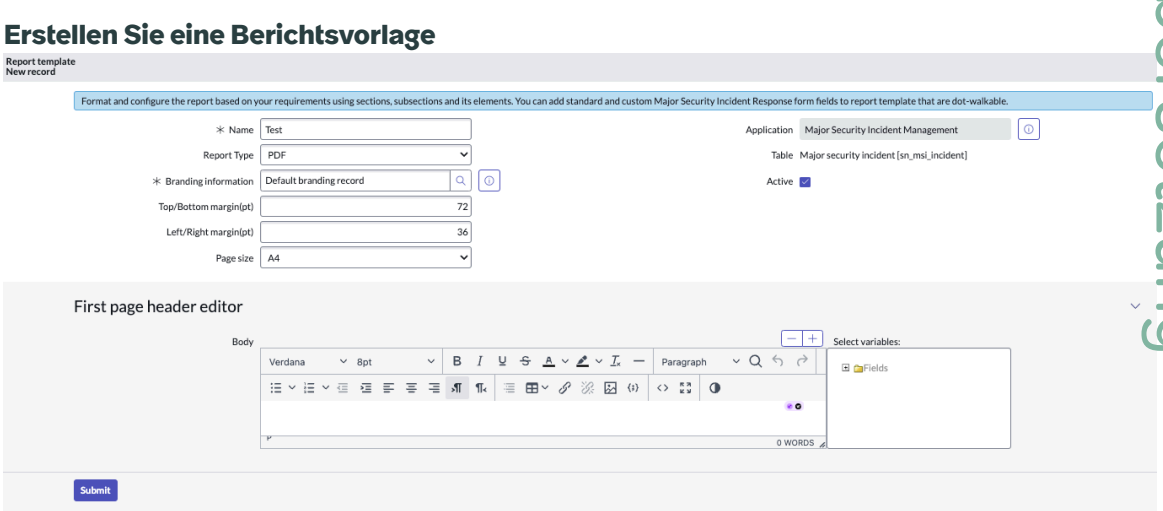
Erforderliche Rolle: sn_msi.workspace_manager

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können Berichtskomponenten für Ihre Berichtsvorlagen definieren und zusätzliche Informationen angeben. Erstellen Sie visualisierte Daten, um Umfang und Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzuzufügen, eine Vorschau anzuzeigen und die Statusberichte zu generieren oder freizugeben.

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Wählen Sie **Neu** aus, um eine Berichtsvorlage zu erstellen.
4. Füllen Sie die Felder im Formular „Berichtvorlage“ aus.




5. **Senden Sie** den neuen Berichtsvorlagendatensatz.
   Auf der Seite „Berichtsvorlagen“ wird eine neue Berichtsvorlage erstellt.

#### Zugehörige Informationen

Erstellen und verteilen Sie MSIM Statusberichte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie Ihren Berichtsvorlagen Branding hinzu

Fügen Sie Ihren Berichten Branding hinzu. Sie können Kopf- und Fußzeilenbilder sowie Kopf- und Fußzeilentext hinzufügen. Sie können diese Branding-Informationen in alle Berichtsvorlagentypen aufnehmen, die Sie erstellen möchten, mit Ausnahme der beiden vordefinierten Berichte.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

#### Warum und wann dieser Vorgang ausgeführt wird

Die wichtigsten Überlegungen beim Hinzufügen von Branding zu Ihren Berichtsvorlagen sind:

- Laden Sie das Kopf- und Fußzeilenbild hoch, und richten Sie die Bildposition aus.
- Die maximale Größe für Kopf- und Fußzeilenbilder beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im schwerwiegenden Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
- Passen Sie die Höhe des Kopf- und Fußzeilenbilds an.
- Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
2. Führen Sie einen Drilldown zu durch **Berichtsvorlage** > **Branding**.
3. Wählen Sie **Konfigurieren** aus.
4. Wählen Sie **Neu** aus, um Ihrer Berichtsvorlage ein Branding hinzuzufügen.
5. Füllen Sie die Felder im Formular „Branding-Vorlage“ aus.
6. Wählen Sie **Absenden**.
   Auf der Seite „Branding-Vorlagen“ wird eine neue Branding-Vorlage erstellt.

### Verwenden Sie Visualisierungen in Berichtsvorlagen

Verwenden Sie Berichts-Widgets, um UIB-Elemente (User Interface Builder) wie Datenvisualisierungen zu definieren und in die MSIM-Statusberichte aufzunehmen.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

#### Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Führen Sie einen Drilldown zu durch **Berichtsvorlage** > **Visualisierungen**.
3. Wählen Sie **Konfigurieren** aus.
   Im Folgenden finden Sie die vordefinierten UIB-Visualisierungen als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zugehörige Informationen**

Erstellen Sie ein Visualisierungstypelement

### Verwenden Sie Berichtslisten in Berichtsvorlagen

Verwenden Sie Berichtslisten, um die zugehörigen Listenartefakte zu definieren und einzubeziehen, um Listen in der PDF-Datei basierend auf Ihren konfigurierten MSI-Listendatensätzen zu generieren.

## Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

## Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Führen Sie einen Drilldown zu durch **Berichtsvorlage** > **Lists**.
3. Wählen Sie **Konfigurieren** aus.
   Im Abschnitt „MSI-Statusberichtslisten“ wird beschrieben, wie jede spezifische zugehörige Liste seit der Erstellung des Incident betroffen ist. Im Folgenden finden Sie die vordefinierten MSI-Berichtslisten als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.

**Zugehörige Informationen**

Erstellen Sie ein Listentypelement

### Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

Erstellen Sie ein Skript, das die Daten der zugehörigen Listen, Datumsvorgänge und andere Daten enthält, die nicht direkt punktweise durchführbar sind.

## Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

## Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses vordefinierte Vorlagenskript in Ihren Berichtsvorlagen verwenden, um zugehörige Daten einzubeziehen, nachdem die Berichtsvorlagen konfiguriert und angepasst wurden.

Erstellen Sie ein Vorlagenskript, um die zugehörigen Listendaten in der Berichtsvorlage anzuzeigen. Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag hinzufügen als: `${template_script:script name}`.

Beispiel: `${template_script:msi_collab_cards}`

**Hinweis:**
Sie können die vordefinierten Vorlagenskripts nicht löschen. Eine Fehlermeldung wird angezeigt, wenn ein Benutzer mit der Administratorrolle versucht, einen Vorlagenskript-Datensatz zu löschen, wenn er einer Berichtsvorlage zugeordnet ist.

## Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Führen Sie einen Drilldown zu durch **Berichtsvorlage** > **Vorlagenskripts**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Konfigurieren** aus.
   Im Folgenden finden Sie die vordefinierten Vorlagenskripts als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.

   **Hinweis:**
   Sie können auch ein eigenes Vorlagenskript erstellen, um zusätzlich zu den aufgeführten Vorlagenskripts die zugehörigen Listendaten, Datumsvorgänge und andere Daten einzubeziehen, die nicht direkt per Dot-Walking ausgeführt werden können.

### Zeigen Sie eine Vorschau der Berichtsvorlage an

Verwenden Sie die Vorschaufunktion, um eine Vorschau Ihrer Designzeit-Berichtsvorlage anzuzeigen, um den Bericht zur Laufzeit im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents zu generieren und für andere Stakeholder freizugeben.

#### Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

#### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Wählen Sie die gewünschte Berichtsvorlage aus.
4. Wählen Sie als Berichtstyp je nach Anforderung E- **Mail** oder **PDF** aus.
5. Wählen Sie die Aktion **Speichern und Vorschau des Berichts** aus.

   Das Dialogfeld „Vorschaubericht“ wird angezeigt.
6. Wählen Sie mithilfe der Suchoption einen schwerwiegenden Security Incident aus, um eine Vorschau eines Berichts mit der ausgewählten Vorlage anzuzeigen.
7. Wählen Sie **Vorschaubericht aus**.
   Der Bericht generiert eine Vorschau gemäß der ausgewählten Vorlagenkonfiguration. Wenn Sie als Berichtstyp E- **Mail**ausgewählt haben, befindet sich die Vorschau im E-Mail-Vorlagenformat. Die Statusberichte im E-Mail-Format sind für Mobilgeräte optimiert.

### Erstellen Sie eine Berichtsabschnittsvorlage

Ein Bericht kann weiter in verschiedene Abschnitte unterteilt werden. Verwenden Sie den Abschnitt „Bericht“, um den Bericht in mehrere Abschnitte aufzugliedern und sie der Reihe nach neu zu organisieren.

#### Vorbereitungen
Erforderliche Rolle: sn_msi.workspace_manager

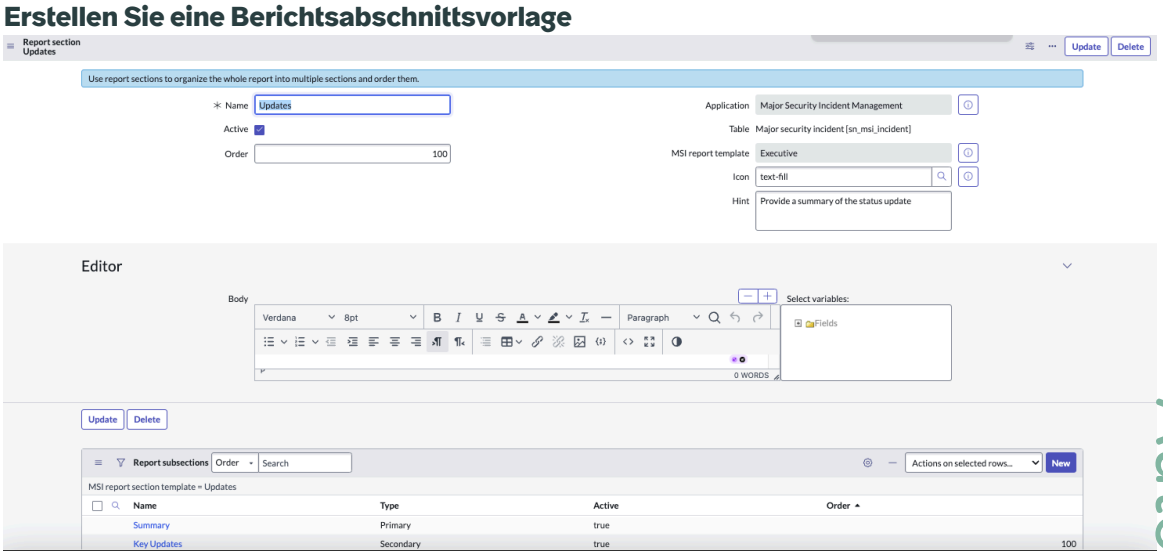
#### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Navigieren zu **Berichtsabschnitte** > **Neu**.
   Die neue Berichtsabschnittsseite wird angezeigt.




5. Füllen Sie die Felder im Formular „Berichtsabschnittsvorlage“ aus.

6. Speichern und **übermitteln** Sie den neuen Berichtsvorlagenabschnitt.

## Erstellen Sie eine Berichtsunterabschnittsvorlage

Verwenden Sie den Berichtsunterabschnitt, um den Abschnitt weiter in mehrere Unterabschnitte zu organisieren und deren Ausrichtung und Position mithilfe der verfügbaren Typen wie „Textseitenbereich“, „Primär“ und „Sekundär“ zu konfigurieren.

### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

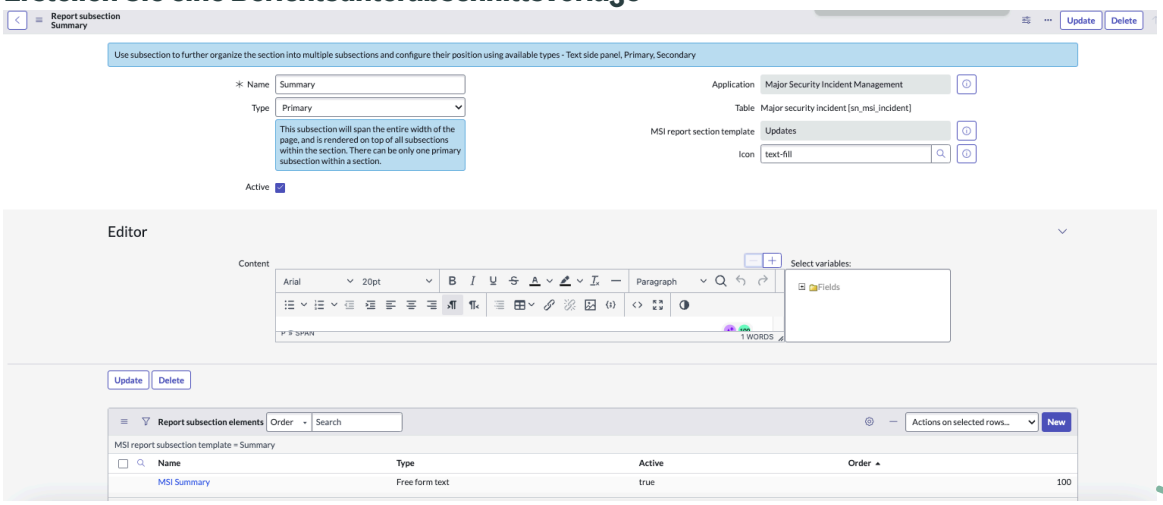
### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Navigieren zu **Berichtsunterabschnitte** > **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie eine Berichtsunterabschnittsvorlage




6. Füllen Sie die Felder im Formular „Berichtunterabschnitt“ aus.

7. Speichern und **übermitteln** Sie den neuen Berichtsvorlagenabschnitt.

### Erstellen Sie eine Vorlage für Berichtsunterabschnittselemente

Verwenden Sie Unterabschnittselemente, um einen Unterabschnitt weiter in mehrere Elemente zu organisieren. Unterabschnittselemente helfen dabei, Visualisierungen, Listen und Freiformtext mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

#### Vorbereitungen

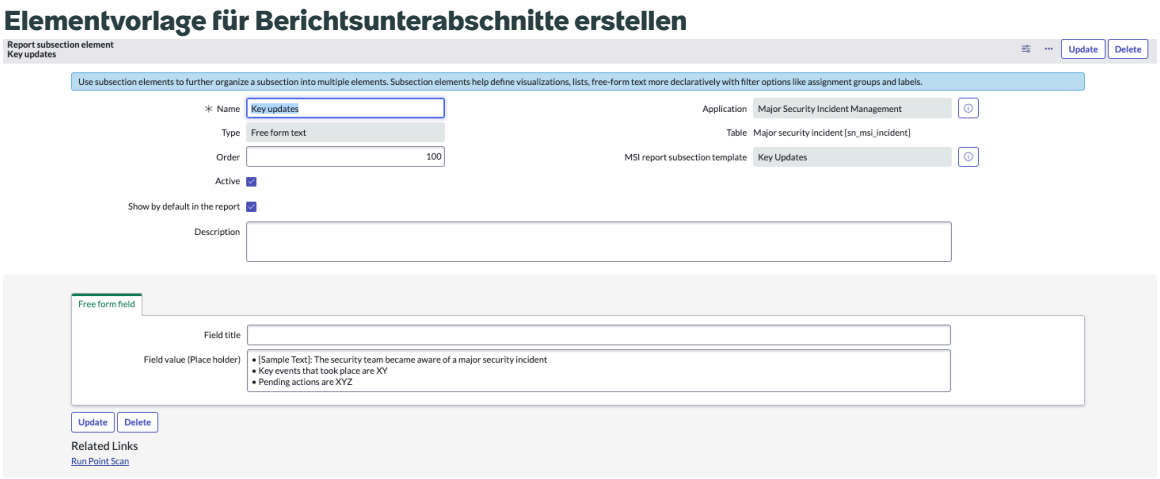
Erforderliche Rolle: sn_msi.workspace_manager

#### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Füllen Sie die Felder im Formular „Berichtunterabschnittselemente“ aus.

8. Speichern und **aktualisieren** Sie den neuen Berichtsvorlagenabschnitt.

### Erstellen Sie ein Freiformtyp-Element

Erstellen Sie einen Freiform-Elementtyp, um den Freiformtext mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

#### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

#### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Erstellen Sie eine Vorlage für Berichtsunterabschnittselementeerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Freiformfeld aus**.
   Dadurch wird der Abschnitt **Freiformfeld** angezeigt.
9. Füllen Sie die Felder auf der Registerkarte Freiform aus.

### Erstellen Sie ein Visualisierungstypelement

Erstellen Sie einen Visualisierungselementtyp, um die Visualisierungselemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

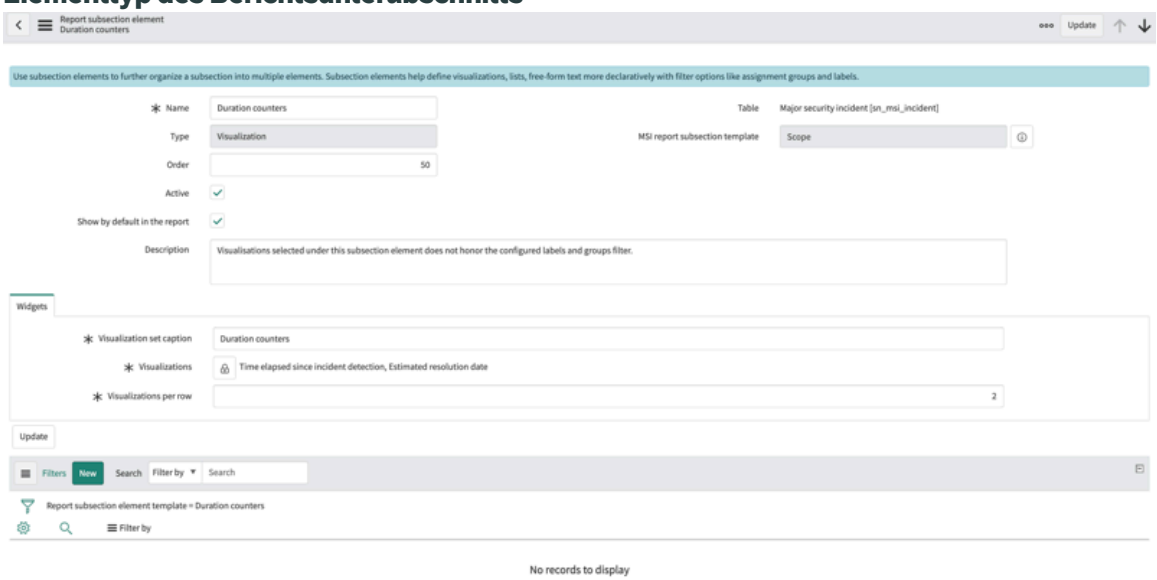
Erforderliche Rolle: sn_msi.workspace_manager

### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Erstellen Sie eine Vorlage für Berichtsunterabschnittselementeerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Visualisierung** aus.
   Dadurch wird der Abschnitt „ **Visualisierung** “ angezeigt.
9. Füllen Sie die Felder des Formulars „Visualisierung“ aus.
10. Wählen Sie **Absenden**.

## Example: Unterabschnittselementtyp der Berichtsvorlage für einen technischen Statusbericht

### Elementtyp des Berichtsunterabschnitts




### Erstellen Sie ein Listentypelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer definiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Erstellen Sie eine Vorlage für Berichtsunterabschnittselementeerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Liste** aus.
   Dadurch wird der Abschnitt „ **Listen** “ angezeigt.
9. Füllen Sie die Felder des Listenformulars aus.

## Erstellen Sie ein benutzerdefiniertes Typelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer definiert.

### Vorbereitungen

Erforderliche Rolle: sn_msi.workspace_manager

### Prozedur

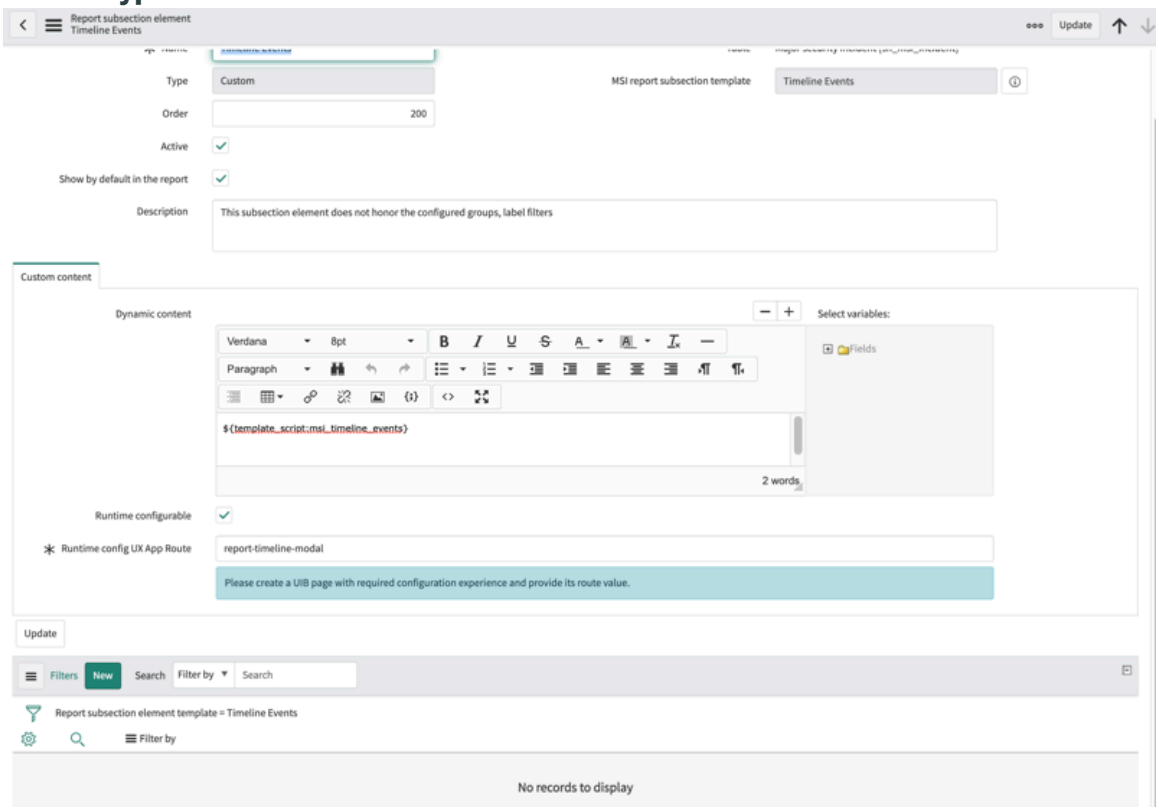
1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**.
   Die Seite MSI-Statusbericht-Setup wird angezeigt.
2. Wählen Sie im Abschnitt „Berichtsvorlage“ die Option **Konfigurieren**aus.
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur entsprechenden Liste der Berichtsabschnitte.
4. Öffnen Sie in der Liste „Berichtsabschnitte“ eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste der Berichtsabschnittsvorlagen eine vorhandene Berichtsunterabschnittsvorlage.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**.
7. Füllen Sie das Formular „Berichtsunterabschnittselemente“ mit den erforderlichen Details aus, wie in Erstellen Sie eine Vorlage für Berichtsunterabschnittselementeerläutert.
8. Navigieren Sie zum Feld Typ des Berichtsunterabschnittselements, und wählen Sie die Option **Benutzerdefiniert** aus.
   Dadurch wird der Abschnitt „ **Benutzerdefinierter Inhalt** “ angezeigt.
9. Füllen Sie die Felder des Formulars „Benutzerdefinierter Inhalt“ aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Example: Das folgende Beispiel zeigt den Unterabschnittselementtyp der Berichtsvorlage für einen technischen Statusbericht

### Elementtyp des Berichtsunterabschnitts




### Fügen Sie Systemeigenschaften hinzu

Fügen Sie Systemeigenschaften hinzu, um das Verhalten der MSIM-Anwendung zu steuern. Im Folgenden finden Sie die Standardsystemeigenschaften, die als Teil der Management schwerwiegender Sicherheits-Incidents -Statusberichte eingeführt werden.

### Systemeigenschaften

| Eigenschaftsname | Beschreibung |
|---|---|
| sn_msi.export_img | Verwenden Sie diese Eigenschaft, um den Export von Images zu steuern. Der Standardwert ist auf EIN festgelegt. |
| sn_msi.export_img_log | Verwenden Sie diese Eigenschaft, um die Anmeldung bei der Browserkonsole zu aktivieren. Der Standardwert ist AUS. |
| sn_msi.export_img_parallel_threshold | Verwenden Sie diese Eigenschaft, um die maximale Anzahl paralleler Anforderungen zum Generieren der Bilder aus Berichts-Widget-Konfigurationen zu steuern. Der Standardwert ist auf 14 festgelegt. |
| sn_msi.img_export_log | Verwenden Sie diese Eigenschaft, um die Konsolenprotokolle im Browser zu aktivieren. |
| sn_msi.img_export_poll_interval | Verwenden Sie diese Eigenschaft, um den Zeitabstand zwischen Abfragen zu steuern, der überprüft, ob das Image generiert wird oder nicht. Das standardmäßige |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Systemeigenschaften (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| | Abfrageintervall ist auf 3000 Millisekunden festgelegt. |
| sn_msi.export_poll_request_timeout | Verwenden Sie diese Eigenschaft, um die maximale Zeit zu steuern, in der das System das exportierte Bild abrufen kann. Der Standardwert beträgt 120.000 Millisekunden. |
| sn_msi.msi_report_uib_element_js_path | Verwenden Sie diese Eigenschaft, um den generischen Pfad zum Erfassen des Bildes aus dem UIB-Seitenteil zu steuern. |
| sn_msi.report_default_style_objects | Verwenden Sie diese Eigenschaft, um das CSS der generierten PDFs zu ändern, z. B. Schriftgröße, Schriftfarbe oder Feldwert. Beispiel: Wenn sn_msi.workspace_manager die Schriftfarbe des linken Bereichs des generierten PDF-Statusberichts ändern möchte, kann der Arbeitsbereichsmanager die Systemeigenschaft Schriftfarbe ändern und die PDF-Datei in einer gewünschten Ansicht rendern. |

## Rollup-Framework für MSIM

Erweitert die Möglichkeit, die Quelldatensätze aus dem Arbeitsbereich Management schwerwiegender Sicherheits-Incidents zu verknüpfen.

## Übersicht

Rollup Framework macht den Rollup-Flow konfigurierbar und erweiterbar. Verwenden Sie dieses Framework-Modell, um die Informationen zu konfigurieren, für die ein Rollup zu einem schwerwiegenden Security Incident durchgeführt werden kann.

Zuvor konnte sn_msi.workspace_manager die Security Incidents und angreifbaren Elemente verknüpfen, die als MSIvorgeschlagen oder heraufgestuft wurden. Nach der Verknüpfung des Security Incident oder des angreifbaren Elements wurde für die Informationen ein Rollup zu einem schwerwiegenden Security Incident durchgeführt. Die Art der Informationen, für die ein Rollup erforderlich ist, wurde in den Skripts hartcodiert.

Sie können das Framework-Modell verwenden, um den Rollup-Flow zu konfigurieren, der die folgenden Funktionen unterstützt und auch die vorhandenen Probleme in der Anwendung behandelt:

Das Rollup-Framework-Modell ermöglicht sn_msi.workspace_manager mit den folgenden Vorteilen:

- Fügen Sie die Datensatzfunktionen „Verknüpfen“, „Vorschlagen“ oder „Heraufstufen MSI “ in einer beliebigen Tabelle hinzu, oder entfernen Sie sie, wodurch die Aufgabentabelle erweitert wird.
- Steuern Sie die Art der Informationen, für die ein Rollup zu MSI durchgeführt werden soll, während Aktionen wie Verknüpfen/Vorschlagen/Heraufstufen für die Incident-Datensätze ausgeführt werden.
- Unterstützen Sie das Verknüpfen, Vorschlagen oder Heraufstufen von Security Incidents, Korrekturaufgaben und sofort einsatzbereiten Security Cases (OOTB) sowohl in der klassischen Umgebung als auch im Management schwerwiegender Sicherheits-Incidents -Arbeitsbereich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Rollup-Framework weist die in der folgenden Tabelle erläuterten Konfigurationen auf.

**Rollup-Framework-Konfigurationen**

| Name | Beschreibung |
|---|---|
| Konfiguration verknüpfter Datensätze | Speichert die Informationen von Aufgabentabellen, die zum Verknüpfen/Heraufstufen/Vorschlagen mit Major Security Incidentverwendet werden können. |
| Konfiguration von Rollup-Datensätzen | Erfasst die Informationen, für die ein Rollup aus der Aufgabentabelle durchgeführt werden kann, wenn Aktionen zum Verknüpfen/Heraufstufen/Vorschlagen ausgeführt werden. |
| Listenlayoutkonfiguration | Steuert die Bezeichnungen und das Listenlayout für verschiedene Tabellen, wie auf den Registerkarten des Arbeitsbereichs Management schwerwiegender Sicherheits-Incidents angezeigt, z. B. Incident-Auswirkung, Verknüpfte Datensätze und Threat Intelligence. |

## Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Verwenden Sie die Konfiguration verknüpfter Datensätze, um die Informationen von Aufgabentabellen zu speichern, die zum Verknüpfen/Heraufstufen/Vorschlagen von Major Security Incidentverwendet werden können.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

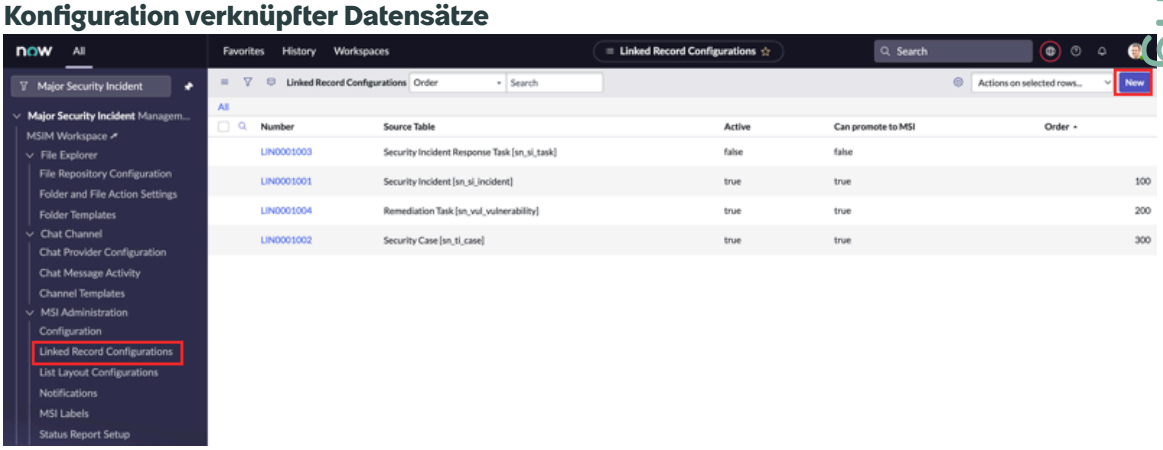
**Hinweis:**
Der Administrator kann den Datensatz erstellen, und der Administrator des Arbeitsbereichs MSIM kann den Datensatz aktualisieren.

### Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfigurationen verknüpfter Datensätze**.

   Die Seite „Konfiguration verknüpfter Datensätze“ wird angezeigt.

**Konfiguration verknüpfter Datensätze**

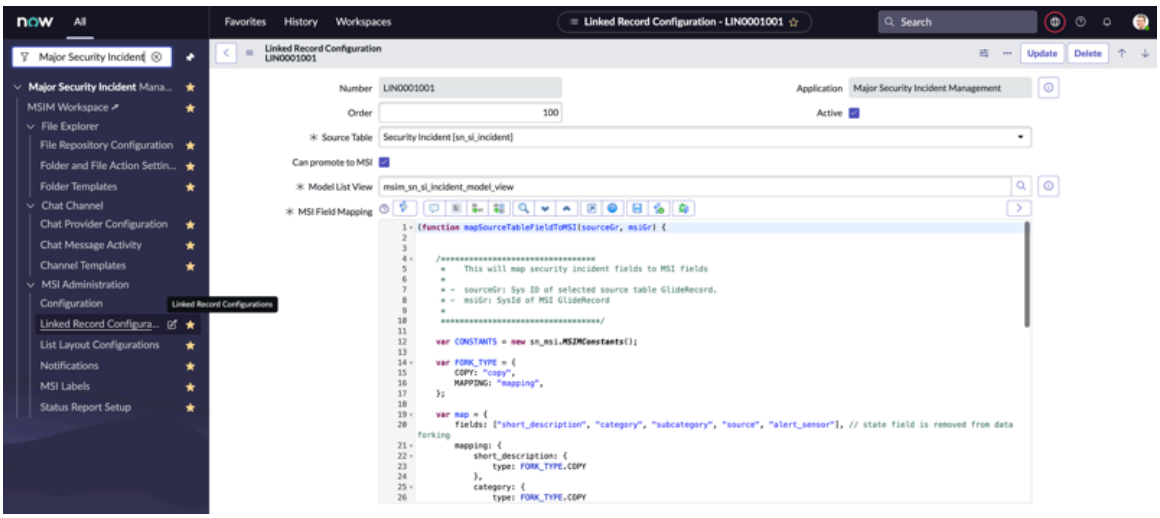



2. Klicken Sie auf der Seite „Konfiguration verknüpfter Datensätze“ auf **Neu**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Stellen Sie sicher, dass sich die Anwendung im Bereich Management schwerwiegender Sicherheits-Incidents befindet.




3. Füllen Sie die Felder des Datensatzkonfigurationsformulars aus.

### Feldbeschreibungen für verknüpfte Datensätze

| Feld | Beschreibung |
|---|---|
| Quelltabelle | Gibt die Aufgabentabelle an, für die verknüpft werden muss und für die ein Rollup zu Major Security Incidentdurchgeführt werden muss. |
| Reihenfolge | Ermöglicht die Steuerung der Reihenfolge der aktuellen Quelltabelle in der Dropdown-Liste des MSIM-Arbeitsbereichs. Nachfolgend sehen Sie ein Beispiel für die **Reihenfolge**.<br><br>Siehe Abbildung 1 unten, die nach dieser Tabelle bereitgestellt wird. |
| Modell-ListView | Wählen Sie eine Ansicht aus, die das Listenlayout steuern kann, das in der modalen Liste für verknüpfte Datensätze angezeigt wird. |
| Kann heraufstufen zu MSI | Aktivieren Sie diese Checkbox, um zu bestätigen, ob der Datensatz ein primärer Datensatz ist. Nachfolgend finden Sie ein Beispiel für die Auswahl der Option **Kann zu MSI** heraufstufen.<br><br>Weitere Informationen finden Sie in der folgenden Abbildung 2, die nach dieser Tabelle bereitgestellt wird.<br><br>Wenn diese Checkbox aktiviert ist und der Wert truelautet, gilt Folgendes:<br><br>○ können Sie einen Quelldatensatz mithilfe der klassischen Umgebungsaktionen mit zusätzlichen Konfigurationen direkt |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | vorschlagen und zu Major Security Incident heraufstufen.<br>○ können Sie Quelldatensätze mit schwerwiegenden Security Incidents sowohl aus der klassischen -Umgebung als auch aus dem MSIM -Arbeitsbereich verknüpfen.<br>○ Management schwerwiegender Sicherheits-Incidents Auf der verknüpften Datensatzseite des -Arbeitsbereichs werden die Datensätze der verknüpften Quelltabelle angezeigt.<br>**Hinweis:**<br>Wenn ein Datensatz direkt als Major Security Incidentvorgeschlagen/heraufgestuft werden kann, ist dieser Datensatz ein primärer Datensatz. Zum Beispiel ist in der Tabellenkonfiguration der Sicherheitsreaktionsaufgabe der Wert von **Kann zu MSI heraufstufen** false, da Sie die Sicherheitsreaktionsaufgabe nicht direkt zu Major Security Incidentheraufstufen können. Daher wird er nicht in der Dropdown-Liste der Registerkarte „Verknüpfter Datensatz“ des Arbeitsbereichs MSIM angezeigt. |
| MSI Feldzuordnung | Schreiben Sie ein Skript, um die Quelldatensatzfelder einem neu erstellten schwerwiegenden Security Incident zuzuordnen, wenn der Datensatz der Quelltabelle vorgeschlagen oder heraufgestuft wird.<br>Dieses Skript wird nur ausgeführt, wenn der Wert **„Kann zu MSI heraufstufen“ auf „** wahr“ festgelegt ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Abbildung 1: Anzeigereihenfolge der Liste „Verknüpfte Datensätze“.**

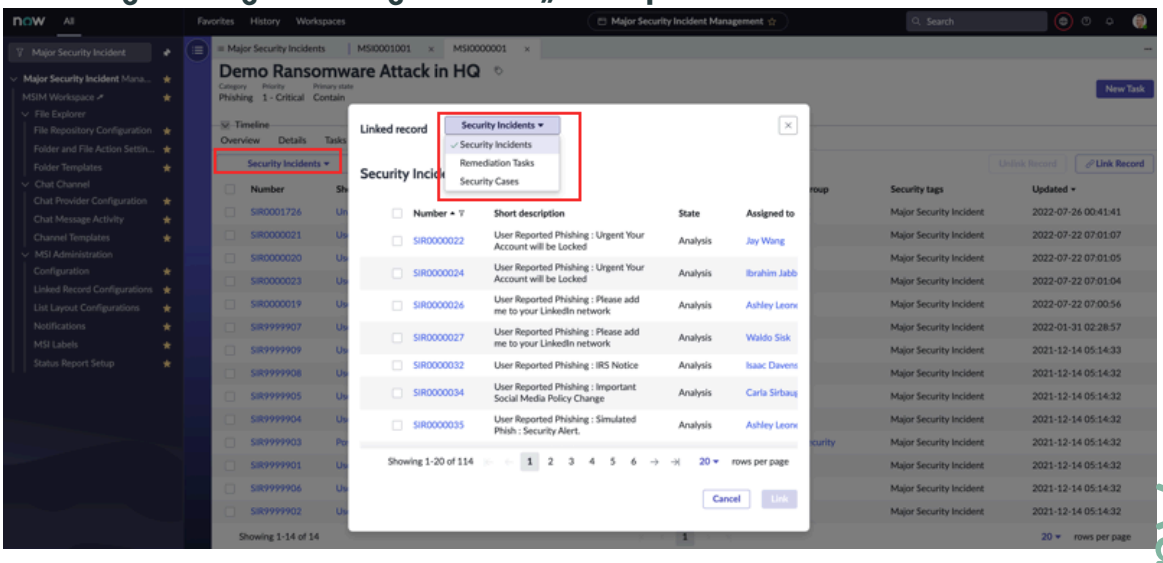
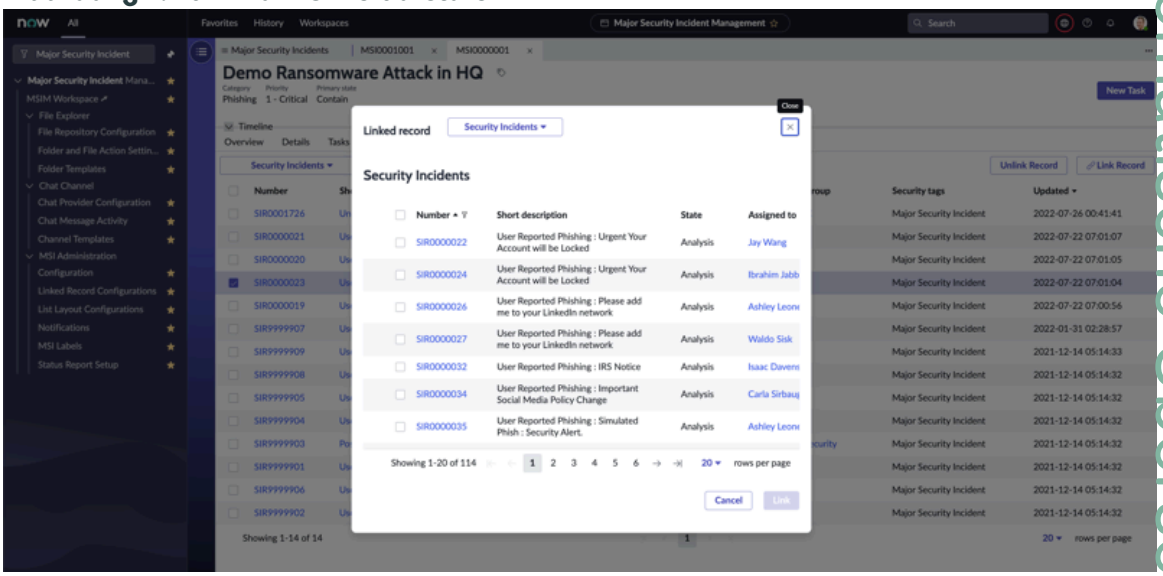



**Abbildung 2: Kann zu MSI heraufstufen**




Automatische Übersetzung

## Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents, um die Informationen zu steuern, für die ein Rollup durchgeführt wird, wenn der Quelldatensatz als schwerwiegende Security Incidents verknüpft/vorgeschlagen/heraufgestuft wird.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

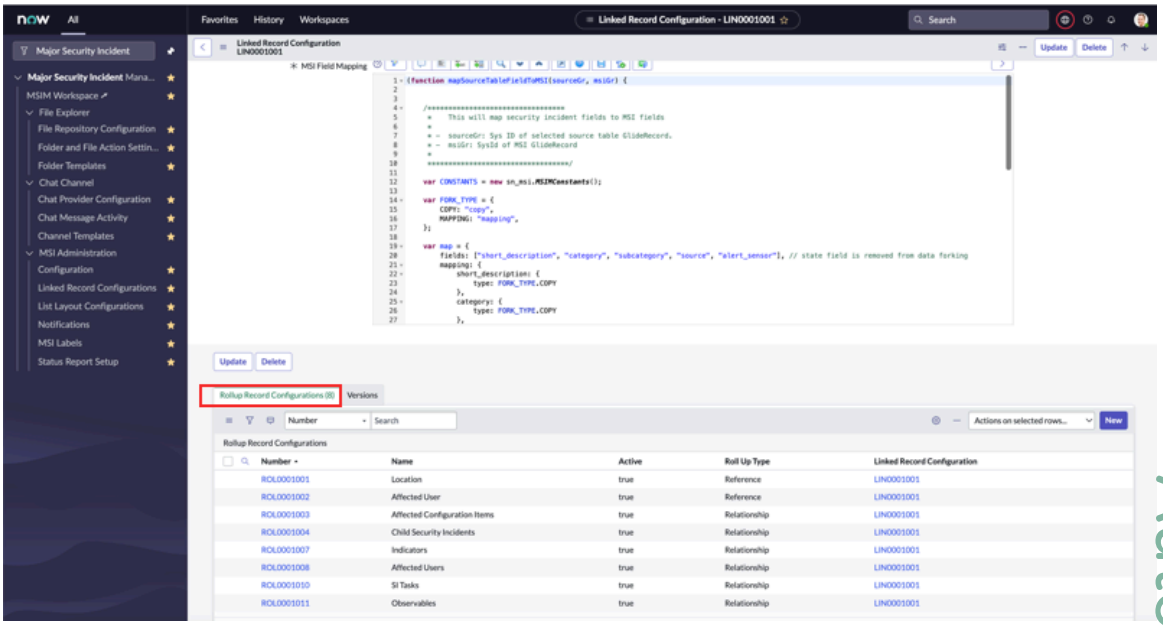
**Hinweis:**
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

### Prozedur

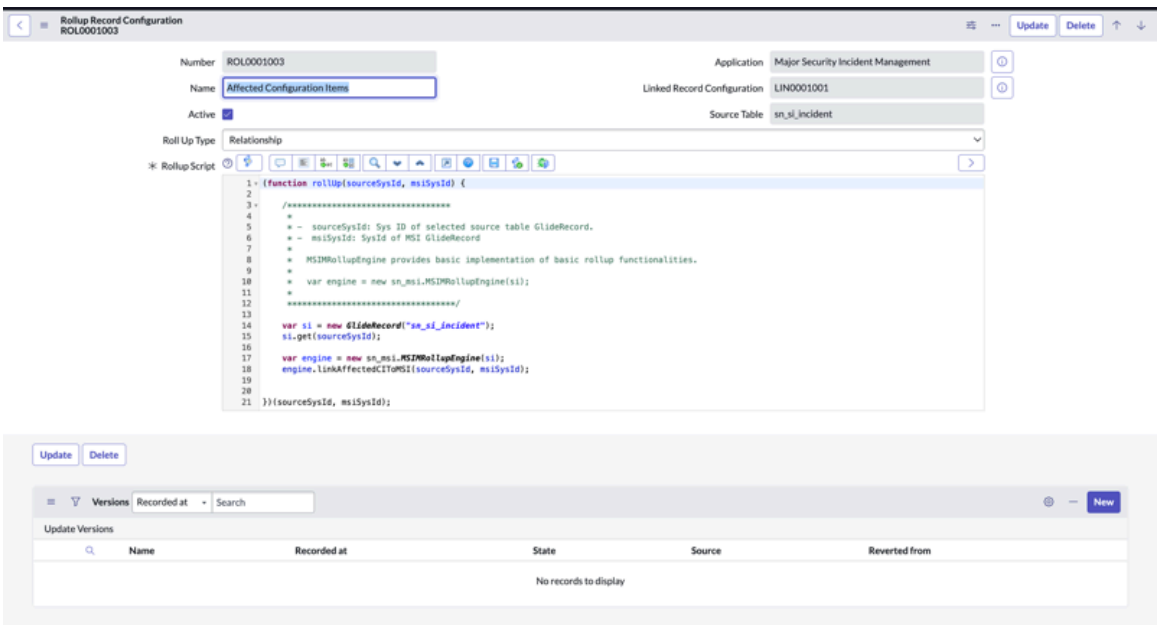
1. Navigieren zu **Reaktion auf schwerwiegende Security Incidents** > **Konfiguration verknüpfter Datensätze**. Die Seite „Konfigurationen verknüpfter Datensätze“ wird angezeigt.
2. Wählen oder erstellen Sie einen neuen verknüpften Datensatz, und navigieren Sie auf derselben Seite zum Abschnitt **Rollup-Datensatzkonfiguration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Abschnitt „Rollup-Datensatzkonfiguration“.**




3. Klicken Sie auf **Neu**.




4. Füllen Sie auf der Konfigurationsseite die Details aus.

**Konfiguration von Rollup-Datensätzen**

| Feldname | Feldbeschreibung |
|---|---|
| Name | Gibt den Namen des Rollup-Datensatzes an. |
| Aktiv | Aktivieren Sie dieses Kontrollkästchen, um die aktuelle Konfiguration zu implementieren, wenn ein Rollup des Quelldatensatzes erfolgt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feldname | Feldbeschreibung |
|---|---|
| Konfiguration verknüpfter Datensätze | Gibt eine eindeutige Nummer an, die sich auf die Konfiguration der übergeordneten verknüpften Datensätze bezieht und schreibgeschützt ist. |
| Quelltabelle | Der in der Konfiguration des verknüpften Datensatzes verwendete Quelltabellenname, der schreibgeschützt ist. |
| Rollup-Typ | Beschreibt die Art der Informationen, für die ein Rollup durchgeführt werden soll.<br>○ **Beziehung**: Wählen Sie diese Option aus, wenn die Daten als zugehörige Liste vorhanden sein müssen.<br>○ **Referenz**: Wählen Sie diese Option aus, wenn die Daten als Referenzfeld im Quelltabellenformular vorhanden sind. |
| Rollup-Skript | Wenn der Rollup-Typ „ **Beziehung**“ lautet, ist das Feld **Rollup-Skript** aktiviert, sodass Sie ein Skript schreiben und Informationen zusammenfassen können.<br>Hier erhält das Skript die Eingaben, die Informationen des Quelldatensatzes und des schwerwiegenden Security Incident enthalten. Das Skript sollte in der Lage sein, die Informationen aus den Beziehungstabellen zu finden und ein Rollup in die Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) durchzuführen. |
| Quellfeld | Wenn der Rollup-Typ **Referenz**ist, ist das **Quellfeld** verfügbar. Dadurch können Sie das Referenzfeld Quelltabelle auswählen, das die Informationen enthält, für die ein Rollup durchgeführt werden muss. |
| Zielfeld | Wenn der Rollup-Typ **Referenz**ist, ist das **Zielfeld** verfügbar. Dadurch können Sie auf das Referenzfeld aus der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) verweisen und die Daten speichern, die im ausgewählten Quellfeld und im Datensatz der Quelltabelle vorhanden sind. |

### Skript für Rollup wird geschrieben

| Name | Beschreibung |
|---|---|
| Eingaben | • sourceSysId: Sys-ID des Quelltabellendatensatzes, der entweder verknüpft/vorgeschlagen/heraufgestuft wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

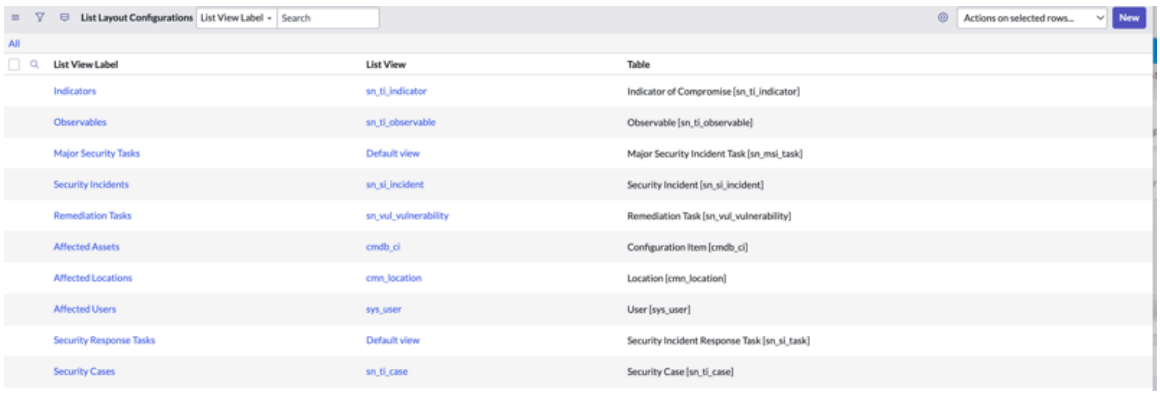
| Name | Beschreibung |
|---|---|
| | • msiSysId: Sys-ID des schwerwiegenden Security Incident, mit dem der Quelldatensatz verknüpft/vorgeschlagen/ heraufgestuft wird. |
| Ausgabe | Kein Ausgaberückgabewert. |
| Verantwortlichkeit | Das Skript sollte Informationen in der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_child) zusammenfassen.<br>• Verwenden Sie sourceSysID, um Daten aus ServiceNow Beziehungstabellen abzufragen.<br>• Nachdem die Daten abgerufen wurden, führen Sie ein Rollup der Daten zu einem verknüpften Datensatz (sn_msi_m2m_child) durch, indem Sie das Dienstprogramm MSIRollupEngine verwenden, um ein Rollup für Daten durchzuführen. |

### Konfigurieren Sie das Listenlayout in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie das Listenlayout, um das Layout und die Bezeichnungen anzupassen, die im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents verwendet werden, z. B. die Registerkarten „Incident-Auswirkung“, „Verknüpfte Datensätze“ und „Threat Intelligence“.

Erforderliche Rolle: admin und sn_msi.workspace_admin.

**Hinweis:**
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.



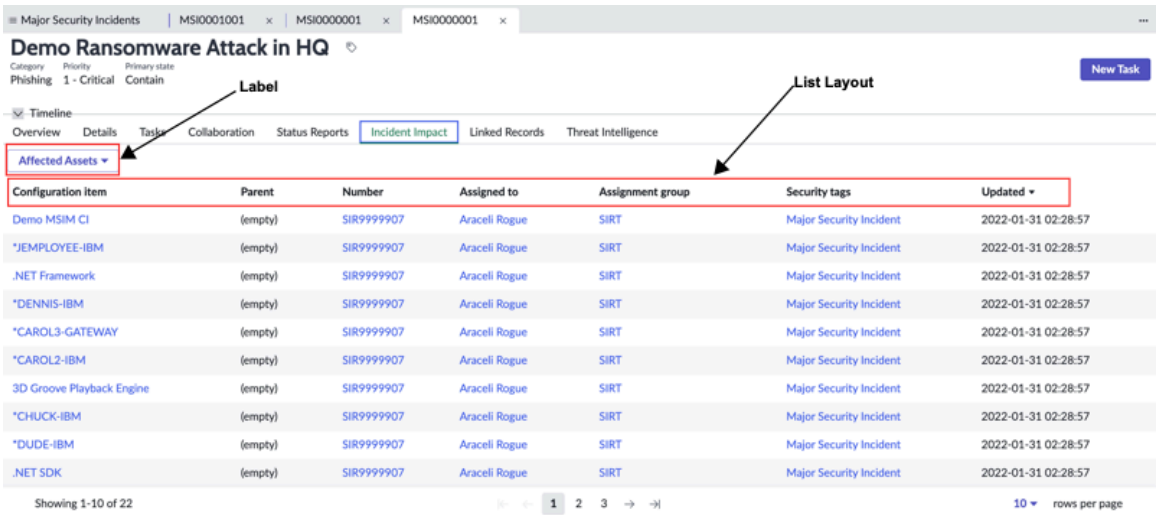

Die Listenlayoutkonfigurationen wurden bereits für vorhandene bekannte Tabellen ausgeliefert, die im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents angezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

- Wenn Sie die benutzerdefinierte Ansicht für die vorhandenen Tabellen rendern möchten, können Sie den entsprechenden Tabellendatensatz in der Listenlayoutkonfiguration mit der benutzerdefinierten Listenansicht aktualisieren.
- Für neue Aufgabentabellen können Sie eine neue Listenlayoutkonfiguration erstellen, um die benutzerdefinierte Listenansicht und Bezeichnungen zu rendern. Eine detailliertere Vorgehensweise finden Sie unter Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte „Verknüpfter Datensatz“ für einen Sicherheitsfall




### Rollup-Beispiel-Anwendungsfallimplementierung für einen Sicherheitsfall

In den folgenden Schritten wird ein Beispiel-Anwendungsfall erläutert, in dem erläutert wird, wie Unterstützung hinzugefügt wird, um die Tabelle „Schwerwiegender Security Incident“ für eine Sicherheitsfalltabelle zu verknüpfen/vorzuschlagen/hochzustufen.

- Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall
- Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall
- Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall
- Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte „Verknüpfter Datensatz“ für einen Sicherheitsfall
- Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsbenutzer hinzu
- Schritt 6. Business Rules für einen Sicherheitsfall erstellen
- Schritt 7. Rollup-Datensatzkonfigurationen erstellen

### Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall

Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall.

**Vorbereitungen**
Erforderliche Rolle: admin und sn_msi.workspace_admin

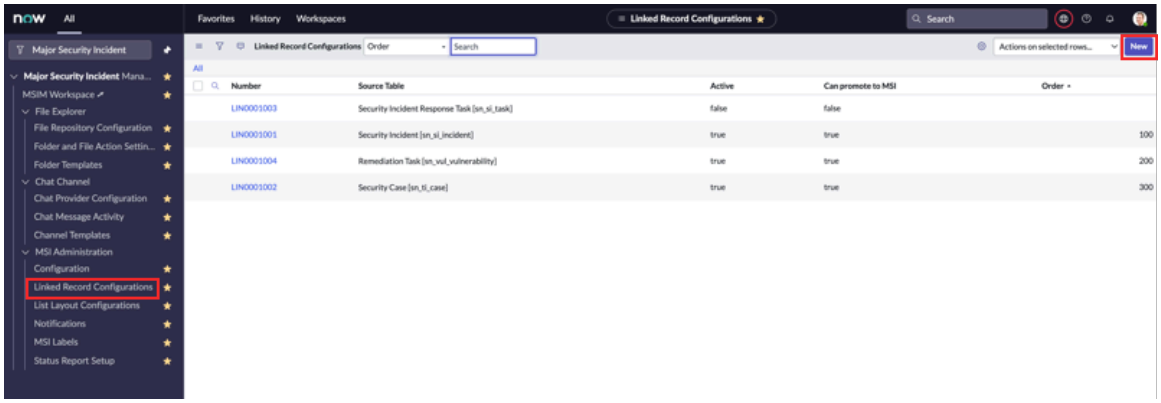
**Hinweis:**
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Automatische Übersetzung

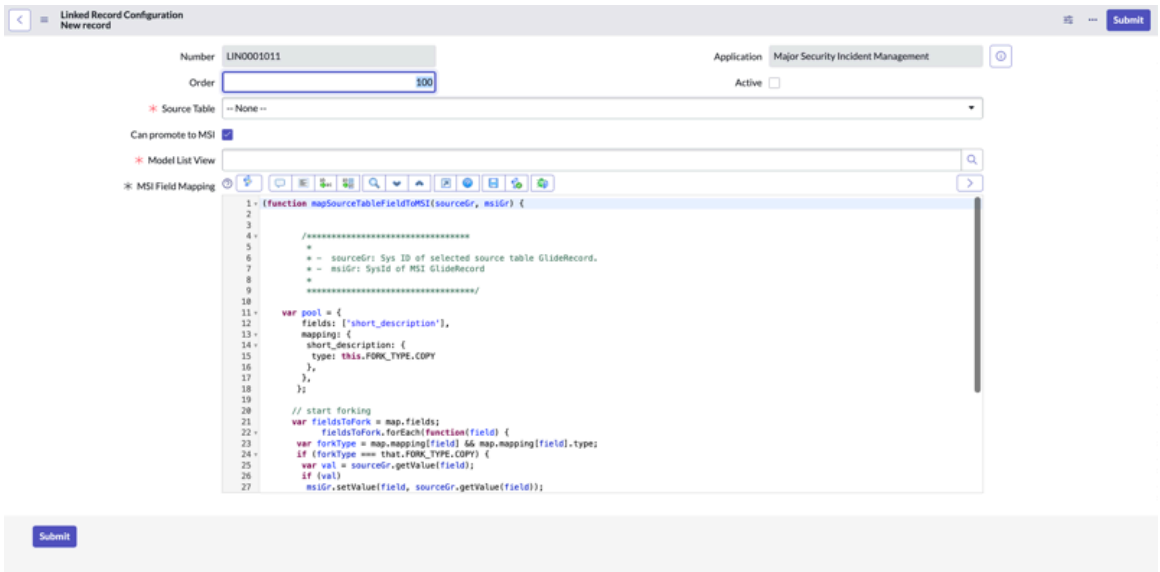
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Suchen Sie im linken Navigationsbereich nach der Konfiguration verknüpfter Datensätze.
2. Klicken Sie auf **Neu**.



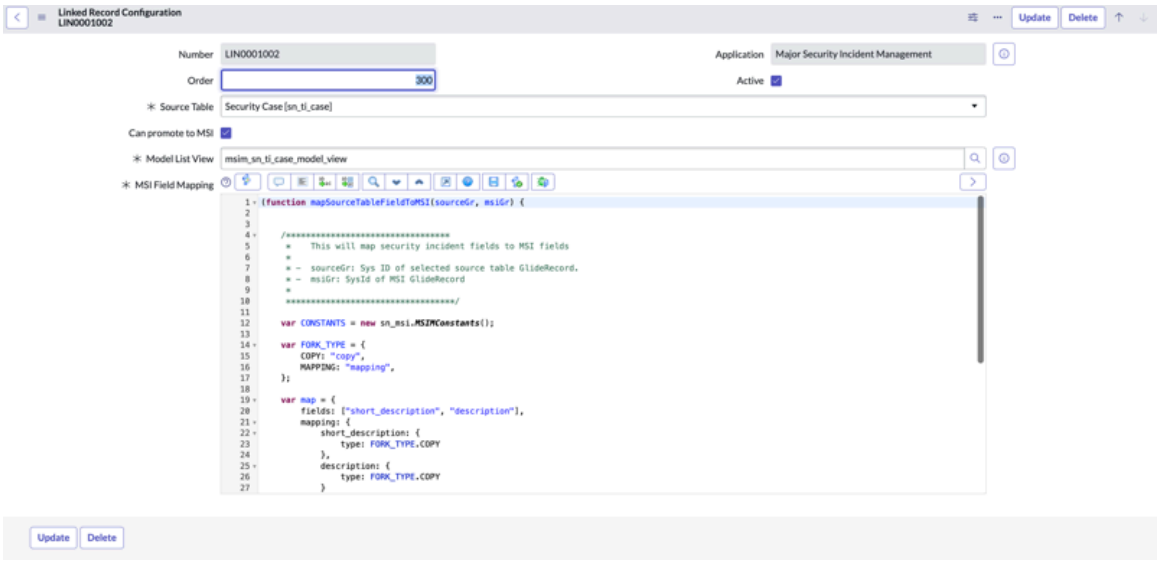

3. Füllen Sie das Formular mit den erforderlichen Spalten aus, und schreiben Sie ein Feldzuordnungsskript.




4. Sie haben jetzt eine verknüpfte Datensatzkonfiguration für den Sicherheitsfall erstellt, indem Sie die in der folgenden Tabelle beschriebenen Werte hinzugefügt haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




| Name | Beschreibung |
|---|---|
| Quelltabelle | Sicherheitsfall (sn_ti_case). Hier in diesem Beispiel wird ein Sicherheitsfall als MSI verknüpft/heraufgestuft/vorgeschlagen. |
| Reihenfolge | Eingabewert: 300<br>**Hinweis:**<br>Niedrigere Reihenfolgen haben Vorrang vor höheren Reihenfolgen. Da ein Sicherheitsfall eine höhere Reihenfolge hat als der Security Incident und die Korrekturaufgabe, wird er in der letzten Reihenfolge angezeigt. |
| Hochstufen zu MSI möglich | True, aktivieren Sie diese Checkbox, um den Sicherheitsfall an MSI hochzustufen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>○ Verknüpfung von Sicherheitsfalldatensätzen mit schwerwiegenden Security Incidents im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents herstellen bzw. aufheben Außerdem ist die Funktion zum Aufheben der Datensatzverknüpfung nur für die verknüpften Datensätze sichtbar.<br>▪ Dadurch wird das Verknüpfen, Heraufstufen und Vorschlagen eines Sicherheitsfalls zu einem schwerwiegenden Security Incident mithilfe klassischer Umgebungsaktionen ermöglicht, diese UI-Aktionen sind jedoch nicht sofort einsatzbereit. Jede UI-Aktion muss manuell erstellt werden. Weitere Informationen finden Sie unter Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall.<br>▪ Die UI-Aktionen Verknüpfen/ Heraufstufen/Vorschlagen sind für Security Incident, Korrekturaufgabe und Sicherheitsfall sofort einsatzbereit.<br>○ Auf der verknüpften Datensatzseite des MSIM-Arbeitsbereichs werden die verknüpften Sicherheitsfalldatensätze angezeigt.<br>In der folgenden Abbildung 1 sehen Sie die Optionen, die nach Aktivieren dieses Kontrollkästchens verfügbar sind. |
| Modale Listenansicht | msim_sn_ti_case_model_view<br>**Hinweis:**<br>Diese Ansicht enthält Felder und die Feldreihenfolge, die in der Listenansicht im modalen Fenster „Linkdatensatz“ im MSIM-Arbeitsbereich angezeigt werden. Weitere Informationen finden Sie unter Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall<br>Sehen Sie sich die folgende Abbildung 2 an, um sie auf der Seite „ **Verknüpfte Datensätze** “ anzuzeigen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Beschreibung |
| --- | --- |
| Feldzuordnungsskript | Dieses Skript beschreibt die Felder aus Quelltabellendatensätzen, die neu erstellten schwerwiegenden Security Incidents zugeordnet werden, wenn Quelltabellendatensätze vorgeschlagen oder heraufgestuft werden.<br><br>, der Eingaben erhält:<br><br>○ sourceGr: Glide-Datensatzobjekt für Sicherheitsfall<br>○ msiGr: Glide-Datensatzobjekt für schwerwiegende Security Incidents<br><br>Das Skript liest die Kurzbeschreibung des Sicherheitsfalls und kopiert sie als Titel für den schwerwiegenden Security Incident. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bild 1: Kann zu MSI heraufstufen**

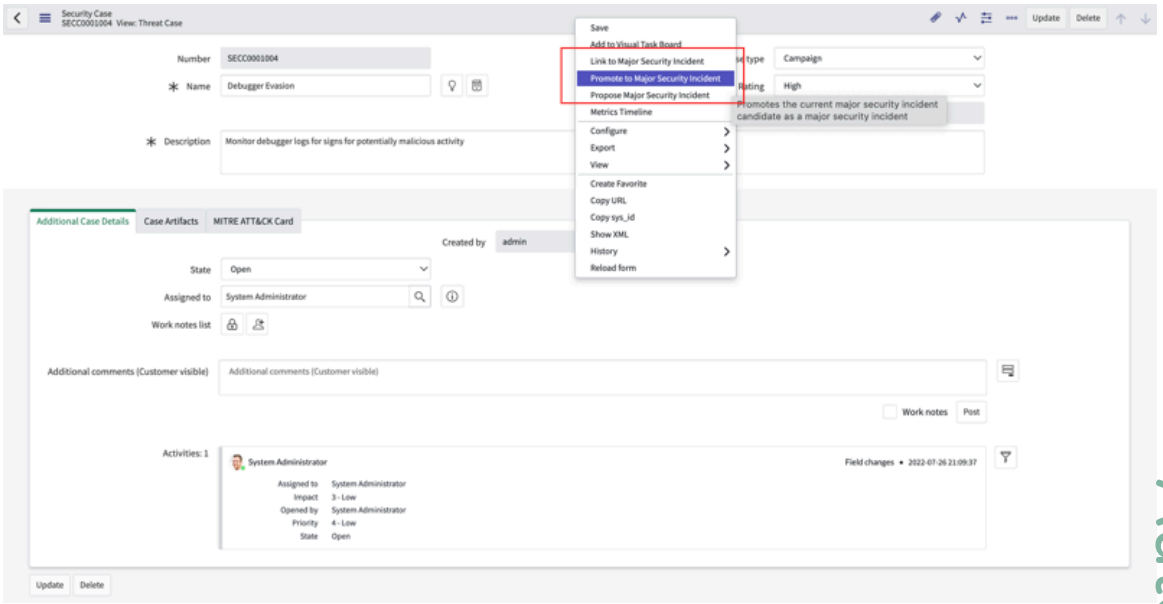
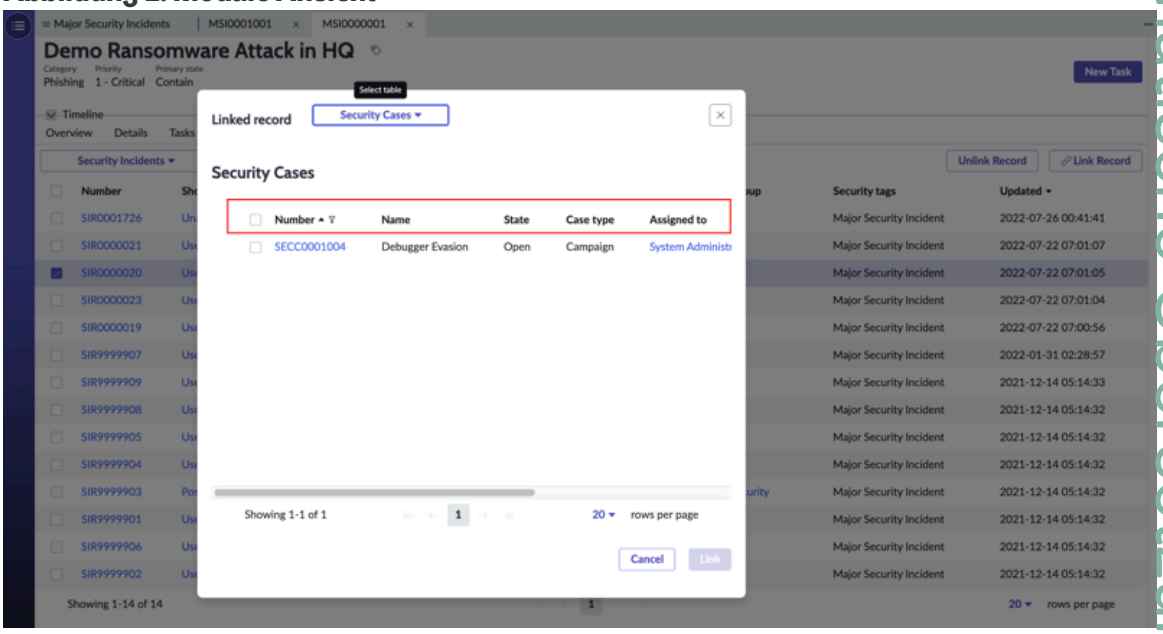



**Abbildung 2. Modale Ansicht**




## Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall

Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall.

### Vorbereitungen

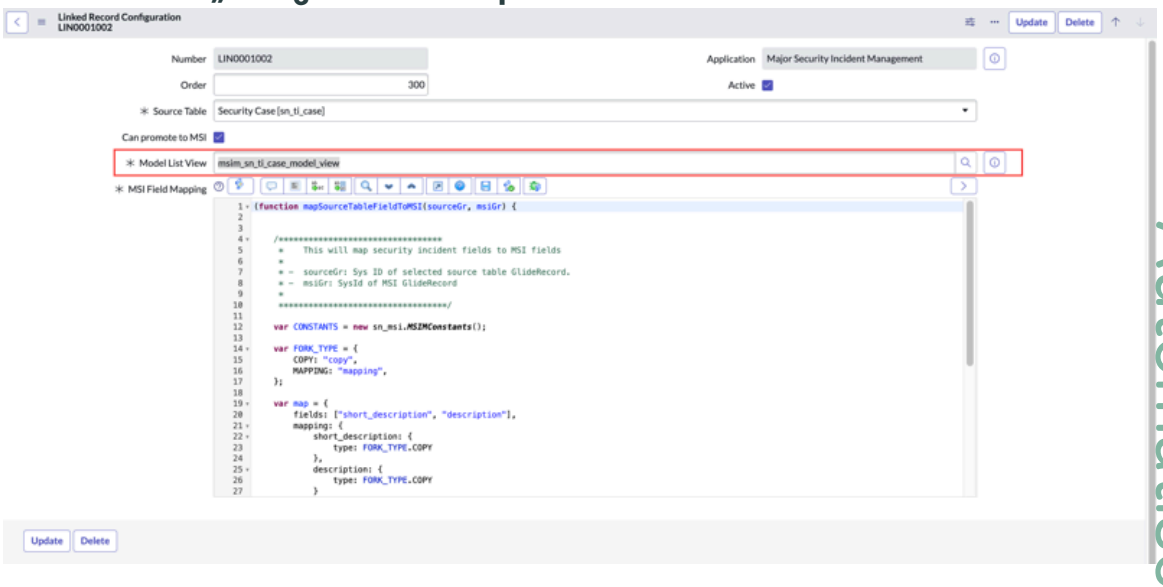
**Wichtige Überlegung:**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standardmäßig wird in der modalen Liste des verknüpften Datensatzes nur das **Standardlistenlayout** angezeigt. Wenn Sie das Listenlayout anpassen möchten, können Sie die **benutzerdefinierte Ansicht** in der Quelltabelle verwenden.
- Wenn Sie die benutzerdefinierte Ansicht rendern möchten, muss die benutzerdefinierte Ansicht auch in der Konfiguration des verknüpften Datensatzes für die Quelltabelle ausgewählt werden.

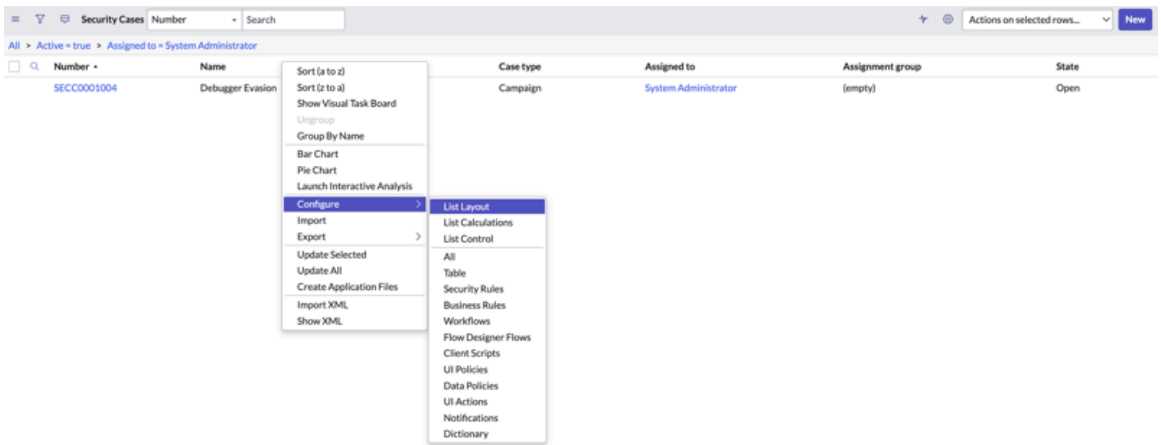
**Modale Ansicht „Konfiguration verknüpfter Datensätze“ für Quelltabelle**




Erforderliche Rolle: admin

## Prozedur

1. Wechseln Sie zur Quelltabelle, und klicken Sie auf **Konfigurieren** > **Listenlayout**.




2. Gehe zu **Listenansicht** > **Namen anzeigen**.
3. Klicken Sie in der Dropdown-Liste Name der Ansicht auf **Neu**, und erstellen Sie eine neue Ansicht, z. B. msim_sn_ti_case_modal_view.
4. Wählen Sie die neu erstellte Ansicht aus.
   Nach der Auswahl können Sie die erforderlichen Felder aus der Liste Verfügbar auswählen.
5. Klicken Sie auf **Speichern**.
6. Navigieren zu **Menü** > **Ansichten** , um zu überprüfen, ob die Ansicht ordnungsgemäß gerendert wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall

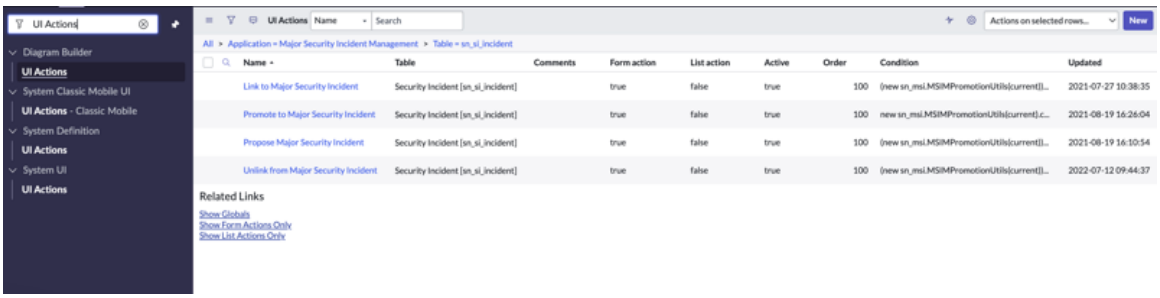
Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall.

**Vorbereitungen**

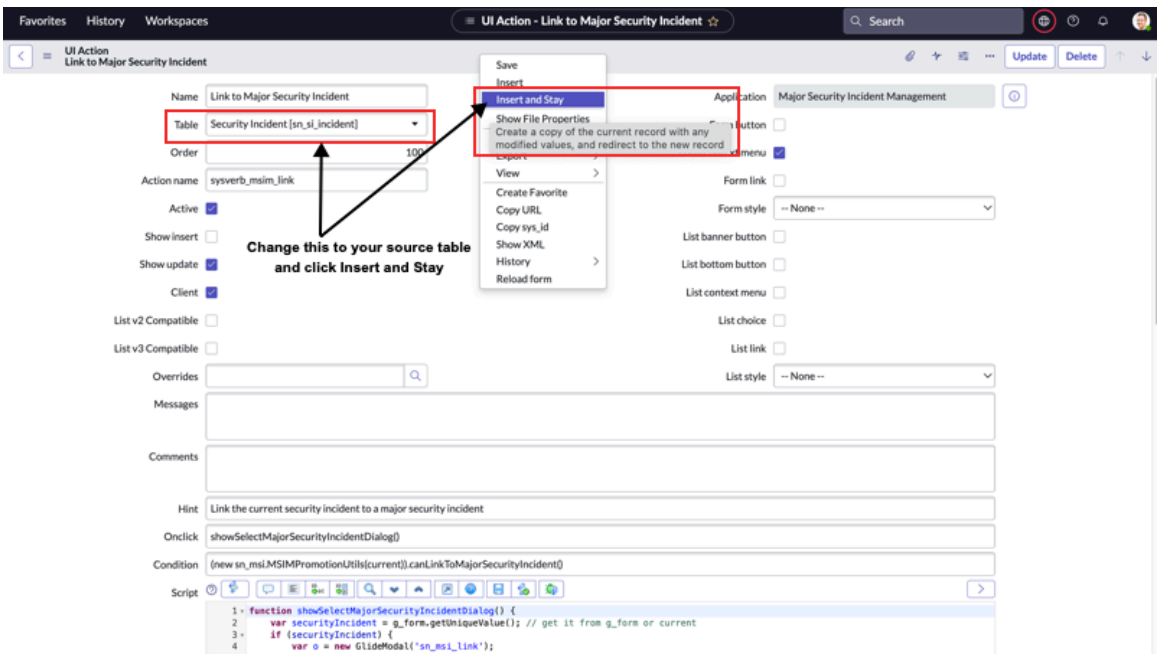
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren zu **Systemdefinition** > **UI-Aktionen**.
2. Führen Sie die Option Filter aus, um die Liste nach **Anwendung**: Major Security Incident Management und **Tabelle**: sn_si_incident zu filtern.




3. Wählen Sie jede UI-Aktion nacheinander aus, und speichern Sie die Details für die Quelltabelle.




4. Wiederholen Sie die gleichen Schritte wie oben für die folgenden UI-Aktionen:
   - Link zu Schwerwiegender Security Incident
   - Vorgeschlagener schwerwiegender Security Incident
   - Verknüpfung mit schwerwiegendem Security Incident aufheben
   - Zu schwerwiegendem Security Incident heraufstufen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

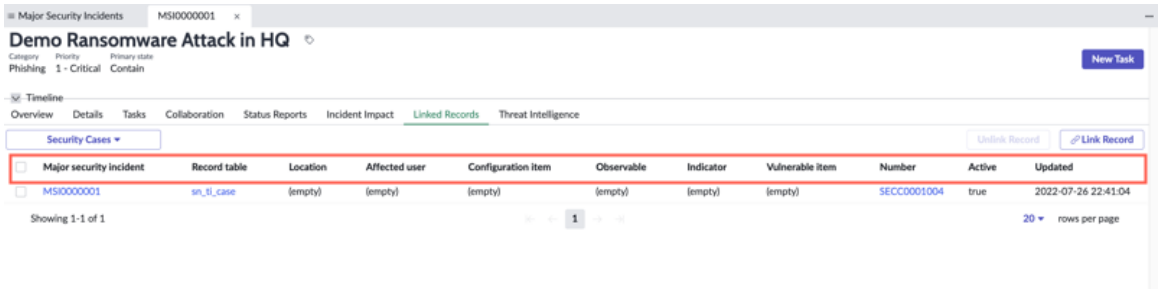
### Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte „Verknüpfter Datensatz“ für einen Sicherheitsfall

Passen Sie das Listenlayout für eine Sicherheitsfalltabelle an, wenn sie auf der Seite „Datensätze verknüpfen“ mit dem Arbeitsbereich Management schwerwiegender Sicherheits-Incidents angezeigt wird.

## Vorbereitungen

**Voraussetzungen:**

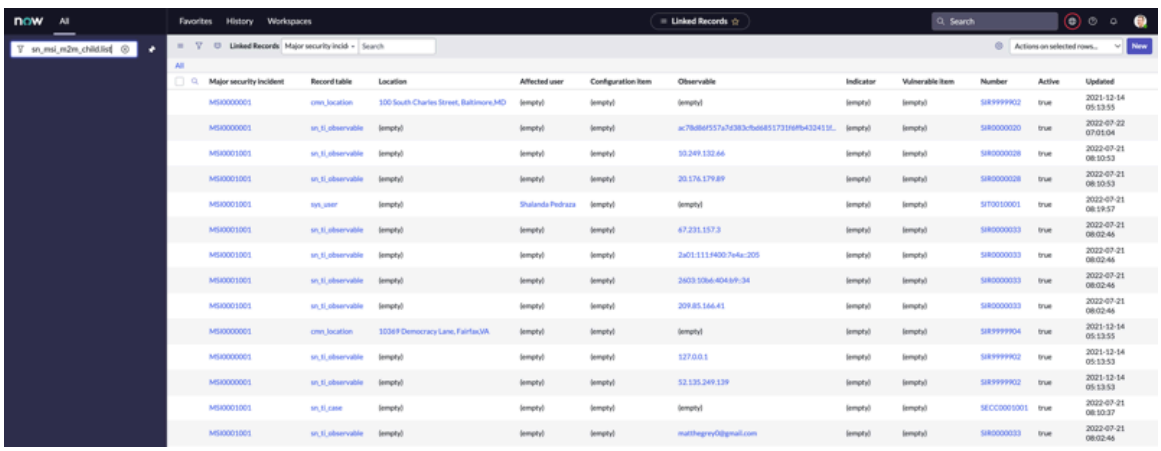
- Wählen Sie die Spalte aus, die sichtbar sein soll, wenn eine Liste für eine Sicherheitsfalltabelle gerendert wird.
- Wählen Sie die Reihenfolge der Felder aus, die in der Dropdown-Liste angezeigt werden sollen.




Erforderliche Rolle: admin

## Prozedur

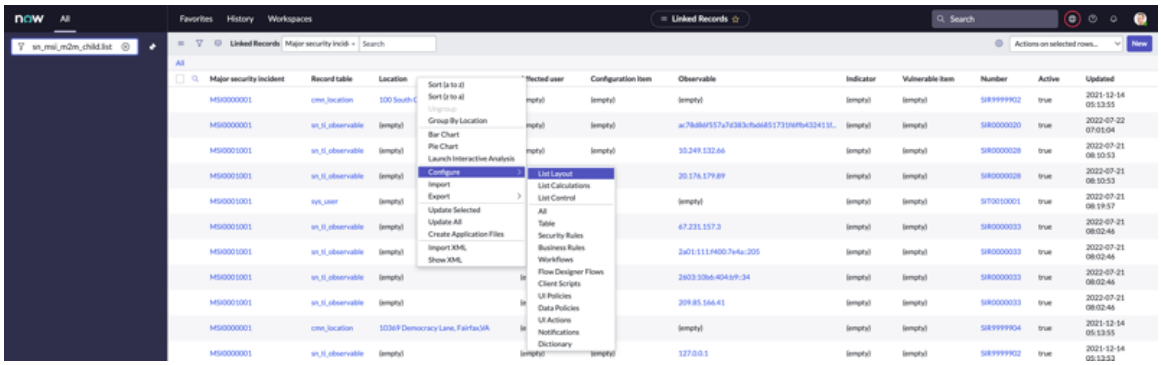
1. Suchen Sie mithilfe der linken Navigation nach **sn_msi_m2m_child.list**.
   Die Tabelle „Verknüpfte Datensätze“ wird angezeigt.



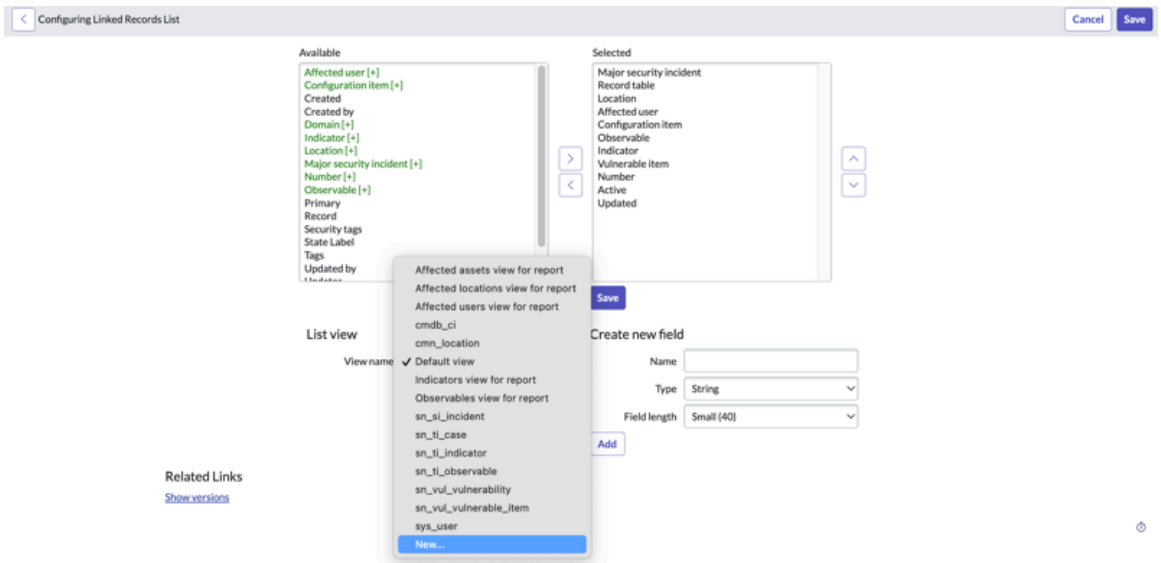
2. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Konfigurieren** > **Listenlayout**.
   Die Seite „Liste der verknüpften Datensätze konfigurieren“ wird angezeigt.



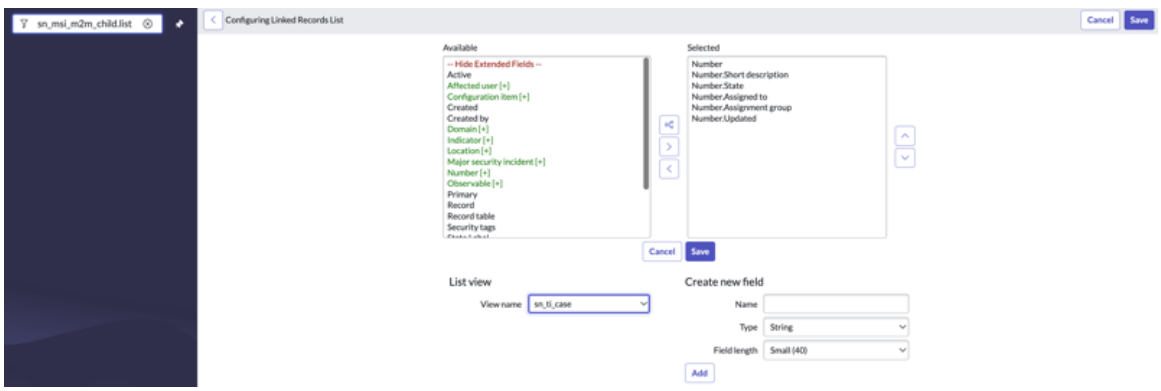
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Gehe zu **Listenansicht** > **Namen anzeigen**.
4. Wählen Sie in der Dropdown-Liste Name anzeigen die Option **Neu** aus.



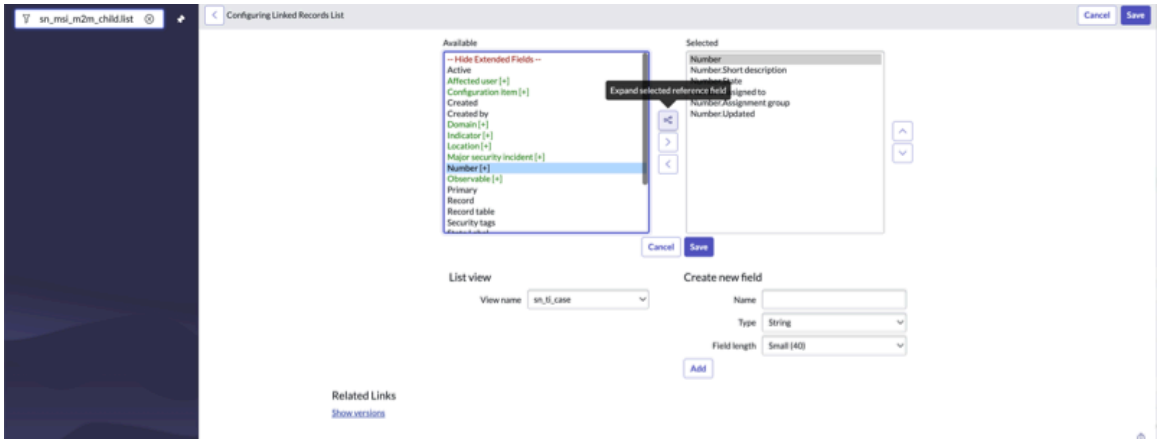

5. Wählen Sie die Spalten aus, die in der Listenansicht des Arbeitsbereichs gerendert werden sollen. Der Sicherheitsfalldatensatz wird in der Spalte **Nummer** gespeichert. Um Informationen aus einem Sicherheitsfall darzustellen, müssen Sie einen Dot-Walk in der Spalte **Nummer** durchführen.



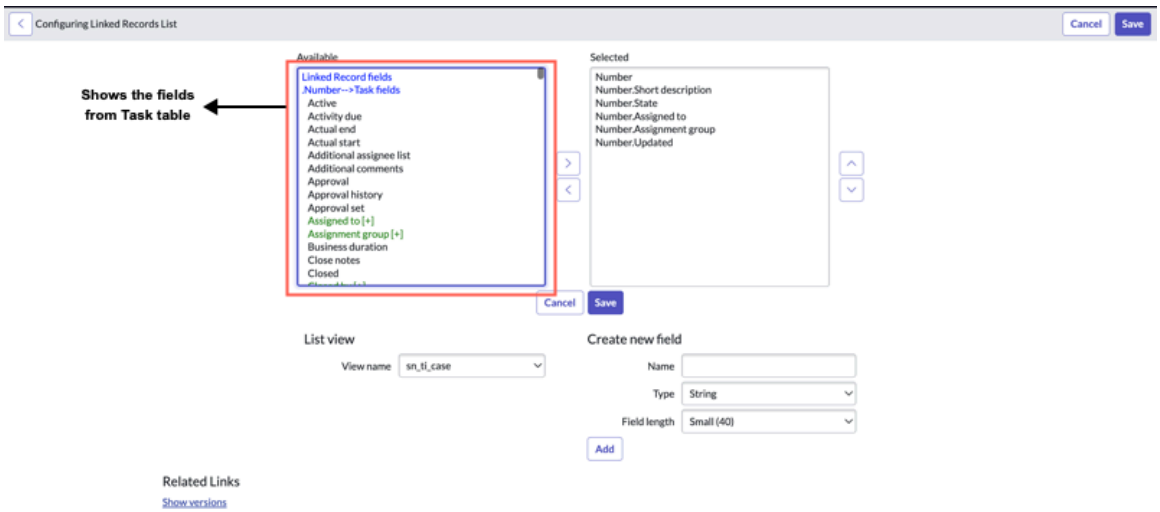



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wählen Sie für Dot-Walk zuerst die Spalte **Nummer** aus der Liste Verfügbar aus, und klicken Sie dann auf **Ausgewähltes Referenzfeld erweitern**.




**b.** Erweitern Sie die Spalten von **Nummer**, um sie auszuwählen, und verschieben Sie sie in die Liste Ausgewählt.




**c.** Klicken Sie auf **Speichern**, um zu speichern und eine Ansicht zu erstellen.

**6.** Der nächste Schritt besteht darin, die erstellte Ansicht im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents zu rendern. Sie müssen eine **Listenlayoutkonfiguration**erstellen.

**a.** Suchen Sie mithilfe der linken Navigation nach der **Listenlayoutkonfiguration**.

**b.** Klicken **MSI-Administration** > **Listenlayoutkonfigurationen**.

**c.** Klicken Sie auf **Neu**, um eine neue Konfiguration zu erstellen.

**d.** Wählen Sie die Quelltabelle aus der Spalte Tabelle und die neu erstellte Ansicht aus dem Feld Listenansicht aus.

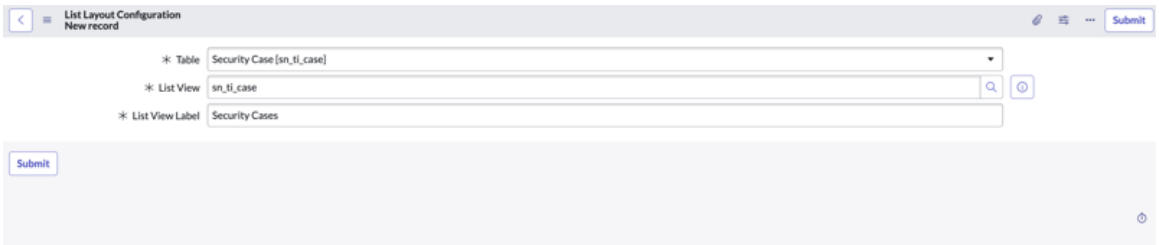
**e.** Mit der Bezeichnung Listenansicht können Sie Bezeichnungen steuern, wenn dieselbe **Quelltabelle** im Arbeitsbereich Management schwerwiegender Sicherheits-Incidents gerendert wird.

**f. Speichern Sie** den Datensatz.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Nachdem der Datensatz gespeichert wurde, navigieren Sie zum Arbeitsbereich Management schwerwiegender Sicherheits-Incidents, um die gerenderte Listenansicht und Bezeichnung im Arbeitsbereich anzuzeigen.




### Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsbenutzer hinzu

Fügen Sie Zugriffskontrolllisten (ACLs) für Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsbenutzer hinzu.

#### Vorbereitungen
Erforderliche Rolle: admin

**Hinweis:**
Die zum Verknüpfen und Aufheben der Verknüpfung erforderlichen Berechtigungen werden von der Rolle sn_msi.linkedsivi_read gesteuert.

Management schwerwiegender Sicherheits-Incidents Persona enthält die Rolle „sn_msi.linkedsivi_read“.

1. sn_msi.workspace_admin (MSIM Workspace-Administrator)
2. sn_msi.workspace_manager (MSIM-Arbeitsbereichsmanager)
3. sn_msi.workspace_responder (MSIM-Arbeitsbereich-Responder)

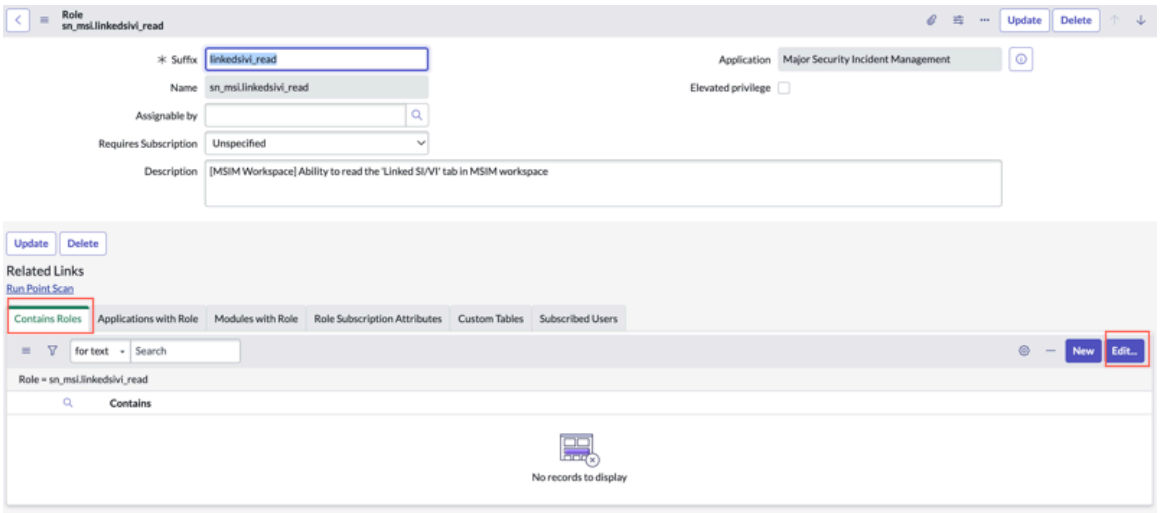
**Hinweis:**
Für jede Quelltabelle müssen Sie sicherstellen, dass die erforderlichen Rollen der Rolle sn_msi.linkedsivi_read hinzugefügt werden.

#### Prozedur

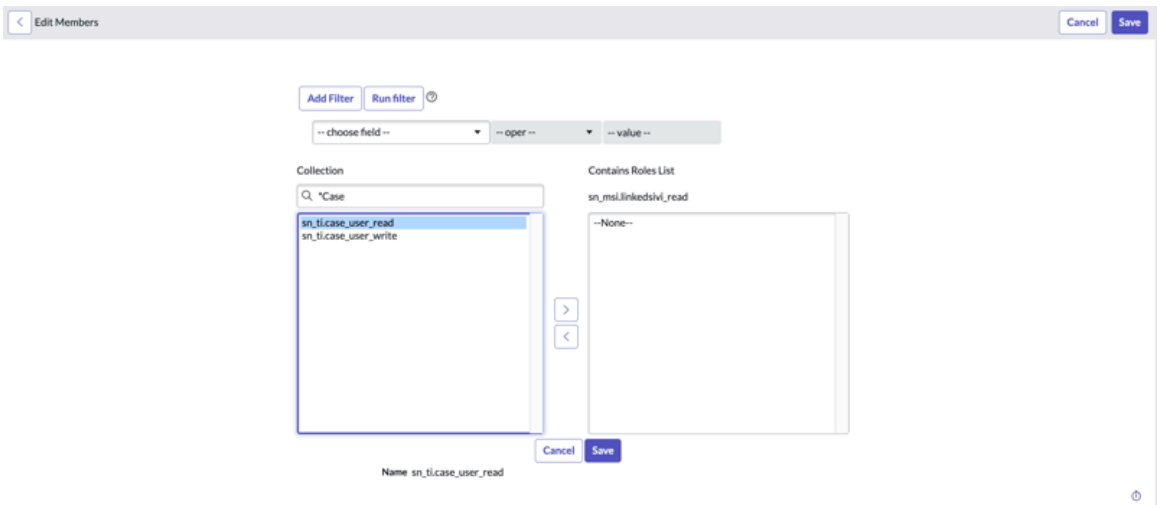
1. Navigieren zu **Benutzeradministration** > **Rollen** und suchen Sie nach der Rolle **sn_msi.linkedsivi_read**.
2. Klicken Sie im Abschnitt „Enthält Rollen“ auf **Bearbeiten**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Stellen Sie sicher, dass Ihre Quelltabellenrollen im Abschnitt „Enthält Rollen“ hinzugefügt werden.
   Die Seite „Mitglieder bearbeiten“ wird angezeigt, um die für einen Sicherheitsfall erforderlichen Rollen zu konfigurieren.




4. Suchen Sie im Abschnitt „Sammlungen“ nach den Quelltabellenrollen.
   Wählen Sie die erforderlichen Rollen aus, die Lese- und Schreibzugriff auf die Quelltabelle für einen Sicherheitsfall zulassen.

**Hinweis:**

- Für einen Sicherheitsfall werden zwei separate Rollen zum Lesen und Schreiben benötigt.
- Schreibzugriff auf Tabellen für die Möglichkeit, den Quelldatensatz aus dem mit dem Management schwerwiegender Sicherheits-Incidents Arbeitsbereich verknüpften modalen Datensatz auszuwählen.

5. Klicken Sie auf **Speichern**, um Rollen hinzuzufügen.
6. Vergewissern Sie sich, dass die Rollen erfolgreich dem zugehörigen Listenabschnitt „ **Enthält Rollen** “ hinzugefügt wurden.

### Schritt 6. Business Rules für einen Sicherheitsfall erstellen

Erstellen Sie die erforderlichen Geschäftsregeln für einen Sicherheitsfall.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vorbereitungen**
Erforderliche Rolle: admin

Erstellen Sie die drei folgenden Geschäftsregeln für die neue Quelltabelle „Sicherheitsfall“ (sn_ti_case). Diese Geschäftsregeln sind erforderlich, um die Konsistenz des Verhaltens mit der vordefinierten Quelltabelle wie Security Incident (sn_si_incident) zu gewährleisten.

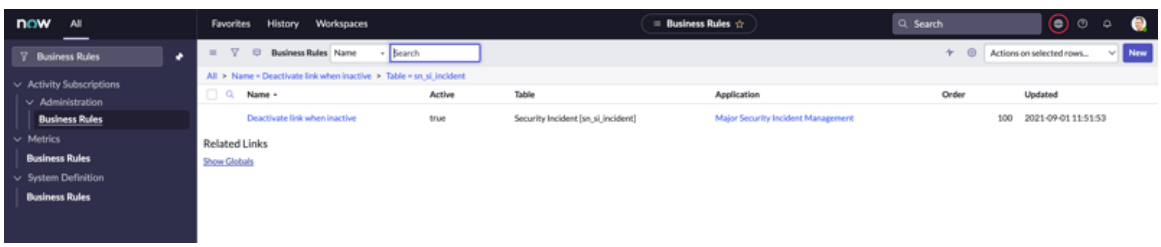
Geschäftsregeln für die neue Quelltabelle:

1. **Link deaktivieren, wenn inaktiv**: Sobald der Sicherheitsfall geschlossen ist, werden zugehörige Informationen nicht mehr auf der Arbeitsbereichsseite Management schwerwiegender Sicherheits-Incidents angezeigt.
2. **Teaminformationen bei Aktualisierung synchronisieren**: Die Registerkarte „Schwerwiegender Security Incident – Details“ zeigt die Informationen zu allen aktiven Teams und Benutzern, die an verschiedenen Aufgaben arbeiten. Sobald der zugewiesene Benutzer oder die Zuweisungsgruppe im Sicherheitsfall aktualisiert wurde, müssen die Informationen zum Sicherheitsfallteam im Abschnitt „Aktives Team des schwerwiegenden Security Incidents“ aktualisiert werden. Diese Geschäftsregeln aktualisieren neue zugewiesene Anwender und Zuweisungsgruppen im aktiven Teamabschnitt.
3. **Teaminformationen beim Löschen synchronisieren**: Auf der Registerkarte „Schwerwiegender Security Incident“ werden Informationen zu allen aktiven Teams und Benutzern angezeigt, die an verschiedenen Aufgaben arbeiten. Sobald wir den Sicherheitsfall geschlossen haben, müssen im Abschnitt „Schwerwiegender Security Incident – aktives Team“ keine Informationen zum Sicherheitsfall-Team mehr angezeigt werden. Diese Geschäftsregeln entfernen den zugewiesenen Anwender und die Zuweisungsgruppe aus dem aktiven Team.

**Geschäftsregeln für neue Quelltabelle erstellen:**

**Prozedur**

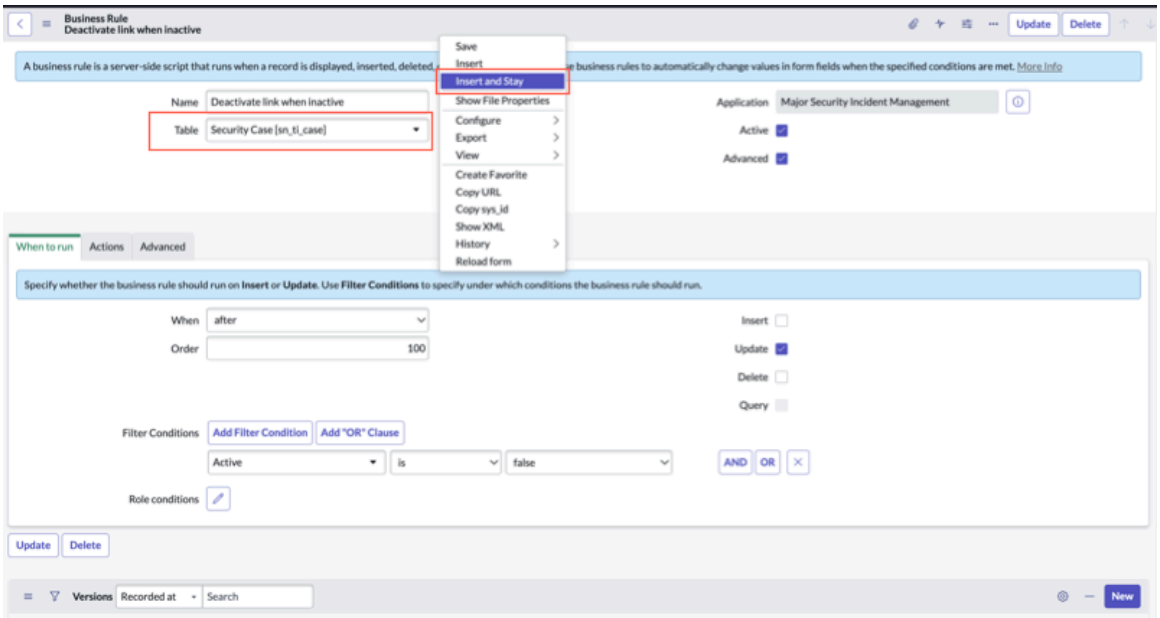
1. Navigieren zu **Systemdefinition** > **Business-Regeln**.
2. Führen Sie die Filteroption aus, um Business Rule-Kriterien mit den folgenden Informationen zu filtern:
   - **Name**: Link deaktivieren, wenn inaktiv
   - **Tabelle**: sn_si_incident




3. Öffnen Sie den Datensatz, und ändern Sie den Tabellennamen in eine neue Quelltabelle: sn_ti_case.
4. Klicken Sie mit der rechten Maustaste auf das Menü auf der Seite, und klicken Sie auf **Einfügen und beibehalten**, um den Datensatz zu erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Wiederholen Sie das Verfahren auch für zwei weitere Business Rules.
   - Teaminformationen beim Löschen synchronisieren
   - Teaminformationen bei Aktualisierung synchronisieren

### Schritt 7. Rollup-Datensatzkonfigurationen erstellen

Erstellen Sie eine Rollup-Datensatzkonfiguration, um zusätzliche Datensätze mit MSI zu verknüpfen und die Verknüpfung aufzuheben.

**Vorbereitungen**
Erforderliche Rolle: admin und sn_msi.workspace_admin

**Hinweis:**
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

Um ein Rollup für Informationen wie Konfigurationselemente, erkennbare Elemente und Gefährdungsindikatoren im Zusammenhang mit einem Sicherheitsfall durchzuführen, erstellen Sie eine Rollup-Datensatzkonfiguration.

**Prozedur**

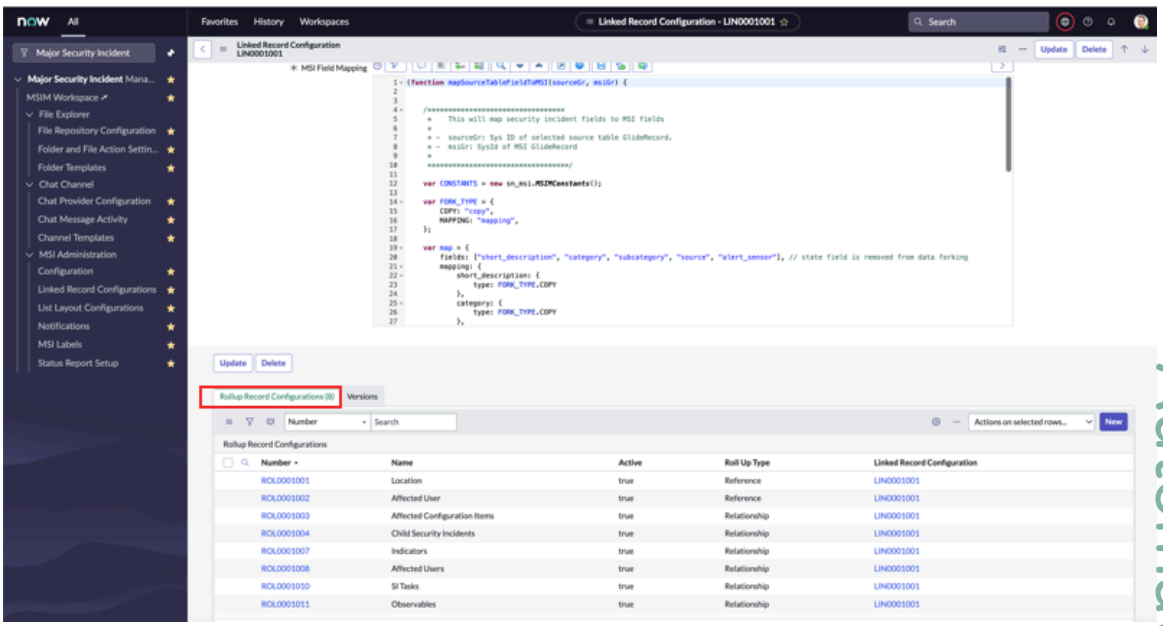
1. Navigieren zu **Reaktion auf schwerwiegende Security Incidents** > **Konfiguration verknüpfter Datensätze**.
   Die Seite „Konfigurationen verknüpfter Datensätze“ wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen oder erstellen Sie einen neuen verknüpften Datensatz, und navigieren Sie auf derselben Seite zum Abschnitt „ **Rollup-Datensatzkonfiguration** “.

**Abschnitt „Rollup-Datensatzkonfiguration“.**




## Nächste Maßnahme

- Ausführlichere Informationen finden Sie unter Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents
- Beispielinformationen für einen Sicherheitsfall finden Sie unterSchreiben eines Skripts für einen Sicherheitsfall

### Schreiben eines Skripts für einen Sicherheitsfall

Schreiben eines Skripts für einen Sicherheitsfall, um ein Rollup für die Datensatzkonfiguration durchzuführen.

## Vorbereitungen

Erforderliche Rolle: admin und sn_msi.workspace_admin

**Hinweis:**
Der Systemadministrator kann den Datensatz erstellen und der MSI-Arbeitsbereichsadministrator kann ihn aktualisieren.

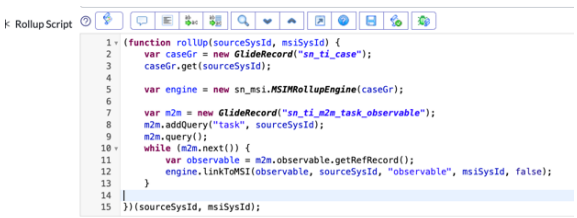
## Prozedur

1. Suchen Sie mithilfe der linken Navigation nach den Konfigurationen für verknüpfte Datensätze.
2. Navigieren zu **MSI-Administration** > **Konfiguration verknüpfter Datensätze**.
3. Öffnen Sie den Konfigurationsdatensatz, der für einen Sicherheitsfall erstellt wurde.
4. Die Konfiguration des Rollup-Datensatzes wird im Abschnitt „Zugehörige Liste“ angezeigt.
5. Klicken Sie auf **Neu**, um eine neue Rollup-Datensatzkonfiguration zu erstellen.

Unten sehen Sie einen Beispieldatensatz, der für ein Rollup von Daten für erkennbare Elemente im Zusammenhang mit dem Sicherheitsfall erstellt wurde, für den ein Rollup durchgeführt wird, mit den folgenden Feldwerten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Beschreibung |
|---|---|
| Rollup-Typ | Beziehung<br><br>**Hinweis:**<br>Die Informationen zum erkennbaren Element sind in einem zugehörigen Listenformat verfügbar. |
| Rollup-Skript | Eingabe „sourceSysId“ enthält die Sys-ID des Sicherheitsfalls, und „msiSysId“ enthält die Sys-ID des schwerwiegenden Security Incidents.<br><br>  <br>Rollup Script<br>1 (function rollUp(sourceSysId, msiSysId) {<br>2 var caseGr = new GlideRecord("sn_ti_case");<br>3 caseGr.get(sourceSysId);<br>4<br>5 var engine = new sn_msi.MSIMRollupEngine(caseGr);<br>6<br>7 var m2m = new GlideRecord("sn_ti_m2m_task_observable");<br>8 m2m.addQuery("task", sourceSysId);<br>9 m2m.query();<br>10 while (m2m.next()) {<br>11 var observable = m2m.observable.getRefRecord();<br>12 engine.linkToMSI(observable, sourceSysId, "observable", msiSysId, false);<br>13 }<br>14<br>15 })(sourceSysId, msiSysId);<br><br>○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table.<br><br>○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case.<br><br>○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method:<br><br>`MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")` |



### Führen Sie bei Bedarf ein atomares Rollup durch

Das Rollup-Framework kann keine Aktualisierungen der vorhandenen verknüpften Datensätze verarbeiten. In solchen Fällen sollte ein atomares Rollup bei Bedarf für verknüpfte Datensätze erfolgen, was über Geschäftsregeln erreicht werden kann.

Um Aktualisierungen an den verknüpften Datensätzen zu erfassen, müssen Business Rules für die Quelltabelle erstellt werden.

Diese Business Rules funktionieren beim Einfügen, Aktualisieren und Löschen. Wenn Sie einfügen oder aktualisieren, müssen Sie Rollup-Informationen zu MSIhinzufügen oder aktualisieren. Wenn Sie löschen, werden die Rollup-Informationen aus MSIentfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald beispielsweise ein Security Incident mit MSIverknüpft ist, wird für die zugehörigen Informationen automatisch ein Rollup durchgeführt MSI. Wenn Sie jedoch später ein neues erkennbares Element zu einem MSIhinzufügen, wird für das neu hinzugefügte erkennbare Element auch ein Rollup zu MSIdurchgeführt. Hier erfasst die Geschäftsregel „ **Rollup** für erkennbares Element synchronisieren“ die Aktualisierung und führt ein Rollup des aktualisierten Datensatzes zu MSIdurch. In ähnlicher Weise behandelt dieselbe Geschäftsregel auch die Entfernung der vorhandenen Rollups für erkennbare Elemente, wenn sie aus dem Security Incident entfernt werden.

**Vordefinierte Geschäftsregeln**

***Im Folgenden finden Sie einige vordefinierte Geschäftsregeln, die Ihnen helfen, den Umgang mit atomaren Rollups zu verstehen***

| Regel | Beschreibung |
|---|---|
| Rollup-Indikator für Synchronisierung (sn_ti_m2m_task_indicator) | Verwenden Sie diese Geschäftsregel, um das Rollup und die Entfernung des Kompromittierungsindikators aus Security Incident, Sicherheitsfall und Korrekturaufgabe durchzuführen. |
| Rollup des erkennbaren Elements synchronisieren (sn_ti_m2m_task_observable) | Verwenden Sie diese Geschäftsregel, um das Rollup und die Entfernung verknüpfter erkennbarer Elemente aus Security Incident, Sicherheitsfall und Korrekturaufgabe zu handhaben. |
| Rollup des betroffenen Benutzers synchronisieren (sn_si_m2m_task_affected_user) | Verwenden Sie diese Geschäftsregel, um das Rollup und die Entfernung verknüpfter betroffener Benutzer aus Security Incident, Sicherheitsfall und Korrekturaufgabe durchzuführen. |
| Rollup für betroffenes CI synchronisieren (task_ci) | Verwenden Sie diese Geschäftsregel, um das Rollup und die Entfernung zugeordneter Konfigurationselemente aus Security Incident, Sicherheitsfall und Korrekturaufgabe zu handhaben. |

## Security Incident Response-Integrationen

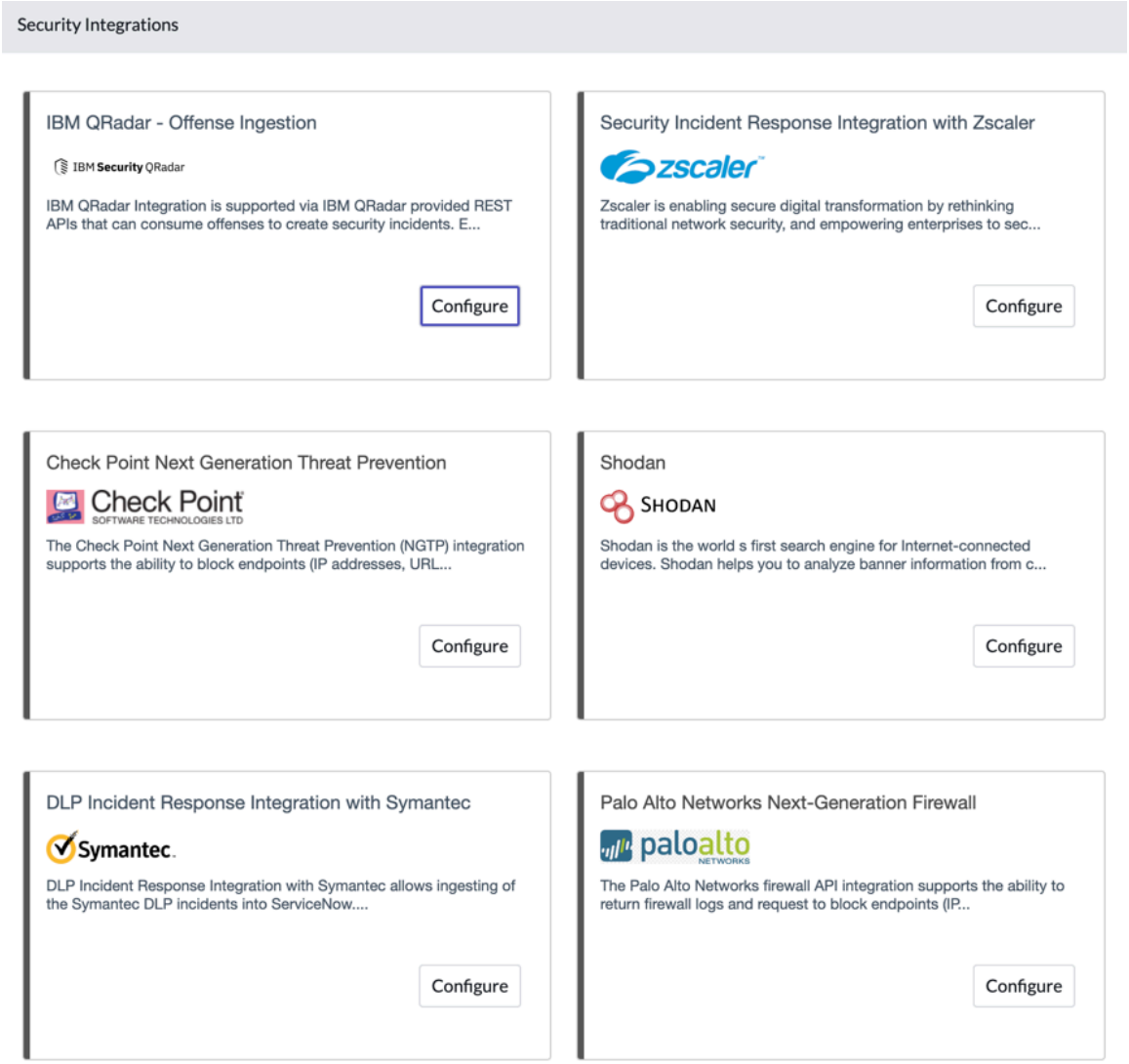
Alle Security Operations Kernanwendungen und nicht zum Kern gehörenden Drittanbieterintegrationen sind über den ServiceNow Storeverfügbar. Mit dieser Integration können Sie neue und aktualisierte Funktionen schneller erhalten. Dieser Abschnitt enthält Anweisungen zum Aktivieren der Integrationen und zum Konfigurieren von ServiceNow und Drittanbieterintegrationen. Außerdem sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen enthalten, die im Basissystem enthalten sind.

### Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Security Operations -Plugins aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie können die sichtbaren Integrationen mithilfe des Dropdown-Menüs „ **Kategorie** “ filtern. Im Dropdown-Menü „ **Konfigurationen** anzeigen“ können Sie mehrere Instanzen von Implementierungen anzeigen, die deren Erstellung zulassen.

## Schaltflächen auf Integrationskarten

Integrationskarten zeigen je nach aktuellem Status der Integration und Quelle der Karte unterschiedliche Schaltflächen an.

| Schaltfläche | Beschreibung |
|---|---|
| Plugin installieren | Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren und die Integration zu aktivieren. Nach der Installation des Plugins ändert sich die Schaltfläche in **Konfigurieren**. |
| Konfigurieren | Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Für einige Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die Sie von der Website der Drittpartei-Integration erhalten haben. |
| Neu | Bei bestimmten Integrationen wie Carbon Black und IBM QRadar können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie für diese Integrationen auf |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Schaltfläche | Beschreibung |
|---|---|
| | **Neu**, nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die Implementierungen für die Verwendung konfigurieren. |
| Seite öffnen | Im Basissystem führt Ihre Instanz eine Abfrage an den ServiceNow Store für alle Anwendungen durch, die von Security Operations -Plugins abhängig sind. Wenn diese Anwendungen gefunden und die zugehörigen Anwendungs-Plugins aktiviert werden, werden Integrationskarten für sie mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie auf **Seite öffnen**, um auf die Website der Drittanbieteranwendung zuzugreifen und die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, ändert sich die Schaltfläche **Seite öffnen** in **Konfigurieren**. |

## ArcSight ESM Event-Erfassung für die Integration von Security Operations .

Die Integration der Ereigniserfassung von ArcSight ESM mit dem Produkt Security Incident Response ermöglicht Security Incident-Analysten die Erfassung korrelierter Ereignisse und die Automatisierung der Erstellung von Security Incidents mit der Plattform ServiceNow. Daten werden kontinuierlich basierend auf einem konfigurierten Abfragezeitplan erfasst und von Analysten verwendet, um potenzielle Cybersicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Mit dieser Integration können korrelierte Events, die Kandidaten für Security Incidents sind, regelmäßig erfasst werden. Sie können Felder in korrelierten Events Security Incident-Feldern zuordnen, eine Vorschau der Einrichtung eines Events als Security Incident anzeigen und die geplante Erfassung von Events einrichten, um Security Incidents kontinuierlich zu erstellen.

### Übersicht

Diese Integration bietet einem SOC-Analysten (Security Operations Center) Einblick in Korrelations-Events in ArcSight ESM. Diese Daten können zur weiteren Untersuchung und Korrektur in Security Incidents von Now Platform Security Incident Response (SIR) integriert werden. Profile werden in Ihrer Instanz Now Platform erstellt, um verschiedene Korrelationsereignistypen zu verarbeiten, die erstellt und über Korrelationsabfrage-Viewer in ArcSight ESMverfügbar gemacht werden. Diese Profile passen an, wie verschiedene ArcSight ESM korrelierte Event-Felder in SIR-Security Incidents angezeigt werden.

### Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere Event-Erfassungsprofile, um SIR Security Incidents für bestimmte Arten von Bedrohungen wie Malware und nicht autorisierte Zugriffsversuche zu erstellen.
- Drag-and-Drop-Zuordnung von ArcSight ESM Korrelations-Event-Feldwerten zu zugeordneten SIR Security Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf Beispiel-Korrelations-Events zur Validierung der Event-Zuordnungsdetails.
- Erfassen Sie historische Korrelationsereignisse sowie neue wichtige Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie Korrelations-Events heraus, die die Kriterien für die Incident-Generierung von SIR nicht erfüllen, z. B. Events mit niedriger Priorität



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fassen Sie Events basierend auf übereinstimmenden Feldwerten zu vorhandenen SIR Security Incidents zusammen, um doppelte Security Incidents zu vermeiden.
- Aktualisieren Sie Korrelations-Events basierend auf SIR Incident-Erstellungs- und/oder -Abschlussbedingungen über eine bidirektionale Schnittstelle.

### Unterstützte Versionen Now Platform .

Diese Integration unterstützt die Releases New York Patch 6 und Orlando Now Platform.

Die folgenden Security Operations-Anwendungen müssen über ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response
4. Event- und Warnungserfassung für Sicherheitsvorgänge
5. Integrations-Hub-Plugins
   a. ServiceNow Integration Hub-Laufzeit
   b. Aktionsschritt ServiceNow Integration Hub – REST

Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store ..

### ArcSight ESM unterstützte Versionen

Diese Integration wurde mit Version 7.0.0.2436 des ArcSight ESM Managers getestet. Die Integration unterstützt sowohl ArcSight ESM lokale als auch Cloud-/gehostete Serviceumgebungen.

### MID-Server

Für diese Integration muss ein installierter und konfigurierter MID Server in Ihrer Now Platform® -Instanz eine Verbindung zum ArcSight ESM -Service herstellen, wenn der ArcSight ESM -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Wenn Sie den Cloud-Service ArcSight ESM verwenden, ist kein MID Server erforderlich. Weitere Informationen zu MID Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .

### Referenzen

| Referenz | Dokumentbezeichner | Dokumententitel |
|---|---|---|
| 1 | ArcSight ESM Produktdokumentation | ArcSight-Produktdokumentation . |
| 2 | ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie Ihre Now Platform® -Instanz für die ArcSight ESM -Integration der Event-Erfassung ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

**Vorbereitungen**
Erforderliche Rolle: admin

**Warum und wann dieser Vorgang ausgeführt wird**
Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform® -Instanz erforderlich.<br>• Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus dem ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform®:<br>◦ Benennt, erstellt und bearbeitet Event-Profile.<br>◦ Wählt Werte aus ArcSight ESM Korrelations-Events aus und ordnet sie Security Incidents zu.<br>◦ Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.<br>◦ Plant die laufende korrelierte Event-Erfassung.<br>◦ Aktiviert korrelierte Event-Aktualisierungen, wenn ein SIR-Incident erstellt und geschlossen wird.<br>◦ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.<br>Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der ServiceNow-Website mit Produktdokumentation . |
| Vergewissern Sie sich, dass Sie Version 7.0.0.2436 oder höher des ArcSight ESM Managers verwenden. Frühere Versionen werden nicht unterstützt. | Wenn Sie Zugriff auf den Abfrage-Viewer ArcSight ESM haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich. |
| Richten Sie den Abfrage-Viewer in ArcSight ESMein. | Bevor Sie Korrelations-Events erfassen können, müssen Sie den Abfrage-Viewer in der ArcSight ESM -Konsole konfigurieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | Details siehe Richten Sie den Abfrage-Viewer ArcSight ESM ein. |
| **Optional**<br><br>Erstellen Sie in ArcSight ESM benutzerdefinierte Phasen für Aktualisierungen von Korrelationsereignissen. | Ein Korrelationsereignis durchläuft viele Phasen in seinem Lebenszyklus, bevor es geschlossen wird. ArcSight ESM bietet Standardphasen wie „Anfänglich“, „Überwachung“, „In der Warteschlange“ und „Geschlossen“. Einige dieser Phasen erfordern Benutzereingaben, andere Phasen werden jedoch automatisch auf das Event angewendet, ohne dass der Benutzer eingreifen muss (das Feld **Benutzer erforderlich** ist in der Konsole ArcSight ESM deaktiviert).<br><br>Sie können benutzerdefinierte Phasen erstellen, für die kein Benutzereingriff erforderlich ist, und sie in Ihrer Now Platform® -Instanz verwenden. Details siehe Zusätzliche Optionen: Automatisieren Sie korrelierte Event-Aktualisierungen und -Abschlüsse basierend auf dem Incident-Status SIR .. |
| Vergewissern Sie sich, dass Sie eine MID Server-Anwendung installiert und konfiguriert haben. | Konfigurierte MID-Server-Anwendung<br><br>Ein MID Server in Ihrer Now Platform® -Instanz ist erforderlich, um eine Verbindung zum ArcSight ESM -Service herzustellen, wenn der ArcSight ESM -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Anweisungen zum Konfigurieren einer MID Server-Anwendung finden Sie unter Installieren und konfigurieren Sie die ServiceNow-Anwendung für die ArcSight ESM Event Ingestion-Integration.<br><br>Informationen zu MID Servern finden Sie unter MID Server .<br><br>Wenn Sie einen gehosteten oder Cloud-Service verwenden, der über das Internet zugänglich ist, ist kein MID Server erforderlich. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Event and Alert Ingestion for Security Operations: Diese Anwendung erfordert: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit<br>○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST<br>**5.** Threat Core<br><br>Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

## Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht darin, die Anwendung ArcSight ESM Security Event Ingestion for Security Operations aus dem ServiceNow Store für die -Integration zu installieren.

### Richten Sie den Abfrage-Viewer ArcSight ESM ein

Erstellen Sie einen Abfrage-Viewer, und definieren Sie Filter, die kürzlich erstellte Korrelationsereignisse enthalten, die erfasst werden ServiceNow.

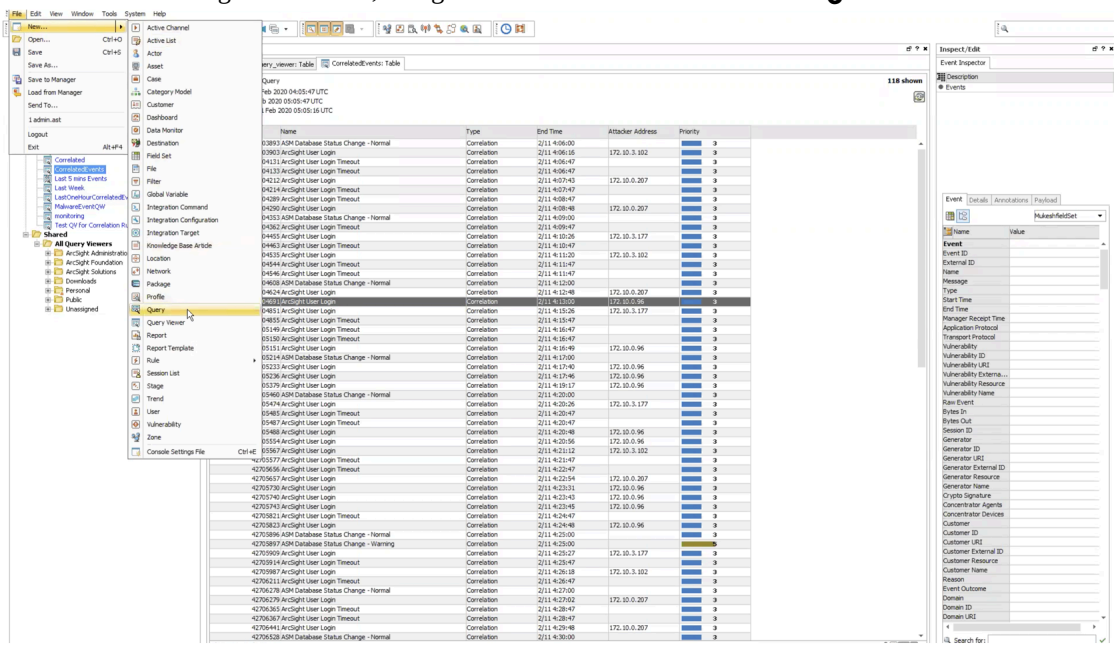
## Vorbereitungen

Erforderliche Rolle: ArcSight-Administrator

## Prozedur

**1.** Melden Sie sich bei der Konsole ArcSight ESM an, um einen Abfrage-Viewer zu erstellen.

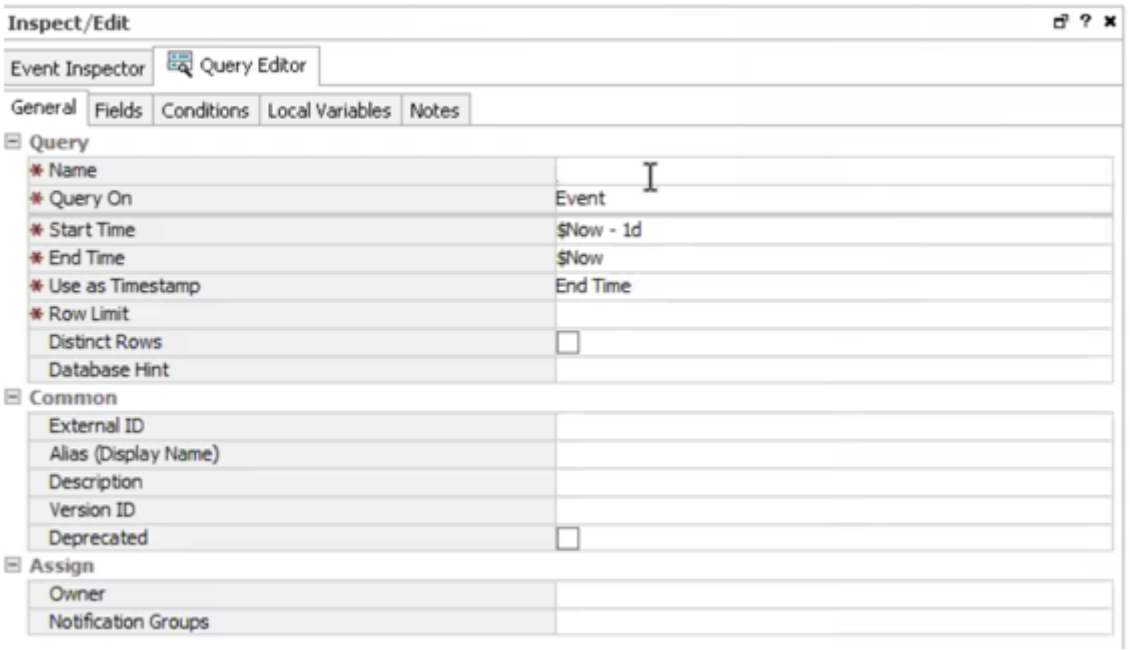
**2.** Um eine neue Abfrage zu erstellen, navigieren Sie zu **Datei** > **Neu** > **Abfrage**.



**3.** Definieren Sie Bedingungen für den Abfrage-Viewer im **Bereich „Inspizieren/Bearbeiten“**.

Automatische Übersetzung

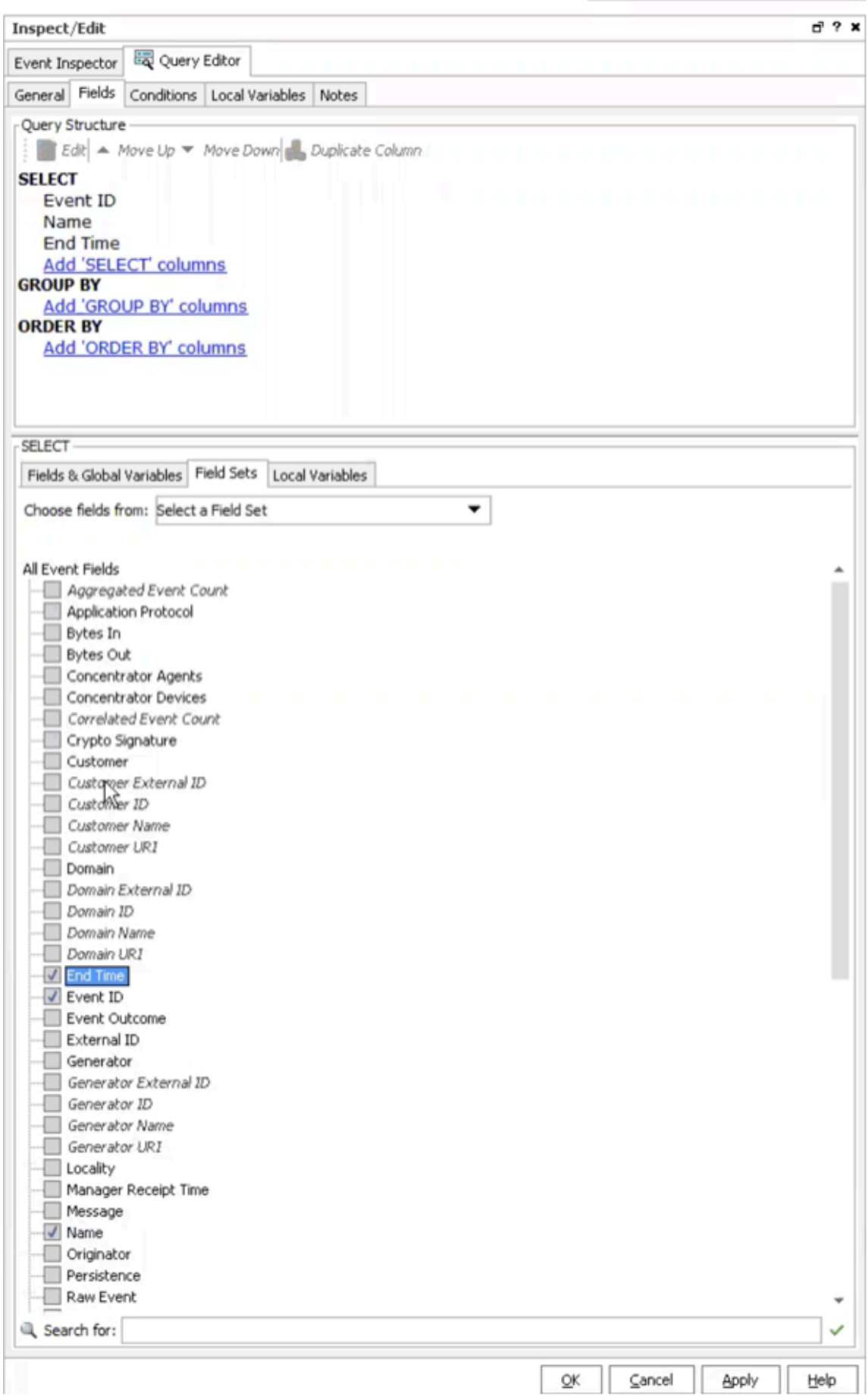
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Klicken Sie auf die Registerkarte **Felder**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

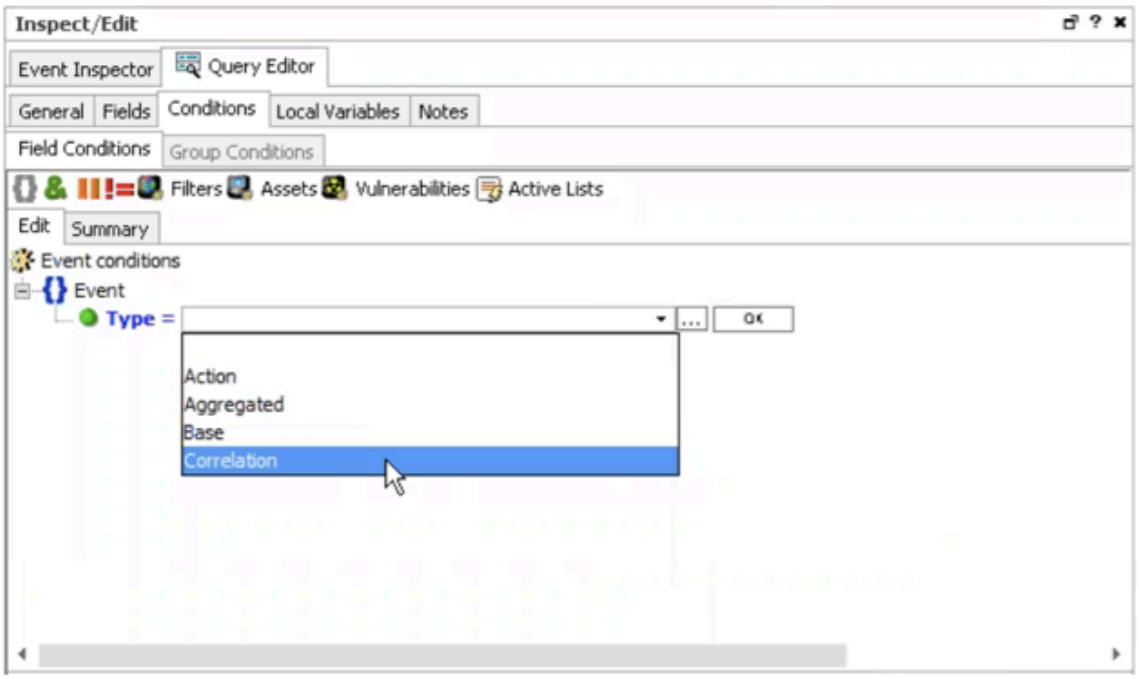



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie die Felder aus, die in die Erfassung einbezogen werden müssen.
   Sie müssen die Felder `Event-ID`, `Name`und `Endzeit` auswählen, damit die Erfassung erfolgreich ist.
6. Klicken Sie auf den Link „Sortieren nach **"-Spalten** hinzufügen, wählen Sie das Feld **Event-ID** aus, und legen Sie die Sortierreihenfolge auf **Absteigend** fest, um sicherzustellen, dass die neuesten Events erfasst werden.
7. Klicken Sie auf die Registerkarte **Bedingungen**.
8. Klicken Sie mit der rechten Maustaste auf **Event** unter **Event-Bedingungen** im Abschnitt „ **Zusammenfassung** “.
9. Klicken **Neue Bedingung** > **Stamm** > **Typ** und wählen Sie als Event-Typ **Korrelation**aus.

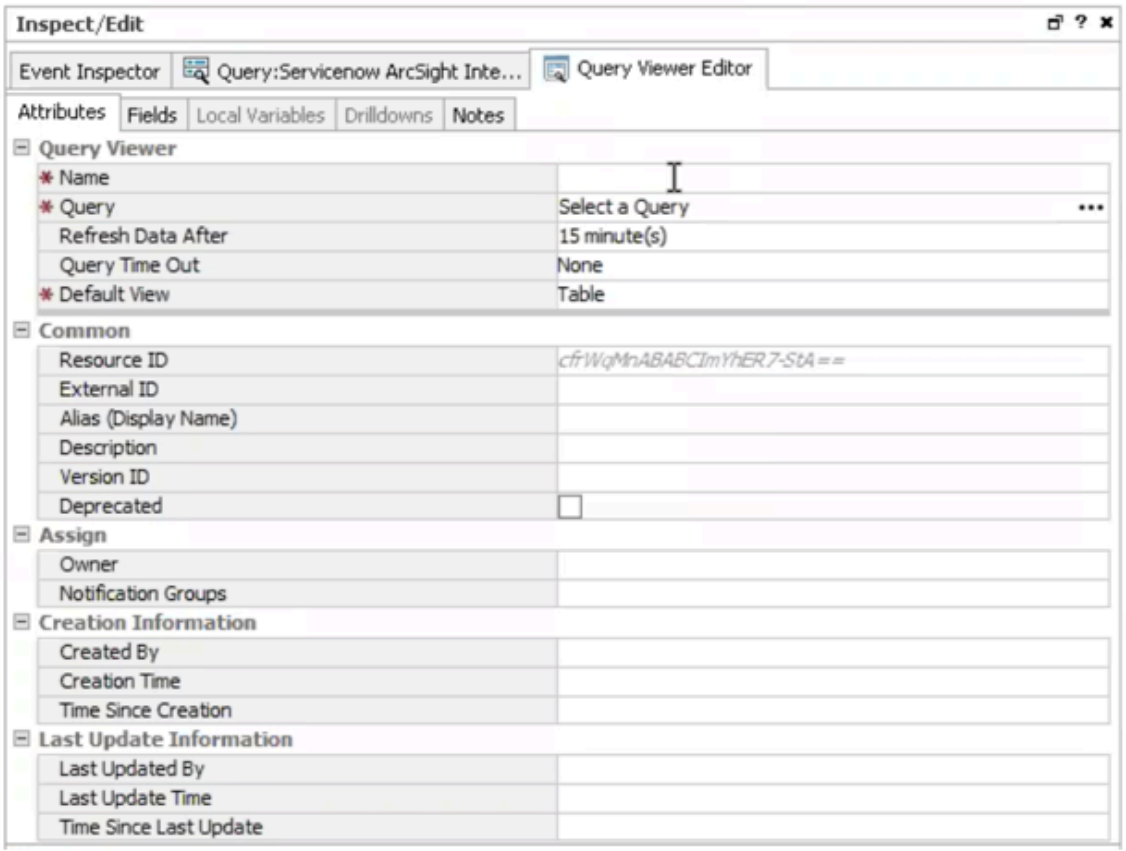
**Wichtig:**
Es werden nur Korrelationsereignisse abgerufen. Basis-Events für Korrelationen werden nicht abgerufen.




10. Klicken Sie auf **OK**, um die Abfrage zu speichern.
    Der nächste Schritt besteht darin, einen Abfrage-Viewer für diese Abfrage zu erstellen.
11. Navigieren zu **Datei** > **Neu** > **Abfrage-Viewer**.



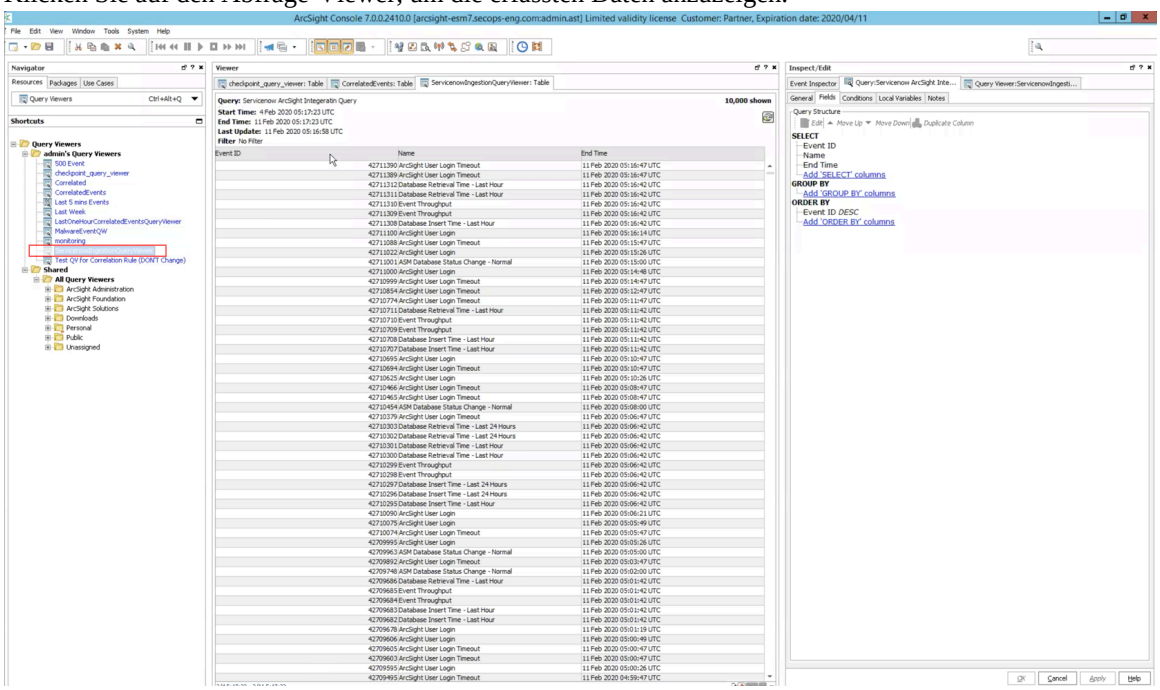
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**12.** Klicken Sie auf die Registerkarte **Felder**, und stellen Sie sicher, dass die Pflichtfelder (`Event-ID, Name, Endzeit`), die Sie in Ihrer Abfrage angegeben haben, ausgewählt sind.

**13.** Klicken Sie auf **Anwenden**, um den Abfrage-Viewer zu speichern.
Der neue Abfrage-Viewer, den Sie erstellt haben, wird im Abschnitt „Query Viewers“ (Abfrage-Viewer) aufgelistet.

**14.** Klicken Sie auf den Abfrage-Viewer, um die erfassten Daten anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Installieren und konfigurieren Sie die ServiceNow-Anwendung für die ArcSight ESM Event Ingestion-Integration

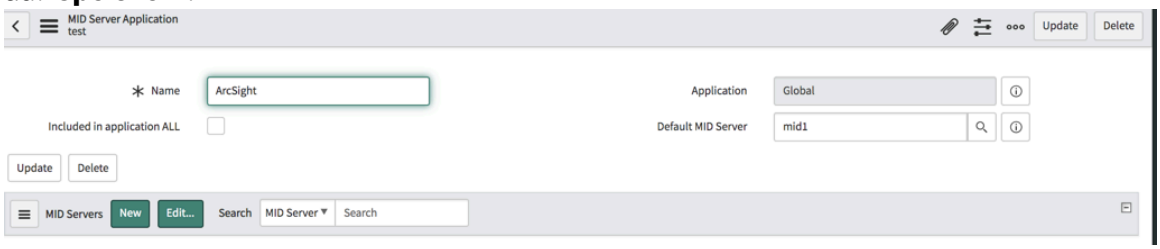
Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform® ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform integriert wird.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Wenn Sie die Anwendung ArcSight ESM nicht aus dem ServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel ArcSight ESM.
3. Um die Anwendung zu konfigurieren, klicken Sie auf **Neu**.
4. Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder des Formulars aus.
   Führen Sie die folgenden Schritte aus, um eine neue MID Server-Anwendung zu erstellen:
   a. Navigieren zu **MID-Server** > **Anwendungen** und klicken Sie auf **Neu**.
   b. Geben Sie einen Namen für die MID Server-Anwendung ein, und wählen Sie einen MID Server aus, der als Standard verwendet werden soll.
   c. Deaktivieren Sie das Kontrollkästchen In Anwendung ALLE enthalten, und klicken Sie auf **Speichern**.

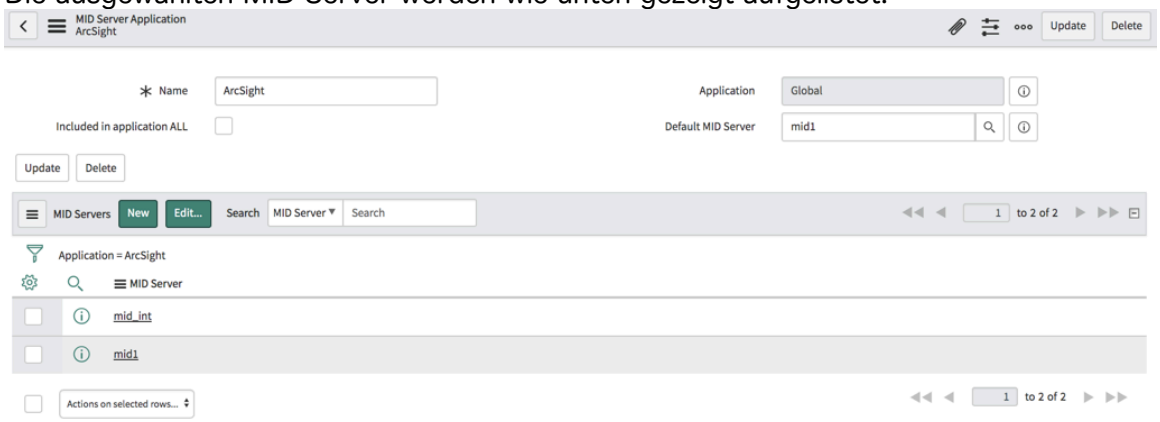



   d. Klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite „ **Mitglieder bearbeiten** “ alle verfügbaren MID Server aus, verschieben Sie sie in die MID Server-Liste, und klicken Sie auf **Speichern**.

Automatische Übersetzung

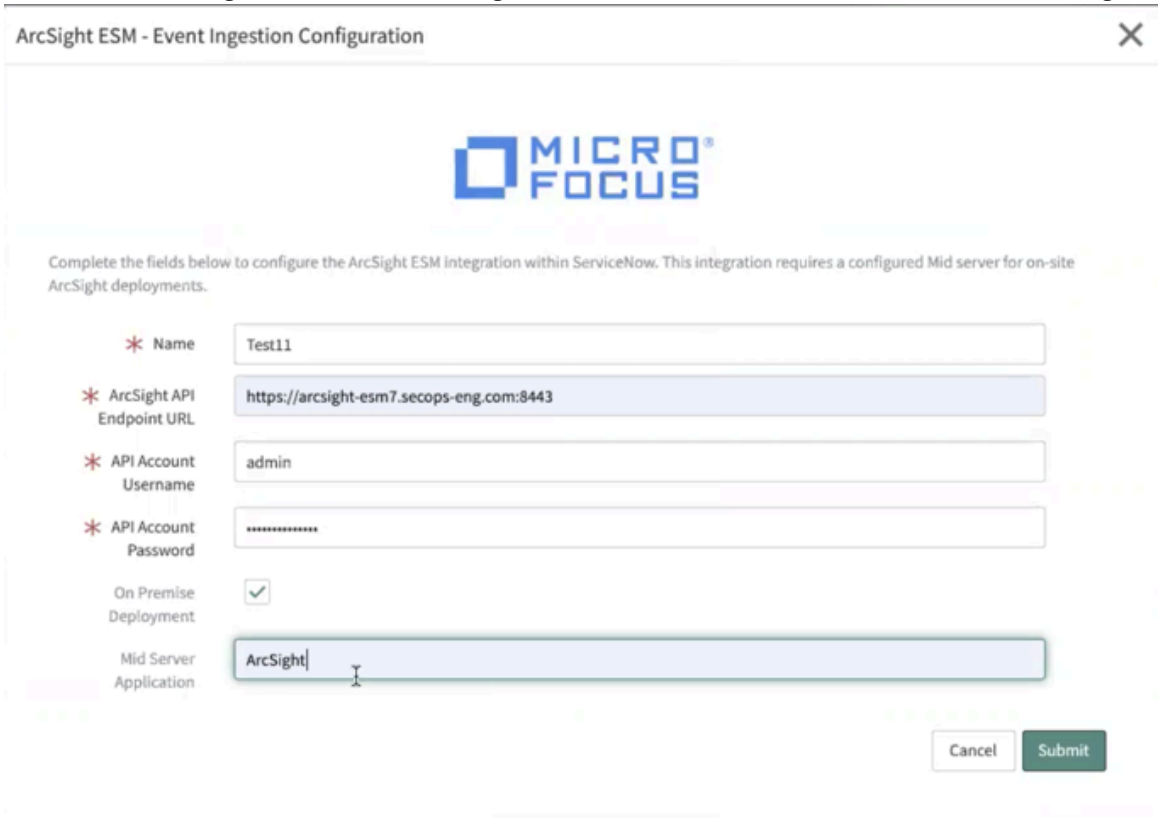
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Die ausgewählten MID Server werden wie unten gezeigt aufgelistet.




Je nach Verfügbarkeit wird einer der mit der MID Server-Anwendung konfigurierten MID Server verwendet.

6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID Server-Anwendung an.




Jedes Korrelationsereignis, das Sie über die Manager-Konsole ArcSight ESM erfassen, erfordert ein eindeutiges Ereignisprofil in Ihrer Instanz. Die Quelle ArcSight ESM, die Sie im Formular Event-Erfassungskonfiguration konfigurieren, kann jedoch für mehrere Profile wiederverwendet werden, solange jedes Profil eindeutige Korrelations-Event-Typen erfasst.

7. Klicken Sie auf **Absenden**.
Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration ArcSight ESM auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

## Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Event-Profil zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

### Erstellen Sie ein Profil für die Integration der Korrelations-Event-Erfassung ArcSight ESM .

Als Benutzer mit der Rolle „sn_si.admin“ erstellen Sie ein Profil in Ihrer Instanz Now Platform und bestimmen, welche Korrelationsereignisse Security Incidents verursachen. Bevor Now Platform Security Incident Response (SIR) Security Incidents aus Korrelations-Events erstellt werden, werden die Feldwerte aus Events in einem Layout eines Now Platform Security Incident angezeigt, sodass Sie eine Vorschau auf die Erstellung des tatsächlichen Security Incident erhalten.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Korrelations-Events werden abhängig vom definierten Profiltyp automatisch in der Umgebung [ Security Operations Ihrer Instanz Now Platform erfasst. Ein Profil ist eine Kapselung einer Art von Korrelationsereignis, z. B. nicht autorisierte Zugriffsversuche oder Malware.

Nachdem ein Korrelationsereignis erfasst wurde, können Sie einzelne Korrelationsereignisfelder den entsprechenden Feldern im Security Incident zuordnen. Sie können Korrelations-Events filtern, um anzugeben, welche Events Security Incidents verursachen. Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für Korrelationsereignisse erstellen, die als hohes Risiko identifiziert wurden. Sie können auch zusätzliche Event-Zusammenfassungskriterien definieren, sodass eingehende doppelte Korrelations-Events zu einem offenen Security Incident zusammengefasst werden. Schließlich können Sie einen Erfassungszeitplan definieren und das Profil aktivieren.

Namen für die Event-Profile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Event-Profil zugeordnet werden.

### Erstellen Sie das Profil für die Integration der ArcSight ESM -Ereigniserfassung, und benennen Sie es

Sie können ein Profil einrichten, um Korrelations-Events zu erfassen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Prozedur

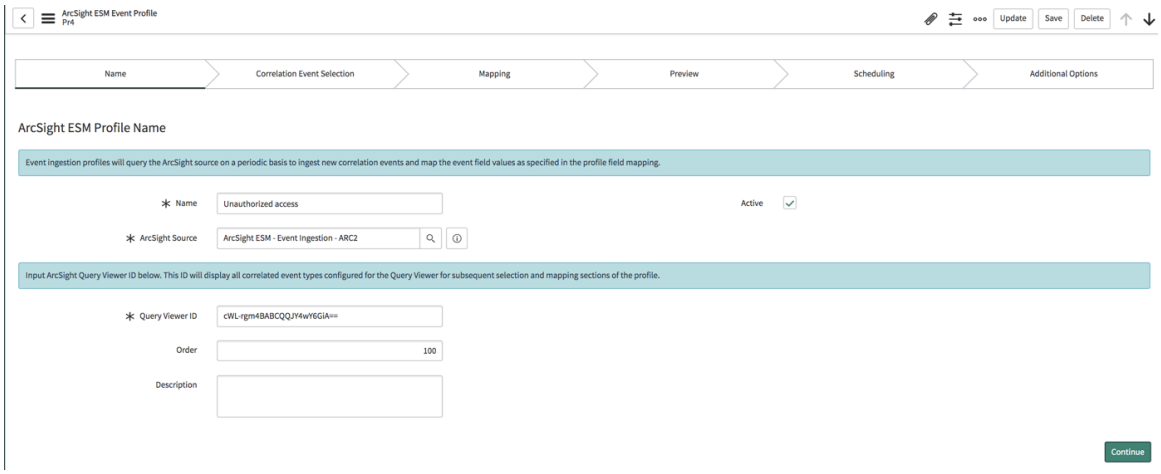
1. Um ein Event-Profil für ein Korrelations-Event in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **ArcSight ESM-Integration** > **ArcSight ESM-Ereignisprofil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

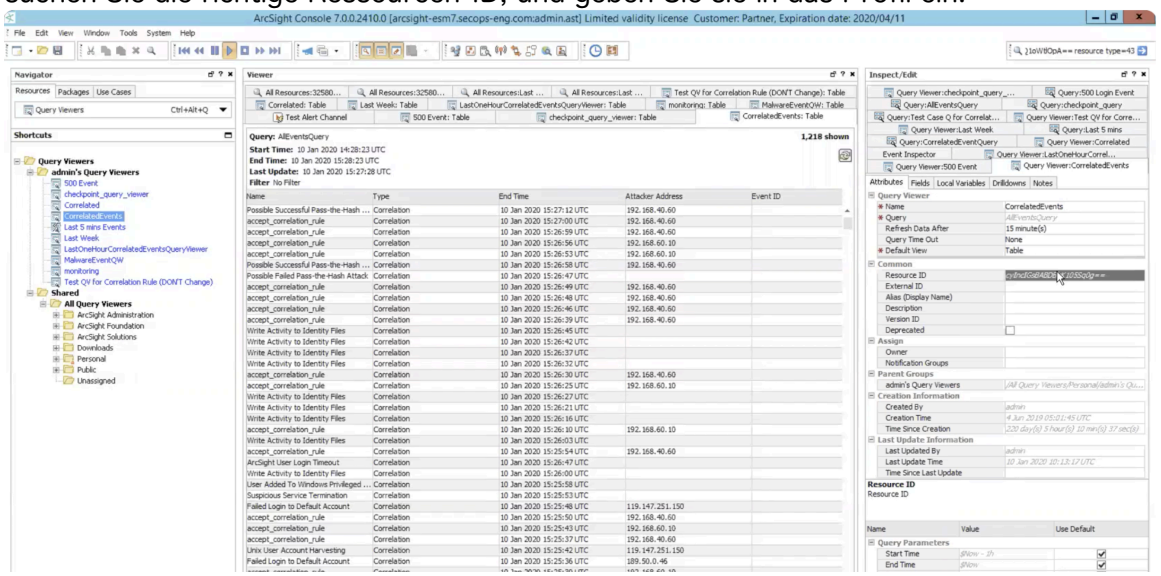
   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nachdem Sie die Profildetails eingegeben haben, klicken Sie auf **Fortfahren**. Die Abfrage-Viewer-ID wird validiert. Wenn eine entsprechende Ressourcen-ID im Abfrage-Viewer ArcSight ESM vorhanden ist, wird der Name des Abfrage-Viewers wie unten gezeigt zurückgegeben. Wenn die Validierung fehlschlägt, überprüfen Sie, ob die Ressourcen-ID in der Konsole ArcSight ESM vorhanden ist. Wenn die Ressourcen-ID nicht gefunden wird, suchen Sie die richtige Ressourcen-ID, und geben Sie sie in das Profil ein.




## Nächste Maßnahme

Der nächste Schritt besteht darin, die Korrelationsereignistypen für die Erfassung aus dem Abfrage-Viewer auszuwählen, der im vorherigen Schritt ausgewählt wurde.

### Wählen Sie Korrelations-Events für die Integration der ArcSight ESM -Event-Erfassung aus

Wählen Sie basierend auf der Quelle ArcSight ESM und dem konfigurierten Abfrage-Viewer eine Korrelationsereignisregel für das Profil aus.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelations-Events an, die in der Auswahl des Korrelationsereignisses in Ihrer Now Platform-Instanz aufgeführt sind, damit Sie bestimmen können, welche Korrelations-Events Sie erfassen und Security Incidents erstellen möchten. Sie können für jedes Profil nur einen Korrelationsregeltyp aus der Liste auswählen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Abfrage-Viewer-ID und der Abfrage-Viewer-Name, wie im Abfrage-Viewer-Formular angegeben, werden angezeigt. Wählen Sie ein Korrelationsereignis aus der Liste aus, das Sie zum Erstellen einer Konfigurationszuordnung für das erfasste korrelierte Ereignis verwenden können.

Klicken Sie auf die Dropdown-Liste im Feld Korrelationsereignisliste. Eine Liste der Korrelationsereignisse, die in der Query Viewer-Konsole ArcSight ESM vorhanden sind, wird angezeigt.

Klicken Sie auf **Fortsetzen**, um mit dem nächsten Schritt im Assistenten fortzufahren.

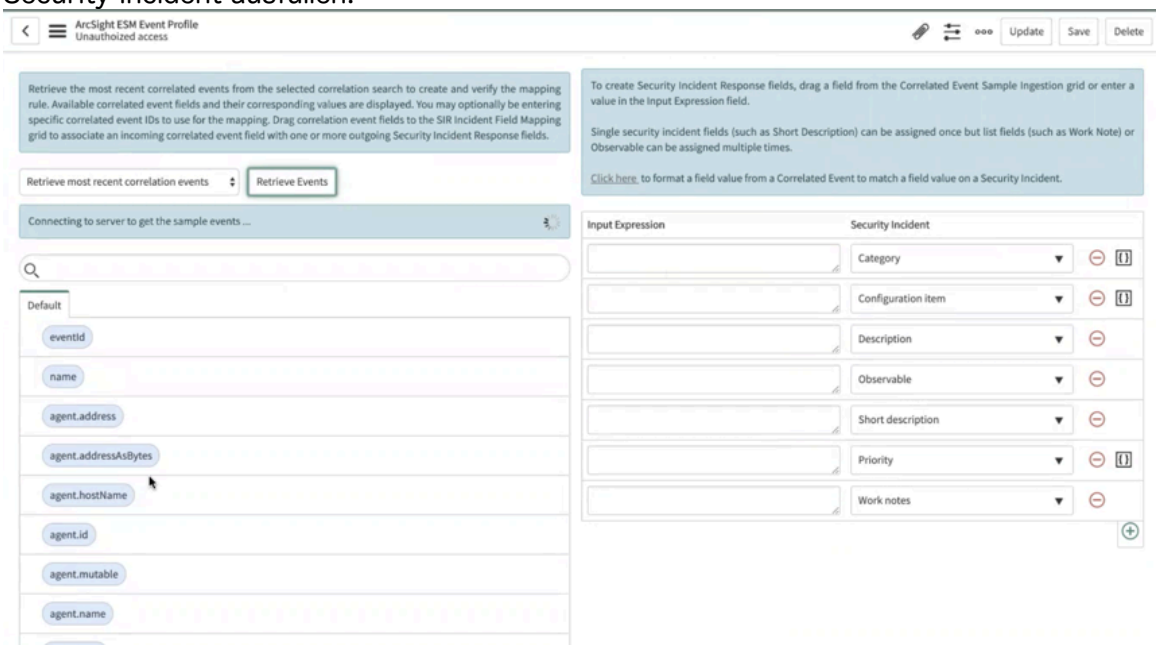
### Zuordnung von Korrelations-Event-Feldern für die ArcSight ESM -Integration der Event-Erfassung

Nachdem Sie die spezifische Korrelationsereignisregel aus der Liste identifiziert haben, besteht der nächste Schritt darin, Korrelationsereignisfelder den Feldern im Security Incident-Formular zuzuordnen.

## Übersicht

Für den Zuordnungsschritt können Sie Beispiele für Korrelationsereignisse für die ausgewählte Korrelationsregel erfassen. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten Korrelations-Event-Felddaten der entsprechenden Stelle im Incident-Formular SIR zugeordnet werden, und dann den Incident SIR im Vorschaubereich visualisieren.

Die folgende Abbildung zeigt die Standardzuordnungskonfiguration, die zum Erstellen des Korrelationsereignisprofils bereitgestellt wird. Sie können die Felder anpassen, die den Security Incident ausfüllen.




Wenn Sie auf **Ereignisse**abrufen klicken, werden die Feldnamen des Korrelationsereignisses und die entsprechenden Werte auf der linken Seite des Formulars ausgefüllt. Dies sind die ArcSight ESM Korrelations-Event-Felder, die zur Zuordnung zu den Security Incident-Feldern verfügbar sind.

Möglicherweise möchten Sie einige Beispiele für Korrelationsereignisse in Ihrer Konsole überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird in der Fortschrittsleiste als Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**. Sie können bis zu



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

fünf Beispielkorrelationsereignisse aus dem Manager ArcSight ESM für die ausgewählte Korrelationsregel erfassen, um den Feldzuordnungsprozess zu unterstützen. Es gibt Optionen, um entweder die fünf letzten Korrelationsereignisse für das ausgewählte Korrelationsereignis oder bis zu fünf bestimmte Korrelationsereignisse basierend auf den Ereignis-IDs zu erfassen.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen von Korrelationsereignissen erforderlich sind:

- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Korrelations-Event-Felder von der linken Seite ziehen und sie im Incident-Zuordnungsabschnitt SIR auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Korrelationsereignisfeld einem ausgehenden Security Incident-Feld zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder mithilfe des Symbols + am unteren Rand des Abschnitts „SIR-Incident-Feldzuordnung“ hinzufügen oder entfernen. Verfolgen Sie übersehene oder zuvor zugeordnete Felder mit der angegebenen Farbcodierung nach (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen definieren, sodass Sie filtern können, welche Korrelationsereignisse Security Incidents erstellen sollen und welche Korrelationsereignisse herausgefiltert werden sollen, z. B. Korrelationsereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Bedingungen für Incident-Generierung“, der sich unter dem Abschnitt „Erfassung von Korrelationsereignisbeispiel“ befindet.
- Event-Zusammenfassungskriterien: Definieren Sie zusätzliche Event-Zusammenfassungskriterien, die ein eingehendes Korrelations-Event zu einem vorhandenen SIR Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Daten zu wichtigen Sicherheitsereignissen in einem einzigen Security Incident platziert werden.
- Formatfeldübersetzung: In bestimmten Fällen werden Event-Feldwerte im Korrelations-Event ArcSight ESM möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

  Zum Beispiel kann mit dem Skript-Editor ein Kategoriewert von Malware-Warnung und Virusinfection unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mit in eine gemeinsame böswillige Codeaktivität im Feld Kategorie des Security Incident SIR übersetzt werden Funktion „Formatfeldübersetzung“.

Der nächste Schritt besteht darin, Beispiele für Korrelations-Events zu erfassen und Werte den SIR Security Incident-Feldern zuzuordnen.

### Erstellen Sie Zuordnungen für die Integration der ArcSight ESM Event-Erfassung

In diesem Schritt erfassen Sie Beispiele für Korrelations-Events und ordnen Werte den SIR-Security Incident-Feldern zu.

#### Vorbereitungen

Erforderliche Rolle: admin, sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Als Benutzer mit der Rolle „sn_si.admin“ können Sie bis zu fünf Beispielkorrelations-Events aus der Spalte „Korrelationsereignis – Beispielerfassung“ auf der linken Seite des Formulars überprüfen, um die Zuordnung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und Übersetzung von Event-Feldwerten in die Security Incident-Felder im SIR-Incident zu unterstützen Spalte „Feldzuordnung“ auf der rechten Seite.
Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardmäßig angezeigte Felder sind in der Regel wichtige Felder, die im Security Incident Response-Formular ausgefüllt werden müssen. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mithilfe der Schaltflächen + und - angezeigt werden. Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie ArcSight ESM Felder zuordnen, die nicht im Standardzuordnungsraster des Security Incident angezeigt werden.

### Prozedur

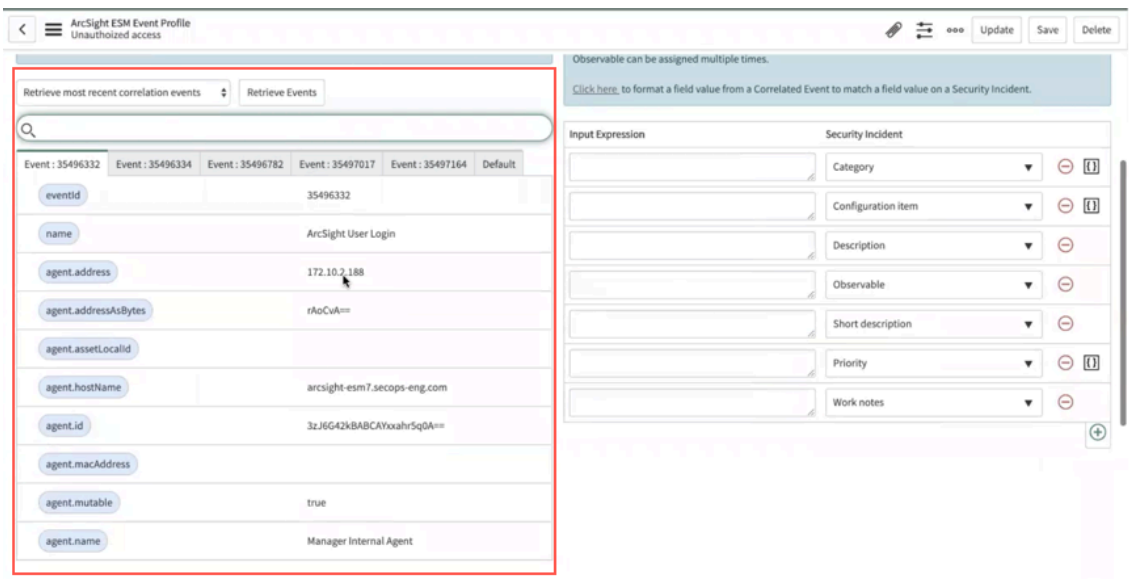
1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Sie können entweder die neuesten Beispielkorrelationsereignisse für die ausgewählte Korrelationsregel abrufen oder die eindeutigen Korrelationsereignis-IDs für die spezifischen Korrelationsereignisse angeben, die Sie für Ihre Korrelationsereigniszuordnungs-Experience verwenden möchten.
3. Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus:
   - Rufen Sie die neuesten Korrelationsereignisse ab
   - Wählen Sie Korrelations-Events basierend auf der Event-ID aus

   Klicken Sie auf **Ereignisse abrufen**, um die neuesten Beispielkorrelationsereignisse aus der Konsole ArcSight ESM für die ausgewählte Korrelationssuchregel abzurufen.

   Die Korrelations-Event-Felder und Werte-Ergebnisse werden als einzelne Registerkarten angezeigt.

   Der Abruf für Beispielkorrelationsereignisse kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   In der folgenden Abbildung werden die Feldname-Wert-Paare für das erfasste Korrelationsereignis oder die importierten Beispielereignisse auf der linken Seite dieses Formulars angezeigt, nachdem der Erfassungsabruf abgeschlossen ist. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.



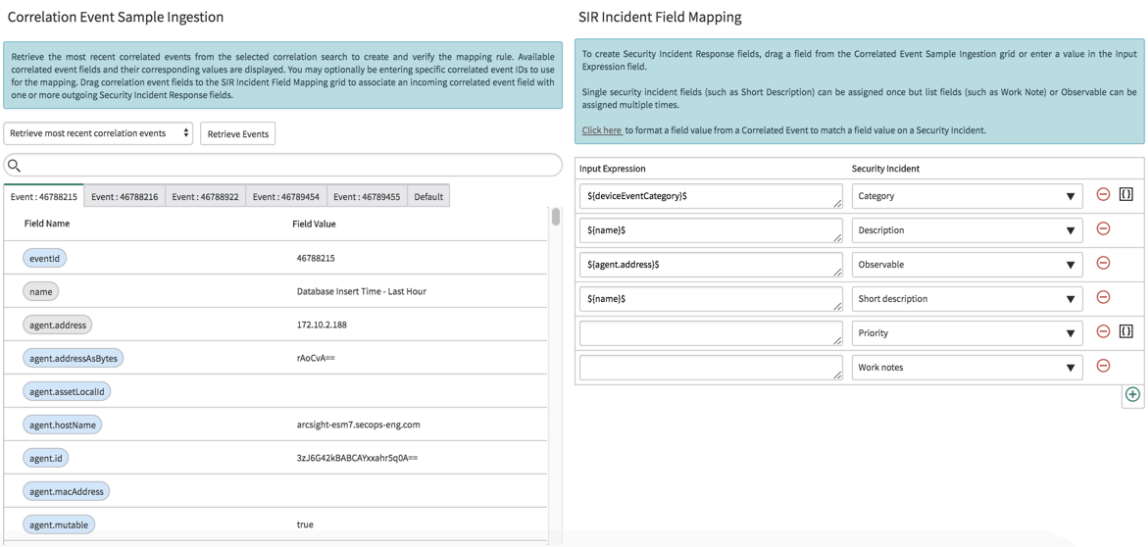



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.
5. Ziehen Sie den Feldnamen, z. B. agent.hostname, in ein Feld in der Spalte Eingabeausdruck neben einem Feldnamen in der Spalte Security Incident.

   Um sicherzustellen, dass keine Event-Felder im Zuordnungsprozess übersehen oder dupliziert werden, sind die Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Korrelationsereignisfeld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes Korrelationsfeld mehr als einem Feld in einem Security Incident zuordnen.

   Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Anhand dieser Farbcodierung können Sie nachverfolgen, welche Event-Felder bereits für zukünftige Security Incident-Feldzuordnungen verwendet wurden.




6. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

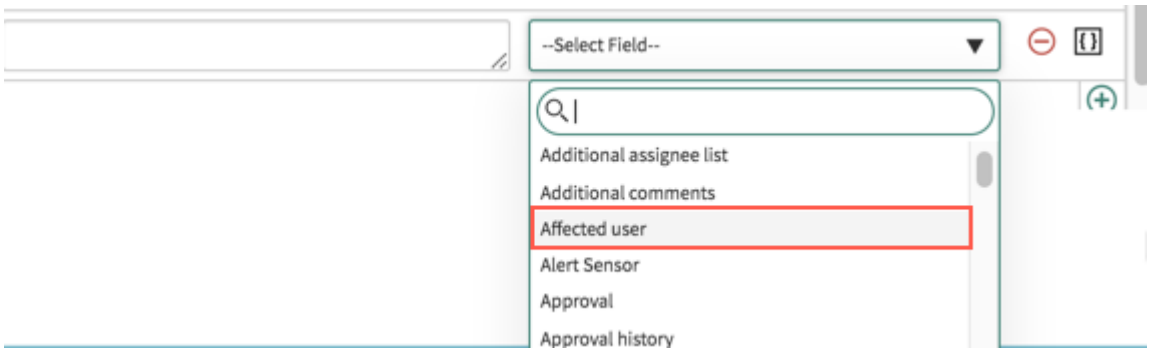
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ am unteren Rand des Rasters auf das Plus-Symbol.
   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat Betroffener Benutzer einen grauen Hintergrund, da er im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Korrelationsereignisfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

**c.** Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

**d.** Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um die **Event-ID** auszuwählen, die Sie im Feld **Eingabeausdruck** auswählen möchten.
Ordnen Sie es mit der Drag-and-Drop-Funktion neben Ihrem neuen Feld zu.

**7. Wahlweise:** Öffnen Sie den Skript-Editor, und setzen Sie die Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor, um Korrelations-Event-Werte für die ArcSight ESM -Integration zu formatieren.**Filterbedingungen für die Incident-Generierung**

**8. Wahlweise:** Nachdem Sie die vorherigen Schritte der Feldzuordnung abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Korrelationsereignis erfüllen muss, um einen SIR Security Incident zu erstellen.
Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

**a.** Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern, um die Option zu aktivieren.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Korrelationsereignis-Beispielerfassung“ für die von Ihnen erfassten Events angezeigt werden. Diese Felder sind dynamisch und ändern sich in Abhängigkeit von den Korrelationsereignissen, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Korrelationsereignisses ArcSight ESM übereinstimmen.



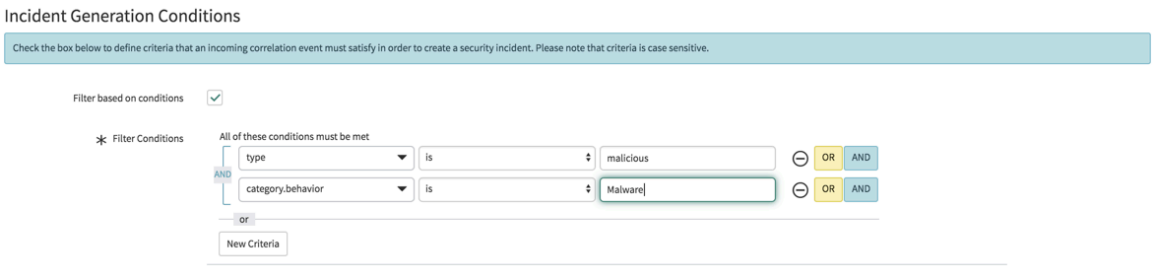
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

**b.** Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**. Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.

**c. Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.




(Optional) Sie haben die Generierungsbedingungen für Incidents so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Filterung der Incident-Generierungsbedingung hilft Ihnen, die Sicherheits-Events einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche zu ändern oder Events in ArcSight ESMherauszufiltern. Wenn zusätzliche Filterkriterien festgelegt werden, werden Incidents nur Korrelations-Events zugeordnet, die allen Kriterien entsprechen.

**Hinweis:**
Wenn einer der Event-Feldnamen Sonderzeichen enthält, z. B. Anführungszeichen (“), Bindestriche (’), Unterstriche (-) oder kaufmännische Und-Zeichen (@), müssen diese Zeichen möglicherweise für Zuordnungsübersetzungszwecke ersetzt werden und möglicherweise ein doppeltes Event erstellen Name. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Event-Namen zu unterscheiden. Beispiel: Wenn das erste Event-Feld „events.event“ und das zweite Event-Feld „events.event“ist, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Event-Feld ein Suffix hinzugefügt, und das Feld wird in Events@event(1)umbenannt.

### Ereigniszusammenfassungskriterien zur Behandlung ähnlicher Korrelationsereignisse und zur Verhinderung doppelter Incidents

**9. Wahlweise:** Um die Erstellung doppelter Security Incidents zu vermeiden, definieren Sie zusätzliche Event-Zusammenfassungskriterien, sodass eingehende Korrelations-Events zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:



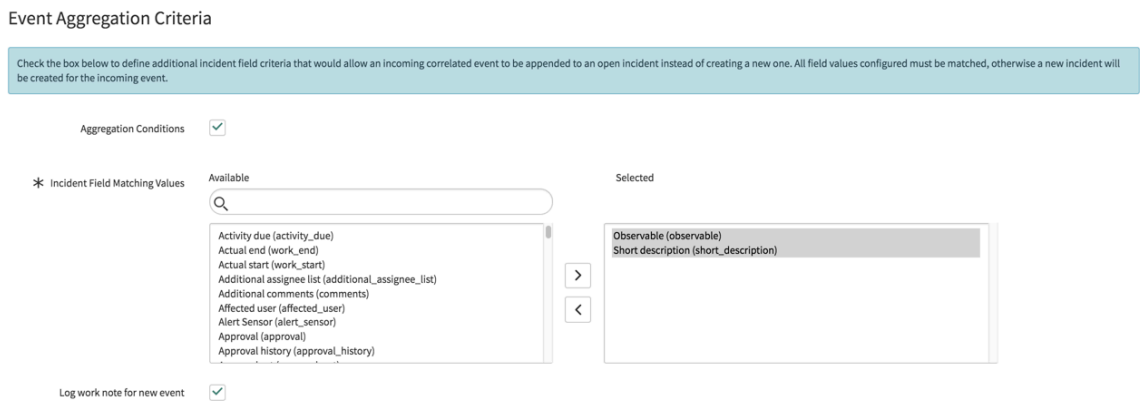
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Scrollen Sie im Formular zum Abschnitt **Event** -Zusammenfassungskriterien, und aktivieren Sie das Kontrollkästchen Zusammenfassungsbedingungen, um diese Option zu aktivieren.

(Optional) Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.

**b.** Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Now Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt.

(Optional) Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um dieses eingehende Korrelationsereignis an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Korrelations-Event-Feldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte abgeglichen wird, sind die Bedingungen für die Event-Zusammenfassung nicht erfüllt, und es wird ein neuer Security Incident erstellt. Im Screenshot unten sehen Sie die Zuordnung von Feldern mit mehreren Werten.



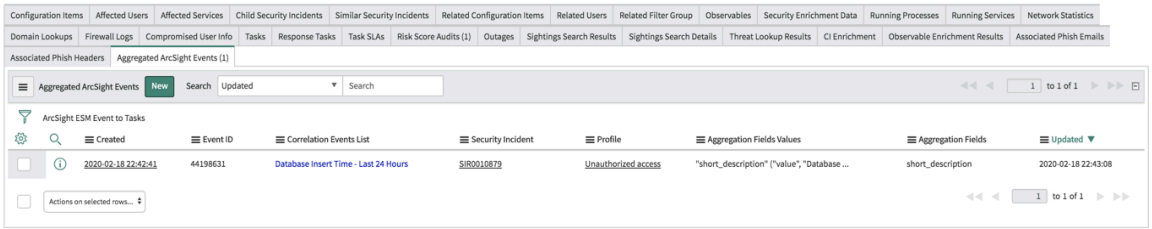

Wenn ein neues Korrelationsereignis mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird das neue Korrelationsereignis automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als SOC-Analyst, der mit Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Korrelations-Events in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Korrelations-Events für einen Security Incident werden in der zugehörigen Liste **Aggregierte ArcSight-Ereignisse** angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum diese Korrelations-Events zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter **Zugehörige Links**, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn diese zugehörige Liste nicht angezeigt wird, führen Sie die folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars, und klicken Sie auf **Konfigurieren** > **Zugehörige Listen**.
- Wählen Sie **Aggregierte ArcSight-Ereignisse** in der Liste Verfügbar aus, verschieben Sie sie in die Liste Ausgewählt, und klicken Sie auf **Speichern**.
- Klicken Sie **auf Zugehörige Listen anzeigen**. Sie sehen jetzt die Registerkarte **Aggregierte ArcSight-Ereignisse** im Abschnitt „Zugehörige Liste“.




**c. Wahlweise:** Um eine Arbeitsnotiz für jedes Mal zu protokollieren, wenn ein Event für den Security Incident zusammengefasst wird, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. Die Arbeitsnotiz protokolliert, dass ein neues korreliertes Event hinzugefügt wurde, zusammen mit einem Link zu den korrelierten Event-Details.

Sie haben Werte aus einem Korrelationsereignis erfolgreich Feldern in einem SIR Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung zu begrenzen. Sie haben auch Korrelations-Events zu vorhandenen SIR Security Incidents zusammengefasst, wenn Event-Feldwerte mit den konfigurierten Zusammenfassungskriterien übereinstimmen.

10. Wählen Sie eines aus, um mit der Profilkonfiguration fortzufahren.

### Zeigen Sie eine Vorschau des Security Incident für die ArcSight ESM -Integration der Ereigniserfassung an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Now Platform Security Incident Response (SIR)-Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Korrelationsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin.

#### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie als Benutzer mit der Rolle sn_si.admin eine Vorschau eines Security Incident an und bearbeiten Sie die Zuordnung bei Bedarf erneut, um fehlerhafte Felder zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von Security Incidents werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

#### Prozedur

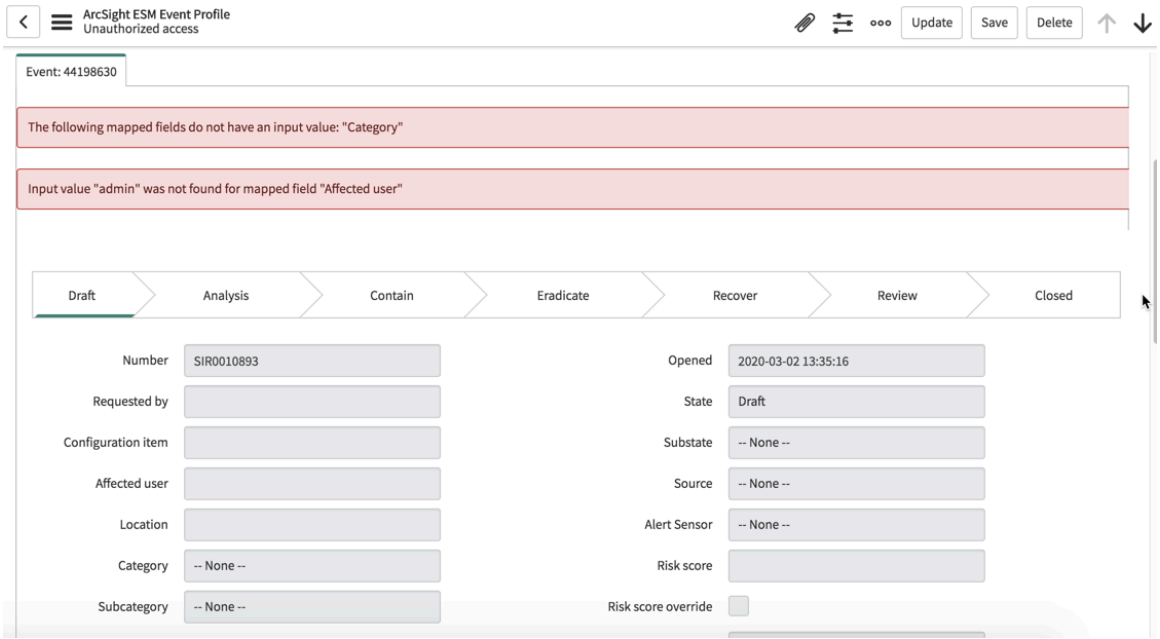
1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
2. Wählen Sie in der Auswahlliste Beispiel-Event-IDs ein Element aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.

3. Überprüfen Sie die Feldzuordnung der Korrelationsereigniswerte für den Security Incident.




Die vorherige Abbildung zeigt eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem Korrelationsereignis keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Eine Fehlermeldung wird angezeigt, die angibt, dass für das Feld Kategorie, das ein Referenzfeld mit einem bestimmten Wertesatz ist, kein Eingabewert gefunden wurde. Daher wird dieser zugeordnete Feldwert nicht ohne weitere Änderung im Security Incident-Formular SIR angezeigt.

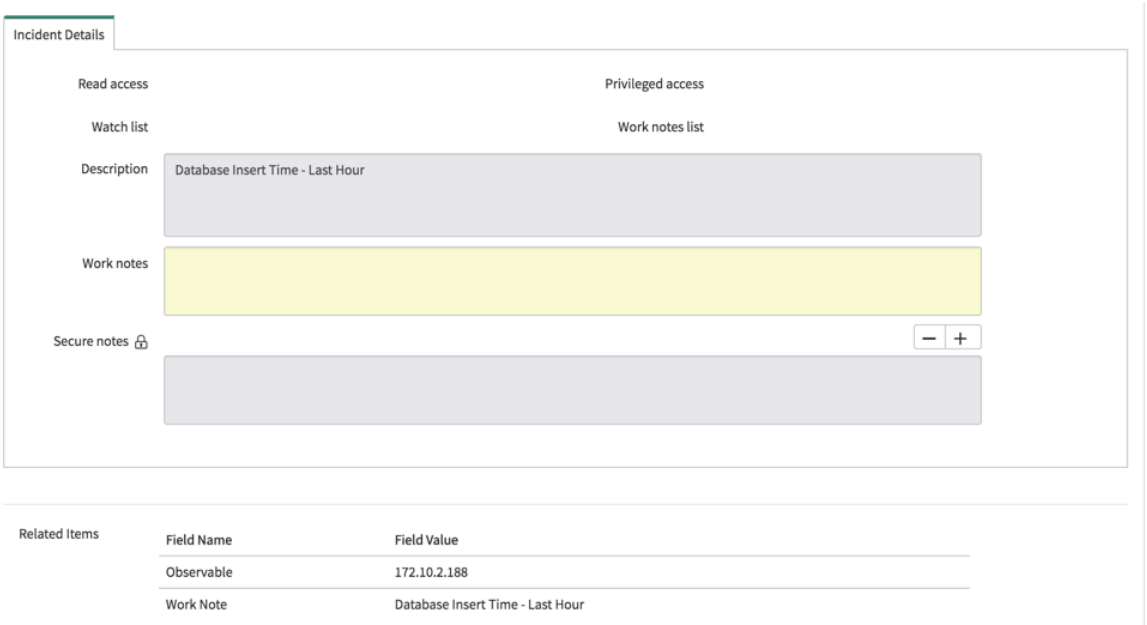
4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Incident-Details“ in der unteren Hälfte eines Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder „Beschreibung“ und „Arbeitsnotizen“ zugeordnet, und



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Felder werden mit den Werten aus den Wertepaaren ausgefüllt, die aus den ArcSight ESM Korrelationsereignisbeispielen abgerufen wurden.






## Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

### Erstellen Sie einen Zeitplan für die Ereigniserfassung ArcSight ESM .

Sie können den Abfrage- oder Abrufzeitplan für neue korrelierte Events definieren. Während dieses Schritts können Sie die vorhandenen Einstellungen für den Abruf von Korrelationsereignissen überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Korrelationsereignisse mithilfe eines Datumsbereichs abrufen.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin.

## Warum und wann dieser Vorgang ausgeführt wird

Sie können wählen, ob Sie historische Korrelations-Events während des Schritts „Zeitplanung“ erfassen möchten. Sie können auch auswählen, wie oft zukünftige neue Korrelations-Events abgefragt werden sollen, die der Profilkonfiguration entsprechen.

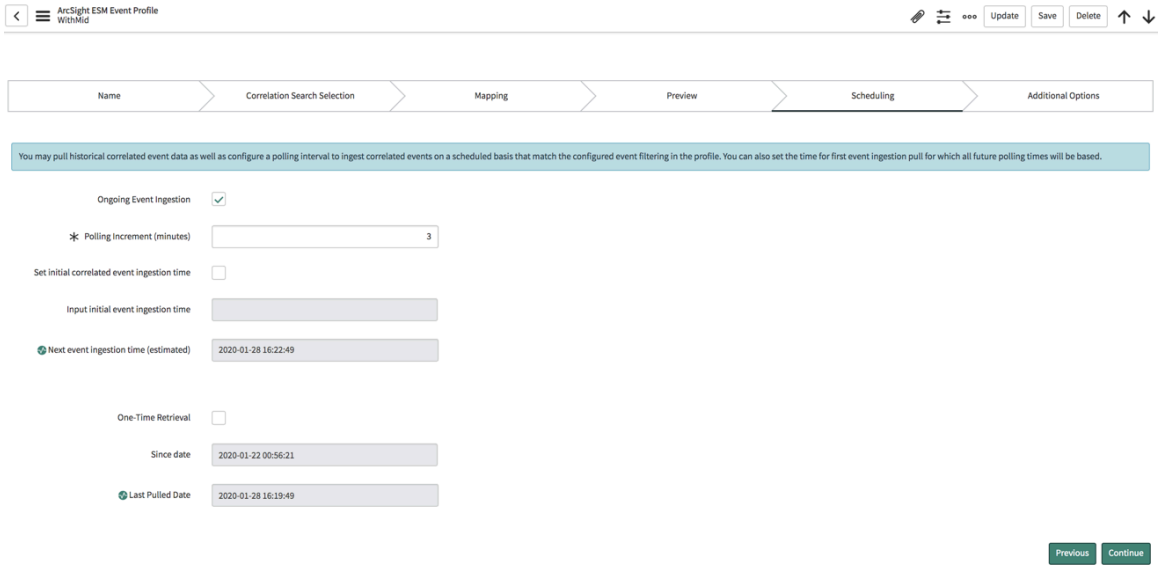
Als Benutzer mit der Rolle „sn_si.admin“ konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung der ArcSight ESM -Integration der Korrelationsereigniserfassung kann durch die unterschiedlichen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrage-Overheads auf dem ArcSight ESM -Server gegen den Wunsch ausgleichen, so schnell wie möglich benachrichtigt zu werden, wenn ein Event erstellt oder aktualisiert wird. Für jedes Profil wird ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

### Neue und aktualisierte Korrelationsereignisse werden abgerufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie eine aus, um zu planen, wie und wann Korrelationsereignisse aus dem abgerufen werden<ArcSight> -Konsole.




Beispiel für die Planung einer anfänglichen Erfassungszeit für Korrelationsereignisse: Wenn Sie eine tägliche Sicherheitsprüfung ArcSight ESM haben, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird, können Sie das entsprechende Korrelationsereignisprofil in Ihrer Instanz von Now Platform so einrichten, dass es um 16 Uhr ausgeführt wird :05 Uhr Ortszeit, um das Sicherheitsfehler-Event sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie `04 05 00` in das Feld Anfängliche Event-Erfassung ein. Geben Sie im Feld Increment (Minutes) (Schritt (Minuten)) `1440` (24 Stunden) ein, um die nächste Event-Erfassung für 24 Stunden nach der ersten Event-Erfassung zu planen. Sowohl die anfängliche Event-Erfassungszeit als auch die nächste Event-Erfassungszeit werden in den Feldern angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie bei angezeigter Seite „Zeitplanung“ das Kontrollkästchen **Ongoing event ingestion** (Laufende Event-Erfassung), um diese Option zu aktivieren.

   b. Geben Sie im Feld Schritt (Minuten) den Wert `1440` (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Anfängliche korrelierte Event** -Erfassungszeit festlegen, um die Bearbeitung der Felder Anfängliche Event-Erfassung und Nächste Event-Erfassung zu aktivieren.

   d. Geben Sie im Feld Anfängliche Event-Erfassungszeit `04 05 00`ein.
   Im Feld Nächste Event-Erfassungszeit (geschätzt) wird die Zeit der nächsten Event-Erfassung angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Fortfahren**, um zur Seite „Zusätzliche Optionen“ zu navigieren.

> **Hinweis:**
> Die Standardanzahl der Security Incidents, die an einem Tag erstellt und zusammengefasst werden können, und der Flow-Zeitraum sind in den ArcSight ESM Integrationseinstellungen definiert. Sie können diese Einstellungen bei Bedarf ändern. Details siehe ArcSight ESM Integration Einstellungen für die Integration der Event-Erfassung.

### Zusätzliche Optionen: Automatisieren Sie korrelierte Event-Aktualisierungen und -Abschlüsse basierend auf dem Incident-Status SIR .

Die ArcSight ESM -Integration verfügt über eine bidirektionale Schnittstelle, die sowohl Korrelationsereignisse zum Erstellen von Security Incidents ermöglicht, als auch die Möglichkeit, die Korrelationsereignisse zu aktualisieren, sobald der Security Incident mit relevanten Incident-Details wie der Security Incident-Nummer erstellt und/oder geschlossen wurde , Zuweisungsgruppe, SIR Incident-URL usw.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

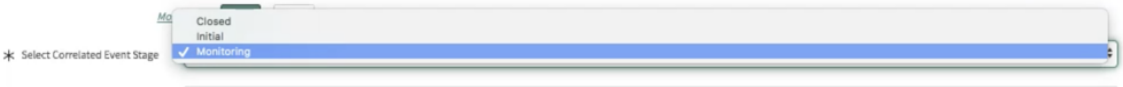
### Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die Anweisungen unten, um die Konfiguration für die Aktualisierung korrelierter Events abzuschließen, wenn der Security Incident erstellt wird.

   **Korrelierte Event-Phase nicht konfiguriert**: Wenn Sie in Ihrer Instanz Now Platform keine korrelierten Event-Phasen konfiguriert haben, wird in der Auswahlliste „Aktualisierung der korrelierten Event-Phase“ nur die **Option Phase zuweisen – Ersteinrichtung angezeigt**. Führen Sie die folgenden Schritte aus, um die Phase zu konfigurieren:

   - Geben Sie eine Ressourcen-ID in das Feld Stufenressourcen-ID eingeben ein, und klicken Sie auf **Absenden**. Die Ressourcen-ID wird in der Konsole ArcSight ESM validiert, und der folgende Bildschirm wird angezeigt.

   - Klicken Sie auf **Speichern**, um die neue Phase (**Überwachung**) zu speichern.
   - Klicken Sie auf die Dropdown-Liste Korrelierte Event-Phase auswählen.




   - Sie können die neu erstellte Phase aus der Liste auswählen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Korrelierte Ereignisphase bereits konfiguriert**: Wenn Sie die korrelierte Ereignisphase bereits konfiguriert haben, führen Sie die folgenden Schritte aus:

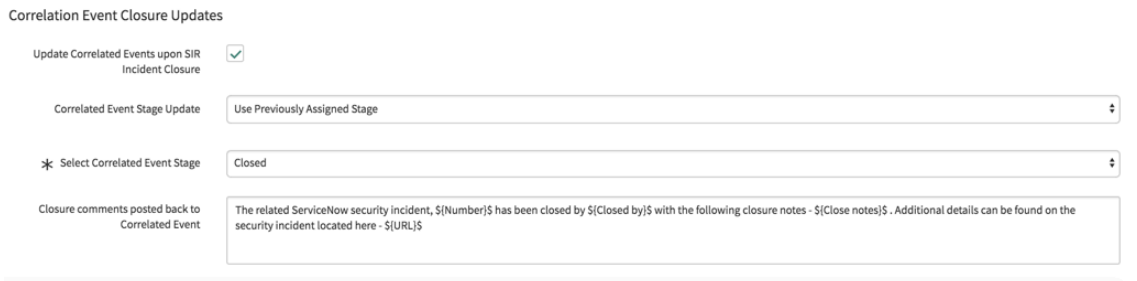
- Wählen Sie in der Auswahlliste „Aktualisierung der korrelierten Event-Phase“ die Option **Zuvor zugewiesene Phase verwenden** aus.
- Wählen Sie eine vorhandene Phase aus der Auswahlliste „Korrelierte Event-Phase auswählen“ aus, wie unten gezeigt.

- Anfangskommentare, die an das korrelierte Ereignis zurückgesendet werden: Sie können nicht nur den Wert der Korrelationsereignisstufe aktualisieren, sondern auch Kommentare zu den Anmerkungen der Korrelationsstufe veröffentlichen. Wie in den Anweisungen angegeben, können Sie den im Kommentarbereich angezeigten Standardtext bearbeiten, einschließlich des Hinzufügens oder Änderns der Ersetzungsvariablen im Format ${Feldname}$ für ein beliebiges Feld im Security Incident Response-Incident-Formular.

**Hinweis:**
Sie können entweder die in der Konsole ArcSight ESM definierten Standardphasen verwenden oder eigene benutzerdefinierte Phasen erstellen. Führen Sie die folgenden Schritte aus, um eine neue Phase zu erstellen:

- Wählen Sie in der Konsole ArcSight ESM aus **Datei** > **Neu** > **Phase**. Die Registerkarte Inspizieren/Bearbeiten wird angezeigt.
- Definieren Sie die neue Phase, und aktivieren Sie nicht das Kontrollkästchen **Benutzer erforderlich**. Stellen Sie sicher, dass die Phase richtig definiert ist und sich an der richtigen Position im Event-Lebenszyklus befindet.

3. Im Abschnitt „Automatisieren des Abschlusses korrelierter Ereignisse“ können Sie definieren, wie der Security Incident aktualisiert wird, wenn er geschlossen wird.
4. Füllen Sie die Felder des Formulars aus.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

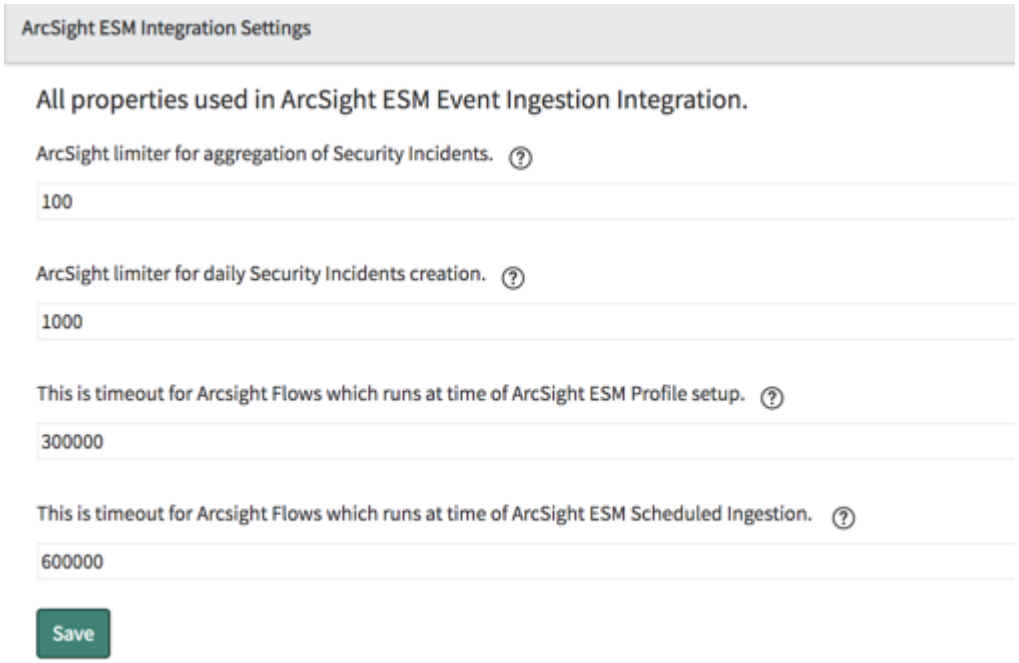
5. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um Korrelations-Events basierend auf Ihrer Planung aus der Konsole ArcSight ESM abzurufen.

### ArcSight ESM Integration Einstellungen für die Integration der Event-Erfassung

Verwenden Sie diese Option, um die standardmäßigen Erfassungseinstellungen von ArcSight ESM zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **ArcSight ESM-Integration** > **Einstellungen für ArcSight ESM-Integration**.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.




### Problembehandlung bei der Integration der ArcSight ESM Event-Erfassung

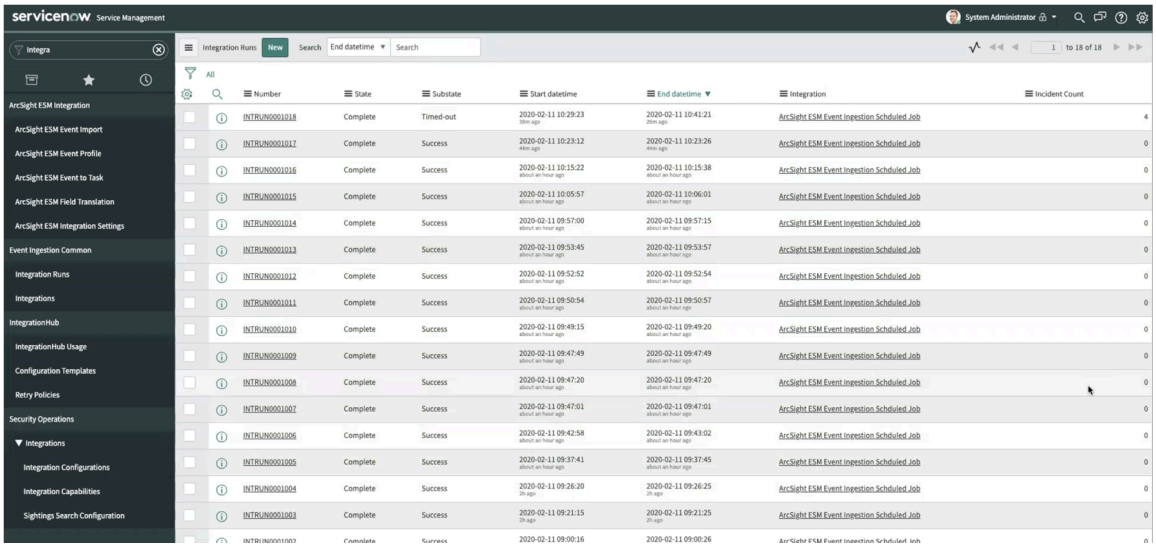
Dieser Abschnitt enthält Informationen zur Behebung von Fehlern, die während der Event-Erfassung auftreten können.

## Integrationsausführungen

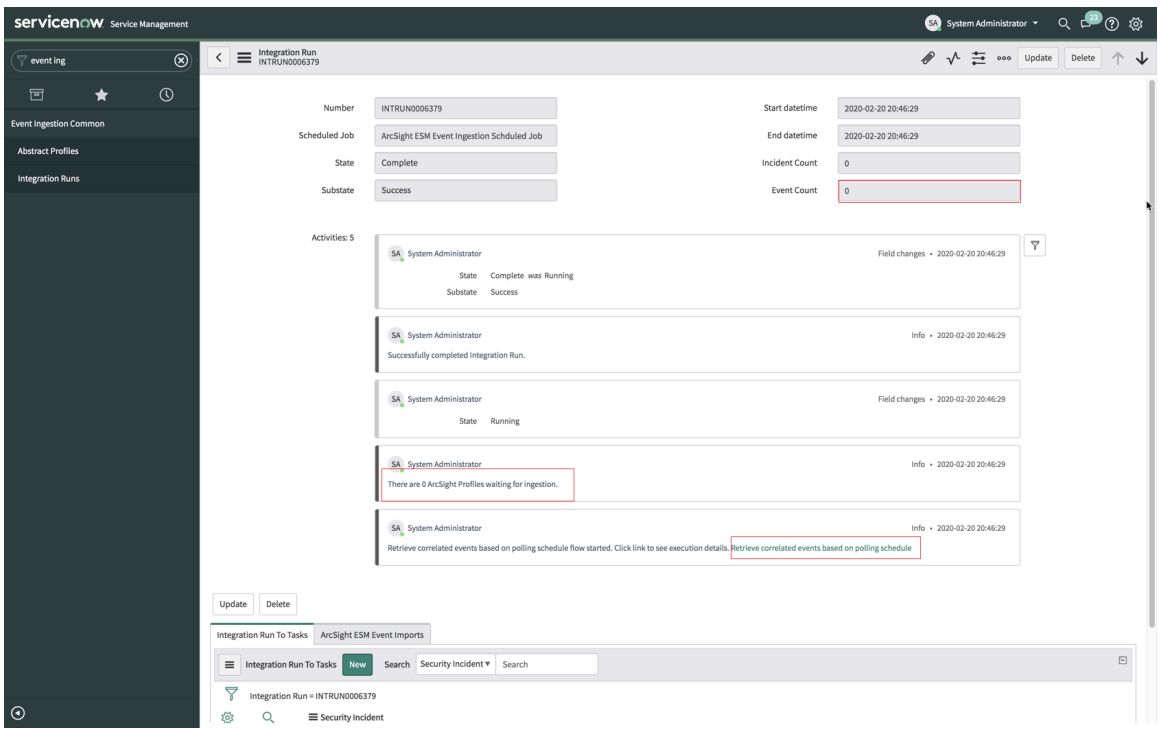
Navigieren zu **Event Ingestion Common** > **Integrationsausführungen**. Eine Integrationsausführung findet jede Minute statt und erfasst Details zu den während der geplanten Aufgabe erfassten Events.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie sehen die Liste der Integrationsausführungen und den Status jeder Ausführung (Erfolg, Zeitüberschreitung, Warten) und die Anzahl der erstellten Security Incidents. Klicken Sie auf den Link Nummer, um Detailinformationen zur Seite „Integrationsausführung“ anzuzeigen.



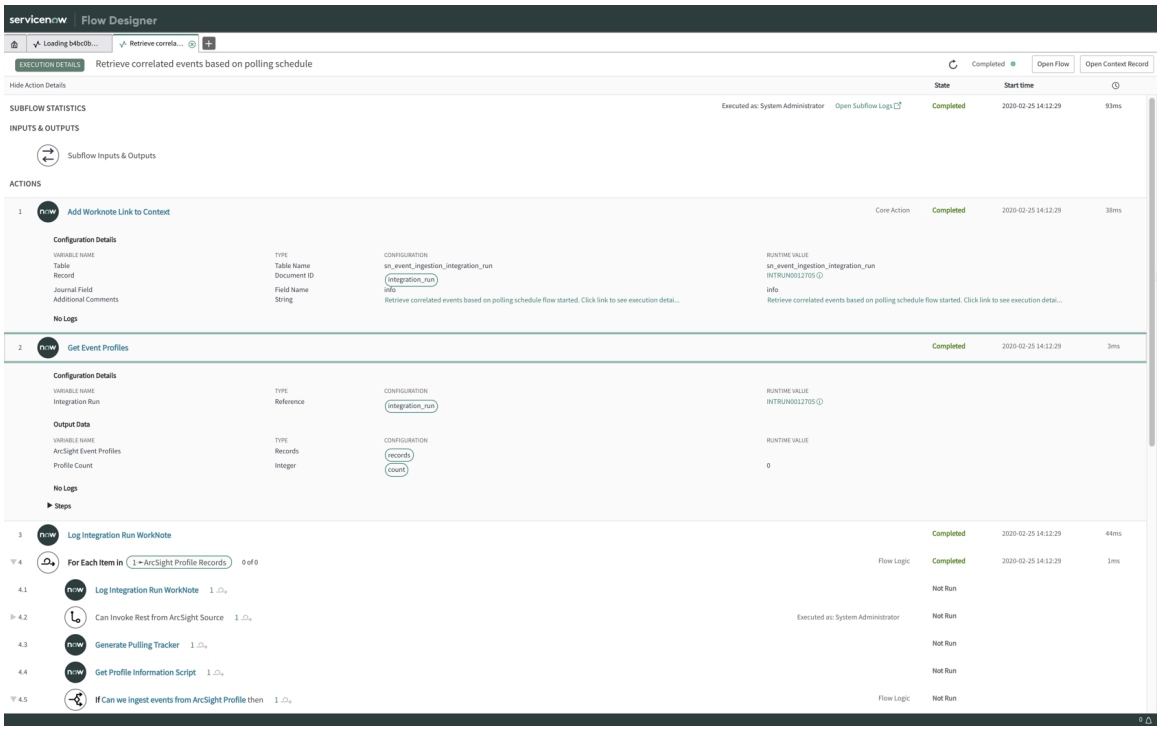

Sie können Details wie die Anzahl der erfassten Events, den Status, das Event, das in einen Security Incident umgewandelt wurde, und die verschiedenen Aufgaben anzeigen, die während der Erfassung ausgeführt wurden. Darüber hinaus können Sie auf den Link klicken, um die Details der Flow-Ausführung anzuzeigen.

## Flow-Ausführungsdetails

Klicken Sie auf den Link Ausführungsdetails, um den mit der Event-Erfassung verknüpften Flow anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie können eine Schritt-für-Schritt-Ausführung des Flows anzeigen, in der die verschiedenen Aktionen und Subflows aufgeführt sind, die als Teil des Flows ausgeführt wurden.

### Kopieren Sie das Profil ArcSight ESM für die Integration der Event-Erfassung

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Profile zu kopieren, um Zeit zu sparen.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

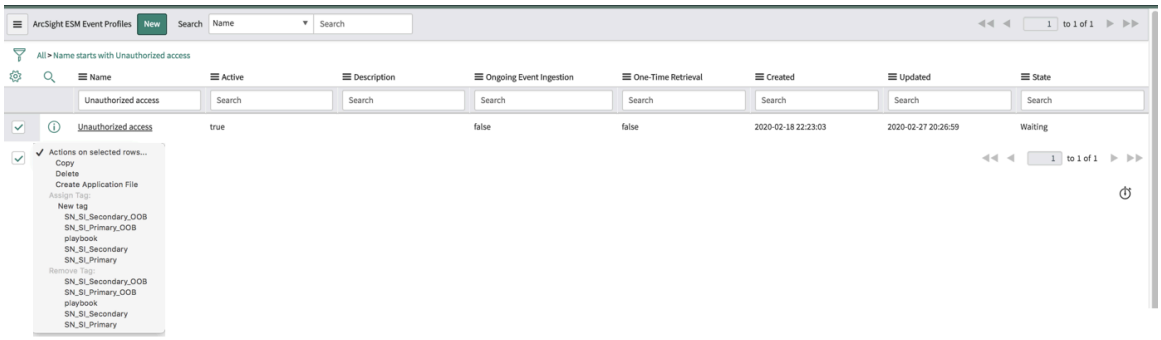
Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

## Prozedur

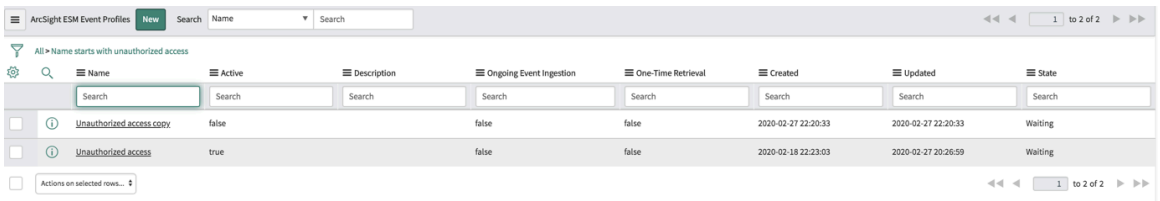
1. Navigieren zu **Alle** > **ArcSight ESM-Integration** > **ArcSight ESM-Ereignisprofil**.
2. Wählen Sie in der angezeigten Liste „ArcSight-Profile“ ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.




Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **Aktiv** auf „false“ gesetzt ist, da das Profil aktiviert werden muss.

### Verwenden Sie den Skript-Editor, um Korrelations-Event-Werte für die ArcSight ESM -Integration zu formatieren

Verwenden Sie zusätzlich zu den direkt zugeordneten Feldern aus den erfassten Korrelationsereigniswerten den Skript-Editor, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Der Skript-Editor ändert die Werte eines ArcSight ESM -Korrelations-Event-Felds, sodass Werte, die vom Now Platform SIR -Security Incident unterstützt werden, der Kategorie, dem Konfigurationselement (CI), dem erkennbaren Element und anderen Security Incident-Feldern zugeordnet werden.

In bestimmten Fällen werden ArcSight ESM Korrelationsereigniswerte Referenzfeldern wie „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ im Security Incident zugeordnet. Als Benutzer mit der Rolle sn_si.admin ziehen Sie es möglicherweise vor, die zugeordneten Event-Feldwerte zu bearbeiten, um Format- oder Datenwerte so zu übersetzen, dass sie den erwarteten Incident-Feldformaten und -Werten entsprechen. Wenn Sie den Wert eines Korrelationsereignisses ArcSight ESM in einen Wert übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.
2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Configuration Item geeignet sein. Für ein Korrelationsereignis kann beispielsweise ein Wert für das Konfigurationselement nicht abgeglichen werden.

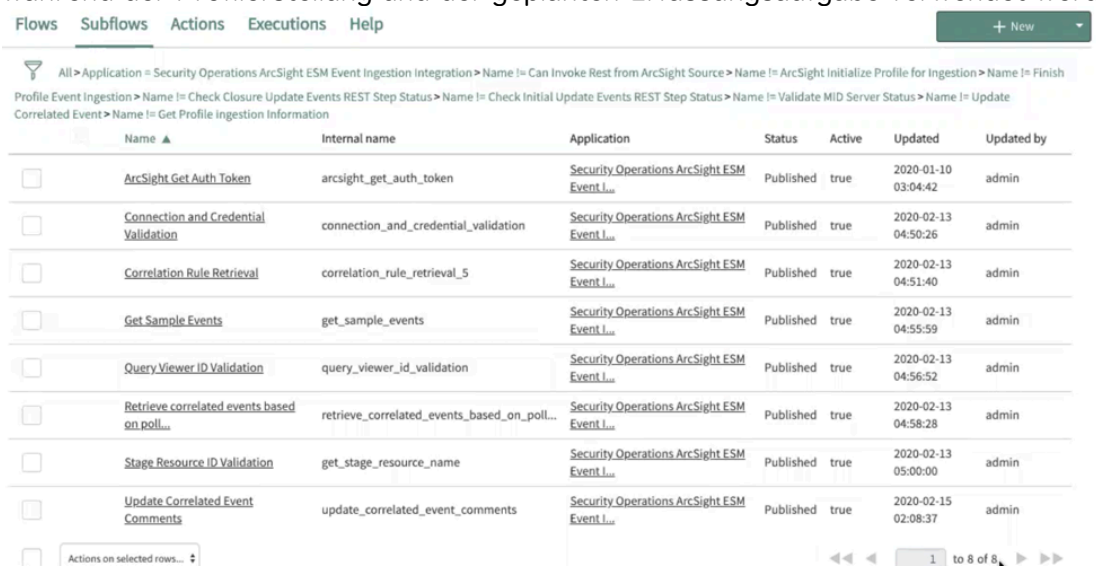
   Wie in der folgenden Abbildung dargestellt, können Sie, wenn in der Now Platform CMDB für das Feld „Konfigurationselement“ keine Übereinstimmung mit einem Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld „Konfigurationselement“ ausgefüllt wird, wenn eine IP-Adresse gefunden wird.

   Der Editor wird geöffnet, und das Feld wird in Zielfeld angezeigt.
4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle ArcSight ESM „ Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Formular „Zuordnung“ zurückzukehren.

### Flow Designer-Nutzung mit ArcSight ESM Integration der Event-Erfassung

Mit Integration Hub und Flow Designer sind mehrere Flows, Subflows und Aktionen mit der ArcSight ESM -Integration verfügbar.

Um diese Subflows anzuzeigen, navigieren Sie zu **Flow Designer** > **Designer** und klicken Sie auf die Registerkarte **SubFlows**. Die folgende Abbildung zeigt die wichtigen Subflows, die während der Profilerstellung und der geplanten Erfassungsaufgabe verwendet werden.




Diese Subflows sind in der Reihenfolge aufgelistet, in der sie ausgeführt werden:

- **Validierung von Verbindungen und Anmeldeinformationen**: Dieser Subflow validiert die Konnektivität von ServiceNow mit dem Server ArcSight ESM und die angegebenen Anmeldeinformationen. Dieser Subflow wird verwendet, wenn Sie in der **Kachel „ArcSight ESM – Event Ingestion“** in auf die Schaltfläche **Konfigurieren**klicken **Security Operations** > **Integrationen** > **Integrationskonfiguration** Seite.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ArcSight**Authentifizierungstoken abrufen: Dieser Subflow generiert das Authentifizierungstoken ArcSight ESM aus dem Benutzernamen und dem Passwort mithilfe des Anmeldeservice ArcSight ESM. Der Login-Service stellt das Authentifizierungstoken bereit, das zum Aufrufen eines anderen ArcSight ESM -Endpunkts verwendet werden kann. Dieser Subflow wird in allen anderen Subflows verwendet.
- **Validierung der Abfrage-Viewer-ID**: Dieser Subflow überprüft, ob die während der Profilerstellung angegebene Abfrage-Viewer-ID auf dem Server ArcSight ESM vorhanden ist.
- **Korrelationsregelabruf**: Dieser Subflow ruft die Korrelationsregeln basierend auf der Abfrage-Viewer-ID ab.
- **Beispielereignis**abrufen: Dieser Subflow ruft die Beispielkorrelationsereignisse vom Server ArcSight ESM ab. Diese Beispiel-Events werden dann den Security Incident-Feldern im Abschnitt „Zuordnung“ des Profils zugeordnet.
- **Validierung der Phasenressourcen-ID**: Dieser Subflow validiert die in der Konsole ArcSight ESM angegebene Phasenressourcen-ID und ruft den Ressourcennamen ab.
- **Korrelierte Ereigniskommentare**aktualisieren: Dieser Subflow aktualisiert die korrelierten Ereigniskommentare in den Abschnitten „Anfang“ und „Abschluss von Incidents“ auf der Seite „Zusätzliche Optionen“ des Profils.
- **Korrelierte Ereignisse basierend auf**Abfragezeitplan abrufen: Dieser Subflow führt die geplante Aufgabe aus, die die korrelierten Ereignisse basierend auf dem Abfrageintervall abruft.

Während der Ausführung lösen die obigen Subflows auch mehrere andere Subflows und Aktionen aus, entweder direkt oder indirekt, wie unten gezeigt.

Flows Subflows Actions Executions Help + New

| | | | | | | |
|---|---|---|---|---|---|---|
| Can Invoke Rest from ArcSight Source | can_invoke_rest_from_arcsight_source | Security Operations ArcSight ESM Event I... | Published | true | 2020-01-07 00:46:32 | admin |
| Check Closure Update Events REST Step St... | check_closure_update_events_rest_step_st... | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:48:08 | admin |
| Check Initial Update Events REST Step St... | check_rest_step_status | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:48:55 | admin |
| Connection and Credential Validation | connection_and_credential_validation | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:50:26 | admin |
| Correlation Rule Retrieval | correlation_rule_retrieval_5 | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:51:40 | admin |
| Finish Profile Event Ingestion | end_process_run | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:53:48 | admin |
| Get Profile Ingestion Information | get_last_run_date | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:54:31 | admin |
| Get Sample Events | get_sample_events | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:55:59 | admin |
| Query Viewer ID Validation | query_viewer_id_validation | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:56:52 | admin |
| Retrieve correlated events based on poll... | retrieve_correlated_events_based_on_poll... | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 04:58:28 | admin |
| Stage Resource ID Validation | get_stage_resource_name | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 05:00:00 | admin |
| Update Correlated Event | update_correlated_event | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 23:12:18 | admin |
| Update Correlated Event Comments | update_correlated_event_comments | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-15 02:08:37 | admin |
| Validate MID Server Status | validate_mid_server_status | Security Operations ArcSight ESM Event I... | Published | true | 2020-02-13 05:03:40 | admin |

## Integration von Carbon Black - Incident Enrichment

Verwenden Sie die Carbon Black-Integration, um Security Incidents mithilfe von APIs zu untersuchen und darauf zu reagieren, um Endpunkte abzufragen und mit ihnen zu interagieren, die mit Security Incidents verknüpft sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Suchen Sie nach Carbon Black - Incident Enrichment-Integrationsressourcen

- Erste Schritte mit der Integration von Carbon Black - Incident Enrichment
- Security Operations Carbon Black Integration - Laufende Prozesse abrufen Workflow
- Security Operations Carbon Black Integration - Host-Workflow isolieren
- Security Operations Carbon Black-Integration – Hostisolierung entfernen
-

## Machen Sie sich mit Integrationskonzepten vertraut

- Typen der bereitgestellten ServiceNow -Integrationen
- Security Operations Workflow-Auslöser

## Holen Sie sich Hilfe von ServiceNow-Ressourcen

- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- Führen Sie ein Upgrade auf Madrid durch

### Erste Schritte mit der Integration von Carbon Black - Incident Enrichment

Die Carbon Black Incident-Ergänzung erleichtert die Untersuchung eines Security Incident, indem Protokolle nach potenziell schädlichen Indikatoren abgefragt werden. Bevor Sie die Integration „Carbon Black - Incident Enrichment“ verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechende Endpunkt-Basis-URL und den MID-Server hinzufügen.

#### Vorbereitungen

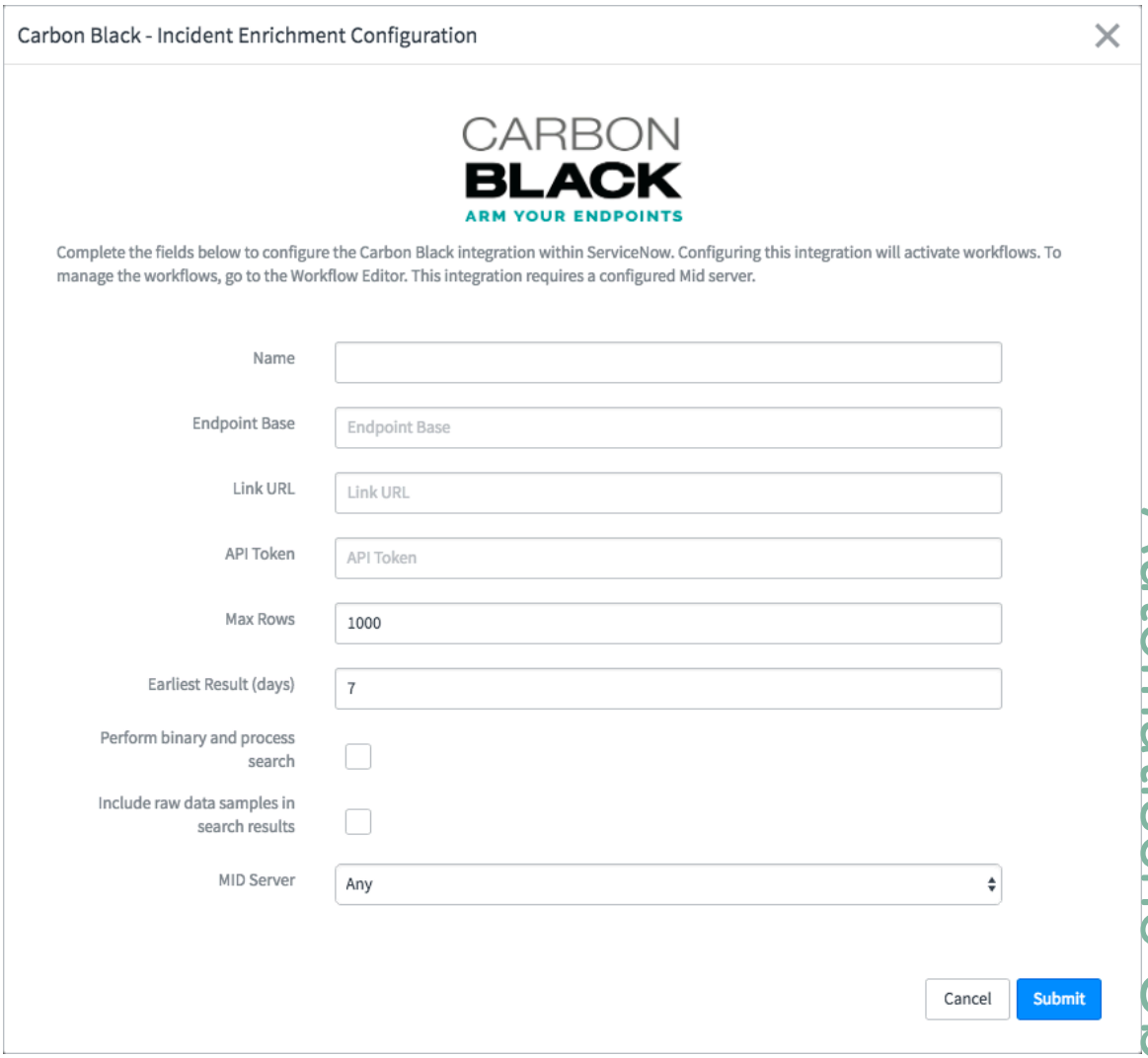
Erforderliche Rolle: sn_si_admin

#### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn der Download abgeschlossen ist, greifen Sie auf die Website Carbon Black zu, und rufen Sie die Endpunkt-Basis-URL und das API-Token unter Ihrem Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
4. Klicken Sie auf der Karte Carbon Black - Incident Enrichment auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**5.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Endpunktbasis | Die Endpunkt-URL, die Sie von der Carbon Black-Website abgerufen haben. |
| Link-URL | Die Link-URL, die auf eine Carbon Black-Instanz verweist, sofern verfügbar. |
| API-Token | Das API-Token, das Sie von der Carbon Black-Website erhalten haben. |
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. Der Standardwert ist 1000 Zeilen. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |
| Binär- und Prozesssuche durchführen | Wählen Sie diese Option aus, um binäre Suchen durchzuführen, um binäre Dateien wie Datei-Hashes zu finden, und Prozesssuchen nach .exe-Prozessen, die möglicherweise ausgeführt wurden. |
| Rohdatenmuster in | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Suchergebnissen berücksichtigen | von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## Integration mit Carbon Black

Mit der Carbon Black-Integration können Sie Security Incidents mithilfe von APIs untersuchen und darauf reagieren, um Endpunkte abzufragen und mit ihnen zu interagieren, die mit Security Incidents verknüpft sind.

### Erkunden

- Security Incident Response-Integrationen
- Integration von Carbon Black - Incident Enrichment

### Einrichten

Beginnen Sie mit der Integration von Carbon Black

### Verwenden

- Security Operations Workflow-Auslöser
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Workflow „Security Operations – Laufende Prozesse abrufen“.
- Security Operations Carbon Black Integration - Laufende Prozesse abrufen Workflow
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Blockierungsanforderung ausführen
- Workflow „Security Operations Integration - Block Request“.
- Führen Sie „Host isolieren“ aus
- Security Operations Carbon Black Integration - Host-Workflow isolieren
- Security Operations Carbon Black-Integration – Hostisolierung entfernen

### Entwickeln

- ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Problembehandlung und Hilfe**

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

## Beginnen Sie mit der Integration von Carbon Black

Carbon Black ist ein fortschrittliches Sicherheitssystem, das sich leicht in Security Operations integrieren lässt. Bevor Sie die Carbon Black-Integration verwenden können, müssen Sie die Integration aus dem ServiceNow Store herunterladen und die entsprechende Endpunktbasis und das API-Token hinzufügen.

### Vorbereitungen

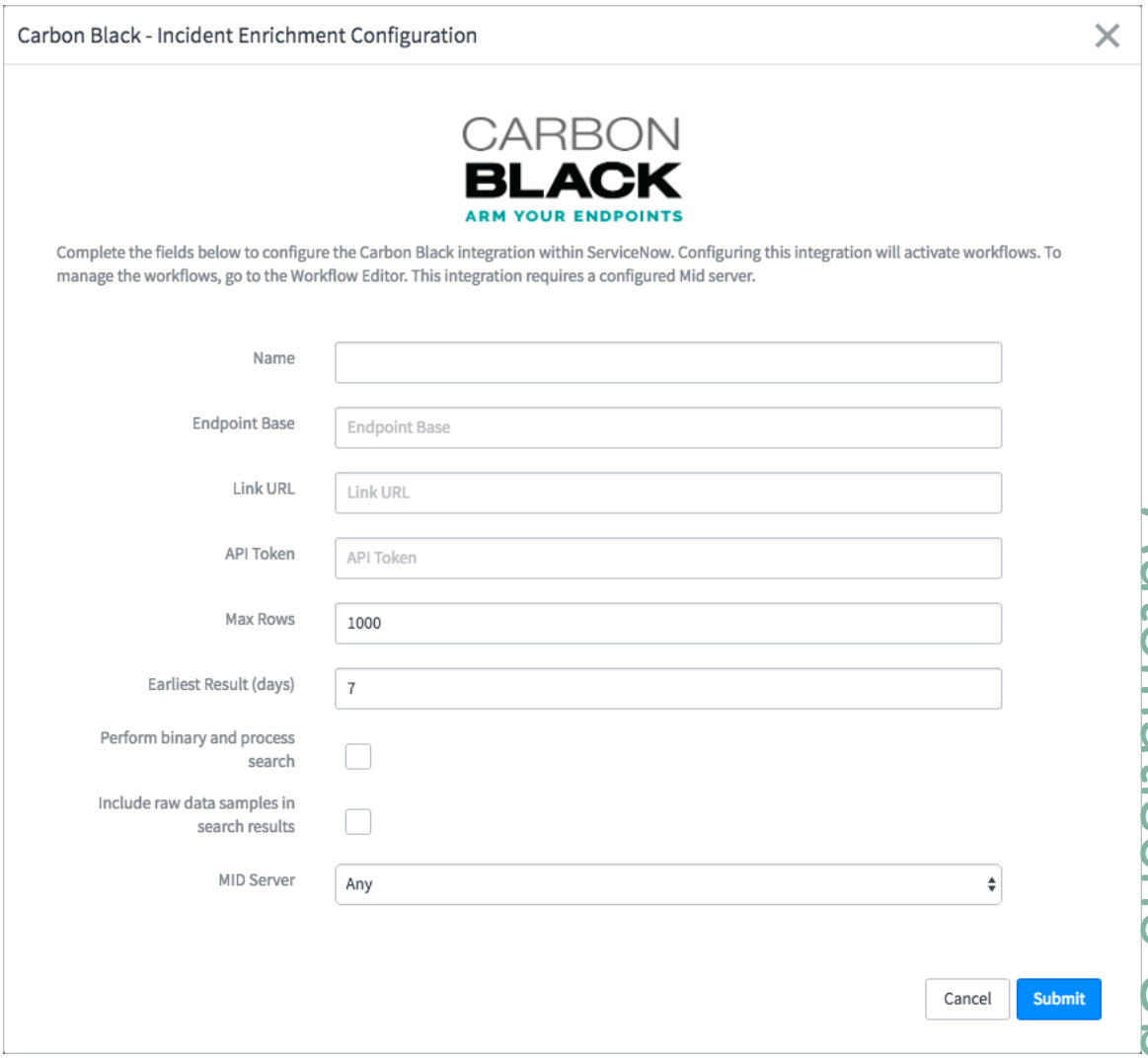
Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Greifen Sie nach Abschluss der Installation auf die Website Carbon Black zu, und rufen Sie die Endpunkt-Basis-URL und das API-Token unter Ihrem Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie in der Karte Carbon Black auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**5.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Endpunktbasis | Die Endpunktbasis, die Sie von der Carbon Black-Website abgerufen haben. |
| API-Token | Das API-Token, das Sie von der Carbon Black-Website erhalten haben. |
| MID-Server verwenden | Aktivieren Sie dieses Kontrollkästchen, wenn es nicht bereits aktiviert ist. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |
| Hostisolierung aktivieren | Aktivieren Sie dieses Kontrollkästchen, damit ausgewählte Konfigurationselemente in einem Security Incident von der Registerkarte „ **Konfigurationselemente** “ der zugehörigen Liste isoliert werden können. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## Integration mit Check Point Anti-Bot - Email Parser

Die Integration von Check Point Anti-Bot – Email Parser wird mithilfe eines E-Mail-Parsers unterstützt, der E-Mail-Benachrichtigungen von Check Point Anti-Bot verwendet, um Security Incidents zu erstellen und Ergänzungs- und Antwort-Workflows zu unterstützen.

### Konfigurieren Sie die Check Point Anti-Bot - Email Parser-Integration

Die Integration von Check Point Anti-Bot - Email Parser verwendet E-Mail-Benachrichtigungen, um die Ergänzungs- und Antwort-Workflows voranzutreiben.

#### Vorbereitungen

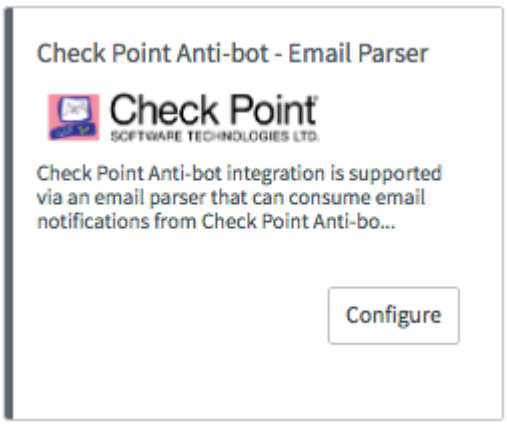
Erforderliche Rolle: sn_si_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Für die Integration wird eine Check Point Anti-Bot-E-Mail-Parser-Vorlage bereitgestellt. Sie muss vor der Integration konfiguriert und aktiviert werden. Durch Aktualisieren des Parsers wird dieser aktiviert.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.




2. Klicken Sie auf der Karte „Check Point Anti-Bot – Email Parser“ auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld „ **Check Point Anti-Bot – Email Parser Configuration** “ auf den Link **Konfigurieren Email Parser**.
4. Klicken Sie auf den Link **Check Point Anti-Bot**, um die Einstellungen im bereitgestellten E-Mail-Parser für Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E- Mail ist von aus. Informationen zum Erstellen eines E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Analyse** “ auf **Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Integration „Check Point Next Generation Threat Prevention“

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um die Fähigkeiten von Check Point Next Generation Threat Prevention (NGTP) mit ServiceNow® Security Incident Response (SIR) zu integrieren, damit -Anwendungen ordnungsgemäß zusammen funktionieren.

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe von Sperranforderungslistenfunktionen mit den ServiceNow Security Incident Response (SIR)-Produkten zu blockieren. Diese Sperranforderungsliste wird auf Prüfpunkt-Gateways als benutzerdefinierter Intelligenz-Feed konfiguriert. Die Funktion „Custom Intelligence Feeds“ bietet die Möglichkeit, der Next Generation Threat Prevention-Engine benutzerdefinierte Cyber Intelligence-Feeds hinzuzufügen. Ermöglicht das Abrufen von Feeds von einem Drittanbieterserver, in diesem Fall die Anwendung ServiceNow Security Incident Response, direkt an das Check Point Next Generation Gateway, um von Anti-Virus- und Anti-Bot-Blades erzwungen zu werden. Der Security Incident Response-Analyst erstellt Einträge für die Check Point-Sperrliste aus erkennbaren Elementen, die bei ServiceNow SIR-Security Incidents als böswillig eingestuft wurden.

Bei den meisten Implementierungen ist eine Sperranforderungsliste eine CSV-Datei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihre Now Platform-Instanz, die es der Check Point Threat Prevention Engine der nächsten Generation ermöglicht, die Liste der zu blockierenden IP-Adressen, URLs und Domänen abzurufen.

Um die blockierenden erkennbaren Elemente auf dem Prüfpunkt-Gateway zu erzwingen, stellen Sie sicher, dass die Bedrohungsabwehrrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist. Wenn die Sperrlisteneinträge geändert werden, importiert die Threat Prevention Engine die Liste dynamisch im konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit für die Firewall. Für diese Integration hat Now Platform eine Tabelle mit Sperrlisteneinträgen erstellt, die vom autorisierten Check Point Next-Gen-Gateway in den konfigurierten Abrufintervallen abgerufen werden.

Die Integration umfasst die folgenden Funktionen:

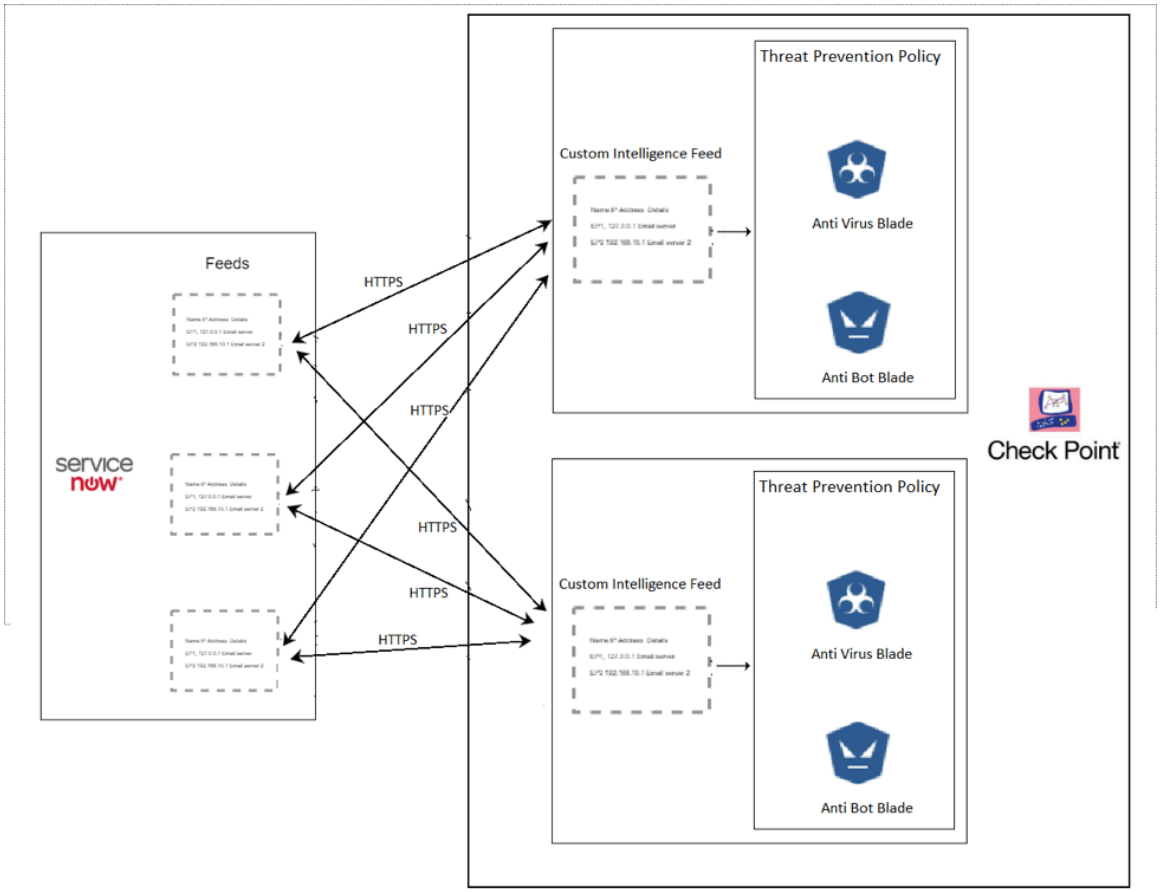
- Flexibilität beim Erstellen mehrerer Sperrlisten, die für mehrere Prüfpunkt-Gateways gelten.
- Detaillierte Berichte über die Arten von Websites, die blockiert werden (Phishing, Malware und auf Allow-Listen aufgeführte Websites).
- Kennzeichnung von Now Platform-Security Incidents mit Sperrlisteneinträgen nach erkennbarem Typ (URL, Domäne, IP-Adresse).
- Konfigurieren der Ablaufzeiträume für Sperrlisten, um die Größe der Sperrliste beizubehalten, indem ältere Einträge automatisch ablaufen oder entfernt werden.
- Durchsuchen von Sperrlisteneinträgen zwischen verschiedenen Sperrlisten.
- Verknüpfen von Sperrlisteneinträgen mit Datensätzen erkennbarer Elemente und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert ist.

## Diagramm der Integrationsarchitektur

Nachfolgend finden Sie das allgemeine Architekturdiagramm, das die beteiligten Komponenten und Integrationspunkte zwischen NOW Platform und Check Point Systems darstellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Das Check Point Systems-Logo, das Anti-Virus Blade-Bild und das Anti Bot Blade-Bild stammen von Check Point Systems ©. Sie sind die Eigenschaft von Check Point Systems.

## Plugins

Die Integration erfordert die Aktivierung des Plugins Security Incident Response (com.snc.security_incident).

So installieren Sie Security Incident Response Plugins:

1. Melden Sie sich mit Ihren HI-Anmeldeinformationen bei Ihrer Instanz an.
2. Vergewissern Sie sich, dass Sie über die Administratorrolle (admin) verfügen.
3. Navigieren Sie in Ihrer Instanz zu Systemdefinition>Plugins.
4. Wählen und klicken Sie auf Security Incident Response.

Sobald diese Plugins installiert wurden, können Sie das neue Check Point-Integrations-Plugin aus dem ServiceNow Store hochladen und die folgenden Konfigurationsanweisungen befolgen.

## Unterstützte Versionen des Prüfpunkt-Betriebssystems

Diese Integration erfordert den benutzerdefinierten Intelligenz-Feed von Check Point. Installieren Sie den Hotfix der benutzerdefinierten Intelligenzfunktion, bekannt als Check Point R80.10 Jumbo HF, Version 121 und höher. Weitere Informationen zur Produktkompatibilitätsmatrix finden Sie im Installationsabschnitt der Check Point Custom Intelligence-Feed-Dokumentation.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Stellen Sie nach der Installation des Hotfixes sicher, dass die folgenden Befehle auf dem Check Point Gateway zugänglich sind. Stellen Sie eine SSH-Verbindung zum Gateway her, und melden Sie sich im Expertenmodus an.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

## Unterstützte ServiceNow-Versionen

Release-Version San Diego oder höher wird unterstützt.

## Referenzen

Im Folgenden finden Sie einige der Prüfpunktreferenzen, die beim Einrichten der Voraussetzungen hilfreich sind.

1. Funktion für benutzerdefinierte Intelligenz-Feeds: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Check Point-Benutzerhandbuch. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Um die HTTPS-Inspektion für Check Point einzurichten, klicken Sie auf den folgenden Link. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

## Berechtigungen und Rollen

Die folgenden ServiceNow-Rollen sind erforderlich.

- Administrator (admin) für die Installation des Integrationsanwendungs-Plugins
- Security Incident-Administrator (sn_si.admin) für die Erstellung von Sperrlisten in ServiceNow und die Genehmigung von Anforderungen zum Hinzufügen und Deaktivieren von Sperrlisteneinträgen.
- Sicherheitsanalyst (hier auch als SOC-Analyst bezeichnet, sn_si.analyst) für die Erstellung und Verwaltung von Sperrlisteneintragsdatensätzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um weitere Informationen zum Zuweisen der Rolle „Sicherheitsanalyst“ zu erhalten, navigieren Sie auf der ServiceNow-Dokumentationswebsite zu Security Operations>Security Incident Response> Sicherheitsanalysten zuweisen.

### Setup von Check Point NGTP

Bevor Sie die Check Point NGTP -Integration verwenden können, müssen Sie ein API-Konto erstellen, Richtlinien einrichten und die Integration aktivieren.

### Erstellen Sie ein API-Konto für die Check Point NGTP -Integration

Für diese Integration ist in Ihrer Now Platform-Instanz eine API-Kontorolle erforderlich. Der Benutzername und das Passwort, die diesem Konto zugeordnet sind, werden in Now Platform erstellt und in Check Point eingegeben, sodass sich Check Point beim Abrufen von Sperrlisteneinträgen bei Now Platform authentifiziert.

#### Vorbereitungen

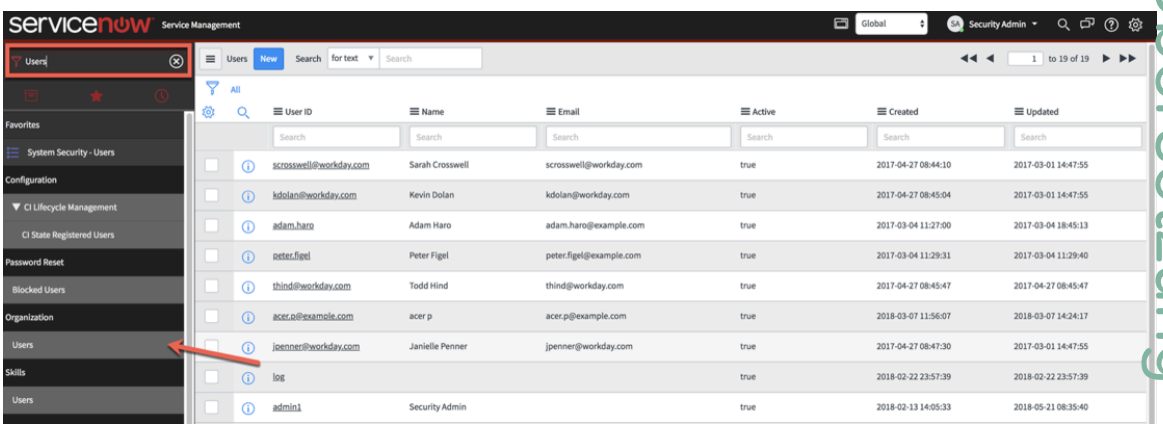
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Der Now Platform-Administrator erstellt eine API-Kontorolle (sn_sec_checkpoint.api_account_access). Dieses Konto wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung am Prüfpunkt erforderlich sind, damit das Gateway Sperrlisten von der Now Platform abrufen kann. Dieser Account ist ein separater, eindeutiger API-Benutzeraccount in der Now Platform-Instanz und wird dem Check Point-Administrator zugewiesen.

#### Prozedur

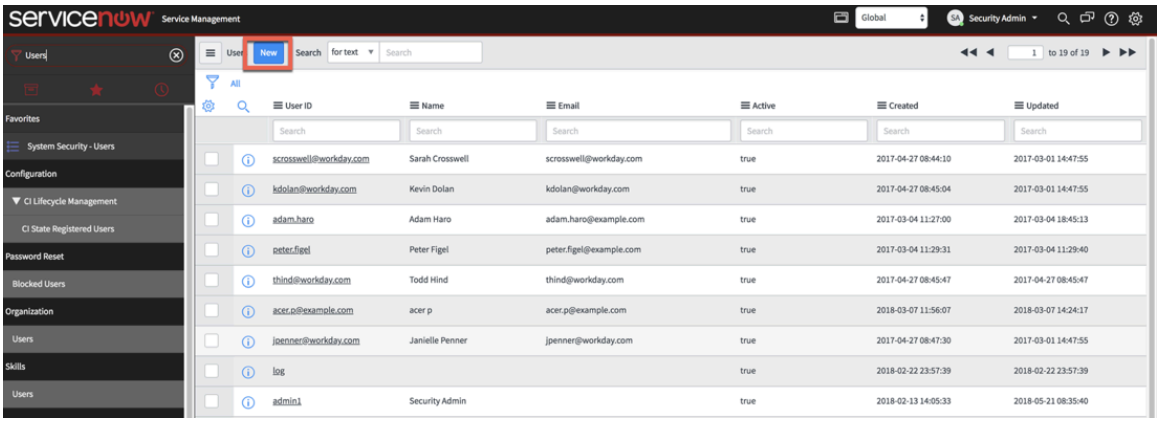
1. Navigieren zu **Alle** > **Organisation** > **Benutzer**.
2. Klicken Sie auf das Modul **Benutzer**.



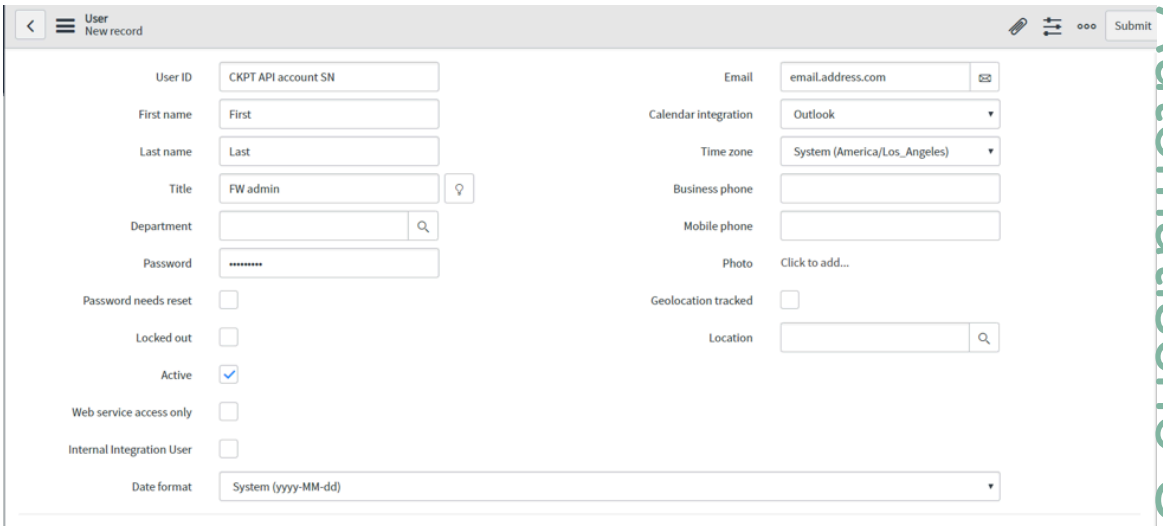

3. Klicken Sie in der angezeigten Benutzerliste auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Ein neues Formular wird angezeigt.




**4.** Füllen Sie das Formular nach Bedarf aus.

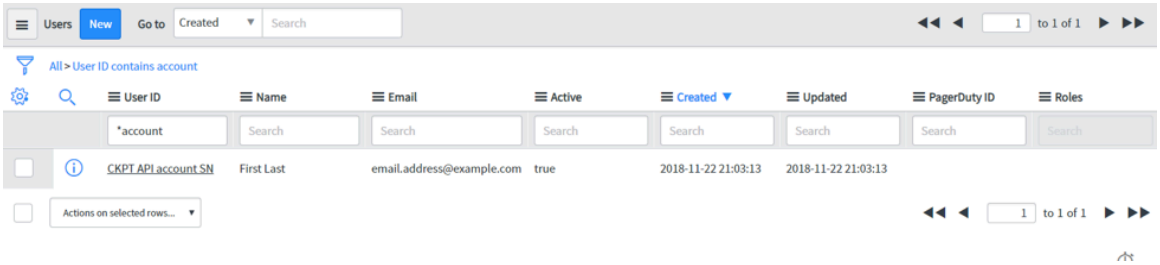
> **Hinweis:**
> Die Werte für Benutzer-ID-Titel und E-Mail-Adresse in der folgenden Tabelle und Abbildung sind Beispielwerte.

| Feld | Beschreibung |
|---|---|
| Anwender-ID | Eindeutige Benutzer-ID für die Rolle in Ihrer Now Platform-Instanz. Diese Benutzer-ID wird in das Feld **Benutzername** im Abschnitt **Client Authentication** des Check Point-Gateways für die Sperrlistenkonfiguration eingegeben. Ein Beispiel ist das CKPT-API-Konto SN. |
| Vorname | Person, die Sie zuweisen |
| Nachname | Person, die Sie zuweisen |
| Titel | Stellenbezeichnung, z. B. FW-Administrator. |
| Passwort | Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird in das Feld **Passwort** im Abschnitt „ **Client Authentication** “ der Sperrlistenkonfiguration auf dem Check Point-Gateway eingegeben. |
| E-Mail | Eindeutige E-Mail-Adresse |

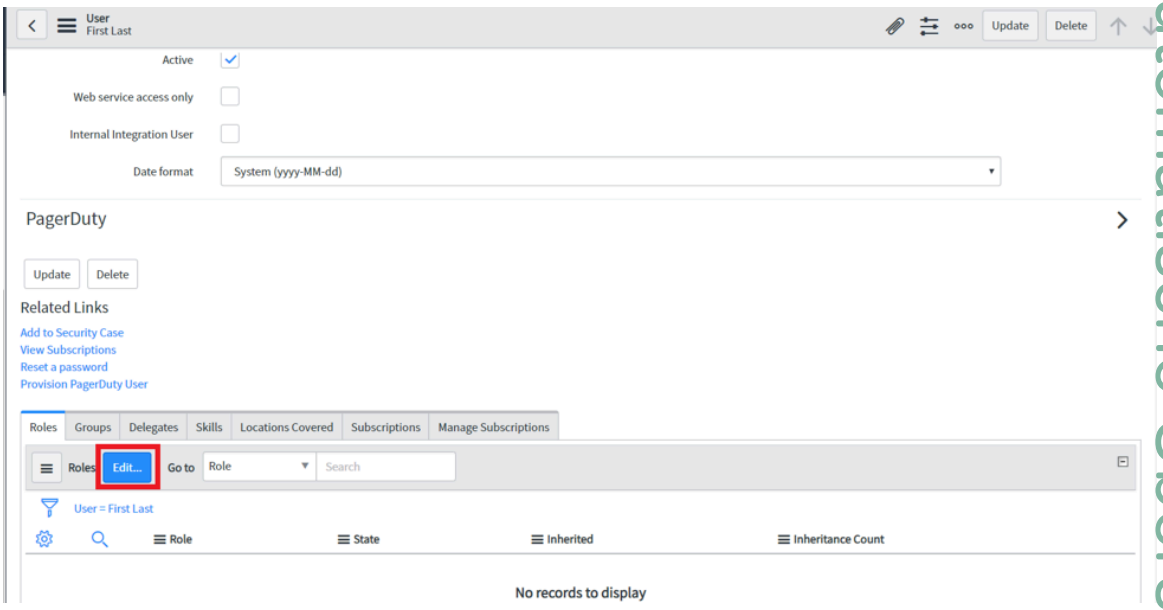
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. Klicken Sie in der Benutzerliste in der Spalte Benutzer-ID auf den Namen der von Ihnen eingegebenen Benutzer-ID, z. B. CKPTAPI-Konto-SN.



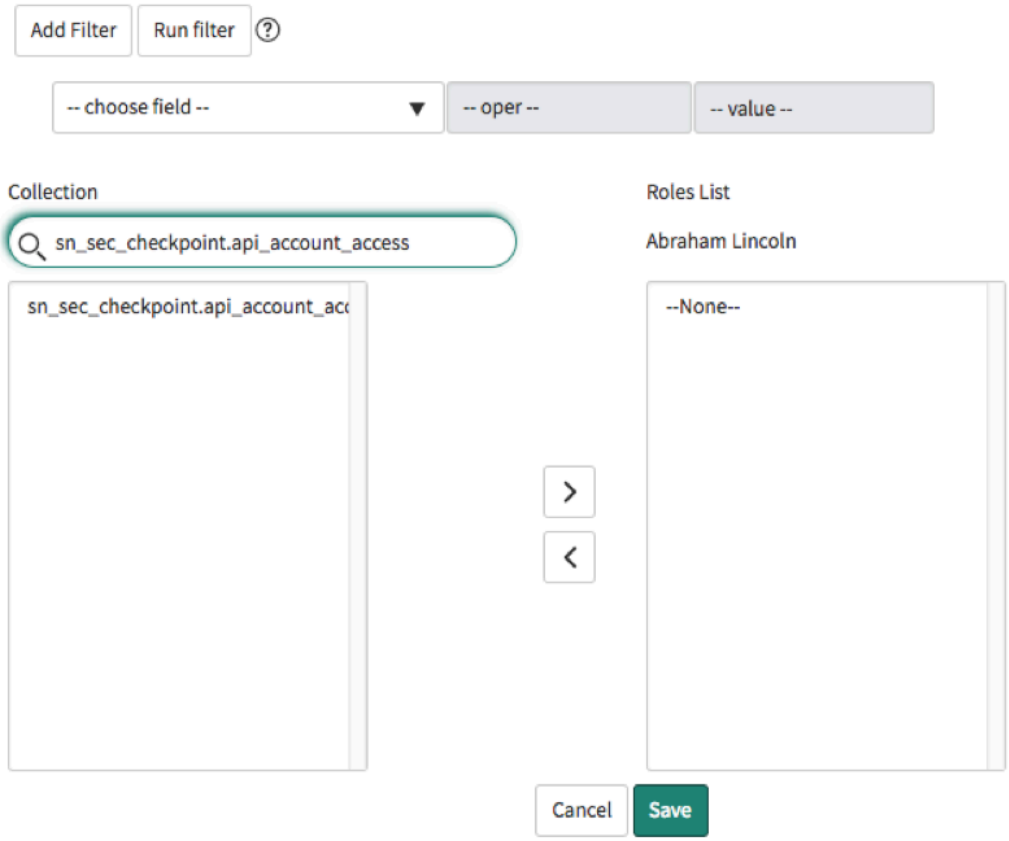

7. Klicken Sie im geöffneten Datensatz im Abschnitt „Rollen“ auf **Bearbeiten**.




8. Geben Sie im angezeigten Formular „ **Mitglieder bearbeiten** “ sn_sec_checkpoint.api_account_access in das Feld **Sammlung** ein.

Automatische Übersetzung

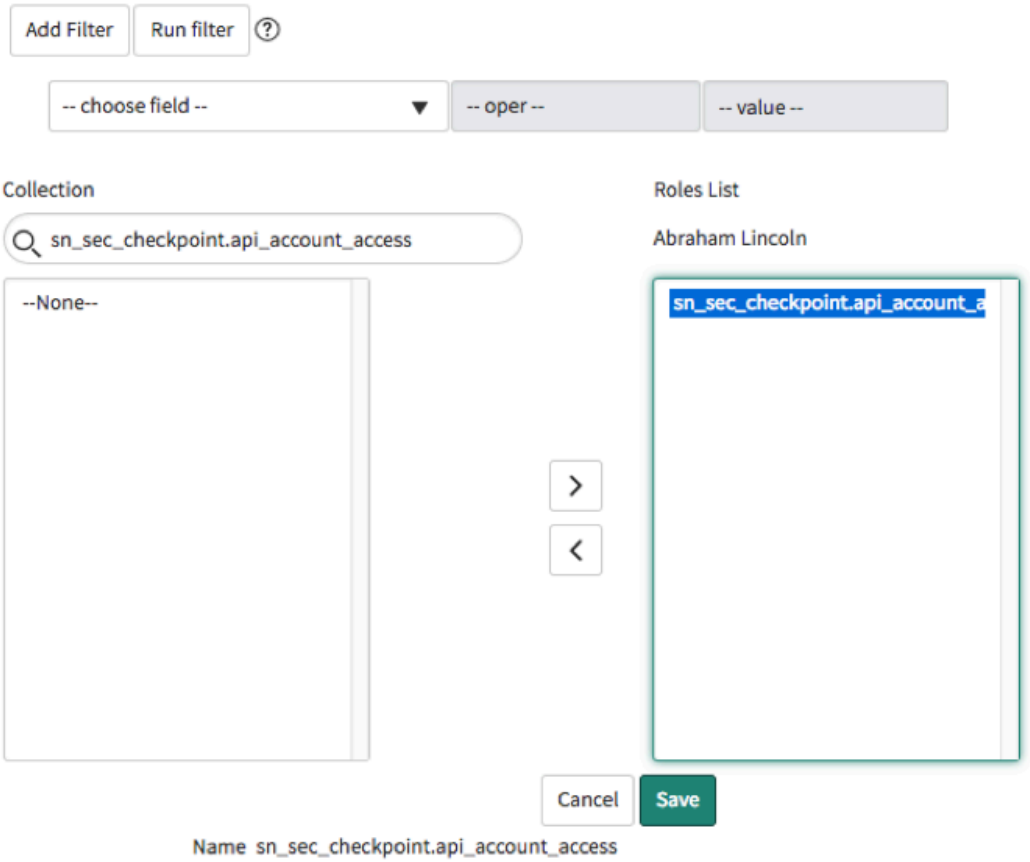
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




9. Wählen Sie in der Spalte **Sammlung** die Option **sn_sec_checkpoint.api_account_access**aus, und verschieben Sie sie in die Rollenliste.
10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Benutzer**, und klicken Sie in der Liste in der Spalte **Benutzer** auf den ID-Namen, den Sie für die Rolle erstellt haben (CKPT-API-Konto SN).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



**12.** Der Benutzerdatensatz wird angezeigt. Dieser Datensatz überprüft, ob der Benutzeraccount zugewiesen wurde.

### Integration mit Check Point NGTP einrichten

Führen Sie die folgenden Schritte aus, um die Check Point Next Generation Threat Prevention -Integration einzurichten. Dadurch würde sichergestellt, dass die Voraussetzungen für eine funktionierende Integration gegeben sind.

**Vorbereitungen**
Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

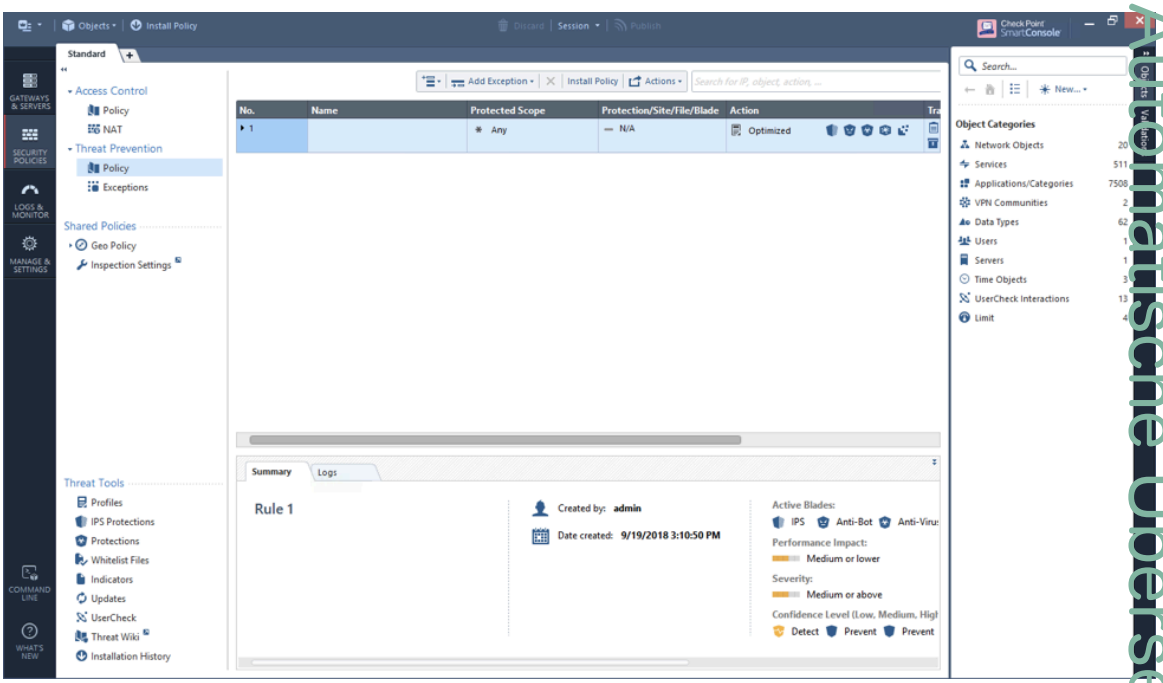
## Prozedur

1. Vergewissern Sie sich, dass die Bedrohungsabwehrrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist.
   Ausführliche Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Check Point-Benutzerhandbuch im Referenzabschnitt.

   **Hinweis:**
   Die Images in diesem Thema sind privilegiert und urheberrechtlich geschützt und werden mit Genehmigung von Check Point Software Technologies, Ltd. verwendet.

   **a.** Melden Sie sich bei der **Smart Console**an.

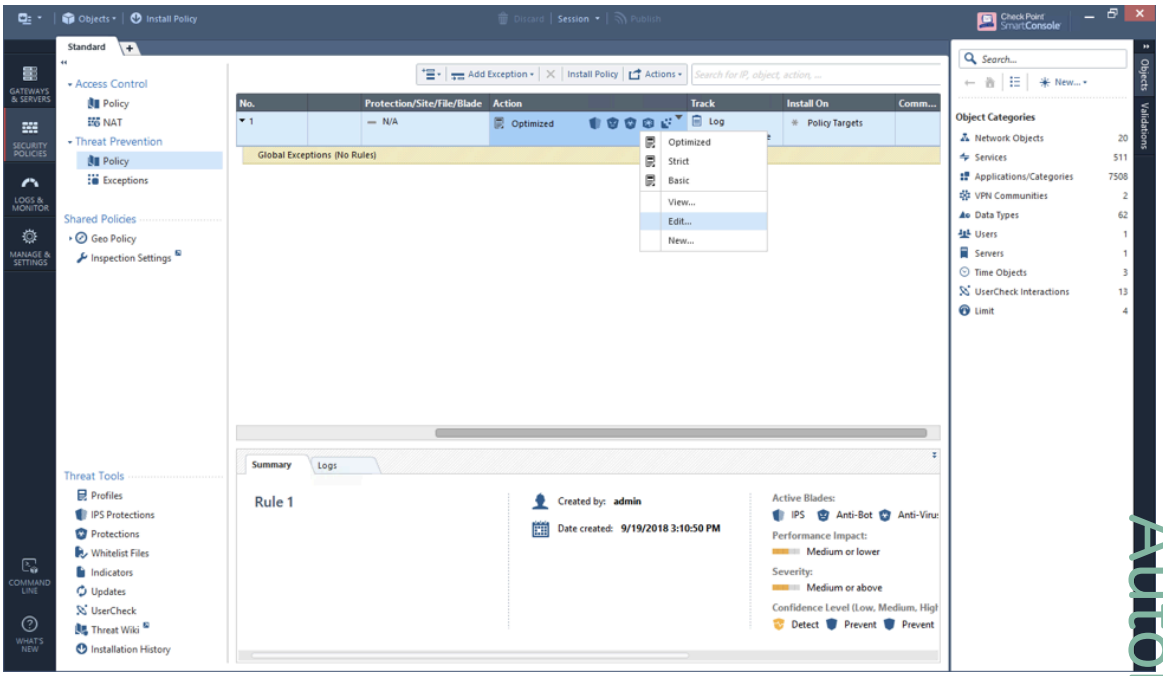
   **b.** Navigieren zu **Sicherheitsrichtlinien** > **Bedrohungsabwehr** > **Richtlinie**.




   **c.** Öffnen Sie die Bedrohungsabwehrrichtlinie im Bearbeitungsmodus.

Automatische Übersetzung

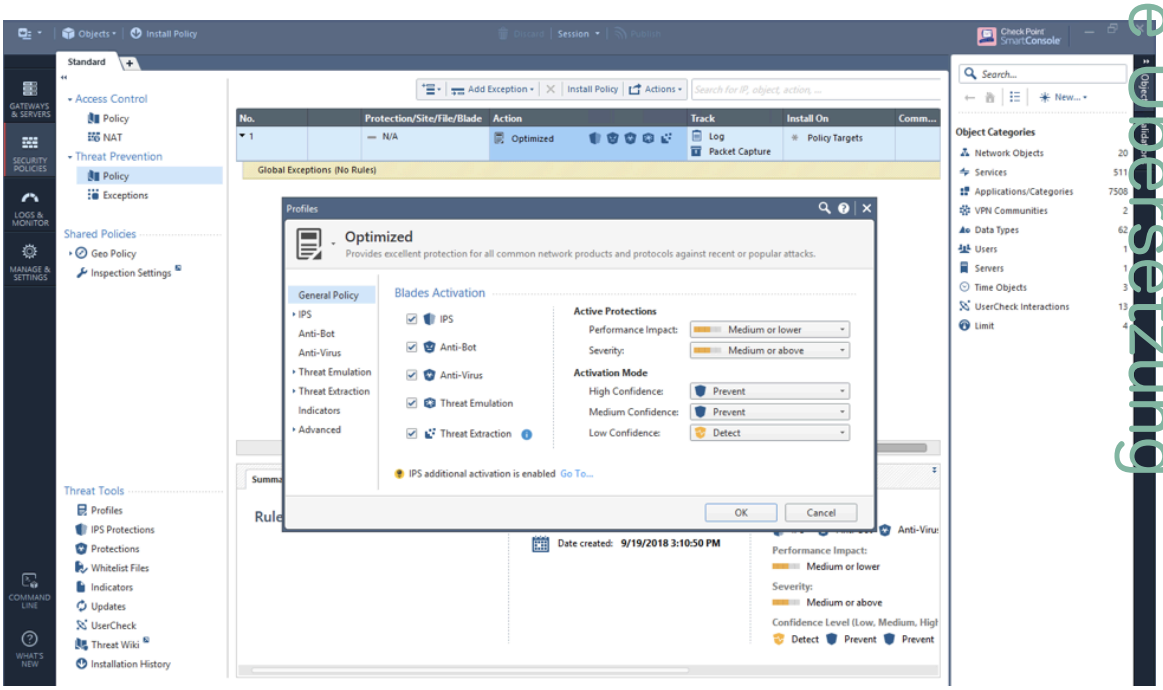
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Aktive Schutzmaßnahmen – Schweregrad muss „Mittel oder höher“ sein

**e.** Aktivierungsmodus > „Hohe Vertrauenswürdigkeit“ muss „Verhindern“ sein.

**f.** Blade-Aktivierung à Anti-Virus und Anti-Bot sollte ausgewählt sein.




**g.** Veröffentlichen Sie die Änderungen (falls vorhanden), und installieren Sie die Richtlinie.

**2.** Falls noch nicht konfiguriert, sollten benutzerdefinierte Intelligenz-Feeds nach der Aktivierung von Anti-Bot- und Anti-Virus-Blades hinzugefügt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

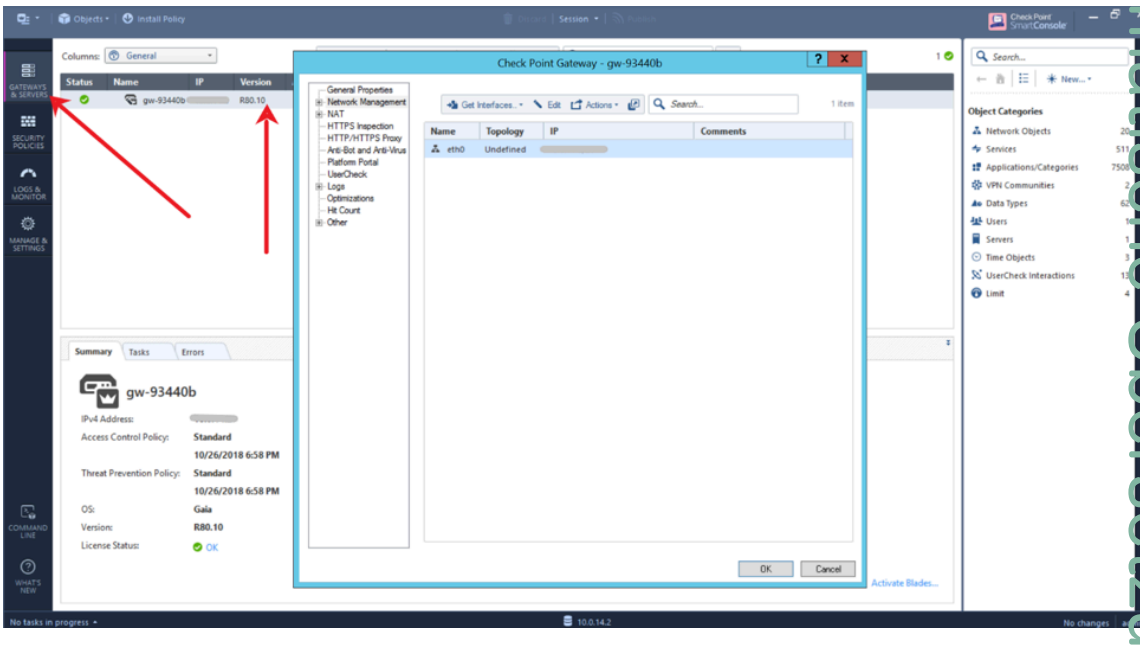
Weitere Informationen finden Sie im Abschnitt „Installation“ der Dokumentation zu Check Point Custom Intelligence Feed Feature.https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Falls noch nicht konfiguriert, richten Sie das Prüfpunkt-Gateway so ein, dass der gesamte Internetdatenverkehr über den HTTP-Proxy weitergeleitet wird (bei Konfiguration der HTTPS-Inspektion).

**Hinweis:**
Für die URL-Blockierung auf Prüfpunkt-NGTP müssen bestimmte Einstellungen sichergestellt werden. HTTPS-Internetverkehr verwendet das SSL-Protokoll (Secure Sockets Layer) und wird verschlüsselt, um Datenschutz zu gewährleisten. HTTPS kann jedoch schädlichen Datenverkehr verbergen, der hätte blockiert werden sollen. Damit Check Point Gateway Einblick in den HTTPS-Datenverkehr erhält, leiten Sie den Datenverkehr entweder über den HTTP-Proxy weiter, oder richten Sie die HTTPS-Inspektion ein (empfohlen). In diesem Abschnitt werden die Schritte zum Einrichten des HTTP-Proxy auf dem Prüfpunkt-Gateway beschrieben.

**a.** Melden Sie sich bei der **Smart Console**an.

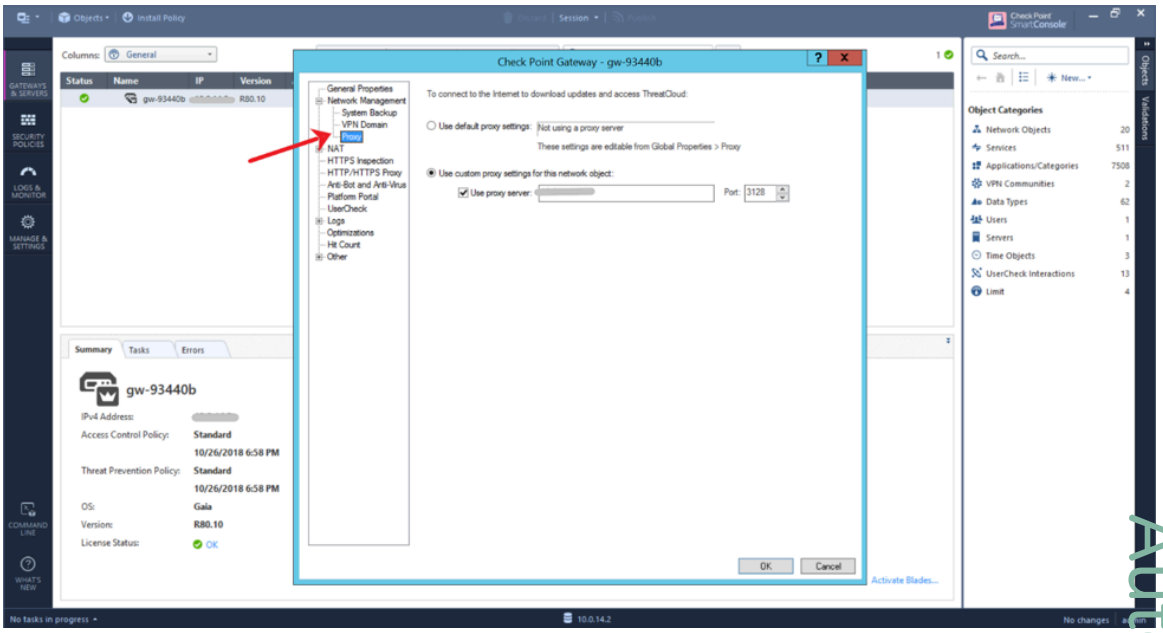
**b.** Navigieren Sie zu **Server und Gateways**, und doppelklicken Sie auf den entsprechenden Server.




**c.** Navigieren zu **Netzwerkverwaltung** > **Proxy**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Geben Sie die Proxy-Details an, die für die Weiterleitung des HTTP-Datenverkehrs verwendet werden sollen.

**e.** Stellen Sie sicher, dass HTTP-Anforderungen vom Clientendpunkt über den HTTP-Proxy erfolgen.

**4.** Wenn noch nicht konfiguriert, aktivieren Sie die HTTPS-Inspektion (wenn HTTP-Proxy konfiguriert ist). Wenn der Großteil des Datenverkehrs über SSL abgewickelt wird, wird die Verwendung von HTTPS-Inspektions-Blade empfohlen. Dadurch wird der Datenverkehr für GW transparent. Aktivieren Sie die HTTPS-Inspektion auf dem Prüfpunkt-Gateway wie folgt.

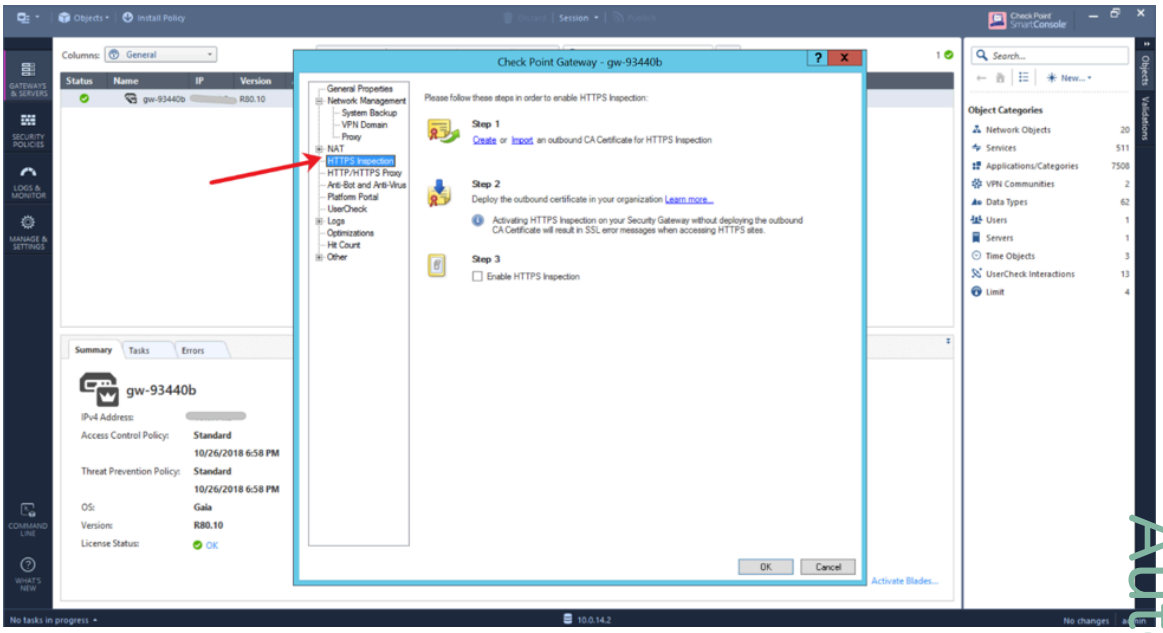
**a.** Melden Sie sich bei der **Smart Console**an.

**b.** Navigieren Sie zu **Server und Gateways**, und doppelklicken Sie auf den entsprechenden Server.

**c.** Navigieren Sie zu **HTTPS-Inspektion**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Befolgen Sie die Schritte zum Konfigurieren der HTTPS-Inspektion im Check Point-Benutzerhandbuch.

### Aktivieren Sie die Check Point NGTP -Integration

Wenn Sie die Anwendung nicht installiert haben, befolgen Sie die Anweisungen, um sie zu installieren.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Melden Sie sich bei der Instanz an, in der Sie die Anwendung installieren möchten.
2. Navigieren zu **Systemanwendungen** > **Anwendungen**.
3. Klicken Sie auf die Registerkarte **Downloads**.
   Eine Liste der für die Installation verfügbaren Anwendungen wird angezeigt.
4. Suchen Sie die Anwendung Check Point Next Generation Threat Prevention, wählen Sie sie aus und klicken Sie auf **Installieren**.
   Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Arbeiten mit Sperrlisten

Die ServiceNow Check Point Next Generation Threat Prevention -Integration unterstützt Sperrlisten, die erkennbare IP-, URL- und Domänenelemente akzeptieren.

ServiceNow Die konfigurierte Sperrliste ist eine CSV-Datei, die auf einem externen Webserver gehostet wird, der für diese Integration die Now Platform-Instanz ist. Benutzerdefinierter Intelligenz-Feed wird auf dem Prüfpunkt-Gateway konfiguriert, das die IP-Adressen, URLs und Domänen in vorkonfigurierten Intervallen aus der Now Platform abruft.

Diese Integration unterstützt drei Arten von Sperrlisten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP-Adresse (Umfasst eine einzelne IP-Adresse (nur IPv4) für die Sperrliste und CIDR-Blöcke (Bereiche) von Adressen für die Allow-Liste.)
- URL
- Domäne

### Von der Check Point NGTP -Integration unterstützte erkennbare Elemente

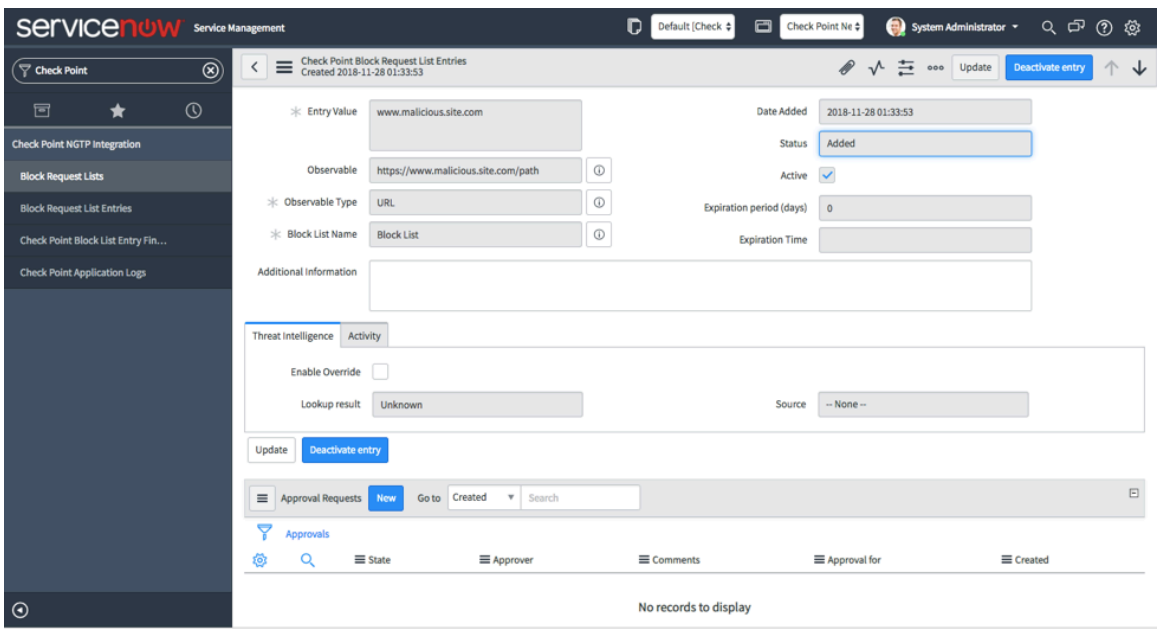
Der Abschnitt enthält Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ.

| Erkennbarer Typ | Beispiele | Beschreibung |
|---|---|---|
| Domäne | • beispiel.com<br>• mail.example.com | Platzhalterzeichen werden nicht unterstützt. |
| IP-Adresse | 95.153.103.54 (IPv4) | Stellt eine einzelne, eindeutige Schnittstellenadresse dar. Die Integration unterstützt nur IPv4- und CIDR-Formate (das CIDR-Format wird nur für Allow-Listen-Zwecke unterstützt).<br><br>Für die Allow-Liste bietet die Integration Unterstützung für erkennbare IP-Adresselemente mit CIDR-Bereichen (Classless Inter-Domain Routing), z. B. 95.153.100.0/22.<br><br>**Hinweis:** Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, eine einzelne IP-Adresse an eine Sperrliste anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs zugelassen haben. Zum Beispiel ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs, der durch 95.153.100.0/22 (95.153.100.0-95.153.103.255) dargestellt wird. |
| URL | • https://www.example.com<br>• http://www.example.com | Beschreibung: Die HTTPS-URL wird von der Anwendung so formatiert, dass der Pfad aus der URL gekürzt und nur der Domänenname beibehalten wird.<br><br>Check Point NGTP basiert auf der HTTP CONNECT-Anforderung, |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

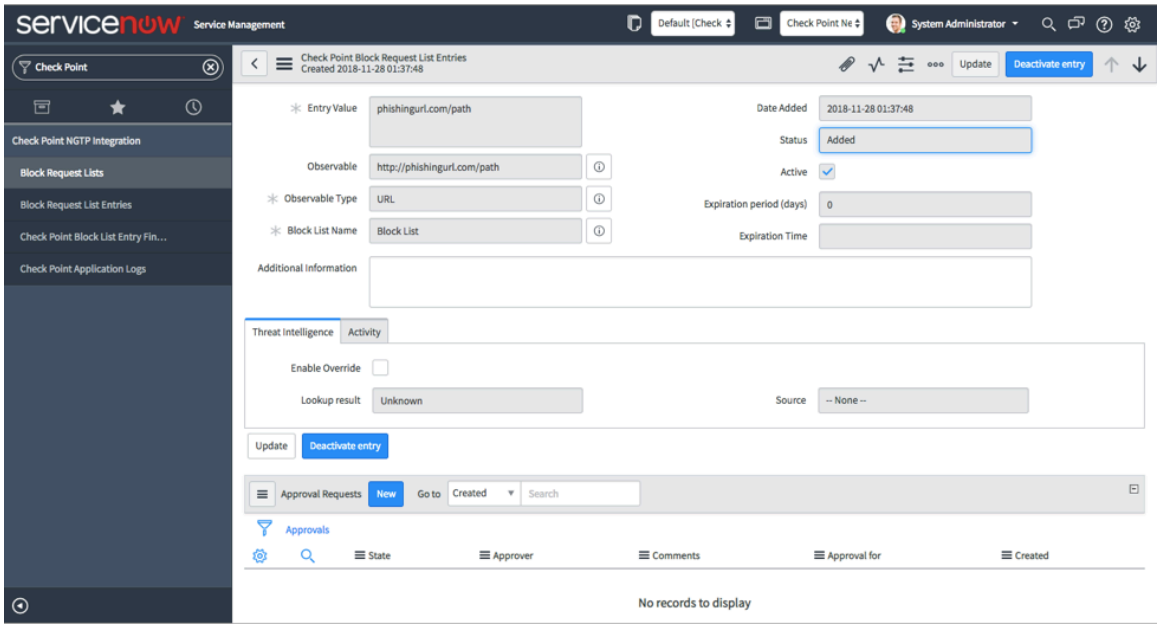
| Erkennbarer Typ | Beispiele | Beschreibung |
|---|---|---|
| | | um den Webdatenverkehr auszuwerten und die Blockierung zu erzwingen. Bei einer HTTPS-CONNECT-Anforderung ist nicht die gesamte URL in der Anforderung sichtbar, sondern nur der Domänenname. Wenn ein Benutzer eine HTTPS-URL mit einem bestimmten Pfad blockiert (Beispiel: https://www.example.com/path), schneidet die Anwendung den Pfad automatisch ab (www.example.com). Die Anwendung verwaltet die Beziehung zwischen dem ursprünglichen erkennbaren Element und der formatierten URL. Unten sehen Sie einen Screenshot des Sperrlisteneintrags, der die formatierte URL und das ursprüngliche erkennbare Element zeigt. |




Bei HTTP-URLs mit einem bestimmten Pfad (z. B. http://www.example.com/path) blockiert der Prüfpunkt die angegebene URL, da die gesamte URL in der CONNECT-Anforderung sichtbar ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Erstellen Sie eine Sperrliste für die Check Point NGTP -Integration

Erstellen Sie eine Sperrliste in Ihrer Now Platform-Instanz. Nach der Genehmigung und Aktivierung können Sie Einträge für diese Sperrlisten aus erkennbaren Elementen erstellen, die bei SIR-Incidents (Now Platform Security Incident Response) als böswillig eingestuft wurden, und die Genehmigung anfordern, um sie zu blockieren.

### Vorbereitungen

Erforderliche Rolle: Security Incident Administrator (sn_si.admin)

### Warum und wann dieser Vorgang ausgeführt wird

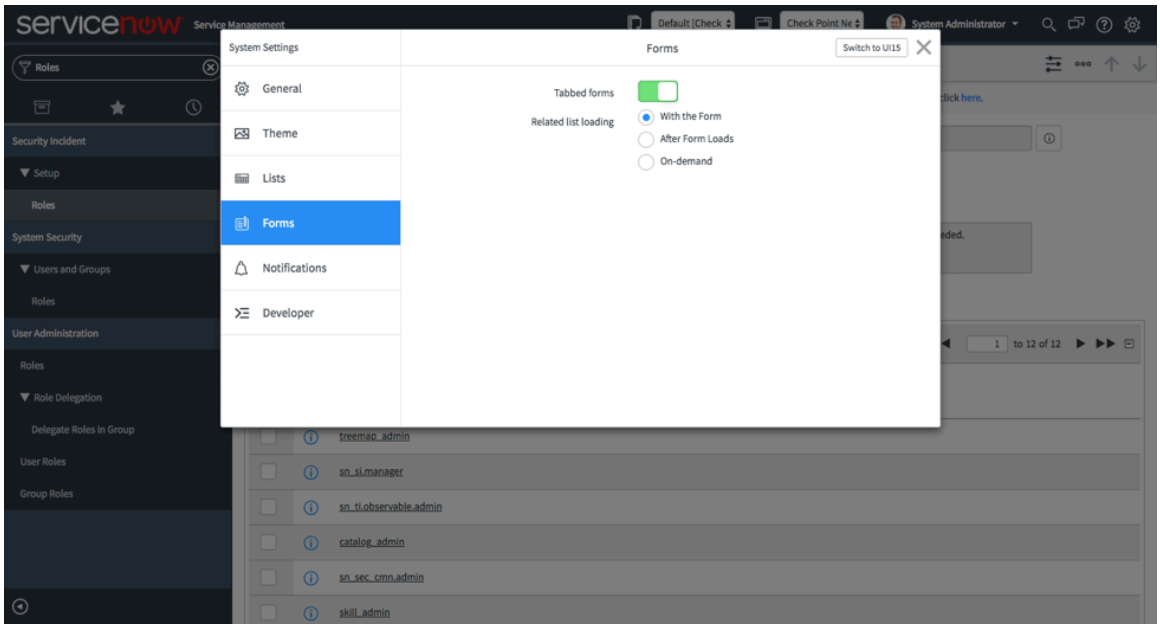
Erstellen Sie die Sperrliste in Ihrer Now Platform-Instanz, damit der Prüfpunkt in der Liste enthaltene Objekte (IP-Adressen, URLs, Domänen) importieren kann. Benutzerdefinierter Intelligenz-Feed wird auf dem Prüfpunkt-Gateway konfiguriert, das die IP-Adressen, URLs und Domänen in vorkonfigurierten Intervallen von der Now Platform abruft.
Um sicherzustellen, dass die erkennbaren Elemente blockiert werden, sollte die Bedrohungsabwehrrichtlinie mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert werden.

### Hinweis:

Die Abbildungen in diesem Thema werden mit **Formularen** mit Registerkarten angezeigt, die in den Systemeinstellungen deaktiviert sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Prozedur

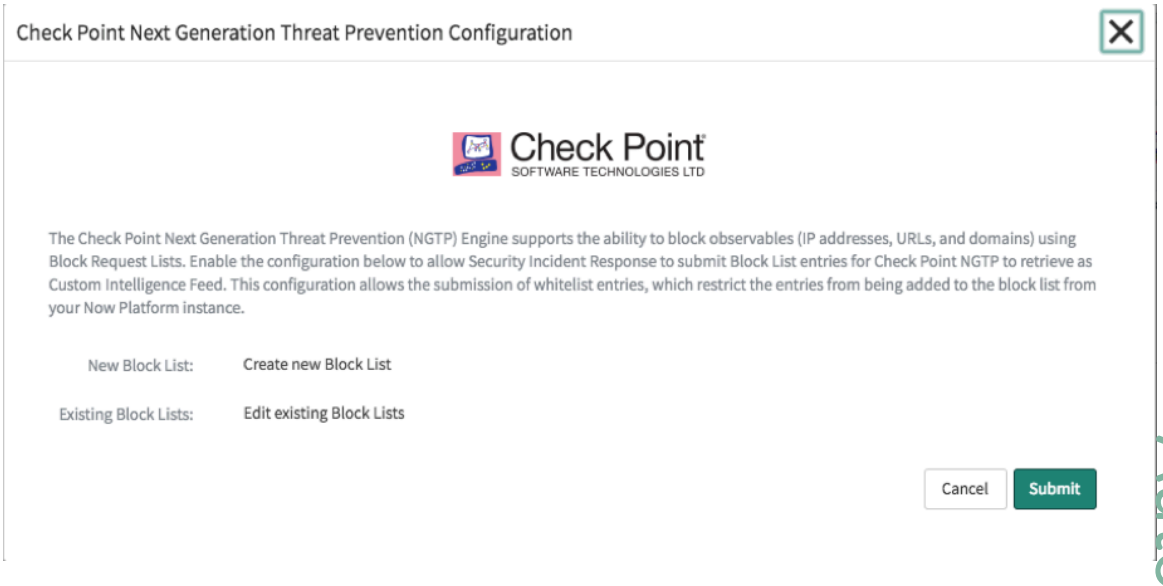
1. Navigieren Sie nach Abschluss der Installation der Anwendung zu **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Karte **Prüfpunkt Next Generation Threat Prevention**, und klicken Sie auf **Konfigurieren**.

**Hinweis:**
Privilegierte und proprietäre Inhalte, die mit Genehmigung von Check Point Software Technologies, Ltd. verwendet werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken **Sie auf Neue Sperrliste erstellen**.




4. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Check Point-Sperranforderungsliste.<br><br>Fügen Sie den erkennbaren Typ (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalyst die Absicht der Sperrliste leicht anhand des Namens erkennen kann. Der Name sollte auch eindeutig angeben, welcher Firewall-Richtlinie diese Sperrlistenobjekte zugeordnet sind. Einige Beispiele für Sperrlistennamen sind „Ausgehende Malware-IP“ oder „Ausgehende Phishing-URL“. |
| Aktiv | Diese Checkbox ist standardmäßig deaktiviert, um anzuzeigen, dass die Sperrliste inaktiv ist.<br><br>Wenn sie inaktiv ist, kann die Sperrliste keine zusätzlichen Einträge erhalten.<br><br>Wenn das Kontrollkästchen aktiviert ist (wenn die Change-Anforderung geschlossen wird oder keine Change-Anforderung generiert wird), wird die Sperrliste aktiviert und ist für Sperrlisteneinträge verfügbar. |
| Tag anzeigen | Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element in der Sperrliste blockiert ist. Wenn diese Option ausgewählt ist, ist das Feld „Tag für erkennbare Elemente“ im Formular verfügbar.<br><br>**Hinweis:**<br>Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie im Feld Name mit einem Check Point-Präfix eingegeben haben, z. B. Check Point – Malware Outbound IP. Sie können den Tag-Namen und die Farbe ändern. Der Tag-Name wird im Feld „Tag für erkennbare Elemente“ angezeigt, sobald die Sperrliste gespeichert wurde. |

Automatische Übersetzung

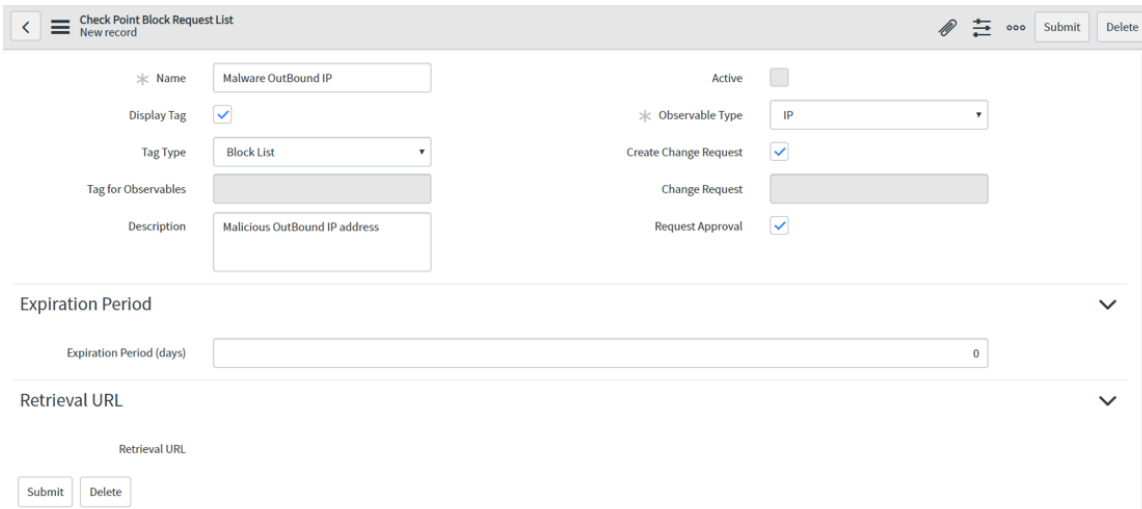
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und das Feld „Tag für erkennbare Elemente“ ist im Formular nicht verfügbar. |
| Erkennbarer Typ | Wählen Sie einen erkennbaren Typ aus der Liste aus, den diese Sperrliste akzeptiert: IP-Adresse (einschließlich CIDR für Allow-Liste), URL oder Domäne. |
| Tag-Typ | Tags, die in der Liste verfügbar sind.<br><br>Eine Sperrliste ist eine Liste der erkennbaren Elemente, die vom Prüfpunkt Next Generation Threat Prevention blockiert werden sollen.<br><br>Eine Allow-Liste ist eine Liste von erkennbaren Elementen, die in Check Point Next Generation Threat Prevention auf keinen Fall blockiert werden sollen.<br><br>Standardmäßig ist die Farbe des Sperrlisten-Tags Schwarz und die Farbe des Allow-Listen-Tags Grau. Sie können die Farbe ändern. |
| Change-Anforderung erstellen | Diese Checkbox ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in Ihrer Now Platform-Instanz zu erstellen, die an den Sperrlisten-Datensatz angehängt sind.<br><br>Die Change-Anforderung wird verwendet, um die Sperrlisten-Abruf-URL im Check Point Next Generation-Firewall-Gateway zu konfigurieren.<br><br>Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch die Now Platform für Firewall-Richtlinien oder -Regeländerungen verwendet. Wenn Sie eine Anforderung erstellen, wird die Sperrliste automatisch aktiviert, nachdem sie geschlossen wurde.<br><br>Deaktivieren Sie die Checkbox, um die Sperrliste manuell zu aktivieren, nachdem Sie per E-Mail vom Firewall-Administrator benachrichtigt wurden, dass der benutzerdefinierte Intelligenz-Feed auf allen Prüfpunkt-Gateways konfiguriert wurde.<br><br>Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar. |
| Genehmigung anfordern | Diese Checkbox ist standardmäßig aktiviert, um Genehmigungen für das Aktivieren/Entfernen von Sperrlisteneinträgen aus Sperrlisten anzufordern. Die Genehmigung wird von den Benutzern mit der Rolle Security Incident Administrator (sn_si.admin) angefordert. Die Genehmigungsanforderung wird per E-Mail an die Genehmiger gesendet.<br><br>Sobald die Genehmigung akzeptiert wurde, wird der Eintrag in dieser Sperrliste aktiviert.<br><br>Wenn das Kontrollkästchen nicht aktiviert ist, folgen die Einträge für diese Sperrliste nicht dem Genehmigungs-Workflow und werden direkt in der Sperrliste aktiviert. |
| Tag für erkennbares Element | Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tag anzeigen aktiviert ist. Das Feld wird automatisch ausgefüllt, nachdem die Sperrliste mit einem Standardwert aus dem Feld Name gespeichert wurde. Wenn die Sperrliste mit dem Namen „Malware-URL“ erstellt wird, lautet der abgeleitete Tag-Name „Sperrliste – Malware-URL“. |



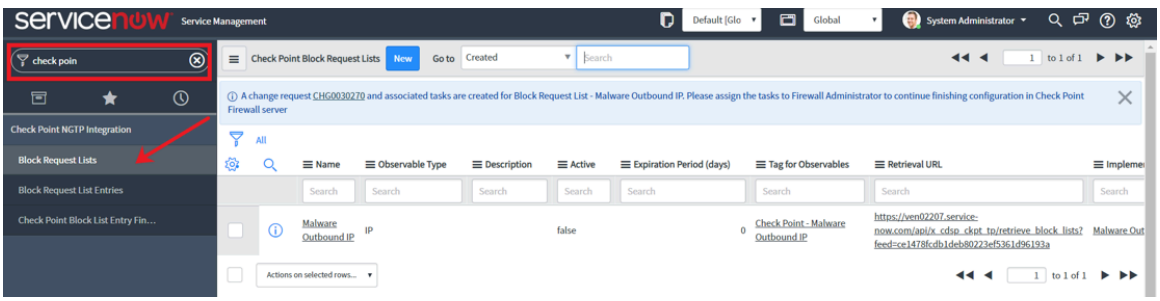
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Change-Anforderung | Wenn das Kontrollkästchen Change Request erstellen aktiviert ist, wird die Change Request-Nummer in der Now Platform-Instanz angezeigt, sobald die Sperrliste gespeichert wurde.<br><br>Wenn das Kontrollkästchen Change Request erstellen deaktiviert ist, wird dieses Feld nicht angezeigt. |
| Beschreibung | Beschreibung der Check Point-Sperrliste. Der Name enthält im Allgemeinen die Arten von Sites und erkennbaren Elementen, die Sie in dieser Sperrliste erwarten würden. Sie können dieses Feld für weitere Details verwenden. |
| Ablaufzeitraum (in Tagen) | Ablaufzeitraum der Sperrliste.<br><br>0 (Standard) gibt an, dass der Sperrlisteneintrag nie abläuft.<br><br>Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, der 24 Stunden entspricht. Es gibt keinen Höchstwert. |
| Abruf-URL | Die Abruf-URL wird automatisch generiert, sobald die Sperrliste gespeichert wurde. Um diese Sperrliste für Prüfpunkt-Gateways zu konfigurieren, müssen Sie diese URL verwenden. Sobald diese URL konfiguriert ist, ruft Check Point die zu blockierenden erkennbaren Elemente im CSV-Format ab. |



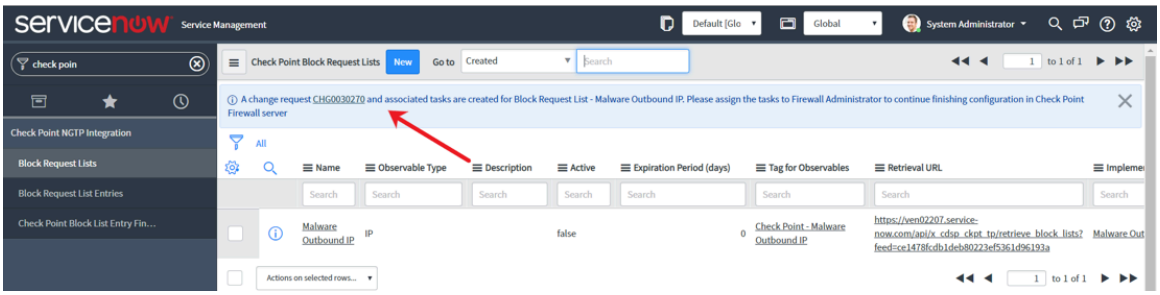

Automatische Übersetzung

5. Klicken Sie auf **Absenden**.
6. Wenn die Sperranforderungsliste für Check Point nicht angezeigt wird, navigieren Sie zu **Check Point – NGTP-Integration** > **Sperranforderungslisten**.

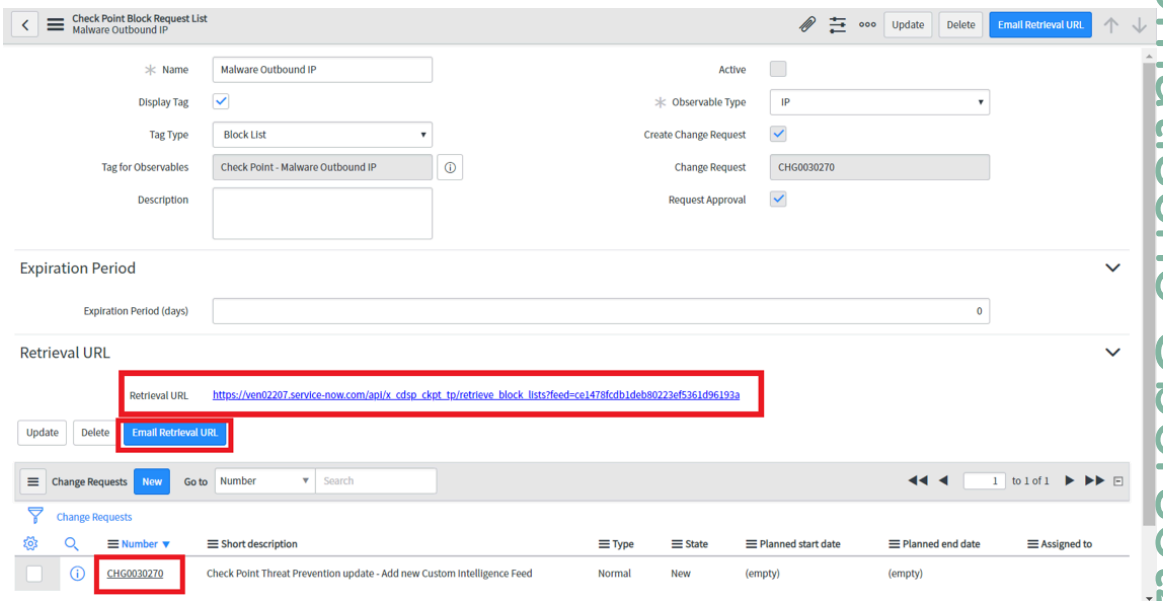



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die neue Sperrliste wird angezeigt. Der Status der Sperrliste ist noch inaktiv (falsch), was bedeutet, dass die Sperrliste keine Einträge annehmen kann. Wenn Change-Anforderung erstellen konfiguriert wurde, wird eine Meldung angezeigt, die angibt, dass eine Change-Anforderung und Aufgaben in Ihrer Now Platform-Instanz erstellt wurden.




7. Klicken Sie in der Spalte **Name** auf ein Element, um den Datensatz zu öffnen.
Der Datensatz der Sperrliste wird angezeigt. Dieses Beispiel zeigt eine ausgehende IP-Sperrliste für Malware. Die folgenden Felder, Optionen und Links werden im neuen Datensatz nach der Übermittlung angezeigt und in der folgenden Tabelle beschrieben.




| Feld | Beschreibung |
|---|---|
| E-Mail-Abruf-URL | Sendet eine Benachrichtigung per E-Mail, dass der Blocklink für die Konfiguration an den Administrator der Check Point-Firewall verfügbar ist. |
| Abruf-URL | Diese URL wird verwendet, um Custom Intelligence Feed für Prüfpunkt-Gateways zu konfigurieren.<br>**Hinweis:**<br>Wenn Sie Ihre Systemeinstellungen auf Formulare mit Registerkarten festgelegt haben, wird dieser Link auf der Registerkarte Informationen zum Abruf von Sperrlisten am Ende des Datensatzes angezeigt. |
| Change-Anforderung | Ein Link zum Change-Anforderungsdatensatz wird im Abschnitt „Change-Anforderungen“ angezeigt, sofern konfiguriert, und die Anforderungsnummer wird im Feld Change-Anforderung angezeigt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| der Now Platform | |
| Aktualisieren | Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder. |
| Löschen | Löschen Sie den Datensatz. |

8. Erstellen und fügen Sie nach Bedarf weitere Sperrlisten hinzu.
   Die Sperrlisten werden auf der Seite „Check Point Sperranforderungslisten“ angezeigt.

### Nächste Maßnahme
Aktivieren Sie die Sperranforderungsliste manuell oder mit einer Now Platform-Change-Anforderung.

#### Aktivieren Sie eine Sperrliste für die Check Point NGTP -Integration

Nachdem die Sperrliste in Ihrer Now Platform erstellt wurde und die URL verfügbar ist, konfiguriert der Prüfpunkt-Administrator die Sperrliste als benutzerdefinierten Intelligenz-Feed auf allen Prüfpunkt-Gateways der nächsten Generation. Bevor Sperrlisteneinträge akzeptiert werden können, muss die Sperrliste in Check Point konfiguriert und in Now Platform aktiviert werden.

### Vorbereitungen
Erforderliche Rolle: Security Incident Administrator (sn_si.admin)

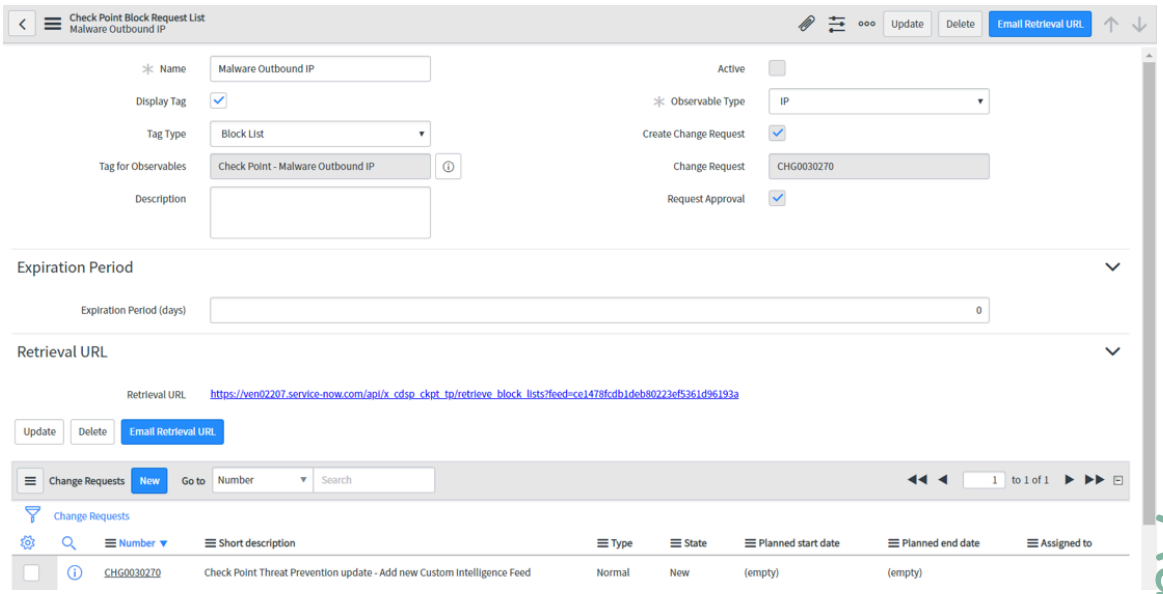
### Warum und wann dieser Vorgang ausgeführt wird
Nachdem die Sperrliste konfiguriert wurde, können Sie als Security Incident-Administrator die Sperrliste manuell aktivieren, oder die Sperrliste wird nach Abschluss einer Now Platform-Change-Anforderung automatisch aktiviert. Die Change-Anforderung muss genehmigt und vom inaktiven Status in den aktiven Status verschoben werden, bevor Sperrlisteneinträge akzeptiert werden können.

### Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Sperranforderungslisten**, und wählen Sie das Modul **Sperranforderungslisten** aus.
2. Wählen Sie in der angezeigten Liste **Check Point Sperranforderungslisten** in der Spalte **Name** die neue Sperrliste aus.
3. Beachten Sie im angezeigten Datensatz die Schaltfläche E- **Mail-Abruf-URL**, den aktiven Link Sperrliste-Abruf-URL und, falls konfiguriert, die Now Platform-Change-Anforderung im Abschnitt „Change-Anforderungen“.
   Beachten Sie auch, dass das Kontrollkästchen Aktiv deaktiviert ist.

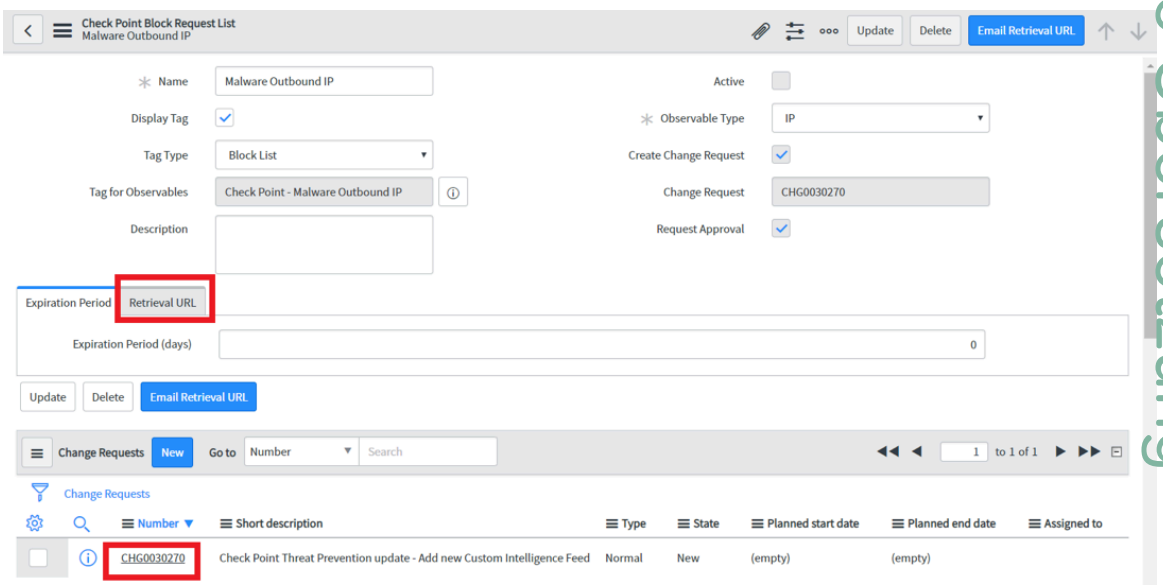


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn Formulare mit Registerkarten in Ihren Systemeinstellungen deaktiviert sind, wird die URL zum Abrufen der Sperrliste im Abschnitt „Abruf-URL“ angezeigt.

4. Klicken Sie auf die Registerkarte **Abruf-URL** der Sperrliste, um die Abruf-URL anzuzeigen.
Die folgende Abbildung zeigt die Sperrlisten-Abruf-URL, die als Registerkarte mit Formularen mit Registerkarten angezeigt wird, die in Ihren Systemeinstellungen ausgewählt sind. Der Link zum Change Request (CH0030270) wird ebenfalls angezeigt.




5. Um die Konfiguration abzuschließen und die Sperrliste von inaktiv in aktiv zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator zu benachrichtigen, dass die Abruf-URL verfügbar ist.

| Option | Beschreibung |
|---|---|
| Klicken Sie auf E-Mail-Abruf-URL. | E-Mail-Sperrlisten-Abruf-URL direkt an den Firewall-Administrator. Mit dieser Option kann der Firewall-Administrator die Konfiguration |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | auf der Check Point-Plattform abschließen. Wählen Sie diese Option aus, wenn der Firewall-Administrator die Now Platform nicht verwendet. |
| Schließen Sie die Change-Anforderung für Now Platform ab, und weisen Sie die Konfigurationsaufgaben dem Firewall-Administrator zu. | Diese Option ist nur verfügbar, wenn der Firewall-Administrator für Check Point auch die Now Platform verwendet und die Change-Management- und Genehmigungsprozesse der Now Platform konfiguriert sind.<br>**Hinweis:**<br>Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) können die Now Platform-Change-Anforderung genehmigen. Sobald die Konfigurationsaufgaben abgeschlossen sind und die Change-Anforderung geschlossen wurde, wird die Sperrliste automatisch aktiviert. |

### Nächste Maßnahme
Nachdem Sie den Firewall-Administrator benachrichtigt haben, dass die Abruf-URL verfügbar ist, und Sie bestätigt haben, dass die Sperrliste in Check Point als Security Incident-Administrator konfiguriert wurde, besteht Ihr nächster Schritt darin, die Sperrliste zu aktivieren. Sie aktivieren die Sperrliste entweder manuell oder verwenden, falls konfiguriert, das Now Platform-Change-Anforderungsformular, um die Sperrliste zu aktivieren. Die Sperrliste wird automatisch aktiviert, wenn die Change-Anforderung geschlossen wird.

## Konfigurieren Sie eine Sperrliste als benutzerdefinierten Intelligenz-Feed in der Check Point NGTP -Integration

Der Firewall-Administrator muss den benutzerdefinierten Intelligenz-Feed entsprechend der in der NOW-Plattform erstellten Sperrliste konfigurieren.

### Vorbereitungen
Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird
Diese Aufgabe muss auf jedem der Prüfpunkt-NGTP-Gateways ausgeführt werden. Der Firewall-Administrator benötigt den SSH-Zugriff der Gateway-Server. Wenn Ihre Organisation über Change-Management- und Genehmigungsprozesse der Now Platform verfügt, stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist.
Der Firewall-Administrator benötigt die Abruf-URL der Sperrliste und die ServiceNow-Benutzeranmeldeinformationen mit der Rolle „Check Point API Account Access Role“ (sn_sec_checkpoint.api_account_access).

Wenn der Firewall-Administrator die NOW-Plattform nicht verwendet, kann der NOW Security Incident-Administrator die erforderlichen Informationen per E-Mail bereitstellen. Wenn der Firewall-Administrator die NOW-Plattform verwendet, kann die mit der Sperrliste verknüpfte Change-Anforderung alternativ dem Firewall-Administrator zugewiesen werden. Diese Change-Anforderung enthält die erforderlichen Informationen zum Konfigurieren von Custom Intelligence Feed.

Weitere Informationen zum Einrichten von benutzerdefiniertem Intelligenz-Feed für Prüfpunkt-Gateways finden Sie unter: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails in Ihrer Now Platform-Instanz aktiviert ist, indem Sie zu navigieren **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**.
2. Überprüfen Sie unter „Konfiguration ausgehender E-Mails“, ob „ **E-Mail senden“** und **„E-Mail empfangen“** ausgewählt sind.
3. Ändern Sie SSH in Check Point Gateway mit Expertenmodus.
4. Führen Sie den Befehl aus, um Custom Intelligence Feed hinzuzufügen.
   Die Befehlsausführung ist interaktiv und fordert zur Eingabe des Feed-Formats und des Passworts auf.
   - Wenn Sie zur Eingabe des Feed-Formats aufgefordert werden, geben Sie „cp_csv“ ein.
   - Wenn Sie zur Eingabe des NOW-Plattform-Benutzerpassworts mit API-Zugriff aufgefordert werden.

   Die Befehlsausführung warnt davor, dass der Computer dem Serverzertifikat (NOW-Plattform) nicht vertraut, und fordert Sie auf, das Serversicherheitszertifikat dem vertrauenswürdigen Speicher des Computers hinzuzufügen. Geben Sie **Y**ein.

   Die Meldung „Status:Erfolg“ wird angezeigt und bestätigt, dass der Feed erfolgreich hinzugefügt wurde.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

## Senden Sie Sperrlisteneinträge aus einem Security Incident für die Check Point NGTP -Integration

An einen Security Incident-Datensatz angehängte erkennbare Elemente werden als Sperrlisteneinträge in verschiedene Sperrlisten zur Genehmigung übermittelt. Ein optionaler Genehmigungsprozess für Sperrlisteneinträge ist Teil des vorkonfigurierten Workflows. Das Gateway importiert Sperrlisteneinträge (IP-Adressen, URLs, Domänen), die in Sperrlisten enthalten sind.

### Vorbereitungen

Erforderliche Rolle:

- Security Incident Analyst (sn_si.analyst), um Sperrlisteneinträge zu übermitteln.
- Security Incident-Administrator (sn_si.admin), um Sperrlisteneinträge zu genehmigen. Diese Berechtigung kann nach Bedarf von Ihrer Organisation zugewiesen werden.

### Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der Rolle „sn_si.analyst“ übermitteln Sperreinträge, indem sie eine Sperre für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind.

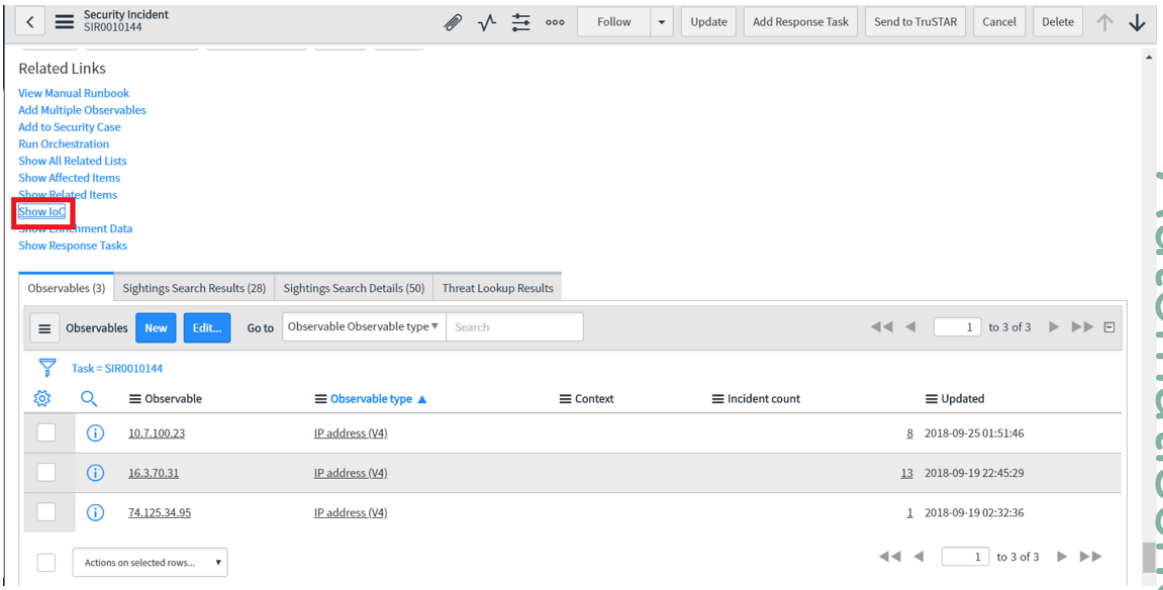


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

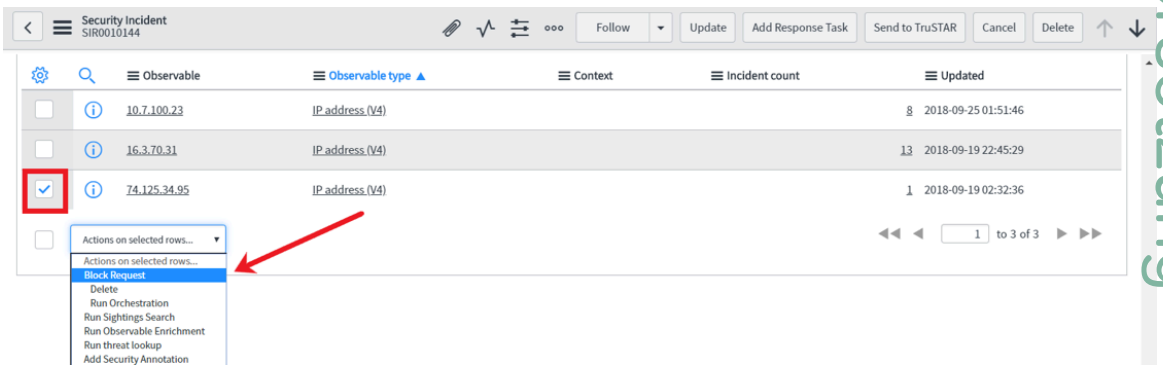
Nach der Übermittlung wird ein Sperrlisteneintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockanforderung für ein erkennbares URL-Element.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**, und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.



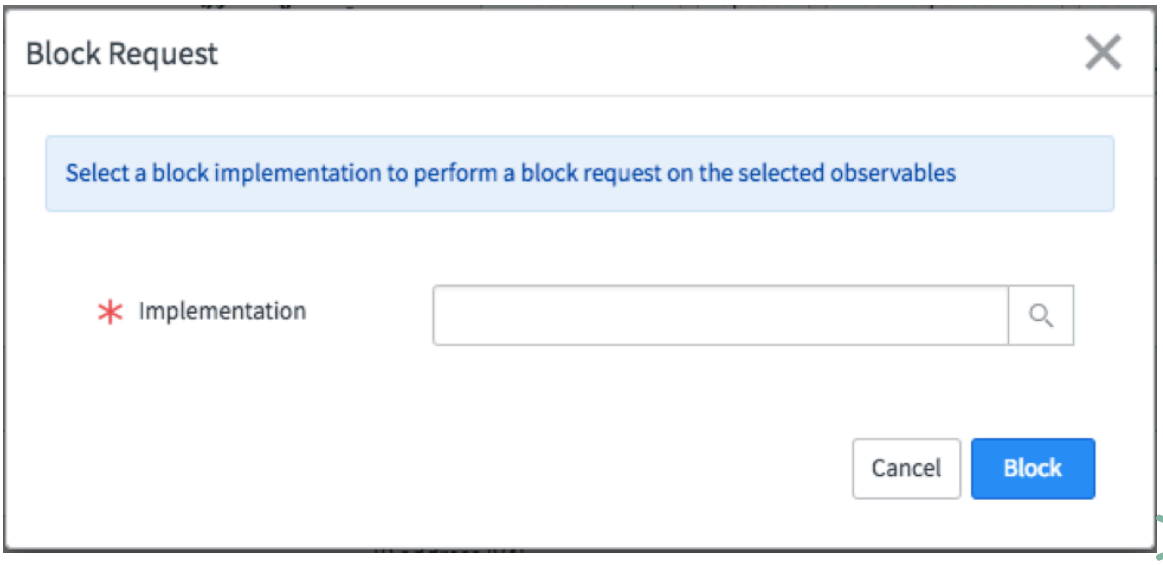

3. Wählen Sie in der zugehörigen Liste „Erkennbare Elemente“ die zu blockierenden erkennbaren Elemente aus, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die **Option Anforderung**blockieren aus.




4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( ).

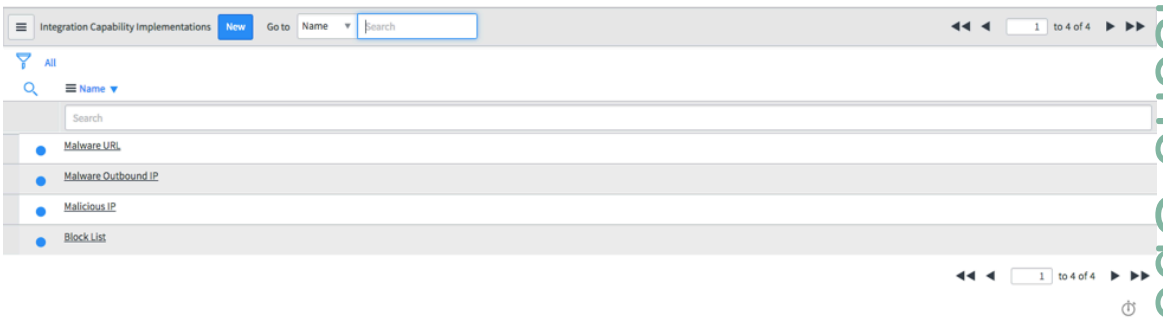
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

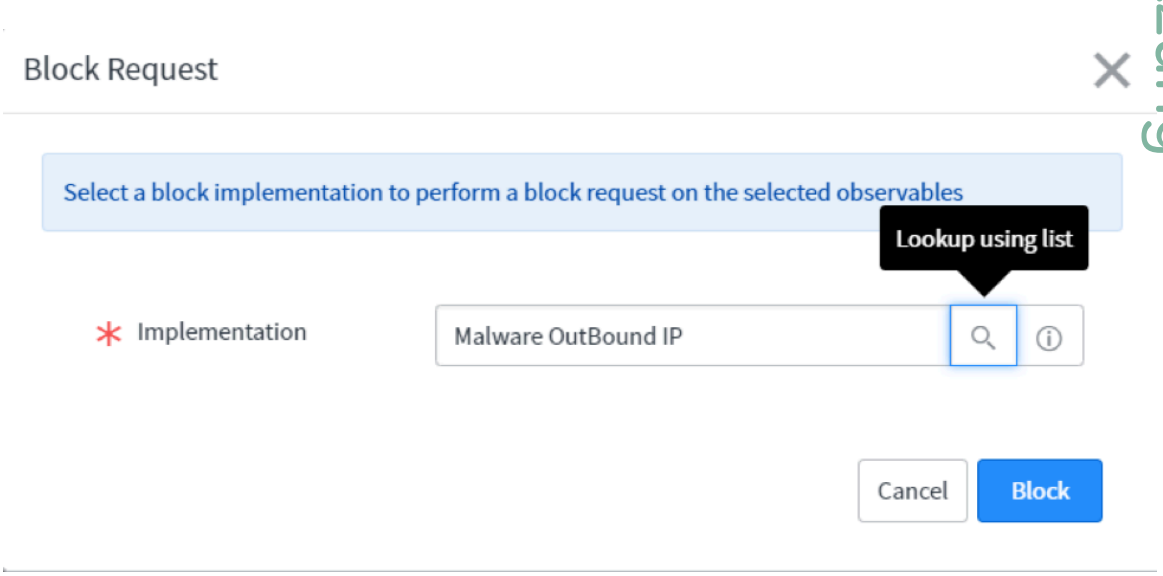



**5.** Wählen Sie in der Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

**Hinweis:**
In diesem Beispiel muss der erkennbare Typ des Eintrags (IP) mit dem erkennbaren Typ der Sperrliste (IP) übereinstimmen.




**6.** Klicken Sie im Dialogfeld **Sperranforderung**mit dem Namen der Sperrliste im Feld Implementierung auf Sperren.

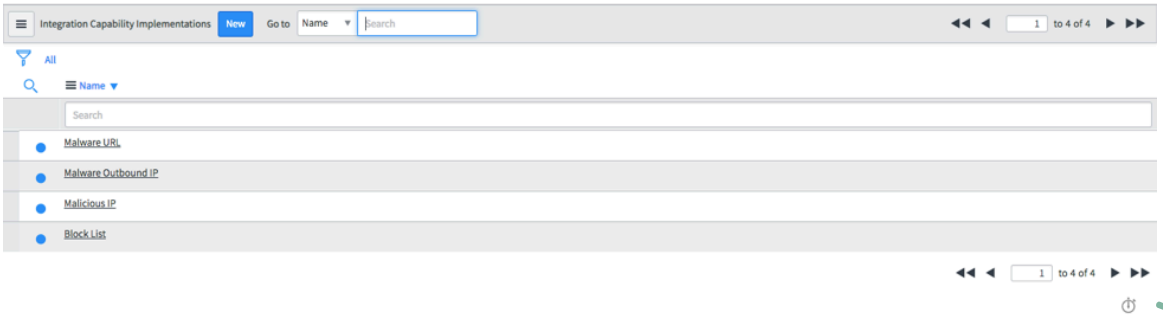



Automatische Übersetzung

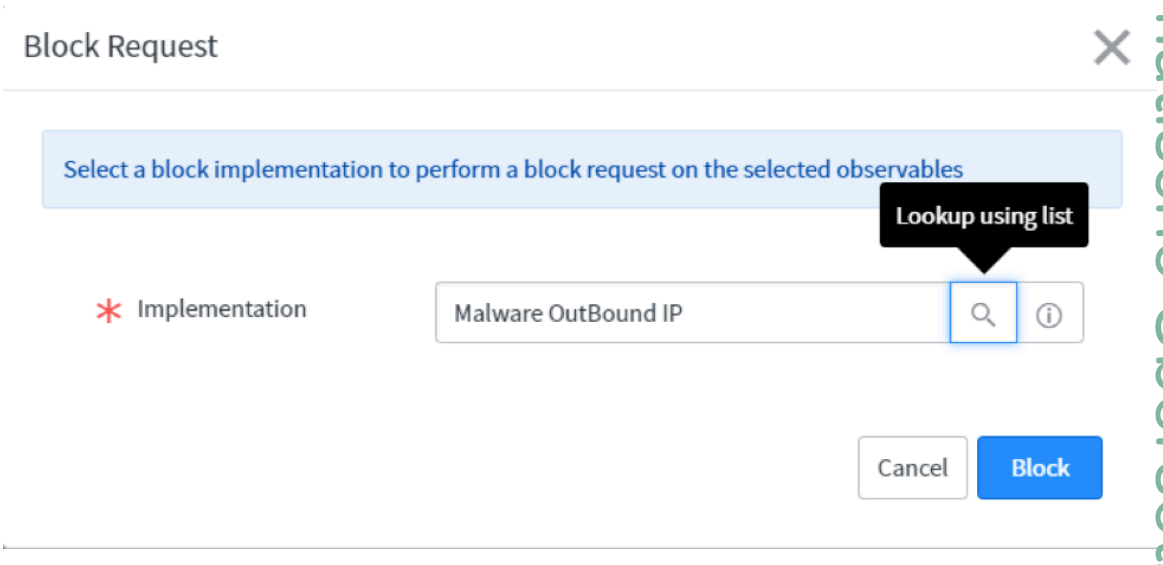
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie in der angezeigten Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

**Hinweis:**
In diesem Beispiel muss der erkennbare Typ des Eintrags (IP) mit dem erkennbaren Typ der Sperrliste (IP) übereinstimmen.



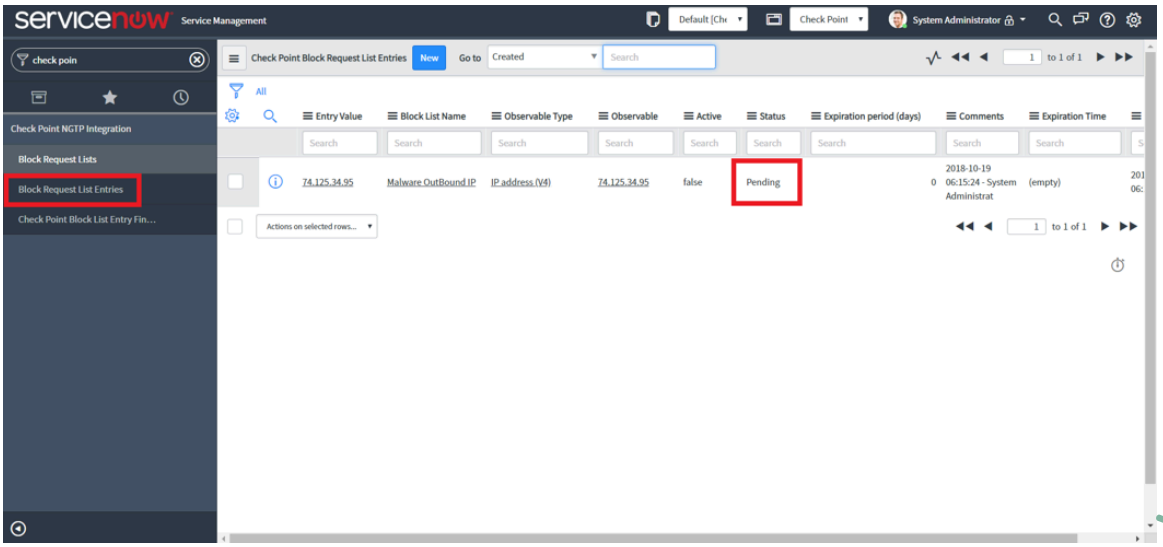

8. Klicken Sie im Dialogfeld **Sperranforderung** mit dem Namen der Sperrliste im Feld **Implementierung**auf Sperren.



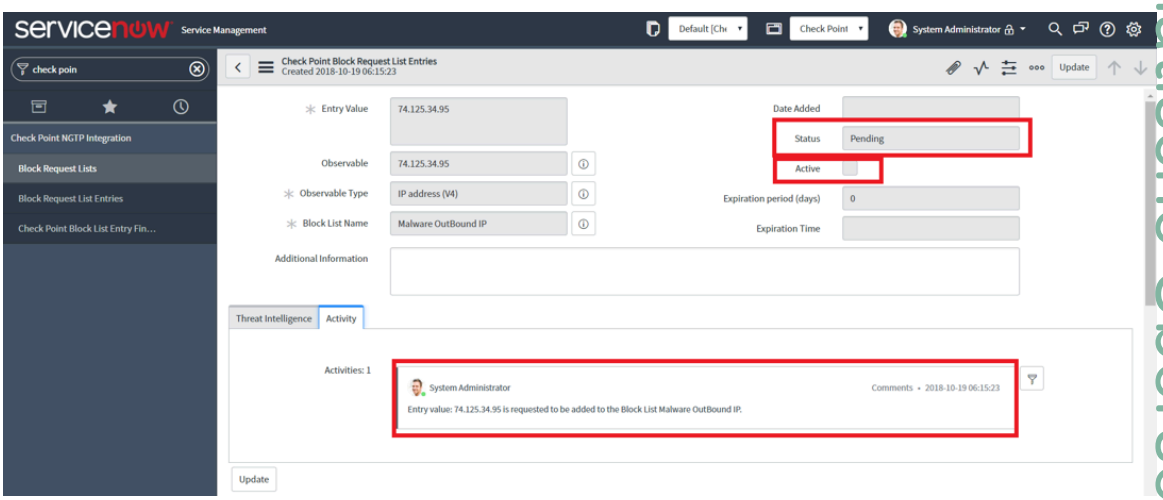

9. Navigieren zu **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**, und klicken Sie auf **Sperranforderungslisteneinträge**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**10.** Klicken Sie in der Liste Check Point Sperranforderungsliste Einträge in der Spalte Eingabewert auf das **erkennbare** Element, um den Datensatz zu öffnen.
In diesem Beispiel wird der Datensatz für **74.125.34.95** angezeigt.




Der Status lautet Ausstehend, das Kontrollkästchen Aktiv ist deaktiviert, und die Arbeitsnotizen zeigen an, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorliegt. Diese Sperrlisteneintragsanforderung ist zur Genehmigung bereit.

Das Symbol neben dem Feld „Erkennbares Element“ ist ein Link zur Tabelle „Erkennbares Element“ der Now Platform.

Der Wert im Feld „Erkennbares Element“ (74.125.34.95) ist mit der Tabelle „Erkennbares Element“ verknüpft und stimmt mit dem Format überein, das aus dem Security Incident Response-Incident-auslösenden Event übernommen wurde.

### Senden Sie Sperrlisteneinträge direkt aus der Sperrlisteneintragstabelle

Für erkennbare Elemente, die als böswillig eingestuft wurden und nicht mit einem bestimmten Now Platform Security Incident verknüpft sind, übermitteln Sie Sperrlisteneinträge aus der Sperrliste.

**Vorbereitungen**
Erforderliche Rolle: Security Incident Administrator (sn_si.analyst)

Automatische Übersetzung

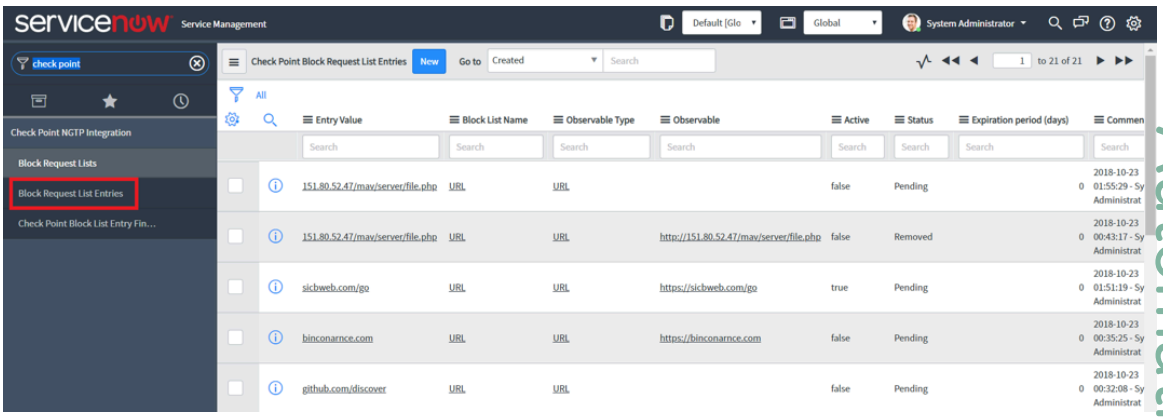
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein erkennbares Element blockieren möchten, von dem Sie festgestellt haben, dass es böswillig ist, oder ein erkennbares Element zulassen möchten, von dem Sie festgestellt haben, dass es nicht böswillig ist, und das erkennbare Element keinem bestimmten Now Platform-Security Incident-Datensatz zugeordnet ist, übermitteln Sie Sperrlisteneinträge direkt aus der Sperrliste. Beispiele für diese Arten von Sperrlisteneinträgen sind URLs oder Domänen für bestimmte Websites.

### Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Anforderungseinträge sperren**.

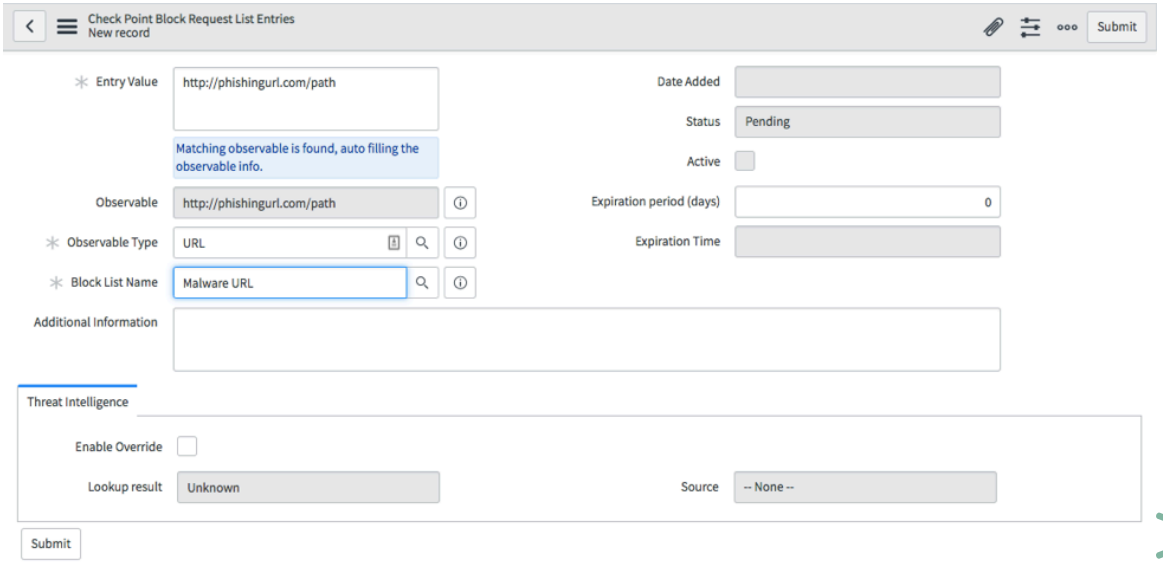



2. Klicken Sie auf das Modul **Sperranforderungslisten**.
3. Klicken Sie in der Liste „Check Point – Sperranforderungslisteneinträge“ auf **Neu**.
4. **Geben** Sie im Feld Eingabewert einen Wert für das erkennbare Element ein.
   Die zwei möglichen Ergebnisse dieses Eintrags:
   - Die verbleibenden Felder im Formular werden automatisch ausgefüllt.
   - Ein übereinstimmendes erkennbares Element wird gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf Absenden. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

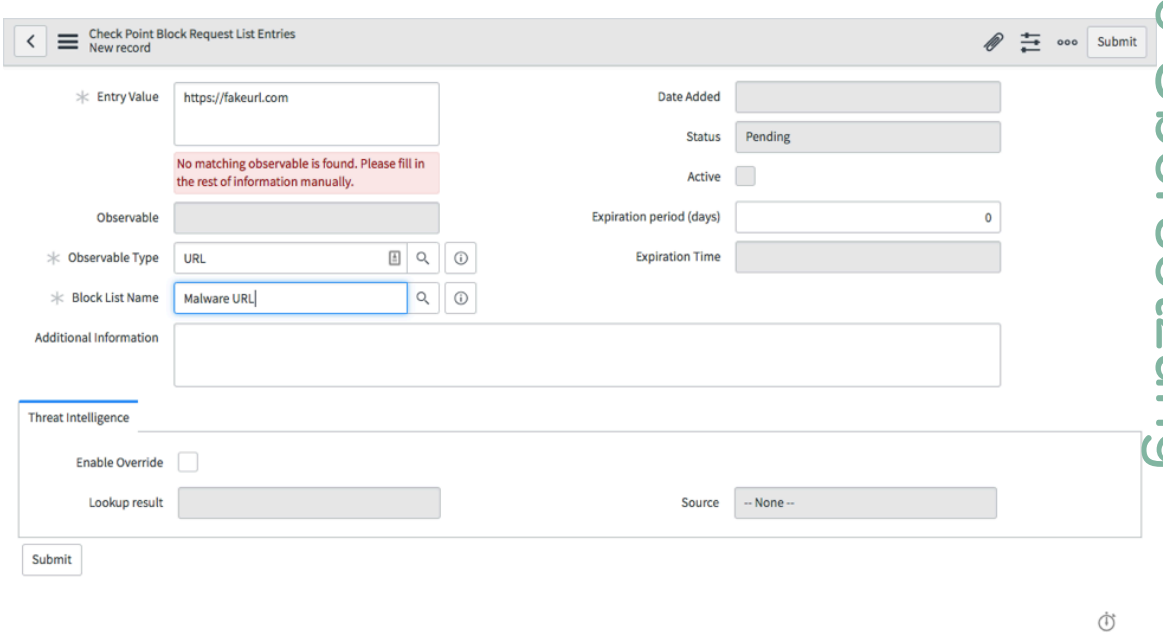
   Eine Nachricht wird angezeigt, in der Sie aufgefordert werden, das Formular auszufüllen. Es wurde kein passendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Wählen Sie nach Abschluss die Sperrliste aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf Absenden. Ein Datensatz für erkennbare Elemente wird erstellt. Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf das Suchsymbol, um die Sperrliste auszuwählen, an die Sie den Eintrag anhängen möchten.
6. Klicken Sie auf **Absenden**.
7. Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
   Wenn eine Meldung angezeigt wird, in der Sie aufgefordert werden, die restlichen Informationen manuell einzugeben, füllen Sie die Felder aus.



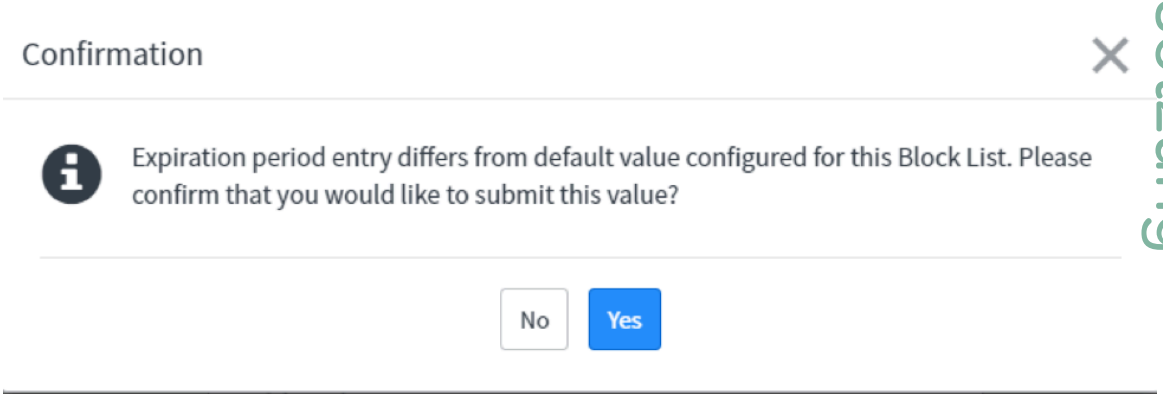

| Feld | Beschreibung |
|---|---|
| Erkennbarer Typ | Typ des erkennbaren Elements, das im Dialogfeld unterstützt wird. |
| Name der Sperrliste | Sperrliste, zu der der Eintrag gehören soll. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:**<br>Wählen Sie die Sperrliste aus, an die Sie den Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen. |
| Überschreibung aktivieren (Standard ist ausgewählt) | Suchergebnis oder -quelle. Wenn konfiguriert, können Sie ein Suchergebnis und die Quelle eingeben, die zum Suchen der Ergebnisse verwendet wird. Diese Felder werden normalerweise ausgefüllt, wenn ein Security Incident-Datensatz erstellt wird. In diesem Fall gibt es kein Suchergebnis oder keine Quelle, und Sie füllen diese Felder manuell aus. |
| Suchergebnis | Wählen Sie **Unbekannt** oder **Böswillig aus**. |
| Quelle | Quelle, die eine Bedrohungssuche für den Sperrlisteneintrag durchführt, z. B. ThreatCrowd usw |
| Ablaufzeitraum | Der Ablaufzeitraum, der standardmäßig von der Sperrliste geerbt wird. Sie können diesen Wert überschreiben, aber nur während der Erstellung des Eintrags.<br>0 gibt an, dass der Sperrlisteneintrag nie abläuft.<br>Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Es gibt keinen Höchstwert.<br>Wenn Sie beispielsweise am 1. Mai um 14:01 Uhr 30 Tage eingeben, läuft der Sperrlisteneintrag am 31. Mai um 14:01 Uhr ab. Der Planer prüft jedoch jeden Tag um 00:00 Uhr auf abgelaufene Einträge und ändert den Status des Eintrags am 1. Juni um 00:00 Uhr in „Abgelaufen“. |

8. Klicken Sie auf **Absenden**.
Wenn Sie den standardmäßigen Ablaufzeitraum des Sperrlisteneintrags geändert haben, wird ein Bestätigungsdialogfeld mit der Meldung angezeigt, dass sich der Zeitraum von der ausgewählten Sperrliste unterscheidet.



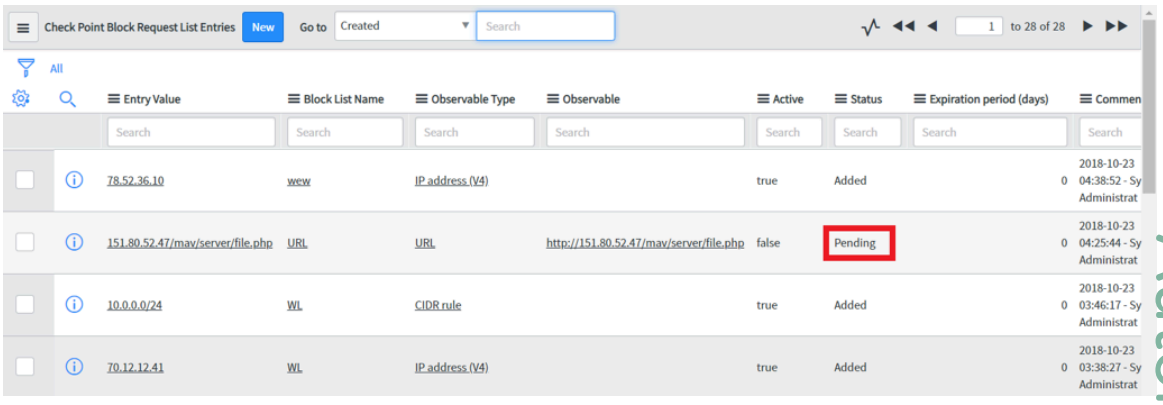

| Option | Beschreibung |
|---|---|
| Ja | Bestätigt Ihre Überschreibung des Ablaufs, speichert den Datensatz und kehrt zu den Check Point-Sperrlisteneinträgen zurück. Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet. |
| Nein | Bricht die Überschreibung ab. An dieser Stelle können Sie den Wert für den **Ablaufzeitraum**ändern. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
|---|---|
| | Klicken Sie nach dem Ändern des Werts auf Absenden, um zur Liste Check Point Block Einträge zurückzukehren. |

9. Wenn nicht angezeigt, navigieren Sie zu **Check Point Sperranforderungslisteneinträge**und beachten Sie, dass der Status für den Eintrag **Ausstehend**lautet.




Der Eintrag ist jetzt zur Genehmigung bereit.

### Genehmigen Sie Sperrlisteneinträge für die Check Point NGTP -Integration

Ein Genehmigungsprozess für Sperrlisteneinträge ist Teil des vorkonfigurierten Workflows. Sie genehmigen Sperrlisteneinträge, bevor die Einträge in Sperrlisten aktiviert werden. Nachdem Sie den Sperrlisteneintrag genehmigt haben, ruft das Gateway den Eintrag ab, und Ihr erkennbares Element ist ab diesem Zeitpunkt blockiert.

### Vorbereitungen

- Die Genehmigung für Sperrlisteneinträge ist standardmäßig dem Security Incident-Administrator (sn_si.admin) zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden. Im folgenden Beispiel verfügt der Now Platform-Administrator über die Genehmigungsberechtigung.

Erforderliche Rolle: sn.si.admin

### Warum und wann dieser Vorgang ausgeführt wird

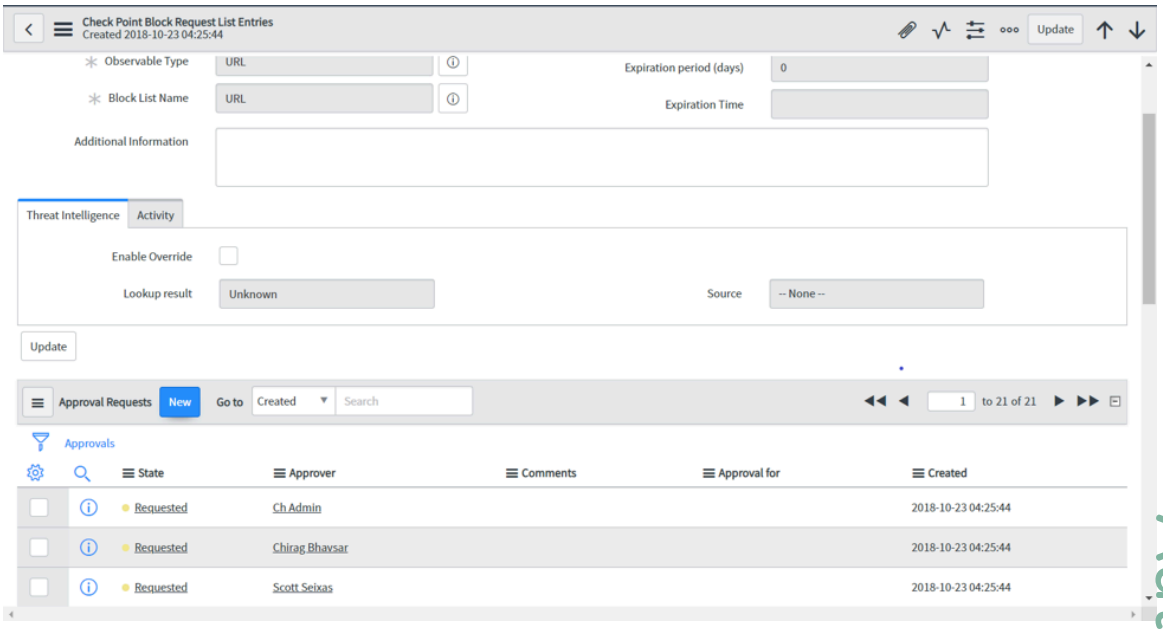
Wenn der Genehmigungsprozess aktiviert ist, wird ein Sperrlisteneintrag in der Sperrliste erst aktiviert oder deaktiviert, wenn er genehmigt wurde.

### Prozedur

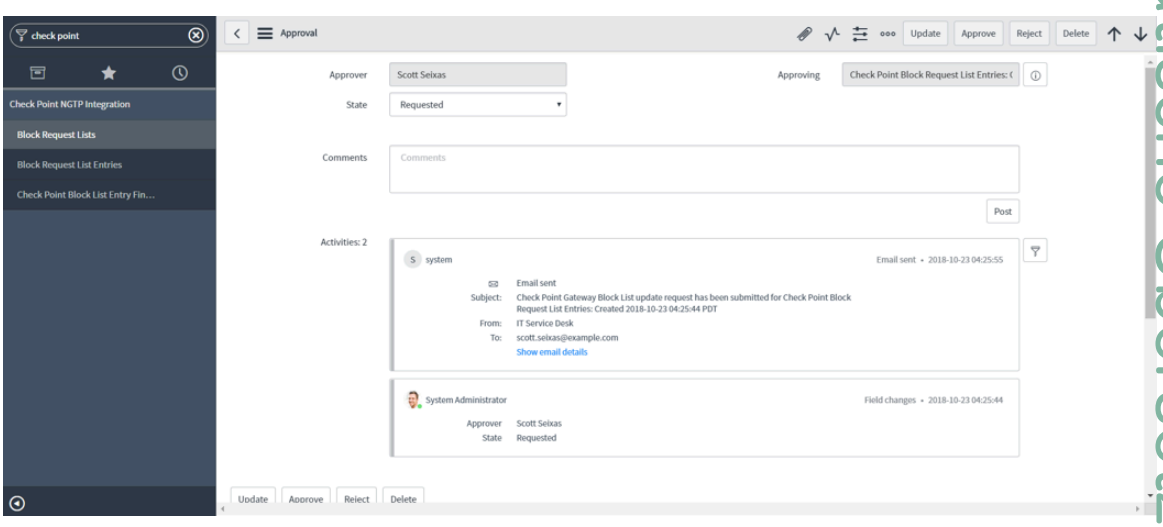
1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**, und öffnen Sie den Datensatz „Sperrlisteneintrag“.
2. Scrollen Sie im Datensatz „Sperrlisteneintrag“ zum Abschnitt „ **Genehmigungsanforderungen** “.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Klicken Sie in Genehmigungsanforderungen auf ein Element in der **Spalte** Status, um es zu öffnen.
Der Genehmigungsdatensatz wird angezeigt.




**4.** Wählen Sie eine Option für die Genehmigung des Sperrlisteneintrags aus.

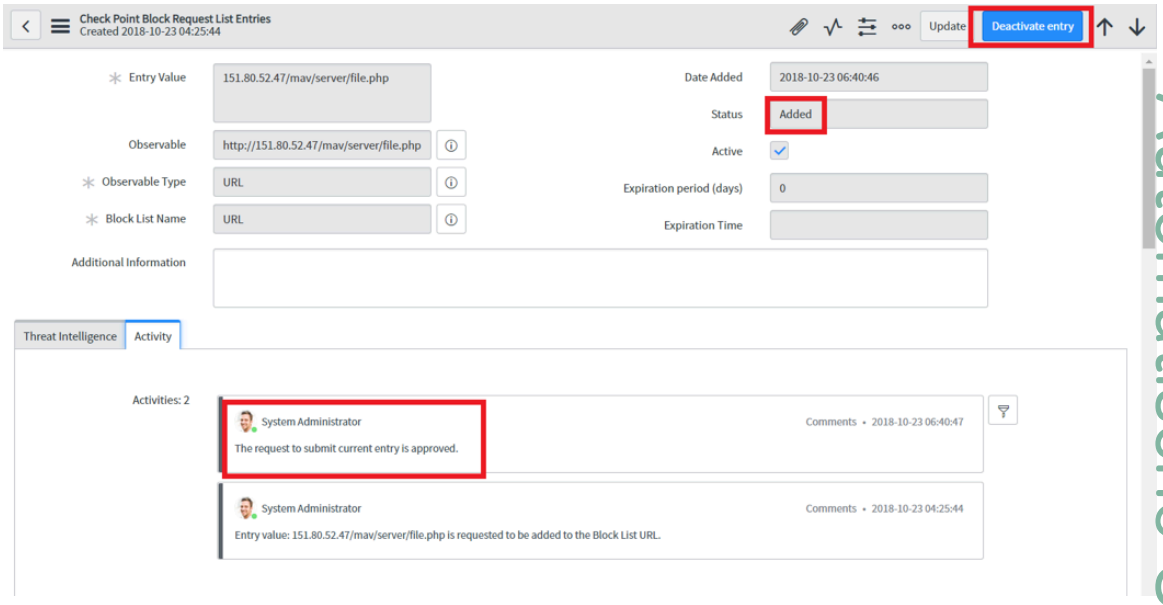
| Option | Beschreibung |
|---|---|
| Genehmigen | Im Zutrittsdatensatz ändert sich das Feld Status in Hinzugefügt, und das Kontrollkästchen Aktiv wird aktiviert.<br><br>Die Schaltfläche Deaktivieren wird angezeigt und ist aktiv.<br><br>Arbeitsnotizen zeigen an, dass die Anforderung für den Sperrlisteneintrag genehmigt wurde. |
| Ablehnen | Im Zutrittsdatensatz ändert sich das Feld Status in Abgelehnt, und das Kontrollkästchen Aktiv wird deaktiviert. Dies zeigt an, dass der Zutritt auf dem Gateway nicht blockiert ist. |

Automatische Übersetzung

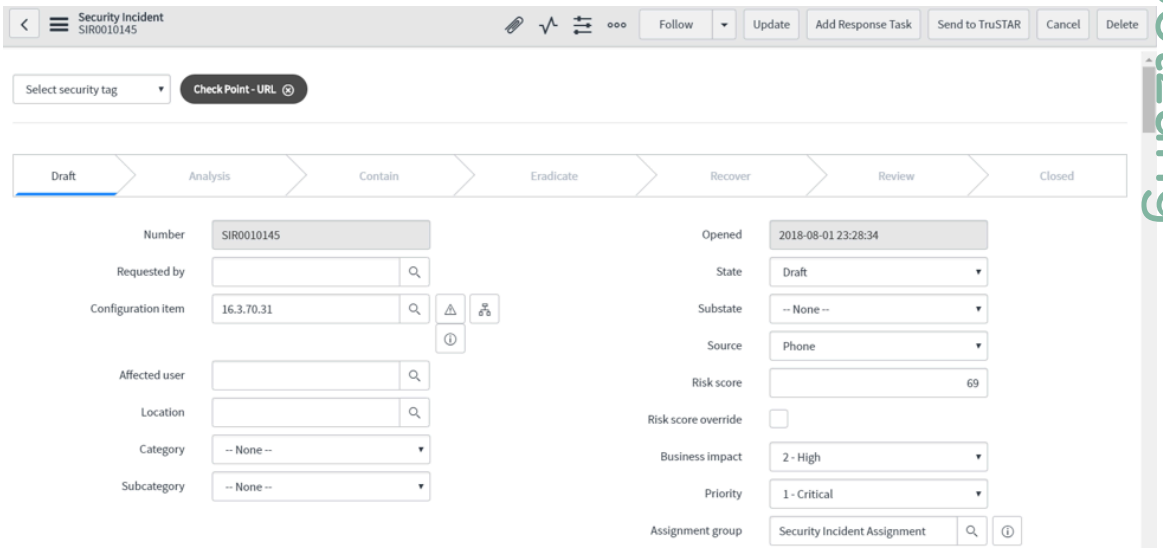
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | Arbeitsnotizen zeigen an, dass die Anforderung für den Sperrlisteneintrag abgelehnt wurde. |

Nachdem Sie den Sperrlisteneintrag genehmigt haben und er aktiviert ist, ruft die Check Point Next-Gen-Firewall den Sperrlisteneintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, ist das erkennbare Element ab diesem Zeitpunkt blockiert. Beachten Sie in der folgenden Abbildung, dass das Kontrollkästchen Aktiv aktiviert ist, der Status Hinzugefügt lautet und die Arbeitsnotizen angeben, dass die Anforderung genehmigt wurde.



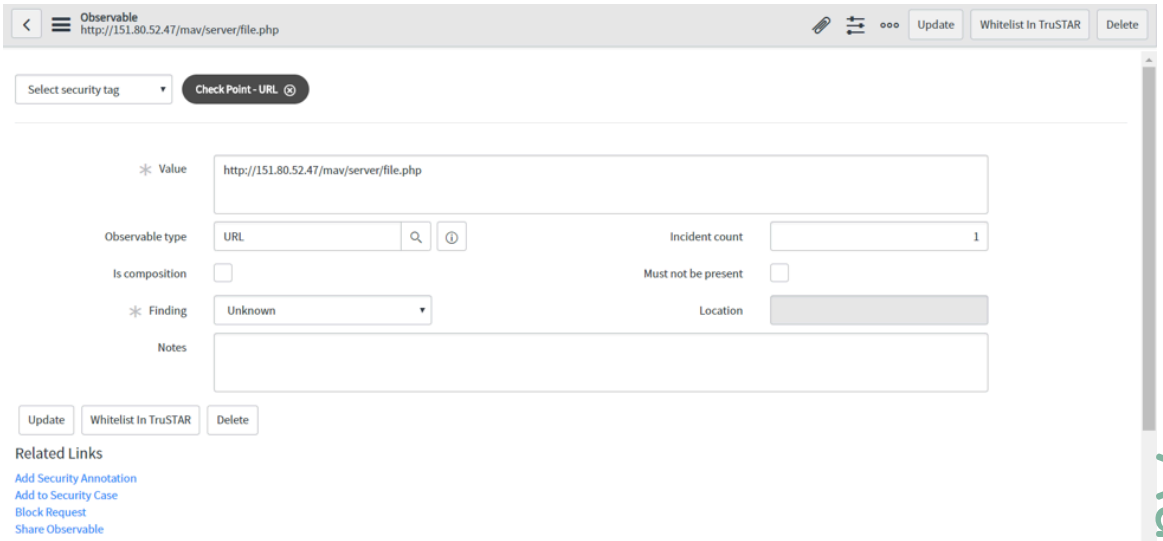

Nachdem der Sperrlisteneintrag genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag markiert. Das Tag wird oben im Datensatz angezeigt.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



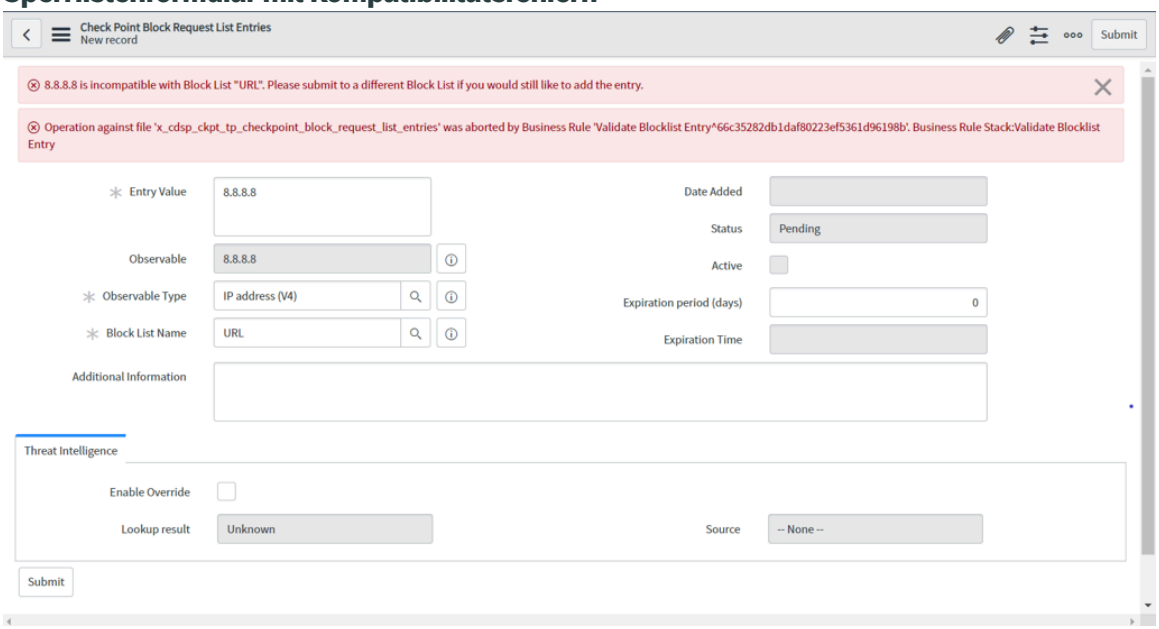

### Ausnahmen für Sperrlisteneinträge für die Check Point NGTP -Integration

Es gibt Einschränkungen für das Hinzufügen von Sperrlisteneinträgen zu Sperrlisten. Wenn Duplikat-, Kompatibilitäts- oder CIDR-Konflikte (Classless Inter-Domain Routing) auftreten, wenn Sie versuchen, Sperrlisteneinträge zu Sperrlisten hinzuzufügen, werden Fehlermeldungen angezeigt, die Ihnen bei der Behebung dieser Fehler helfen.

## Kompatibilitätsausnahme

Jede Sperrliste akzeptiert nur Einträge, die mit ihrem erkennbaren Typ kompatibel sind. Wenn Sie eine Domänensperrliste erstellen und versuchen, eine erkennbare IP-Adresse an sie anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänen-Sperrliste nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

**Sperrlistenformular mit Kompatibilitätsfehlern**

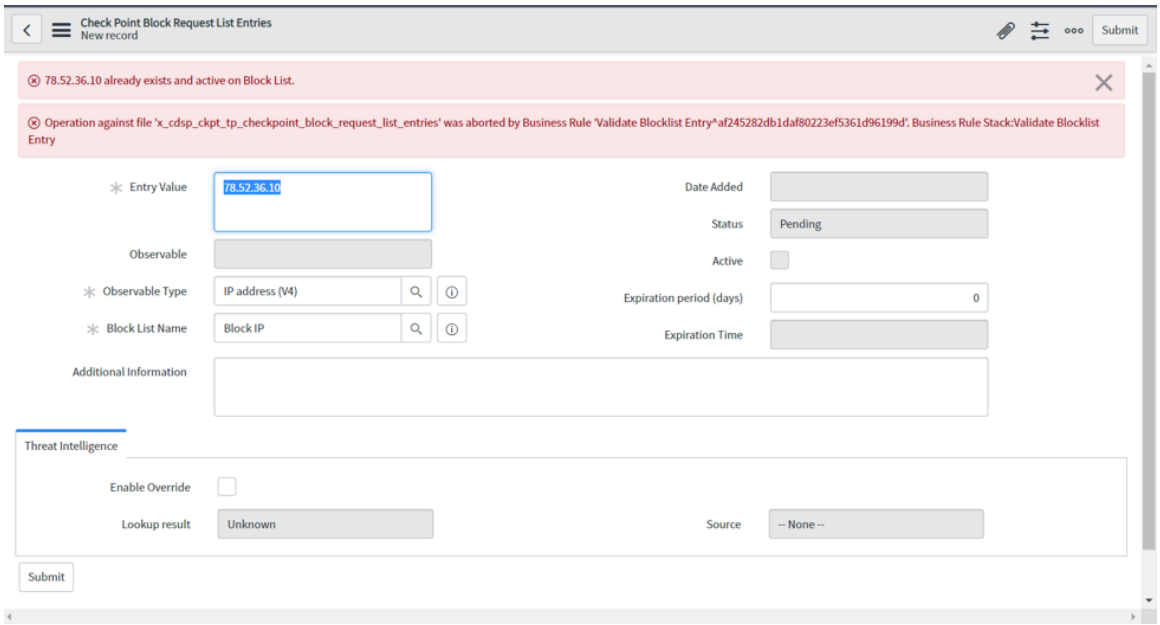





© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

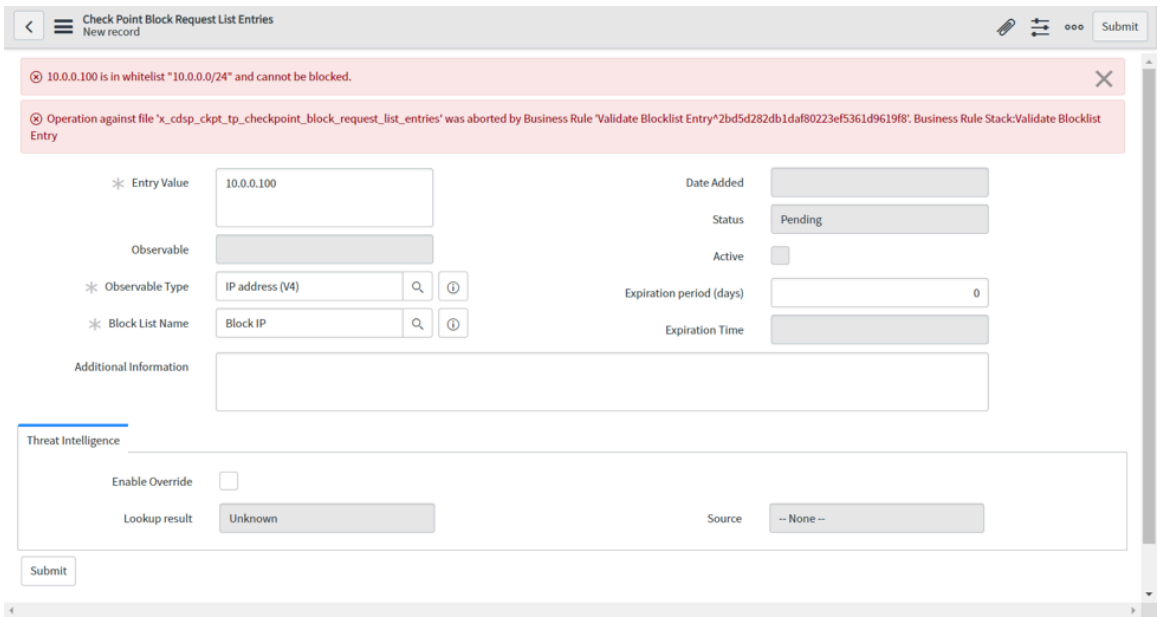
## Duplizierungsausnahme

Ein erkennbares Element kann nicht für mehrere Sperrlisten desselben erkennbaren Typs aktiviert werden. Wenn ein erkennbares URL-Element bereits in einer URL-Sperrliste aktiviert ist und Sie versuchen, dasselbe erkennbare Element in einer Phishing-URL-Sperrliste zu aktivieren, wird eine Duplizierungsfehlermeldung angezeigt.




## CIDR-Ausnahme (Classless Inter-Domain Routing).

Wenn Sie versuchen, eine einzelne IP-Adresse an eine Allow-Liste anzuhängen, und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits in einer Sperrliste/Zulassungsliste befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler weist darauf hin, dass die einzelne IP-Adresse bereits in der Sperrliste oder Allow-Liste als Teil des erkennbaren CIDR-Elements enthalten ist. Zum Beispiel ist 192.168.24.25 Teil des CIDR-Blocks 192.168.0.0/22.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Bearbeiten Sie den Sicherheits-Tag-Namen für die Check Point NGTP -Integration

Wenn beim Erstellen des Sperrlistendatensatzes die Checkbox Tag anzeigen aktiviert ist, können Sie die Tag-Namen und Farben der Sicherheits-Tags bearbeiten. Sicherheits-Tags helfen Ihnen, erkennbare Elemente nachzuverfolgen, die bereits blockiert sind.

#### Vorbereitungen

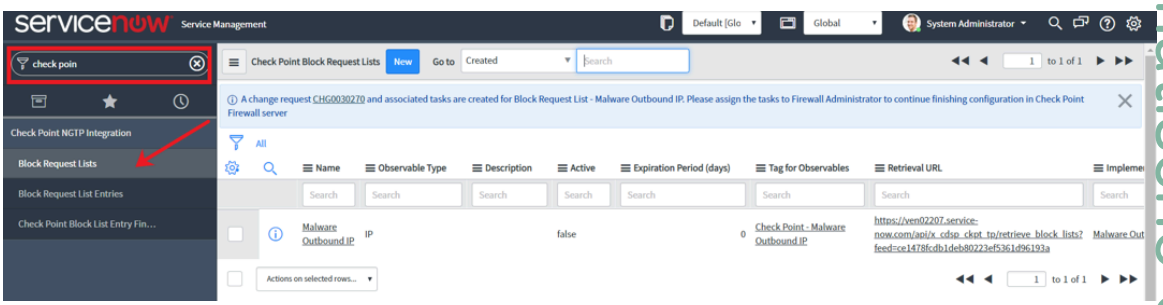
Erforderliche Rolle: sn.si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

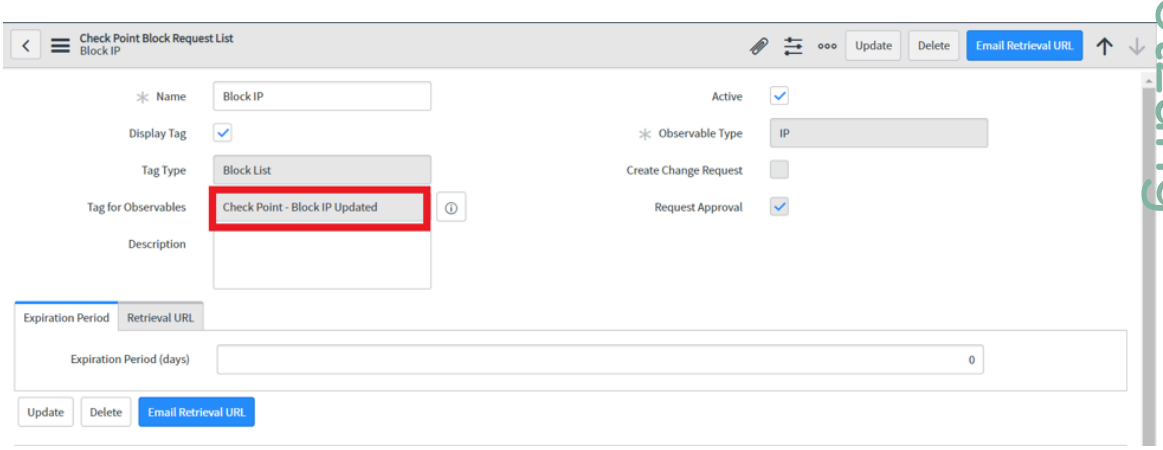
Sicherheits-Tags helfen Ihnen, schnell zu erkennen, welche Security Incidents erkennbare Elemente in einer Sperrliste enthalten. Tags helfen Ihnen auch dabei, zu erkennen, ob ein erkennbares Element bereits blockiert ist oder ob es aus einer Sperrliste entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Sperrlisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, damit Sie bestimmte Tags leichter erkennen können.

#### Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Konfiguration der Sperranforderungsliste**.



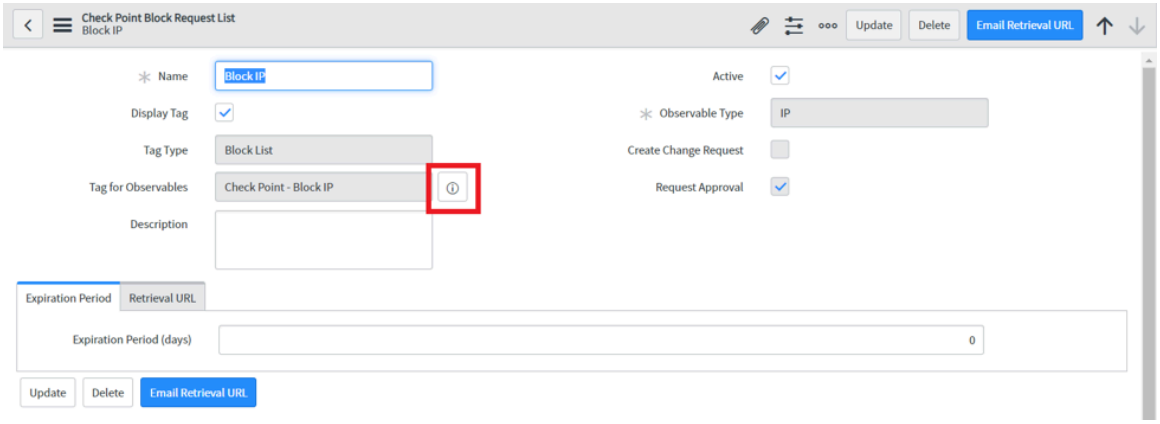

2. Klicken Sie auf ein Element in der Spalte **Name**, um es zu öffnen.
   Der Datensatz der Sperrliste wird angezeigt. Standardmäßig ist der Name des Sicherheits-Tags derselbe Wert, den Sie im Feld Name der Sperrliste eingegeben haben, als Sie die Sperrliste erstellt haben. Standardmäßig enthält der Name auch ein Sperrlisten-Präfix, z. B. Sperrliste – Malware Malicious URLs.



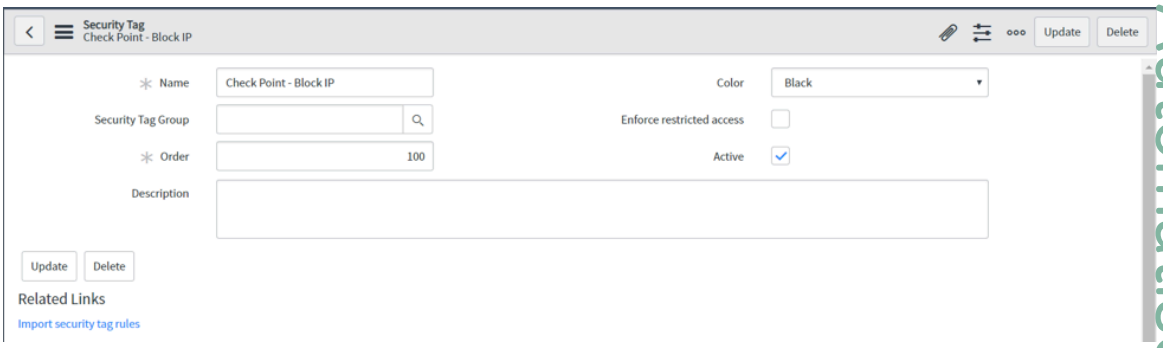

3. Klicken Sie auf das Informationssymbol neben dem Tag für erkennbare Elemente und dann auf Datensatz öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

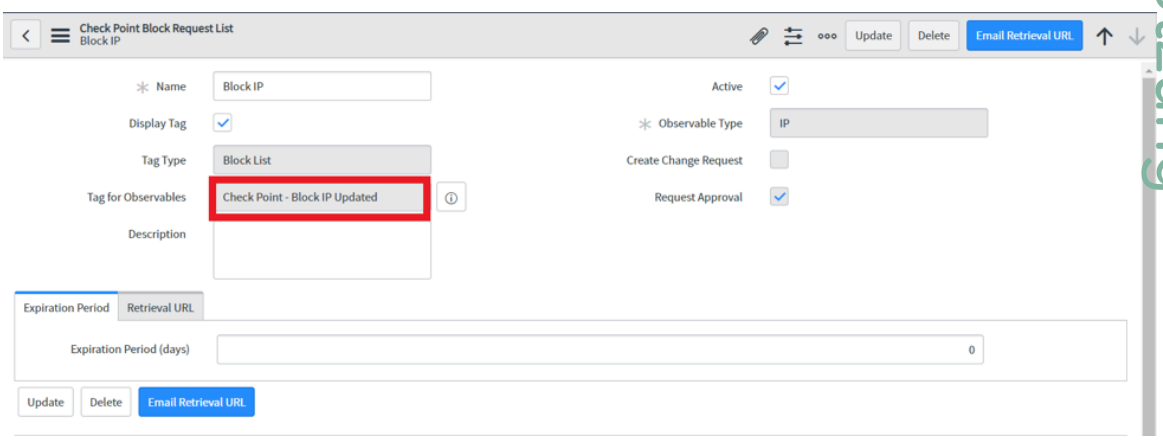



Das Sicherheits-Tag-Formular wird angezeigt.




4. Ändern Sie im Feld **Name** den Sicherheits-Tag-Namen.
5. Klicken Sie auf **Aktualisieren**.
   Der aktualisierte Sperrlistendatensatz wird mit dem geänderten Tag-Namen angezeigt.

**Hinweis:**
Im folgenden Beispiel wurde dem Tag-Namen Ausgehend hinzugefügt. Behalten Sie das Check Point-Präfix in Ihrem neuen Tag-Namen bei, damit Sie leichter erkennen können, ob das Tag der Check Point-Firewall-Integration der nächsten Generation zugeordnet ist.

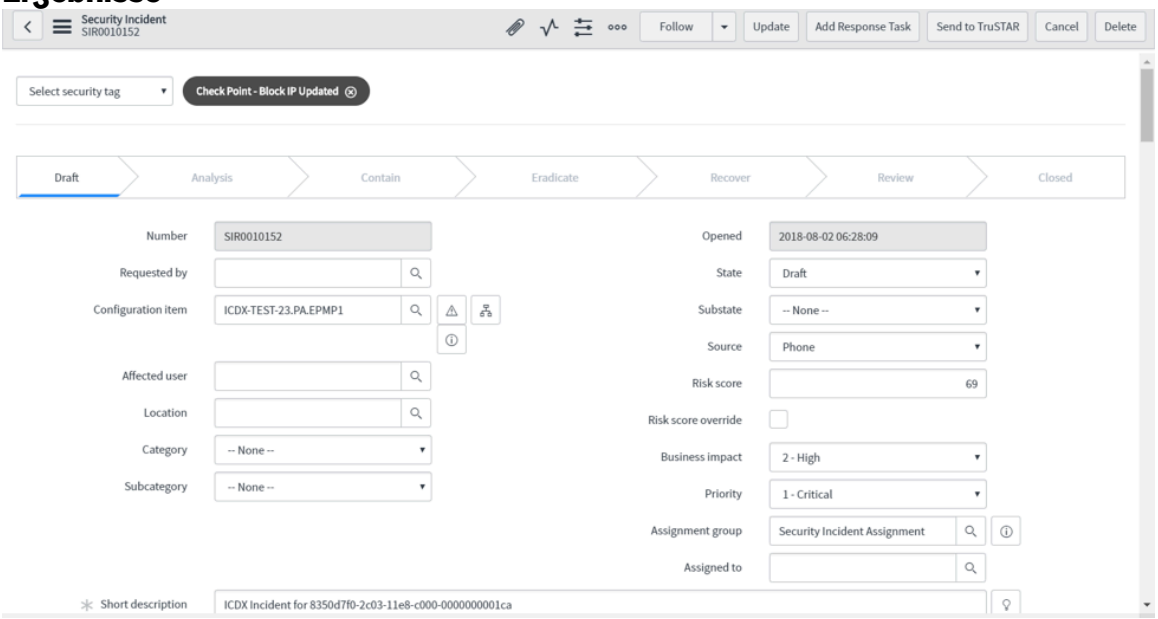



Die Sicherheits-Tags werden für jeden erkennbaren Typ (IP, URL, Domäne) im Security Incident-Datensatz und im Datensatz des erkennbaren Elements angezeigt, jedes Mal, wenn das erkennbare Element der Sperrliste hinzugefügt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse




Wenn ein erkennbares Element bereits einer Sperrliste hinzugefügt wurde und ein Sicherheits-Tag für einen Security Incident für dieses erkennbare Element angezeigt wird, wird das Sperrlisten-Sicherheitstag auch automatisch in allen nachfolgenden Security Incident-Datensätzen angezeigt, die erstellt werden. Diese Duplizierung teilt Ihnen mit, dass sich das erkennbare Element bereits in einer Sperrliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In diesem Fall weist kein Sicherheits-Tag darauf hin, dass das Ablaufdatum des erkennbaren Elements möglicherweise abgelaufen ist oder das erkennbare Element in einer Sperrliste deaktiviert wurde.

#### Deinstallieren Sie die Check Point NGTP -Integration

Wenn Sie Check Point NGTP Integration aus Ihrer Now Platform-Instanz deinstallieren und alle Reste aus der Integration entfernen möchten, finden Sie auf der ServiceNow-Dokumentationswebsite Anweisungen zum Deinstallieren von Anwendungen.

### Vorbereitungen

Erforderliche Rolle: admin

## Integration mit CrowdStrike Falcon Host

Mit der CrowdStrike Falcon Host -Integration können Sie erkennbare Elemente in einem Security Incident in eine Beobachtungsliste verschieben, sodass sie zusätzliche Warnungen generieren können. Diese Integration ist eine Implementierung des Workflows CrowdStrike Falcon Host – In Beobachtungsliste veröffentlichen.

| | |
|---|---|
| Erkunden<br>Security Incident Response-Integrationen | Einrichten<br>Beginnen Sie mit der Integration von CrowdStrike Falcon Host . |
| Verwenden | Entwickeln |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| • Suchvorgänge für erkennbare Elemente durchführen<br>• Aktivität „In Beobachtungsliste veröffentlichen“. | • ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und Hilfe | |
| • Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Beginnen Sie mit der Integration von CrowdStrike Falcon Host .

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der CrowdStrike Falcon Host -Integration, schnell aktivieren und einrichten. Bevor Sie die CrowdStrike Falcon Host -Integration verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und dann einen Benutzernamen und ein Passwort hinzufügen.

### Vorbereitungen

- Wenn Sie die CrowdStrike Falcon Host -Integration von einer früheren Version aktualisieren, müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die neue Integration unterstützt die OAuth2-Authentifizierung. Für dieses Update müssen Sie die **API-Client-ID** und den **API-Client-Secret** eingeben, um sich zu authentifizieren und die Konfiguration abzuschließen.
- Aktivieren Sie in den **API**-Umfängen des Portals CrowdStrike Falcon Host die Einstellung **Lesen** und **Schreiben** für **IoCs (Indicators of Compromise)**.

Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte „CrowdStrike Falcon Host“ auf **Konfigurieren**.
4. Füllen Sie die Felder im Formular aus, um die Konfiguration abzuschließen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CrowdStrike Falcon-Hostkonfiguration**

| Feld | Beschreibung |
|---|---|
| **Name** | Name der Integration, z. B. `demo-1`. |
| **API-Client-ID** | Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils im CrowdStrike Falcon Host -Portal erhalten. |
| **API-Client-Geheimnis** | Geheimer Clientschlüssel, den Sie aus dem Einstellungsabschnitt Ihres Kontoprofils im CrowdStrike Falcon Host -Portal erhalten. |

5. Klicken Sie auf **Absenden**.

## Ergebnisse

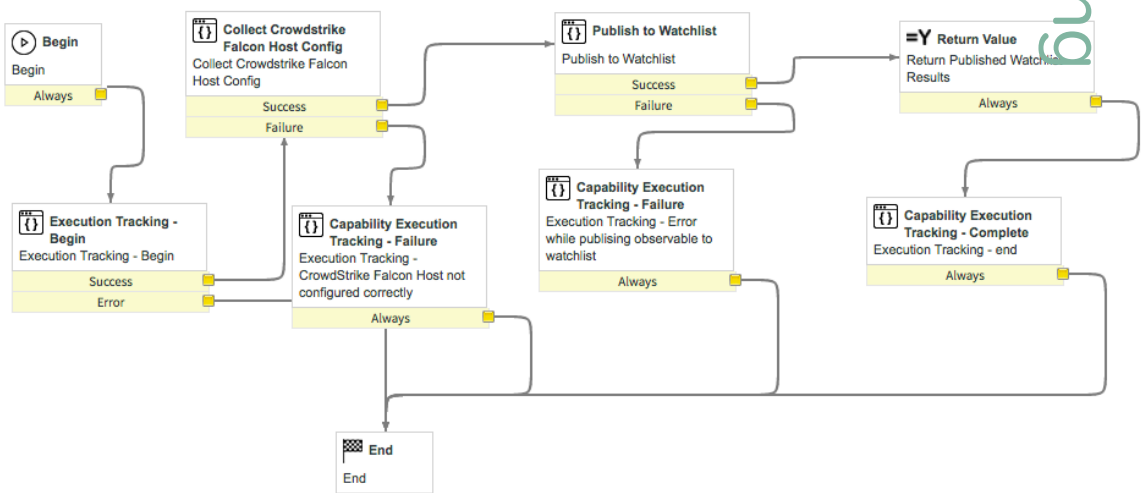
Nach der Konfiguration kann die CrowdStrike Falcon Host -Integration für die Veröffentlichung von erkennbaren Elementen in Beobachtungslisten in Security Incident Responseausgewählt werden.

### Security Operations CrowdStrike Falcon Host – In Beobachtungsliste veröffentlichen – Workflow

Der Workflow **„CrowdStrike Falcon Host – In Beobachtungsliste veröffentlichen“ von Security Operations** wird verwendet, um die Beobachtungsliste für die Generierung von Warnungen oder Events anzugeben. Die Warnungen und Events werden je nach Konfiguration im CrowdStrike Falcon Host-System angezeigt.

### Workflow „In Beobachtungsliste veröffentlichen“.

Dieser Workflow wird von Integration von Sicherheitsvorgängen – Fähigkeit „In Beobachtungsliste veröffentlichen“. ausgelöst, wenn Sie ein oder mehrere erkennbare Elemente auswählen, die einem Security Incident zugeordnet sind, und die UI-Aktion In Beobachtungsliste veröffentlichen verwenden, um die erkennbaren Elemente in eine Beobachtungsliste zu verschieben. Die erkennbaren Elemente können dann zum Generieren zusätzlicher Warnungen verwendet werden. Weitere Informationen finden Sie unter Veröffentlichen Sie erkennbare Elemente in einer Drittanbieter-Beobachtungsliste.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „CrowdStrike Falcon-Hostkonfigurationen erfassen“.

Die Workflow-Aktivität **„CrowdStrike Falcon Host-Konfigurationen erfassen“ erfasst** Konfigurationsinformationen, die im Workflow verwendet werden sollen.

Die **CrowdStrike** Falcon Host-Konfigurationsaktivität erfassen kann mit jedem Workflow verwendet werden, um die CrowdStrike Falcon Host-Konfigurationseinstellungen zu erfassen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. an. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| user_name | CrowdStrike Falcon Host-Benutzername |
| Kennwort | Passwort des CrowdStrike Falcon-Hosts |

### Aktivität „In Beobachtungsliste veröffentlichen“.

Die Workflow-Aktivität In Beobachtungsliste **veröffentlichen verschiebt erkennbare** Elemente in einem Security Incident in eine Beobachtungsliste, um Warnungen oder Ereignisse zu generieren. Die Warnungen und Events werden je nach Konfiguration im CrowdStrike Falcon Host-System angezeigt.

Die Aktivität In **Beobachtungsliste** veröffentlichen kann mit jedem Workflow verwendet werden, um erkennbare Elemente in einer Beobachtungsliste zu veröffentlichen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. an. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ergebnisse (Fortsetzung)**

| Ergebnis | Beschreibung |
|---|---|
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Security Incident Response. |
| user_name | Benutzername der Person, die für die CrowdStrike Falcon Host-Integration verantwortlich ist. |
| Kennwort | Das Passwort der Person, die für die CrowdStrike Falcon Host-Integration verantwortlich ist. |
| task_sys_id | Der Systembezeichner für diesen Auftrag zum Veröffentlichen in der Beobachtungsliste. |
| capabilityExecutionId | Der Name der zugeordneten Fähigkeit. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status | Der Status der Veröffentlichungsaktivität. |

## CrowdStrike Falcon Insight für die Integration von Security Operations .

Mit der Integration von CrowdStrike Falcon Insight für Security Operations können Sie Korrekturaktionen für die Endpunkte in Echtzeit durchführen, Profile verwenden, um Details zum Host zu erfassen, und mit dem Produkt Now Platform Security Incident Response bestimmte Abfragen oder Aktionen für den Endpunkt ausführen.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Die Integration von CrowdStrike Falcon Insight für Security Operations funktioniert mit Now Platform, sodass Sie zusätzliche Einblicke in den Umfang eines Incident erhalten. Der CrowdStrike Falcon Insight erfasst alle relevanten Endpunkt-Event-Aktivitäten. Sie können den Now Platform verwenden, um sich auf Untersuchungen und Korrekturmaßnahmen zu konzentrieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |
| CrowdStrike Falcon Insight für Security Operations | Erste Schritte mit der CrowdStrike Falcon Insight -Integration |

### Erste Schritte mit der CrowdStrike Falcon Insight -Integration

Sie können CrowdStrike Falcon Insight aktivieren und so einrichten, dass er mit Ihrer Now Platform -Instanz und Ihrem [ Security Incident Response -Produkt verbunden ist.

### Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie CrowdStrike Falcon Insight für die Security Operations -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

### Warum und wann dieser Vorgang ausgeführt wird

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie. | Diese Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Die Administratorrolle installiert die Integration aus dem ServiceNow Store und weist die Rolle sn_si.admin zu.<br>• Die Rolle „sn_si.admin“ konfiguriert die Integration, erstellt und aktiviert Profile und weist dann die Rolle „sn_si.analyst“ zu.<br>• Die Rolle „sn_si.analyst“ reagiert auf Security Incidents, startet Profile manuell und kann Anforderungen für Aktionen wie das Isolieren des Hosts und das Entfernen der Hostisolierung für eine genehmigte Gruppe senden. |
| Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren. | Das Plugin ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] ist erforderlich. Dieses Plugin ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows:<br><br>Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
| --- | --- |
| | des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren, die für die Integration erforderlich sind.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten:<br><br>**1.** Security Incident Response Abhängigkeit (com.snc.si_dep)<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br>**5.** Threat Intelligence Support Common<br>**6.** Trusted Security Circles<br>**7.** Security Operations Setup-Assistent<br>**8.** Security Incident Response |
| Richten Sie eine Genehmigungsgruppe ein. | Eine optionale Genehmigungsfunktion ist verfügbar, um Hostcomputer zu isolieren, im Netzwerk wiederherzustellen und Sichtungssuchen zu initiieren.<br><br>Um diese Option zu aktivieren, benötigen Sie die vorherige Genehmigung durch die Rolle „sn_si.admin“, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden oder wenn Sichtungssuchen durchgeführt werden. Wenn Sie eine zusätzliche Steuerungsebene für diese Aktionen **benötigen, aktivieren Sie beim Konfigurieren des Profils die Option Genehmigung** erforderlich. Die Genehmigungsberechtigung wird dem Benutzer mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe neu zuweisen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| Weisen Sie die CrowdStrike Falcon Platform-Rollen zu, und überprüfen Sie sie. | Die folgenden Rollen sind auf der CrowdStrike Falcon-Plattform für die Integrationskonfiguration erforderlich:<br>• Die Falcon-Administratorrolle ist erforderlich, um API-Clients oder -Schlüssel anzuzeigen, zu erstellen oder zu ändern.<br>• Die Rolle „Real Time Responder – Administrator“ ist zum Erstellen und Ausführen von benutzerdefinierten Skripts erforderlich.<br>• Die Rolle „Real Time Responder – Active Responder“ ist zum Erstellen und Ausführen von benutzerdefinierten Skripts erforderlich. |
| Stellen Sie sicher, dass die benutzerdefinierten Skriptrollen und -berechtigungen in CrowdStrike Falcon Platform aktiviert sind. | Diese Integration verwendet die benutzerdefinierten Skripts von CrowdStrike für einige der Ergänzungsfunktionen.<br>• Stellen Sie sicher, dass die Rollen „Real Time Responder – Administrator“ und „Real Time Responder – Active Responder“ verfügbar sind.<br>• Vergewissern Sie sich, dass die **Richtlinienoption Standard (Windows)** unter Konfiguration > Antwortrichtlinien in der CrowdStrike Falcon-UI aktiviert ist.<br>• Stellen Sie sicher, dass **Echtzeitantwort** und **benutzerdefinierte Skripts** unter Echtzeitfunktionalität in der CrowdStrike Falcon-UI aktiviert sind. |
| Generieren von API-Clients und -Schlüsseln in der CrowdStrike Falcon-Plattform. | Erstellen Sie die CrowdStrike-API-Clients oder -Schlüssel in der CrowdStrike Falcon-Plattform, die in der Now Platform -Integrationskonfiguration verwendet werden sollen. |

### Erstellen Sie einen CrowdStrike-API-Client, und generieren Sie Schlüssel

Erstellen Sie den CrowdStrike-API-Client und generieren Sie die Client-ID und den Schlüssel, die Sie zum Konfigurieren der CrowdStrike Falcon Insight -Integration verwenden.

**Vorbereitungen**
Erforderliche Rolle: CrowdStrike Falcon-Administrator



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren Sie auf der CrowdStrike Falcon-Plattform zu **API Clients und Schlüssel**.
2. Klicken Sie in der Tabelle „OAuth2-API-Clients“ auf **Neuen API-Client**hinzufügen.
3. Geben Sie die folgenden Details ein, um Ihren API-Client zu definieren:

| Feld | Beschreibung |
|---|---|
| Client-Name | Geben Sie den Client-Namen ein. Dies ist ein Pflichtfeld. |
| Beschreibung | Geben Sie die Beschreibung für den Client-Namen ein. |
| API-Umfänge | Das Definieren der Bereiche ist erforderlich.<br>**Wichtig:**<br>Stellen Sie sicher, dass Sie das API-Konto aktivieren, und stellen Sie sicher, dass die folgenden Bereiche für das API-Konto aktiviert sind:<br>○ Aktivieren Sie Lese- und Schreibbereiche für die Hosts-API<br>○ Aktivieren Sie den Lesebereich für die Indikatoren-API |

4. Klicken Sie auf **Hinzufügen**, um den API-Client zu speichern und die Client-ID und den geheimen Schlüssel zu generieren.

## CrowdStrike Falcon Insight installieren und konfigurieren

Installieren und konfigurieren Sie die Anwendung CrowdStrike Falcon Insight für Security Operations aus dem ServiceNow Store in Ihrer Instanz Now Platform.

### Vorbereitungen

Erforderliche Rolle: admin

**Hinweis:**
Sie können eine Fähigkeit nur einem Profil zuordnen. Sie können eine Fähigkeit nicht mehreren Profilen zuordnen. Wenn Sie CrowdStrike-Server konfigurieren, können Sie eine CrowdStrike-Fähigkeit nicht mit mehreren Profilen wiederverwenden, die den CrowdStrike-Server gemeinsam nutzen. Ihre Profile können dieselbe CrowdStrike-Fähigkeit haben, jedes Profil sollte seinen eigenen CrowdStrike-Server verwenden.

### Prozedur

1. Laden Sie CrowdStrike Falcon Insight für die Integration von Security Operations aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Integrationskachel CrowdStrike Falcon Insight für Security Operations, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder im Formular aus, um die Konfiguration abzuschließen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CrowdStrike Falcon Insight-Konfiguration**

| Feld | Beschreibung |
|---|---|
| Name | Name der Integration, z. B. `demo-1`. |
| CrowdStrike Falcon Insight-API-URL | Basis-URL, die die CrowdStrike-API hostet. Geben Sie die URL mit dem HTTPS-Protokoll ein. Beispiel: https://api.rowdstrike.com. |
| Client-ID | Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils im Portal CrowdStrike Falcon Insight erhalten. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel, den Sie im Abschnitt „Einstellungen“ Ihres Kontoprofils im Portal CrowdStrike Falcon Insight erhalten. |

5. Klicken Sie auf **Absenden**.

## Ergebnisse

Nachdem die Integration erfolgreich validiert und übermittelt wurde, wird sie auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können das Modul CrowdStrike Falcon Insight im Anwendungsnavigator anzeigen.

### Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für die Integration von CrowdStrike Falcon Insight für Security Operations, die Anforderungen zum Isolieren von Hostcomputern, zum Wiederherstellen im Netzwerk und zum Initiieren von Sichtungssuchen genehmigen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Sie können die Genehmigungsberechtigung nicht einer Gruppe neu zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

**Hinweis:**
Die Genehmigungsoption in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.
2. Klicken Sie in der Gruppenliste auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsgruppe“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppe, die angezeigt wird, wenn Sie eine Genehmigungsanforderung übermitteln. |
| Gruppen-E-Mail | Gruppen-E-Mail-Verteilerliste oder E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers |
| Manager | Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen. |
| Übergeordnet | Name der übergeordneten Gruppe, falls einer übergeordneten Gruppe zugeordnet. |
| Typ | Kategorien von Gruppen. |
| Lieferanten | Rolle vendor_manager, die Sie Benutzern im Lieferantenverwaltungsprozess Ihrer Organisation zuweisen. |
| Beschreibung | Zusätzliche Informationen zur Gruppe. |

4. Klicken Sie auf **Absenden**.
   Die neue Gruppe wird in der Gruppenliste angezeigt.

   Diese Gruppe ist für die Verarbeitung von Anforderungen verfügbar, wenn Sie während der Konfiguration dieses Profils die Option **Genehmigung** erforderlich aktivieren.

   Um von Benutzern mit der Rolle „sn_si.analyst“ übermittelte Anforderungen zu überwachen und zu verarbeiten, navigiert jedes Mitglied der Genehmigungsgruppe zur Registerkarte **Meine Genehmigungen** in Now Platform.

### Nächste Maßnahme

Der nächste Schritt besteht in der Installation und Konfiguration der Anwendung CrowdStrike Falcon Insight aus dem ServiceNow Store.

#### Erstellen Sie ein Fähigkeitsprofil für die CrowdStrike Falcon Insight -Integration

Erstellen Sie ein Profil, und wählen Sie die Fähigkeiten CrowdStrike Falcon Insight aus, die das Profil ausführen soll.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Überlegen Sie, warum Sie ein Profil erstellen möchten, bevor Sie CrowdStrike Falcon Insight -Fähigkeiten hinzufügen. In der folgenden Tabelle sind die Fähigkeiten aufgelistet, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll.

Sie können ein einzelnes Profil erstellen, das Systemdetails abfragt, angemeldete Benutzer auflistet, laufende Services abruft, laufende Prozesse abruft, Netzwerkstatistiken abruft, den Host isoliert und den isolierten Host entfernt. Alternativ können Sie mehrere Profile mit jeweils einer eigenen Fähigkeit erstellen.

**Hinweis:**
Die Fähigkeiten „Host isolieren“, „Isolierung entfernen“ und „Datei abrufen“ können beim Erstellen eines Profils nicht mit anderen Fähigkeiten zusammengeführt werden.

**Profiltypen und erforderliche CrowdStrike Falcon Insight-Fähigkeiten**

| Profilzweck | CrowdStrike-Fähigkeiten |
|---|---|
| Erfasst Hostdetails und angemeldete Benutzer | • **Hostdetails abrufen**<br>• **Angemeldete Anwender abrufen** |
| Rufen Sie die Netzwerkstatistiken, Prozesse und Services ab, die für einen Host ausgeführt werden | • **Netzwerkstatistiken abrufen**<br>• **Laufende Prozesse abrufen**<br>• **Laufende Services abrufen** |
| Isolieren Sie einen Host | **Host isolieren** |
| Entfernen Sie die Isolierung für einen Host | **Isolation entfernen** |
| Ruft eine Datei von einem Host-Endpunkt ab | **Datei abrufen** |

### Prozedur
1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike-Fähigkeitenprofile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

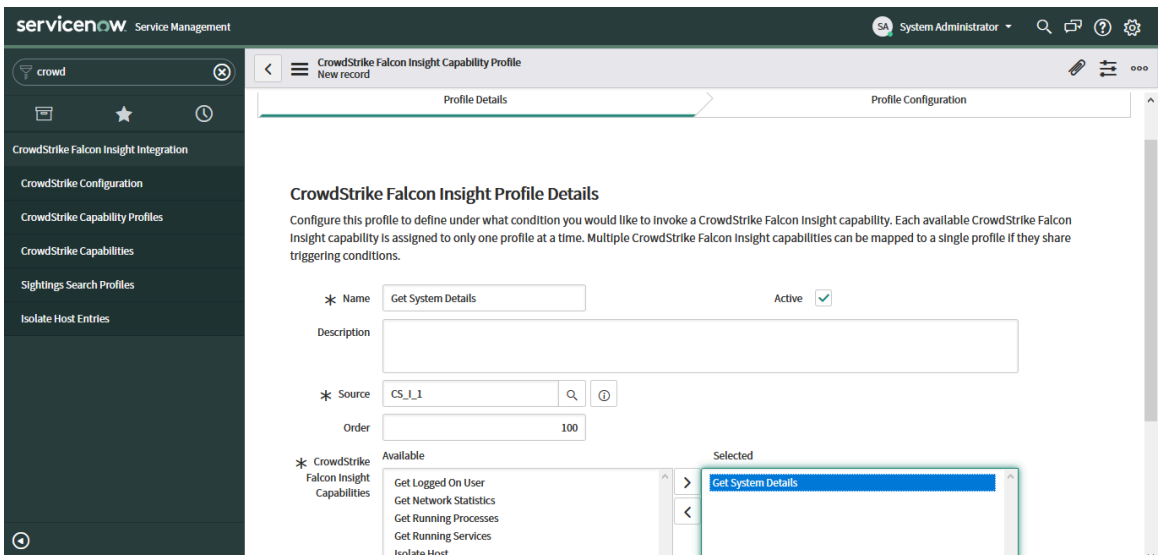
| Feld | Beschreibung |
|---|---|
| Name | Name für das neue Fähigkeitsprofil.<br><br>Dieser Name hilft Ihnen, den Profiltyp zu identifizieren, und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist. |
| Aktiv | Gibt an, ob das Profil aktiv ist oder nicht. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben. |
| Beschreibung | Eindeutige Beschreibung für das Fähigkeitsprofil. |
| Quelle | Name des Servers. Sie können zuvor konfigurierte Server nur aus der Liste anzeigen. |
| Reihenfolge | Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen.<br><br>Der Flow mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300, 400.<br><br>Standard: 100 |
| CrowdStrike Falcon Insight-Fähigkeiten | Fähigkeiten des CrowdStrike Falcon Insight-Profils.<br><br>Wählen Sie die Fähigkeiten, die Sie für dieses Profil benötigen, aus der Spalte **Verfügbar** in der Spalte **Ausgewählt**aus. |

Das folgende Beispiel zeigt ein vollständiges Formular für ein Profil mit der Fähigkeit Systemdetails abrufen.




4. Klicken Sie auf **Next (Weiter)**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Jetzt können SieIhr Profil konfigurieren. Stellen Sie sicher, dass Sie die Konzepte zum Konfigurieren von Profilen und Auslöserbedingungen überprüft haben, bevor Sie das Profil konfigurieren.

## Konfigurieren Sie Profile und Security Incidents für die CrowdStrike Falcon Insight -Integration

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die automatisch die Fähigkeiten CrowdStrike Falcon Insight auslösen, die Sie für das Profil ausgewählt haben. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld können Sie Filterbedingungen festlegen, sodass nur die Security Incidents, die sich auf Ihr auslösendes Event beziehen, das Profil automatisch auslösen.

**Hinweis:**
Navigieren Sie erst zur Seite „Profilkonfiguration“, nachdem Sie die Profildetails eingegeben haben. Weitere Informationen finden Sie unter Fähigkeitsprofile für die CrowdStrike Falcon Insight-Integration erstellen.

### Prozedur

1. Überprüfen und konfigurieren Sie auf der Seite „Profilkonfiguration“ die folgenden Abschnitte:

   **Incident-Kriterien definieren (Automatisierung)**

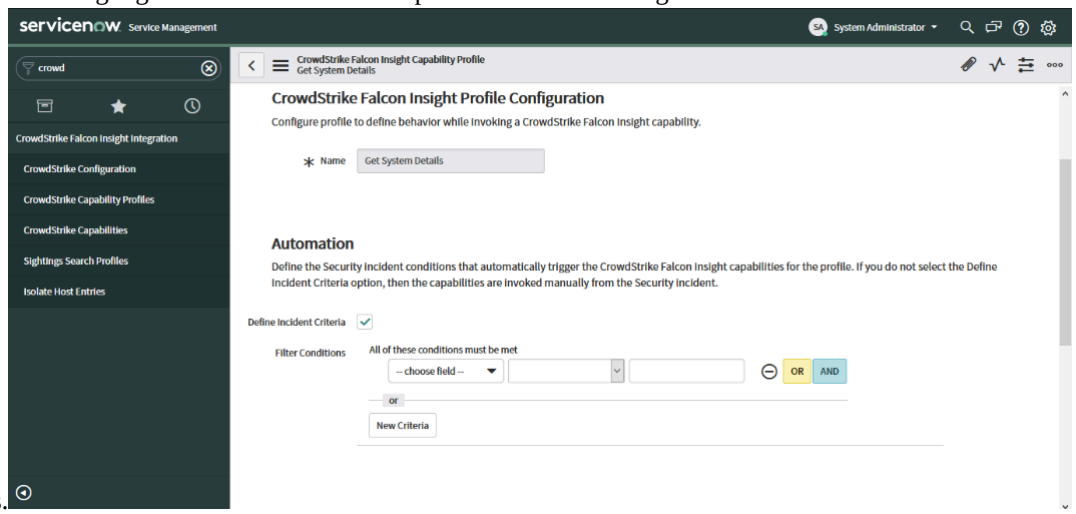
   Definieren Sie die Bedingungen für Security Incidents, die automatisch die CrowdStrike Falcon Insight -Fähigkeiten für das Profil auslösen. Wenn Sie die Option **Incident-Kriterien definieren** nicht auswählen, werden die Fähigkeiten manuell über den Security Incident aufgerufen.



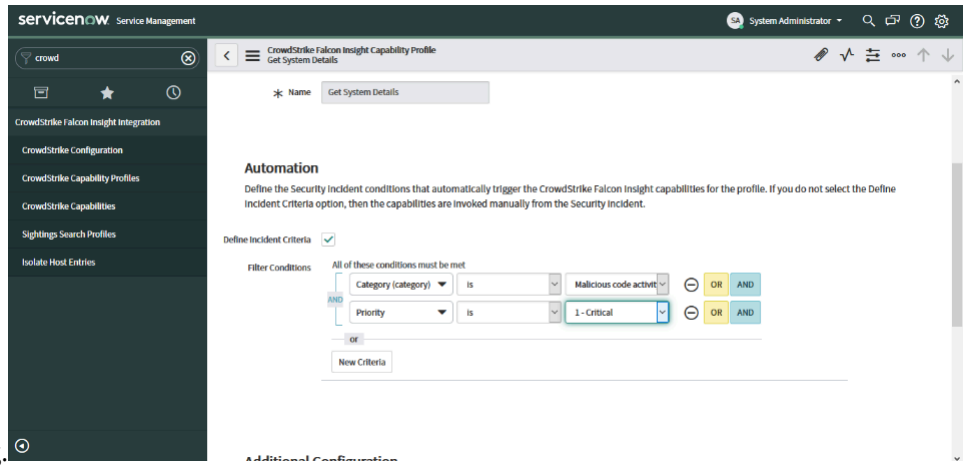
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wählen Sie die Option **Incident-Kriterien definieren aus**.

**b.** Um die Bedingungen zu definieren, wählen Sie im Abschnitt „Filterbedingungen“ ein Feld und die entsprechende Anforderung aus.




**c.** Geben Sie im Feld **Neue Kriterien** die neuen Kriterien ein, und definieren Sie dann die **ODER-** oder **UND-**Bedingung.



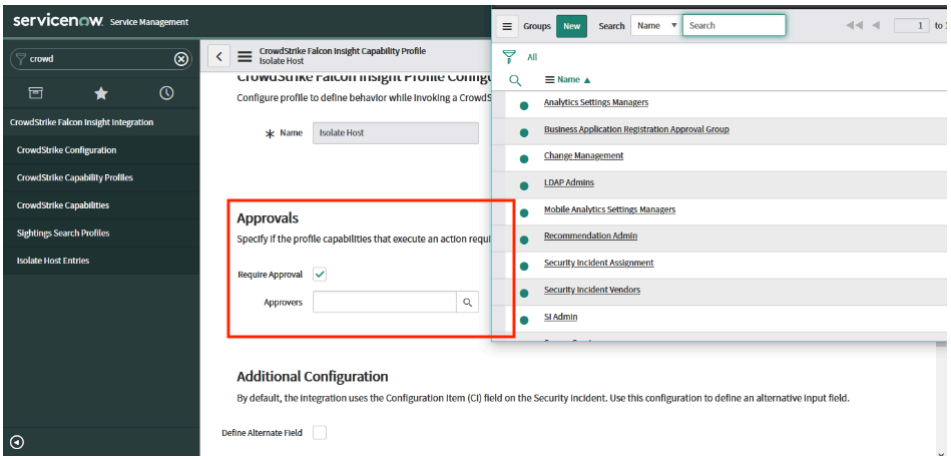

### Genehmigungen

Um bei Verwendung der CrowdStrike Falcon Insight-Fähigkeiten eine zusätzliche Steuerungsebene bereitzustellen, wählen Sie die Option **Genehmigung** erforderlich aus. Die Genehmigungsoption in der Profilkonfiguration wird nur für die Funktionen Host isolieren und Hostisolierung entfernen angezeigt.

**Hinweis:**
Die Genehmigungsberechtigung wird dem Benutzer mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe neu zuweisen. Weitere Informationen finden Sie unter Genehmigungsgruppen einrichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Zusätzliche Konfiguration

Wählen Sie ein alternatives Feld im Security Incident aus, um übereinstimmende CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets finden. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident.

**a.** Wählen Sie die Option **Alternatives Feld definieren** aus.

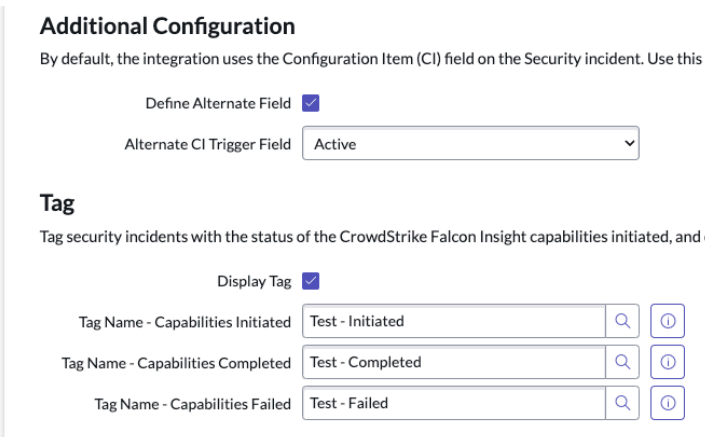
**b.** Wählen Sie im **Feld „Alternatives CI-Auslöserfeld“** ein Eingabefeld aus.

**Hinweis:**
Weitere Informationen finden Sie unter Funktionsweise von Auslöserbedingungen mit einem Konfigurationselement für ein Profil.

### Tags

Um Security Incidents mit den Tags CrowdStrike Falcon Insight Fähigkeiten – Initiiert, Fähigkeiten – Abgeschlossen und Fähigkeiten – Fehlgeschlagen zu kennzeichnen, wählen Sie die Option **Tags anzeigen aus**. Standardmäßig ist diese Option für alle Profile deaktiviert.

**Hinweis:**
Diese Tags werden mit dem Basissystem bereitgestellt. Sie können bei Bedarf eigene Tags erstellen.




**2.** Klicken Sie auf **Erledigt**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Funktionsweise von Auslöserbedingungen mit einem Konfigurationselement für ein Profil

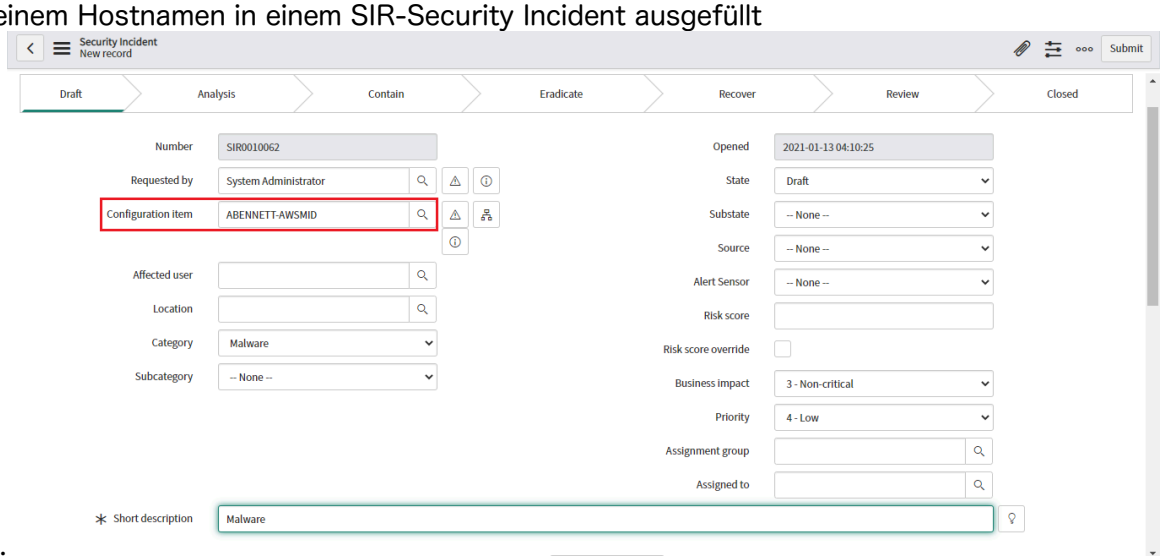
Sie können die Profileinstellungen so konfigurieren, dass ein Profil nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind, oder Sie können ein Profil einrichten, um nach bestimmten Feldwerten für einen Security Incident zu suchen.

Nachdem Sie ein Profil erstellt und die CrowdStrike Falcon Insight -Fähigkeiten ausgewählt haben, für die das Profil ausgeführt werden soll, können Sie Auslöserbedingungen festlegen, sodass Ihr Profil automatisch ausgeführt wird, wenn die Standardfeldwerte mit dem Security Incident Now Platform übereinstimmen.

Standardmäßig verwendet die Integration das Feld **Configuration Item** (CI) für einen Security Incident. Dieses Feld wird verwendet, um Ihre Asset-IDs mit den Informationen abzugleichen, die in der Datenbank Now Platform gespeichert sind. Wenn ein SIR-Security Incident durch ein Sicherheitsereignis erstellt wird und ein Profil aktiviert ist, werden Ihre Assets nach einem übereinstimmenden Wert für den Hostnamen oder eine IP-Adresse gescannt.

Wenn in der Datenbank ein übereinstimmender Wert gefunden wird, werden diese Daten in der Konsole CrowdStrike Falcon Insight gesammelt und in Ihre Instanz Now Platform abgerufen, wo sie in den zugehörigen Listen eines Security Incident angezeigt werden.

Das folgende Beispiel zeigt ein Konfigurationselement-Feld, das mit einem Hostnamen in einem SIR-Security Incident ausgefüllt wird.



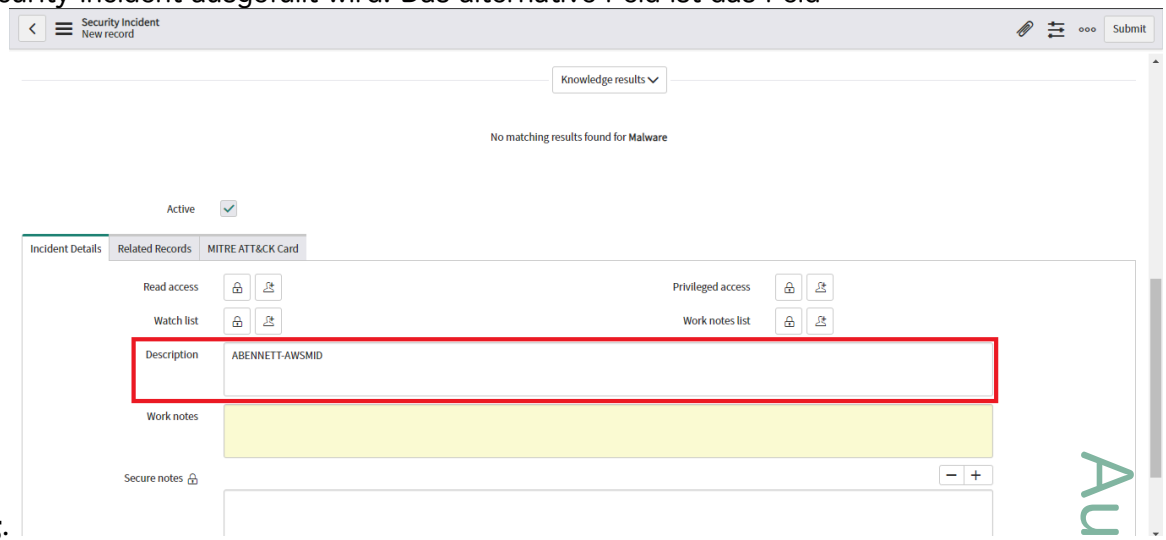

Wenn das Feld **Konfigurationselement** (CI) nicht mit einem Hostnamen oder einer IP-Adresse gefüllt ist, die der Datenbank entspricht, können Sie ein anderes Feld im Security Incident auswählen, um übereinstimmende CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets finden.

Wenn Sie das Profil-Setup konfigurieren, können Sie ein alternatives **CI-Auslöserfeld** für die Endpunktidentifizierung auswählen, um sicherzustellen, dass die CI-Daten aus der Suche CrowdStrike Falcon Insight für den zugeordneten Security Incident ausgefüllt werden. Sie können ein beliebiges Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich benutzerdefinierter Felder, die Sie erstellen. Wenn das CI-Feld beim Erstellen des zugeordneten Security Incident nicht ausgefüllt wird, wählen Sie das alternative CI-Feld aus, um sicherzustellen, dass Ihre Profile ausgelöst werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt ein alternatives Feld, das mit einem Hostnamen in einem SIR-Security Incident ausgefüllt wird. Das alternative Feld ist das Feld **Beschreibung**.




### Überprüfen Sie die CrowdStrike Falcon Insight Profilauslöserbedingungen

Testen Sie das Profil, und vergewissern Sie sich, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

### Vorbereitungen

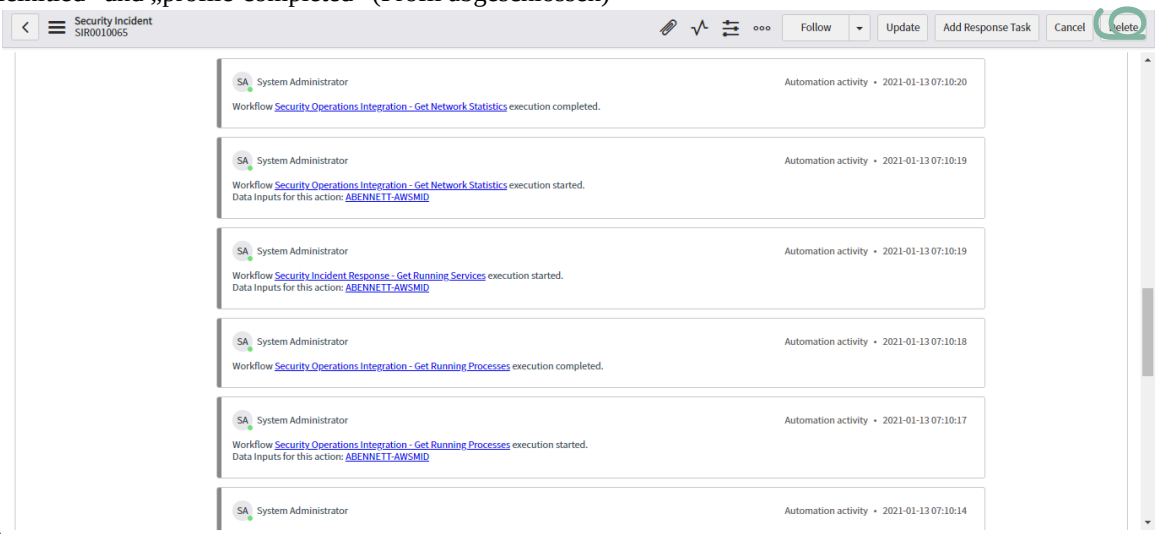
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie das Profil, das auf den von Ihnen angegebenen konfigurierten Auslösebedingungen basiert, damit Sie die Abfrageergebnisse in den Now Platform Security Incidents anzeigen können.

### Prozedur

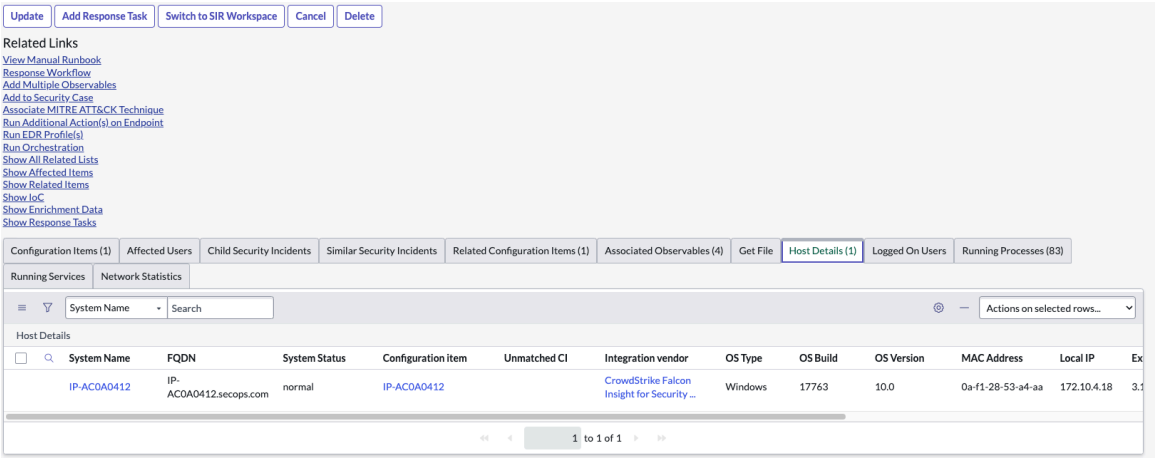
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie **Neu** aus, um einen Security Incident zu erstellen.
3. Um einen Security Incident zu erstellen, geben Sie die erforderlichen Informationen ein und klicken auf **Speichern**.
4. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“, um die Tags „profileinitied“ und „profile-completed“ (Profil abgeschlossen) anzuzeigen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Überprüfen Sie die Details in den zugehörigen Listen CrowdStrike Falcon Insight Details, z. B. Datei abrufen, Hostdetails, Angemeldete Benutzer, Laufende Prozesse, Laufende Services, Netzwerkstatistiken usw.




## Lösen Sie ein CrowdStrike Falcon Insight -Profil manuell aus einem Security Incident aus

Lösen Sie ein Profil manuell aus, nachdem Sie einen Security Incident überprüft haben.

### Vorbereitungen

Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie das Profil basierend auf den konfigurierten Auslöserbedingungen aktiviert haben, können Sie die Abfrageergebnisse in den Now Platform Security Incidents anzeigen. Mit CrowdStrike Falcon Insight können Sie auch einzelne Fähigkeiten für Konfigurationselemente (CIs) ausführen, ohne ein Profil zu verwenden.

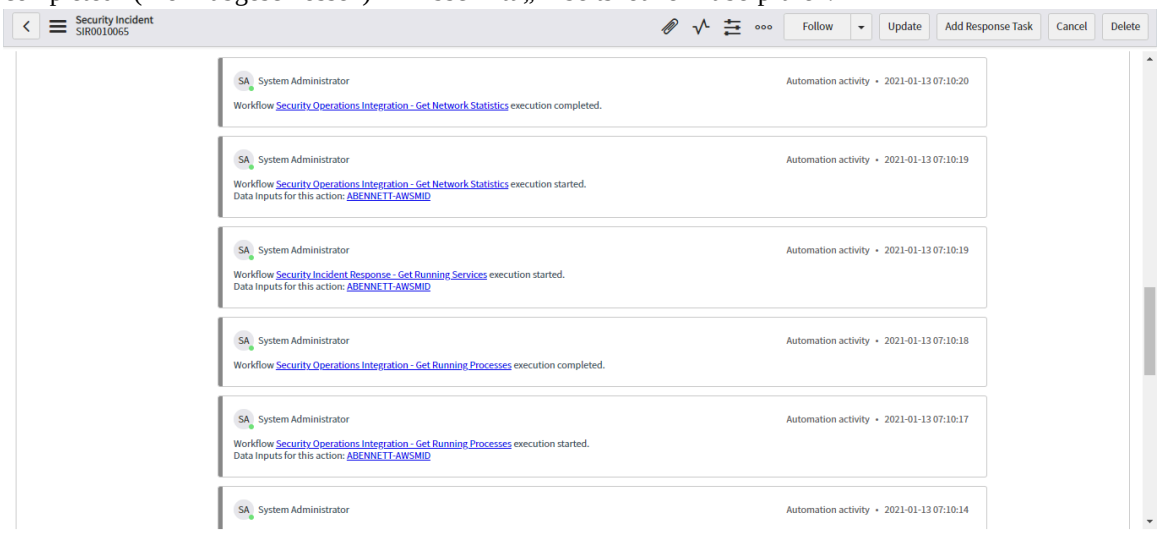
### Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen CrowdStrike Falcon Insight.
3. Wählen Sie im Abschnitt „Zugehörige Listen“ die **Option EDR-Profil(e) ausführen**aus.
4. Suchen Sie ein Profil und wählen Sie es aus der Liste der verfügbaren Profile aus.
5. Wählen Sie **Zugehöriges CI einschließen** aus, um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.
   Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ und die Tags „profileinitied“ und „profile-

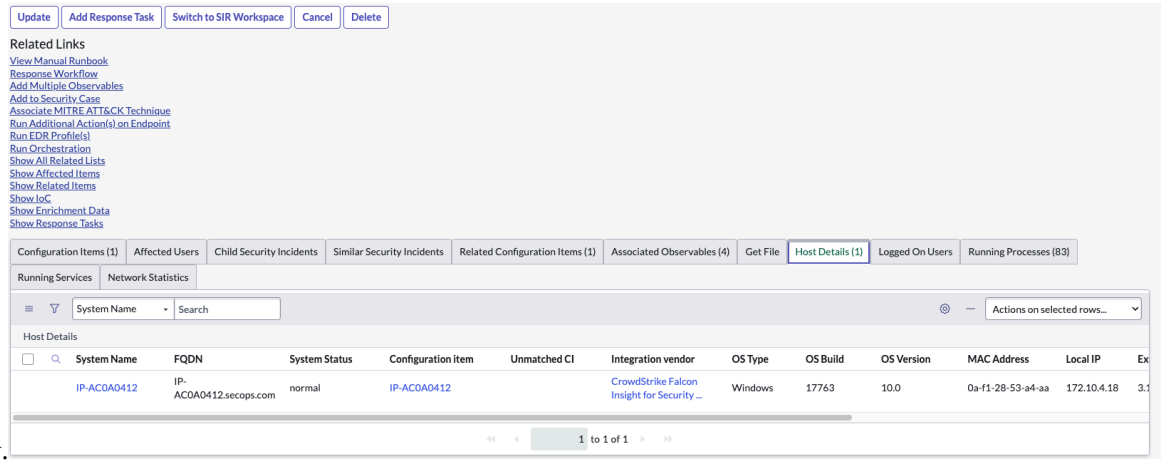


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

completed“ (Profil abgeschlossen) im Abschnitt „Arbeitsnotizen“ überprüfen.




7. Die Ergebnisse werden in Form von zugehörigen Listen angezeigt, z. B. Datei abrufen, Hostdetails, Angemeldete Benutzer, Laufende Prozesse, Laufende Services, Netzwerkstatistiken usw.




8. Führen Sie die folgenden Schritte aus, um einzelne Fähigkeiten für ein CI auszuführen:

   a. Wählen Sie in der zugehörigen Liste Konfigurationselemente das erforderliche CI aus.

   b. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie die erforderliche Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Suchen Sie mithilfe der Suchoption nach der erforderlichen Fähigkeitsimplementierung für das CI, und wählen **Sie CrowdStrike Falcon Insight Isolate Host**(CrowdStrike Falcon Insight-Host isolieren) aus.

   d. Klicken Sie auf **Host isolieren**, um sie für das ausgewählte CI auszuführen.

## Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche

Verwenden Sie Sichtungssuchen für CrowdStrike Falcon Insight, um infizierte Computer im Netzwerk Ihrer Organisation zu finden und Security Incident Response-Fälle zu bearbeiten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in CrowdStrike Falcon Insight durch, um die Verbreitung einer Bedrohung im Laufe der Zeit zu bestimmen.

### Prozedur

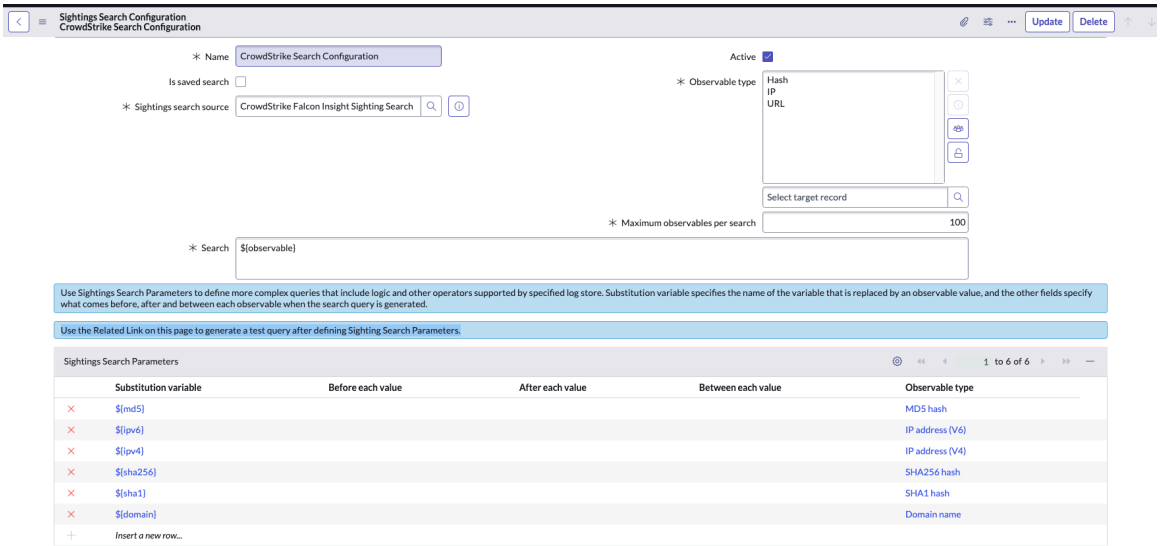
1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **Sichtungssuchprofile**.
2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie dieses Profil, um zu bestimmen, auf welchen Servern nach einer bestimmten CrowdStrike Falcon Insight-Suchfunktion gesucht werden soll.
4. Füllen Sie im Formular die folgenden Felder aus:

| Feld | Beschreibung |
|---|---|
| Name | Name für das Sichtungssuchprofil. |
| Ist gespeicherte Suche | Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt. |
| Sichtungssuchquelle | Die Quelle für die Sichtungssuche. Wählen **Sie CrowdStrike Falcon Insight-Sichtungssuche** als Quelle aus. |
| Aktiv | Option, um anzugeben, ob der Zusatz aktiv ist oder nicht. |
| Erkennbarer Typ | Die CrowdStrike Falcon Insight-Integration unterstützt die folgenden erkennbaren Typen:<br>○ Hash<br>○ IP<br>○ URL<br>Die Sichtungssuche wird für die folgenden erkennbaren Elemente unterstützt:<br>○ Domänenname<br>○ IP-Adresse (V4)<br>○ IP-Adresse (V6)<br>○ MD5-Hash<br>○ SHA1-Hash<br>○ SHA256-Hash |
| Maximale erkennbare Elemente pro Suche | Maximale Anzahl von erkennbaren Elementen, die Sie in einer Suchabfrage anzeigen können. |
| Suchen | Die Standardsuchzeichenfolge ist `$(observable)`, aber Sie können Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die von der CrowdStrike Falcon Insight -Integration unterstützt werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Sichtungssuchparameter | Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden<br><br>Sie können die zugehörigen Links am Ende der Seite verwenden, um nach der Definition der Sichtungssuchparameter eine Testabfrage zu generieren. |




5. Klicken Sie auf **Absenden**.
   Die Konfiguration ist abgeschlossen, und Sie können die Sichtungssuche über den Security Incident Now Platform aufrufen.
6. Führen Sie die folgenden Schritte aus, um die Konfiguration zu überprüfen und eine Sichtungssuche auszuführen:

   a. Öffnen Sie einen Security Incident, scrollen Sie zum Ende des Security Incident und klicken Sie auf **Alle zugehörigen Listen anzeigen**.

   b. Wenn Sie ein oder mehrere Configuration Items (CI) aus den zugehörigen Listen **Laufende Prozesse** auswählen.

   **Hinweis:**
   Wenn Sie eine Sichtungssuche für ein CI aus der zugehörigen Liste „Laufende Prozesse“ ausführen, handelt es sich nur um eine Prozess-Hash-Sichtungssuche.

   c. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen **Sie CrowdStrike-Sichtungssuche ausführen aus**.

   d. Suchen Sie mithilfe der Suchoption nach dem erforderlichen Sichtungssuchprofil.

   e. Wählen Sie das erforderliche Sichtungssuchprofil aus, und klicken Sie auf **Absenden**.

   f. Wenn Sie ein oder mehrere erkennbare Elemente aus den zugehörigen Listen **Zugeordnete erkennbare** Elemente auswählen.

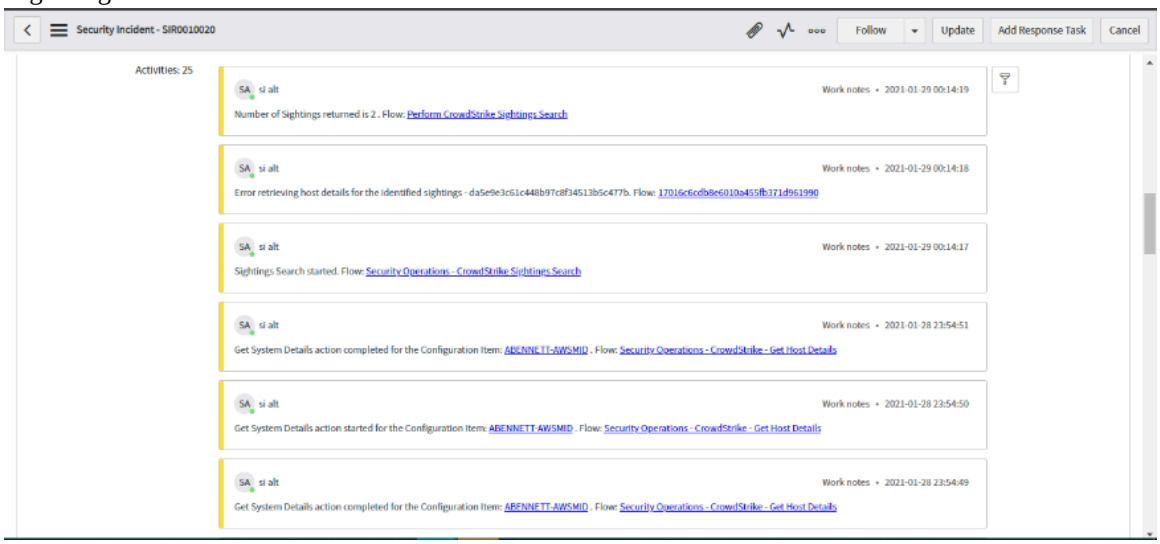
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen **Sie Sichtungssuche ausführen**aus.

h. Wählen Sie im Popup-Fenster „Zeitrahmen“ einen beliebigen zufälligen Wert aus, und klicken Sie auf **Suchen**.

i. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den Arbeitsnotizen und zugehörigen Listen.




j. Wechseln Sie zur Registerkarte **Sichtungen**, um die Sichtungsdetails anzuzeigen.

k. Klicken Sie auf das **Vorschausymbol** neben dem CI, um weitere Informationen zu CrowdStrike-Sichtungsdetails anzuzeigen.

l. Klicken Sie auf **Sichtungssuchdetails, um die Sichtungssuchdetails anzuzeigen, und klicken Sie auf die Registerkarte Sichtungssuchergebnisse, um Suchergebnisseanzuzeigen**.

## Konfigurieren und lösen Sie zusätzliche Aktionen in aus CrowdStrike Falcon Insight

Die CrowdStrike Falcon Insight -Integration unterstützt die Ausführung zusätzlicher Aktionen wie reguläre Ausdrücke (reguläre Ausdrücke). Die CrowdStrike Falcon Insight -Integration bietet 40 zusätzliche Aktionen mit dem Basissystem.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike: zusätzliche Aktionen**.
2. Klicken Sie auf **Neu**, um eine eigene zusätzliche Aktion zu erstellen, oder wählen Sie eine vorhandene Aktion aus, die im Basissystem enthalten ist.
   Erstellen wir beispielsweise eine neue zusätzliche Aktion.
3. Füllen Sie die Felder im Formular aus.



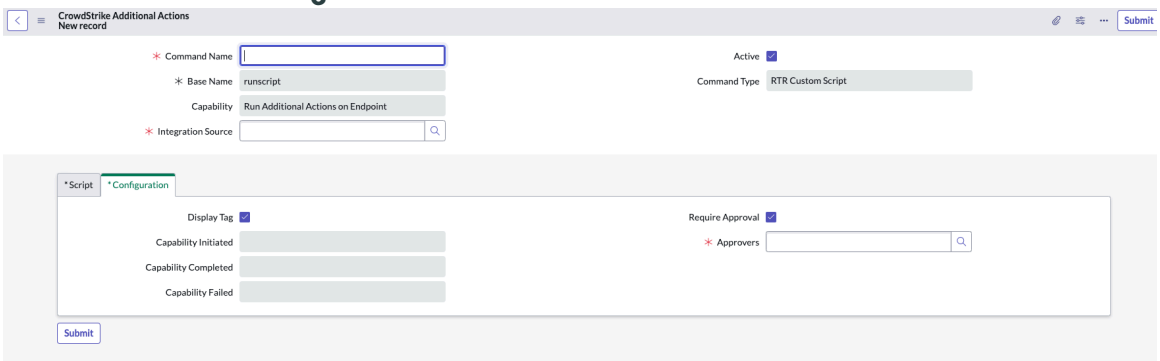
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Befehlsname | Befehlsname für die zusätzliche Aktion. Beispiel: reg set. |
| Basisname | Basisname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: reg. |
| Fähigkeit | Fähigkeitsname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Zusätzliche Aktionen für Endpunkt ausführen. |
| Integrationsquelle | Die Quelle für die zusätzliche Aktion. Beispiel: CrowdStrike Falcon Insight-Integration. |
| Aktiv | Option, um anzugeben, ob der Zusatz aktiv ist oder nicht. |
| Befehlstyp | Befehlstyp für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Benutzerdefiniertes RTR-Skript. |
| Skript | ○ **BS-Typ**: Option zur Auswahl des BS-Typs für Ihr Skript. Wählen Sie eine der folgenden Optionen aus:<br>▪ **Windows**<br>▪ **Mac OS X**<br>▪ **Linux**<br>▪ **Keine**<br>○ **Skript**: Option zur Eingabe Ihres Skripts, wenn Sie eines der folgenden Betriebssysteme ausgewählt haben, mit Ausnahme der Option Keine. |
| Konfiguration | ○ **Tag**anzeigen: Option zum Anzeigen des Tags für die Konfiguration. Sie können das Tag für die folgenden Felder auswählen:<br>▪ Fähigkeit: Initiiert. Beispiel: reg set – Initiiert.<br>▪ Fähigkeit – Abgeschlossen. Beispiel: reg set – Abgeschlossen.<br>▪ Fähigkeit – Fehlgeschlagen. Beispiel: reg set – Fehlgeschlagen.<br>○ **Genehmigung**erforderlich: Option zum Auswählen eines Genehmigers oder einer Gruppe, die die Konfiguration genehmigen muss. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CrowdStrike Falcon Insight – zusätzliche Aktionen**




4. Klicken Sie auf **Absenden**.

5. Sie können auch aus den folgenden vorhandenen zusätzlichen Aktionen auswählen.
   Das Basissystem enthält 40 zusätzliche Aktionen, mit denen Sie zusätzliche Konfigurationen durchführen können.

   **Hinweis:**
   Stellen Sie sicher, dass Sie die Liste „Zusätzliche CrowdStrike-Aktionen“ öffnen und die erforderliche zusätzliche Aktion auf **true**festlegen, andernfalls ist die zusätzliche Aktion nicht im Arbeitsbereich verfügbar.

**Liste zusätzlicher Aktionen, die mit dem Basissystem bereitgestellt werden**

CrowdStrike Additional Actions — Command Name — Search — Actions on selected rows... — New

All

| Command Name | Active | Base Name | Integration Source | Command Type | Approvers | Require Approval |
|---|---|---|---|---|---|---|
| reg set | true | reg | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| unmap | false | unmap | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| update list | false | update | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| update query | false | update | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| eventlog list | false | eventlog | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| eventlog view | false | eventlog | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| reg unload | false | reg | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| reg load | false | reg | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| reg delete | false | reg | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| update history | false | update | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| xmemdump | false | xmemdump | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| users | false | users | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| eventlog export | false | eventlog | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| filehash | false | filehash | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| eventlog backup | false | eventlog | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| memdump | false | memdump | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| run | false | run | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| restart | false | restart | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| rm | false | rm | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| zip | false | zip | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| kill | false | kill | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |
| getsid | false | getsid | CrowdStrike Falcon Insight for Security ... | RTR Standard Action | (empty) | false |

1 to 40 of 40

6. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.

7. Wählen Sie den Security Incident aus, den Sie überprüfen möchten, und führen Sie zusätzliche Aktionen für den Endpunkt aus.

   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.

   b. Durchsuchen Sie die erforderliche Fähigkeit, und wählen Sie sie aus.
   Klicken Sie beispielsweise auf die Fähigkeit **reg set**.

   c. Wählen Sie **Zugehöriges CI einschließen** aus, um die zusätzlichen Aktionen für alle zugehörigen CIs des Endpunkts auszuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Sie können den **Unterschlüssel** für die Ausführung der zusätzlichen Aktionen auf dem Endpunkt definieren.
Dieser Unterschlüssel kann ein HKLM/Software/neuer Schlüssel sein.

8. Um die zusätzlichen Aktionen für den Endpunkt zu initiieren, klicken Sie auf **Zusätzliche Aktion**ausführen.
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
10. Validieren Sie den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

### Verwenden der CrowdStrike Falcon Insight -Integration in Analyst Workspace

Verwenden Sie die Integration von CrowdStrike Falcon Insight, um die Fähigkeiten von CrowdStrike Falcon Insight im SIR-Analystenarbeitsbereich zu nutzen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Bevor Sie die CrowdStrike Falcon Insight -Integration im Security Incident Response-Arbeitsbereich verwenden, müssen Sie sie aus dem ServiceNow Store herunterladen und konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit der CrowdStrike Falcon Insight -Integration.

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können die CrowdStrike Falcon Insight -Integration verwenden, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, Profile zum Sammeln von Details zum Host zu verwenden und im Arbeitsbereich Security Incident Response bestimmte Abfragen oder Aktionen für den Endpunkt durchzuführen.

Die CrowdStrike Falcon Insight -Integration ermöglicht Analysten die Verwendung der folgenden CrowdStrike Falcon Insight -Fähigkeiten im Analyst Workspace Security Incident Response :

- **Hostdetails abrufen**
- **Angemeldete Anwender abrufen**
- **Netzwerkstatistiken abrufen**
- **Laufende Prozesse abrufen**
- **Laufende Services abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Datei abrufen**

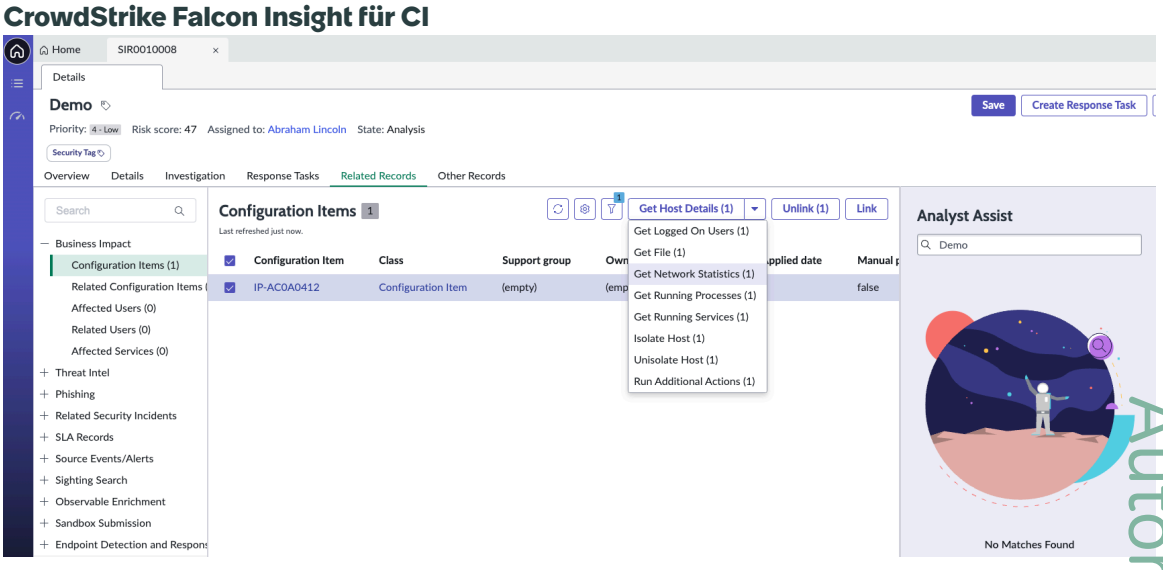
#### Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich den erforderlichen Security Incident, und wählen Sie die Registerkarte **Zugehörige Datensätze** aus.
2. Sie können die CrowdStrike Falcon Insight-Fähigkeiten in der zugehörigen Liste „Geschäftsauswirkung“ zur Analyse verwenden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wählen Sie ein **Konfigurationselement**aus, und wählen Sie eine Fähigkeit aus der Dropdown-Liste aus.




**b.** Wählen Sie die **CrowdStrike Falcon Insight-** Implementierung aus, und klicken Sie auf **Absenden**. Die Fähigkeit „Netzwerkstatistiken abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

**3.** Sie können die CrowdStrike Falcon Insight-Fähigkeiten in der zugehörigen Liste **Endpoint Detection and Response (EDR)** zur Analyse verwenden.

**a.** Wählen Sie in der zugehörigen Liste Endpoint Detection and Response (EDR) einen EDR aus der Liste aus.

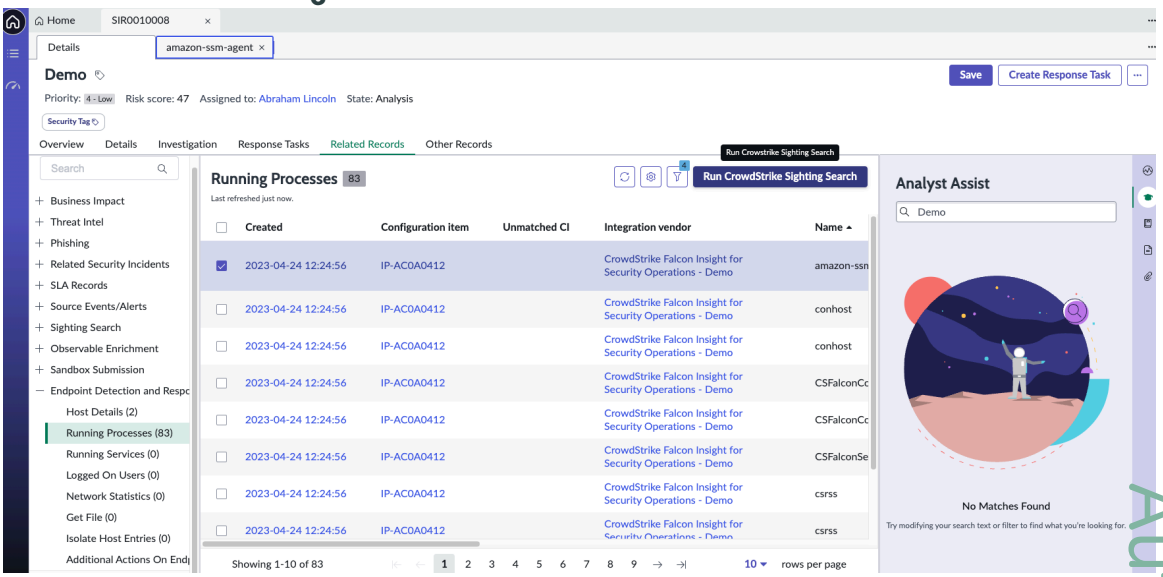
**b.** Klicken Sie auf einen bestimmten laufenden Prozess, um die Details des laufenden CrowdStrike Falcon Insight-Prozesses anzuzeigen.

**c.** Um eine CrowdStrike Falcon-Sichtungssuche für einen bestimmten laufenden Prozess auszuführen, wählen Sie den laufenden Prozess aus und klicken Sie auf **CrowdStrike-Sichtung ausführen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CrowdStrike Falcon Insight für EDR**



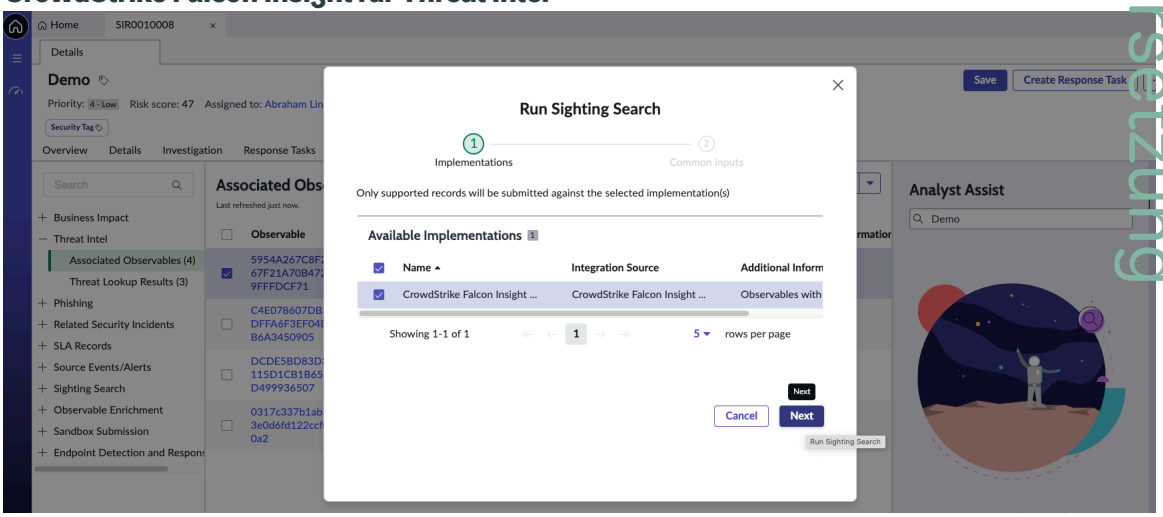

**d.** Wählen Sie die **CrowdStrike Falcon Insight-** Implementierung aus, und klicken Sie auf **Suche**ausführen.
Anschließend wird eine Hash-Sichtungssuche für den ausgewählten laufenden Prozess ausgeführt. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

**4.** Sie können die CrowdStrike Falcon Insight-Fähigkeiten für **Threat Intel** zur Analyse verwenden.

**a.** Wählen Sie in der Gruppe „Bedrohungsinformationen“ ein erkennbares Element aus, und wählen Sie eine CrowdStrike Falcon Insight**-Fähigkeit**aus der Dropdown-Liste aus.

**b.** Wählen Sie die **CrowdStrike Falcon Insight-** Implementierung aus, und klicken Sie auf **Weiter**.

**CrowdStrike Falcon Insight für Threat Intel**




**c.** Wählen Sie im Popup-Fenster Datum/Uhrzeit auswählen einen zufälligen Wert aus, und klicken Sie auf **Absenden**.
Anschließend wird eine Sichtungssuche für das ausgewählte erkennbare Element ausgeführt. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Integration von CrowdStrike Falcon X Sandbox für Security Operations

Mit der Integration von CrowdStrike Falcon X Sandbox für Security Operations können Sie Dateien und URLs als Teil des Security Incident Response-Prozesses an CrowdStrike Falcon X Sandbox senden, um eine detaillierte Malware- und Bedrohungsanalyse durchzuführen.

Die CrowdStrike Falcon X Sandbox -Integration bietet Ihnen eine isolierte virtuelle On-Demand-Umgebung, in der Sie die Malware-Analyse durchführen und über die Integration Ergebnisse für den ServiceNow Security Incident bereitstellen können.

Wenn Sie Ihre Malware-Incidents übermitteln, werden sie als Teil des Security Incident-Datensatzes gespeichert. Sie können diese Datensätze füroder weitere Incident-Lösungen verwenden und die Übermittlung von Dateien und URLs automatisieren.

Die Integration unterstützt die Automatisierung von Phishing- und Malware-Antwort-Playbooks , wodurch Ihr Center-Personal Security Operations produktiver und effizienter auf Security Incidents reagieren kann.

### Hauptvorteile

Mitseiner Integration, können Sie die folgendenSchritte ausführen :

- Automatisieren Sie die Übermittlung von Dateien und URLs von Benutzer–, der Phishing (URP), E-Mail-Nachrichten, Anhänge und andere Security Incidents gemeldet hat.
- Übermitteln Sie zuvor analysierte Dateien und URLs manuell oder übermitteln Sie sie erneut für eine aktualisierte Analyse.
- Erstellen Sie mehrere Übermittlungskonfigurationen, die automatisch CrowdStrike Falcon X Sandbox Übermittlungsparameter wie Betriebssystem, Scan-Typ und Laufzeitoptionen anwenden.
- Analysieren Sie die Malware- - und Bedrohungsergebnisse in einem HTML-formatierten Bericht innerhalb des Incident SIR. Sie können tHR-Suchergebnisse und den Indikatorverlauf für Dateien und URLs anzeigen, die mehrmals analysiert wurden.
- Kennzeichnen Sie ServiceNow Incidents mit dem Verarbeitungsstatus der Übermittlung sowie den Ergebnissen der Bedrohungssuche.

### Siehe auch

| Dokumentbezeichner | Dokumententitel |
|---|---|
| CrowdStrike Falcon X Sandbox | Häufig gestellte Fragen zu CrowdStrike Falcon Sandbox |
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |

#### Beginnen Sie mit der Integration von CrowdStrike Falcon X Sandbox .

Aktivieren und richten Sie CrowdStrike Falcon X Sandbox als Schnittstelle mit Ihrer Instanz von [ ServiceNow und Ihrem Produkt von Security Incident Response ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

- Bevor Sie CrowdStrike Falcon X Sandbox für die Integration mit Security Operations verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.
- Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose CrowdStrike Falcon X Sandbox -Integration abgeschlossen haben.

Erforderliche Rolle: admin, sn_si.admin

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben. | Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Administrator (admin) installiert die andbox-Integration saus dem ServiceNow-App-Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Der sn_si.admin erstellt und bearbeitet die Konfigurationund die globalen Einstellungen . Anschließend weist die Rolle „Security Incident Analyst“ (sn_si.analyst) zu.<br>• Der Security Incident Analyst (sn_si.analyst) reagiert auf Security Incidents, , z. B., übermittelt Dateien und URLs an die sund analysiert die Übermittlungsergebnisse. |
| Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren. | Diese Integration wird in den Releases Paris und Orlando unterstützt.<br><br>Stellen Sie sicher, dass diese abhängigen Plugins installiert sind. Diese Plugins ermöglichen die Ausführung von IntegrationHub Aktionen und Flows:<br><br>• ServiceNow IntegrationHub-Aktionsschritt – REST (com.glide.hub.action_step.rest)<br>• ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime)<br><br>**Hinweis:**<br>Wenn Sie ein Plugin nicht finden können, müssen Sie es möglicherweise von einem Mitarbeiter vonanfordern ServiceNow . Um ein Plugin anzufordern, befolgen Sie die in Plugin anfordern erläuterten Schritte. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
| --- | --- |
| | Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations Anwendungen installieren und aktivieren, die für die Integration erforderlich sind.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response Abhängigkeit (com.snc.si_dep)<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br>**5.** Threat Intelligence Support Common (erforderlich für die Verwendung der Sandbox-Integrationsfunktionen vonse )<br>**6.** Trusted Security Circles<br>**7.** Security Operations Setup-Assistent<br>**8.** Security Incident Response<br><br>Weitere Informationen zum Einrichten Ihrer Now Platform -Instanz für die Integration finden Sie unter Berechtigungen für ein Security Operations-Produkt oder eine Security Operations-Anwendung erhalten und ServiceNow Store-Anwendungen aktivieren. |
| Vergewissern Sie sich, dass Sie für den privaten API-Schlüssel von Falcon Sandbox lizenziert sind und oderden vollständigen API-Schlüssel CrowdStrike Falcon X Sandbox erhalten. | Diese Integration unterstützt nur die Falcon Sandbox Private Cloud.<br><br>**Hinweis:**<br>Diese Version unterstützt keine Falcon X-Integration.<br><br>CrowdStrike Falcon X Sandbox bietet einen selbstsignierten eingeschränkten API- |

Automatische Übersetzung

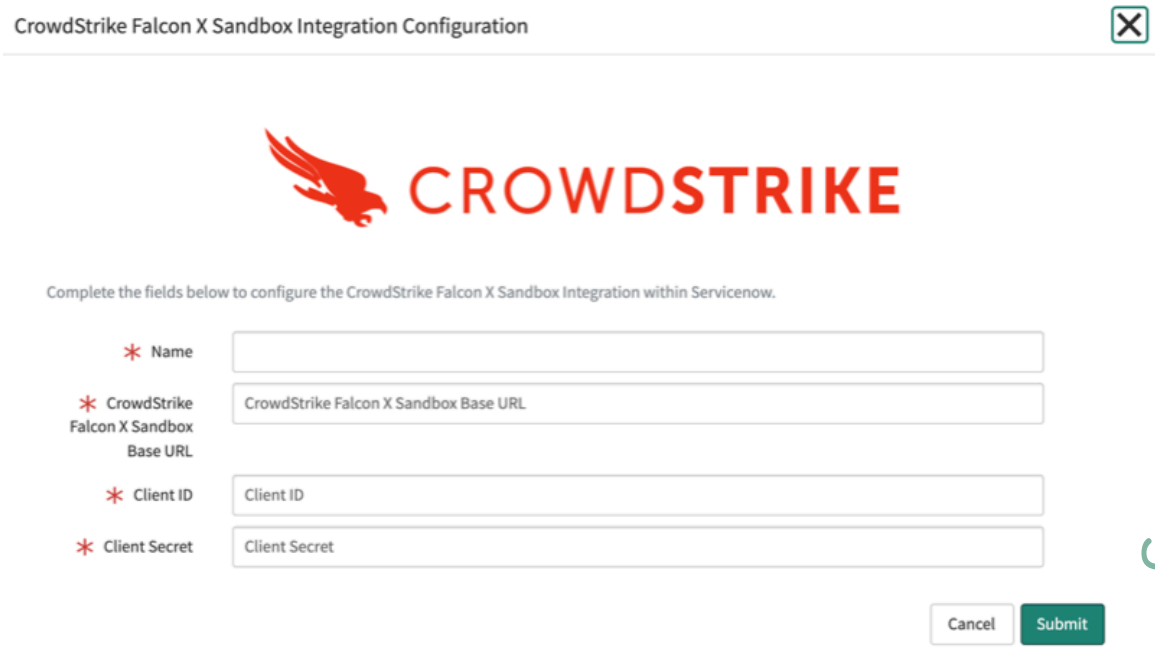
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| | Schlüssel und einen aktualisierten vollständigen API-Schlüssel. Verwenden Sie den vollständigen API-Schlüssel für diese Integration , da damit uneingeschränkten Zugriff für automatisierte Übermittlungen ermöglicht.<br><br>Weitere Informationen finden Sie in der CrowdStrike Falcon Sandbox-Knowledge Base . |

## Prozedur

1. Laden Sie die CrowdStrike Falcon Sandbox for Security Operations-Integration aus dem ServiceNow Store herunter.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrations** > **Integration Configurations**(Sicherheitsvorgänge > Integrationen > Integrationskonfigurationen).
3. Suchen Sie nach der Integrationskachel CrowdStrike Falcon X Sandbox, und klicken Sie auf **Konfigurieren**.




4. Geben Sie die folgenden Details ein, um die Konfiguration abzuschließen:

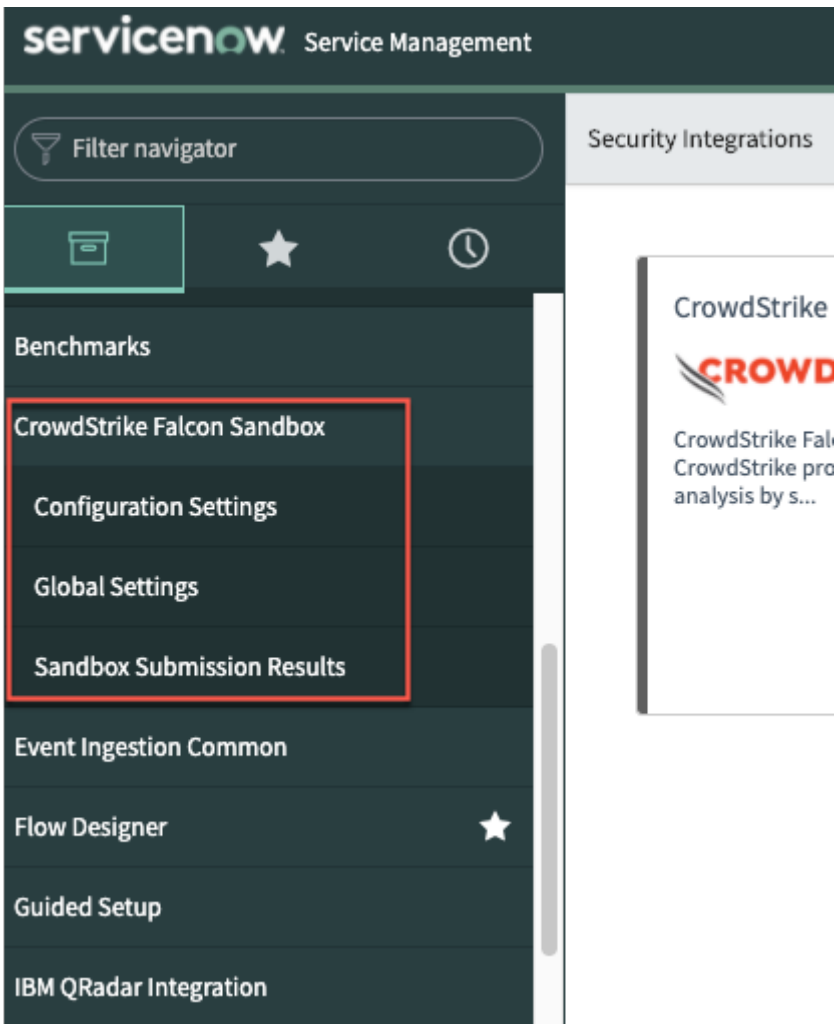
| Feld | Beschreibung |
|---|---|
| **Name** | Name dieser Integration, z. B. `demo-1`. Dies ist zwar ein eindeutiger Name zur Identifizierung der andbox-Konfiguration s, Sie können jedoch nur eine Integration pro ServiceNow-Instanz konfigurieren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| **CrowdStrike Falcon Sandbox-Basis-URL** | Sandbox-Basis-URL. Diese URL ist verfügbar , nachdem Sie die sandbox konfiguriert haben.Beispiel: `https://servicenow.falcon-sandbox.com` ist eine Basis-URL. |
| **Client-ID** | OAuth2-API-Client-ID Weitere Informationen finden Sie unter API-Clients und -Schlüssel . |
| **Geheimer Clientschlüssel** | Geheimer Schlüssel des OAuth2-API-Clients. Weitere Informationen finden Sie unter API-Clients und -Schlüssel . |

5. Klicken Sie auf **Absenden**.
   Nachdem die Sandbox erfolgreich validiert und übermittelt wurde, wird sie auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können das Sandbox-Modul jetzt im -Anwendungsnavigator anzeigen.




## Nächste Maßnahme

Nachdem Sie die Integration erfolgreich abgeschlossen haben, besteht der nächste Schritt darin, Sandbox-Übermittlungskonfigurationeneinzurichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie Sandbox-Übermittlungskonfigurationen ein

Richten Sie die Sandbox-Konfiguration ein, um die Analyseumgebung und die Laufzeitoptionen für die Übermittlungen von Security Incident-Datensätzen für die Malware-Analyse zu definieren.

## Vorbereitungen

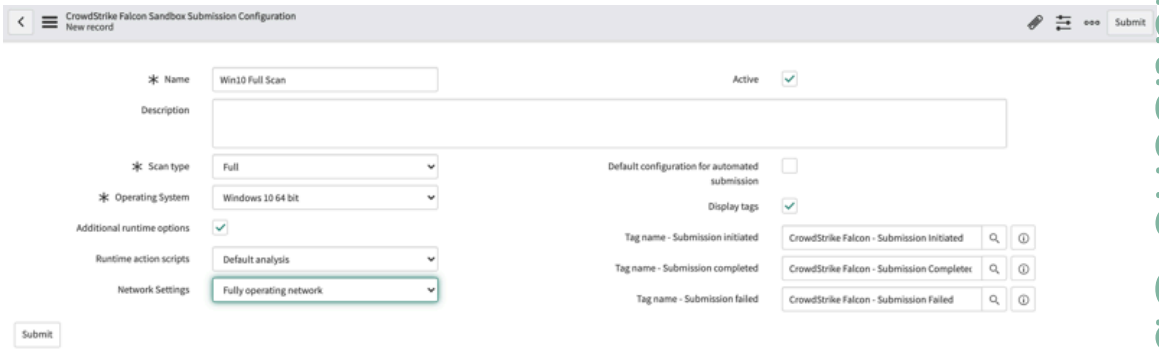
Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Dateien oder URLs mithilfe der -Integration an CrowdStrike Falcon X Sandbox senden können, müssen Sie mindestens eine Übermittlungskonfiguration konfigurieren. Die Übermittlungskonfiguration definiert das Sandbox-Betriebssystem, den Scan-Typ, die Ausführungszeitoptionen und andere Incident-Bearbeitungsmerkmale. Möglicherweise möchten Sie mehrere Konfigurationen erstellen, um die verschiedenen Optionen zu verwenden, die [] in der Umgebung CrowdStrike Falcon X Sandbox verfügbar sind.

## Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon X Sandbox** > **Konfigurationseinstellungen**.
2. Klicken Sie auf **Neu**.




3. Füllen Sie die folgenden Felder aus, um eine Konfiguration für einen vollständigen **Scan vom Typ**zu erstellen.

| Feld | Beschreibung |
|---|---|
| Name | Eindeutiger Name für die Übermittlungskonfiguration. Dieser Name wird Analysten angezeigt, wenn sie eine Datei übermitteln. Es ist wichtig sicherzustellen, dass der Name aussagekräftig und leicht von den anderen Konfigurationen zu unterscheiden ist (z. B. Win 10 Full Scan). Wenn der Name nicht eindeutig ist, wird ein Fehler angezeigt, und doppelte Konfigurationsdatensatznamen werden nicht gespeichert. |
| Überprüfungstyp | Skann als **Vollständig eingegeben**werden. Ein **Schnell** -Scan-Typ bietet eine eingeschränkte Bedrohungsanalyse. |
| Betriebssystem | EineAnalyse-VM-Umgebung, in der die sandbox die Datei oder URL in scannt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

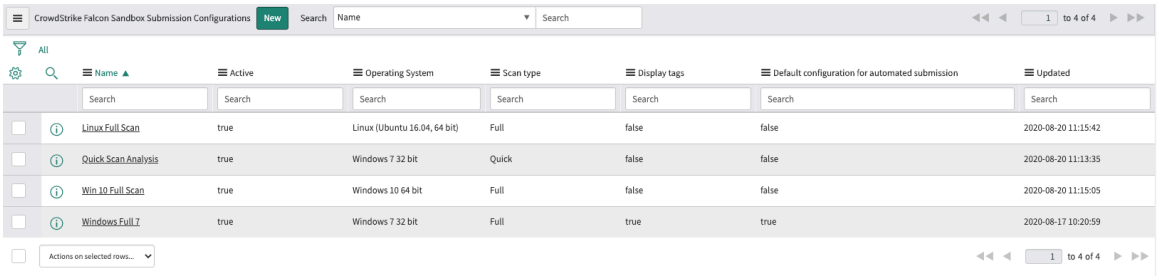
| Feld | Beschreibung |
|---|---|
| Aktiv | Option [Option , die Sie auswählen, wenn Sie Dateien oder URLs manuell übermitteln. |
| Standardkonfiguration für automatisierte Übermittlung | Option [Option , für die standardmäßig deaktiviert ist. Wenn Sie diese Option auswählen, wird diese Konfiguration für die Automatisierung von Malware-Analyseübermittlungen verfügbar gemacht.<br>**Hinweis:**<br>Sie können nur eine aktive Übermittlungskonfiguration als Standardkonfiguration für automatisierte Übermittlungen haben. |
| Tags anzeigen | Option [Option , für die standardmäßig deaktiviert ist. Wenn Sie diese Option auswählen, werden Tags angezeigt, um den Status einer Datei- oder URL-Übermittlung anzugeben. Die Verarbeitung der Analyse kann einige Minuten dauern. Die Anzeige-Tags sind Übermittlung initiiert, Übermittlung abgeschlossen, oder Übermittlung fehlgeschlagen. |
| Weitere Laufzeitoptionen | Option [Option , für die standardmäßig deaktiviert ist. Wenn Sie diese Option auswählen, sind zusätzliche Laufzeitparameter verfügbar, die von Sandbox unterstützt werden. |
| Laufzeit-Aktionsskripts | Option, mit der Sie ein-Aktionsskript verwenden können, das menschliches Verhalten von [s ] simuliert unds mit der Datei oder URL während der Analyse interagiert.<br>https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/<br>Weitere Informationen finden Sie in der Dokumentation CrowdStrike Falcon X Sandbox. |
| Netzwerkeinstellungen | Option, mit der Sie den Typ der Netzwerkeinstellungen auswählen können, die beim Senden einer URL oder Datei an Sandbox verwendet werden. |
| | |
| | |
| | |
| | |
| | |

4. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Konfiguration gesendet haben, wird sie auf der Seite „Konfigurationseinstellungen“ als Datensatz gespeichert. Die Konfiguration muss**Aktiv** sein, um in sandbox-Übermittlungen verwendet zu werden.




## Nächste Maßnahme

Nachdem Sie sund Box-Übermittlungen konfiguriert haben, besteht der nächste Schritt darin , Dateien oder ULRs manuell an Sandbox zu übermitteln

.

### Senden Sie Dateien oder URLs manuell an die Sandbox

Sie können eine Datei oder URL manuell an eine Sandbox senden, wenn bestimmte Incident-Kriterien erfüllt sind, z. B. die Kategorie „Phishing“.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Warum und wann dieser Vorgang ausgeführt wird

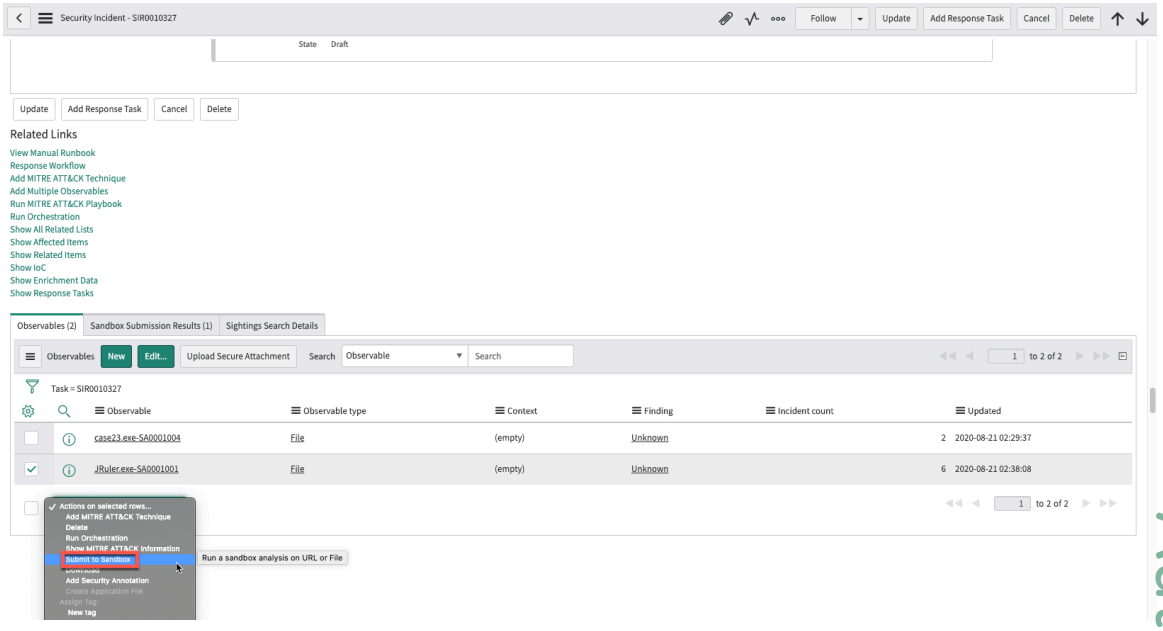
Nachdem Sie den Security Incident und die Datei oder URL überprüft haben, können Sie die Option An **Sandbox senden** auswählen, um eine Malware-Analyse durchzuführen.

## Prozedur

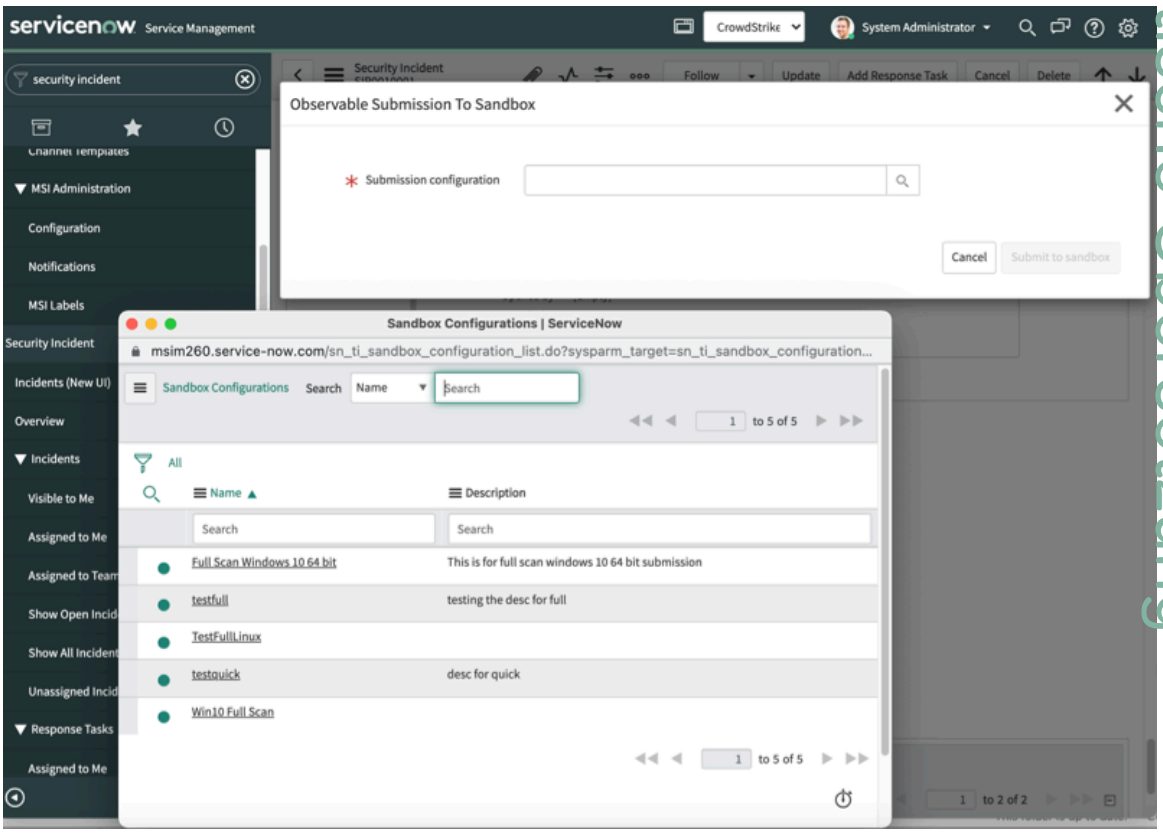
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie einen Datei- oder URL-Datensatz für erkennbare Elemente übermitteln möchten.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. **Wählen** Sie auf der Registerkarte Erkennbare Elemente einen Datensatz oder mehrere Datensätze aus, für die Sie eine Malware- oder Bedrohungsanalyse durchführen möchten, und klicken Sie **auf An Sandbox senden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



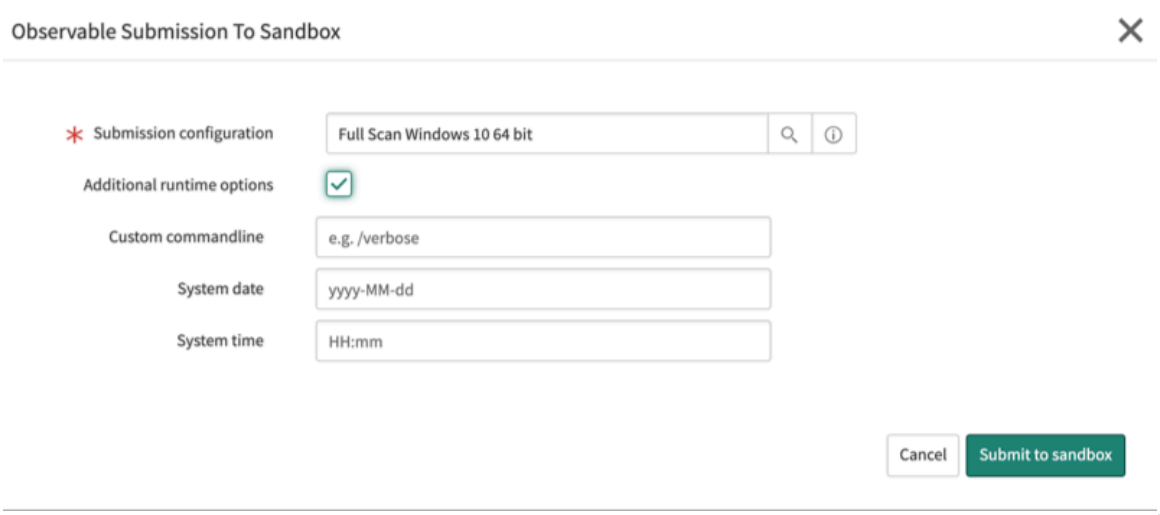

4. Wenn der Filter Dateiübermittlung angezeigt wird, wählen Sie Ihre bevorzugte Sandbox-Konfiguration unter **Übermittlungskonfiguration**aus und klicken Sie **auf An Sandbox senden**.




5. **Wahlweise:** Wählen Sie **Zusätzliche Laufzeitoptionen** aus, wenn Sie weitere benutzerdefinierte Optionen bereitstellen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




| Feld | Beschreibung |
|---|---|
| Benutzerdefinierte Befehlszeile | Reguläre Anwendungsbefehlszeile oder ein spezieller Vorgang. |
| Systemdatum | Systemdatum im Format jjjj-MM-tt. |
| Systemzeit | Systemzeit im Format HH:mm. |

Nachdem Sie die Übermittlung initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen. Um weitere Informationen zum Status der Übermittlung zu erhalten oder die Ergebnisse zu analysieren, zeigen Sie die **Sandbox-Übermittlungsergebnisse**an.

**Hinweis:**
In CrowdStrike Falcon X Sandbox wird Schnell-Scan für URLs nicht unterstützt. Wenn die Arbeitsnotizen zu viele Informationen enthalten, können Sie die Option Filter verwenden, um Detailinformationen zu den erforderlichen Arbeitsnotizen anzuzeigen, die für Sie relevant sind.

### Nächste Maßnahme
Wenn Sie die erkennbaren Elemente zur Malware-Analyse an die Sandbox senden, zeigen Sie die Ergebnisse der Sandbox -Übermittlung an, um die nächsten Schritte bei potenziellen Bedrohungen zu unternehmen.

## Automatisieren Sie CrowdStrike Falcon Sandbox-Übermittlungen mit Flow Designer

Die CrowdStrike Falcon X Sandbox -Integration umfasst Flow-Vorlagen, die mit Flow Designer erstellt wurden und mit Security Incident-Datensätzen arbeiten.

### Vorbereitungen

- Vergewissern Sie sich, dass Sie eine Sandbox-Übermittlungskonfiguration erstellt und eine Konfiguration als **Standardkonfiguration für die automatisierte Übermittlung**aktiviert haben. Wenn der Flow ausgelöst wird, erfolgt die Sandbox-Übermittlung in Ihrer Standardkonfiguration.

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Diese Flows sollen Ihnen in erster Linie den Einstieg erleichtern, wenn Sie Datei- oder URL-Übermittlungen als Teil Ihres Incident-Antwort-Workflows automatisieren möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie einen Beispiel-Flow aktivieren, werden Ihre Phishing-Dateianhänge automatisch übermittelt, wenn Sie die Security Incidents in Ihrem Beispiel-Flow als Phishing definieren. Alternativ können Sie alle .exe-Dateien übermitteln, wenn dieser Dateityp an einen Datensatz für erkennbare Elemente angehängt ist.

Sie können diese Beispiel-Flows ändern, um eine automatisierte Übermittlung unter verschiedenen Bedingungen, Kategorien, zusammengesetzten Bedingungen usw. auszulösen.

Die Sandbox-Integration besteht aus zwei Basissystem-Flows, die standardmäßig deaktiviert sind.

- **Datei übermitteln, wenn Kategorie Phishing ist**: Dieser Flow sendet eine Datei zur Malware-Analyse an die Sandbox, wenn die Security Incident-Kategorie als Phishing definiert ist. Sie müssen eine Datei an den erkennbaren Datensatz des Security Incident anhängen. Wenn Sie die URP-Funktion (User Reported Phishing) verwenden, wird jeder E-Mail-Anhang automatisch analysiert und dem SIR-Incident-Datensatz als Datensatz für erkennbare Elemente hinzugefügt. Es ist keine weitere Aktion erforderlich, um die Übermittlung zu automatisieren.
- **Absenden, wenn Dateityp für erkennbares Element exe ist**: Dieser Flow sendet eine Datei zur Malware-Analyse an die Sandbox, wenn das erkennbare Element des Security Incident eine exe-Datei ist. Ähnlich wie beim Phishing-Kategorie-Flow müssen Sie eine Datei an einen erkennbaren Datensatz im Security Incident anhängen. Sie können dies manuell tun, indem Sie die Datei hochladen, oder automatisch, wenn ein Phishing-E-Mail-Anhang oder ein anderer Mechanismus, der den Incident erstellt, den erkennbaren Datensätzen zugeordnet ist.

Wenn die Flows konfiguriert sind und die Incident-Bedingungen die Parameter erfüllen, werden die Sandbox-Übermittlungen automatisch ausgelöst, wenn Sie den Security Incident überprüfen. Überprüfen Sie die Arbeitsnotiz, die angibt, dass eine Übermittlung initiiert wurde, ein Tag angezeigt wird, falls in der Konfiguration aktiviert, und einen Datensatz mit ausstehenden Übermittlungsergebnissen enthält.

Die Sandbox-Integration enthält auch mehrere Subflows. Die Subflows sind interne Komponenten der allgemeinen Integrationsübermittlungsfunktionen. Sie können die Subflows an Ihre Sicherheitskriterien anpassen und bearbeiten.

Sie können auf die Subflows verweisen, um Probleme mit Sandbox-Übermittlungen zu beheben. Ein Ausführungsdatensatz wird jedes Mal erstellt, wenn Sie einen Subflow aufrufen. Dieser Datensatz gibt an, wo im Flow ein bestimmter Fehler aufgetreten ist, und ermöglicht Ihnen, das Problem zu beheben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Sandbox-Integration: Mehrere Workflows

Flows | Subflows | Executions | Help | + New

All > Application Name contains Sandbox

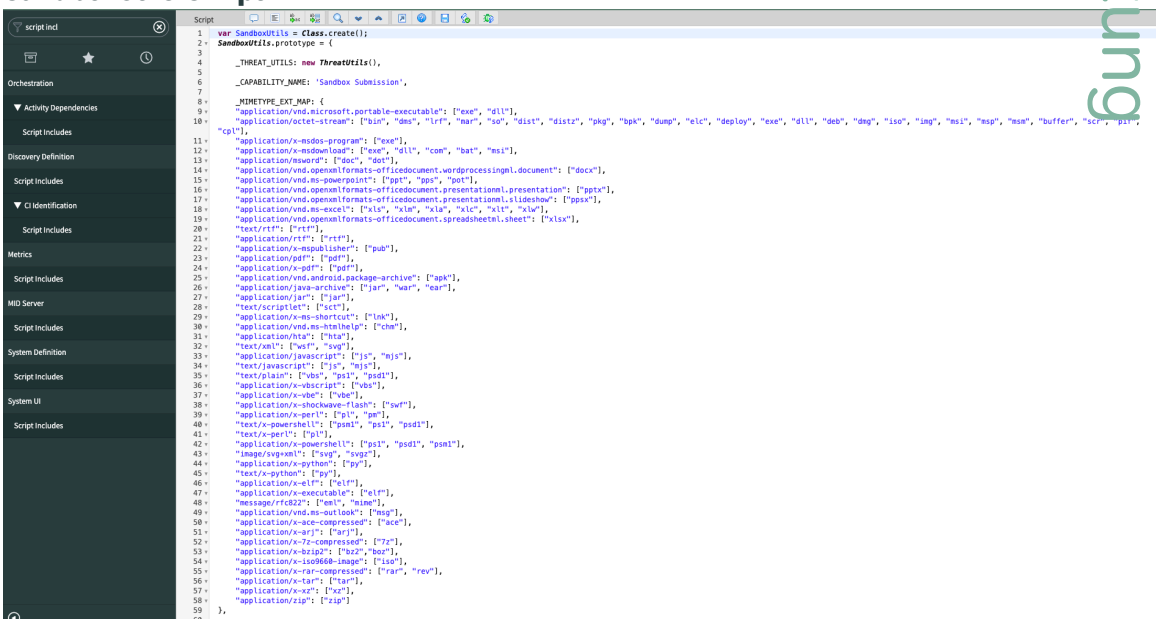
| Name ▲ | Internal name | Application | Status | Active | Updated | Updated by |
|---|---|---|---|---|---|---|
| Search | Search | *Sandbox | Search | Search | Search | Search |
| Add submission status tag on SIR | add_submission_status_tag_on_sir | Security Operations CrowdStrike Falcon S... | Published | true | 2020-07-16 12:33:57 | admin |
| Aggregate Additional Runtime Options | aggregate_additional_runtime_options | Security Operations CrowdStrike Falcon S... | Published | true | 2020-07-16 08:47:54 | admin |
| Connection and Credential Validation | connection_and_credential_validation | Security Operations CrowdStrike Falcon S... | Published | true | 2020-05-18 02:52:33 | admin |
| CrowdStrike Falcon Sandbox Poll Submission | crowdstrike_falcon_sandbox_polling | Security Operations CrowdStrike Falcon S... | Published | true | 2020-08-02 05:11:53 | admin |
| CrowdStrike Falcon Sandbox Submission | submit_file_to_sandbox | Security Operations CrowdStrike Falcon S... | Published | true | 2020-08-13 06:17:57 | admin |
| CrowdStrike Falcon Submission Results | crowdstrike_falcon_submission_results | Security Operations CrowdStrike Falcon S... | Published | true | 2020-08-13 06:30:16 | admin |
| CrowdStrike Polling Quick/Full Scan | crowdstrike_polling_quickfull_scan | Security Operations CrowdStrike Falcon S... | Published | true | 2020-07-20 20:23:07 | admin |
| Fetch Environment Ids from Sandbox | fetch_environment_ids_from_sandbox | Security Operations CrowdStrike Falcon S... | Published | true | 2020-05-25 07:45:54 | admin |
| Submit File or URL to CrowdStrike Quick ... | submit_fileurl_to_crowdstrike | Security Operations CrowdStrike Falcon S... | Published | true | 2020-07-20 19:04:42 | admin |
| Submit File/URL to Sandbox | submit_fileurl_to_sandbox | Security Operations CrowdStrike Falcon S... | Draft | true | 2020-05-25 07:50:18 | admin |
| Submit Observable for Automated submission | submit_observable_for_automated_submission | Security Operations CrowdStrike Falcon S... | Published | true | 2020-08-06 06:15:35 | admin |

Actions on selected rows... | 1 to 11 of 11

## Hinweis:

- Wenn Sie die Standard-Flows anpassen möchten, sollten Sie überprüfen, ob der Subflow „Erkennbares Element für automatisierte Übermittlung übermitteln“ in Ihrem Flow enthalten ist, um automatische Übermittlungen auszulösen.
- Sie können Ihre Dateierweiterungen für eine EXE-Datei anpassen und definieren. Erstellen Sie eine Kopie des Flows **Absenden, wenn der Dateityp für das erkennbare Element exe ist**, und nehmen Sie Änderungen an der Kopie vor. Inhaltstyp und Dateierweiterungen werden im SandboxUtils- Skript zugeordnet. Um auf Skripteinbindungen zuzugreifen, navigieren Sie zu Systemdefinitionen > Skripteinbindungen, und suchen Sie nach SandboxUtils.

### SandboxUtils-Skript

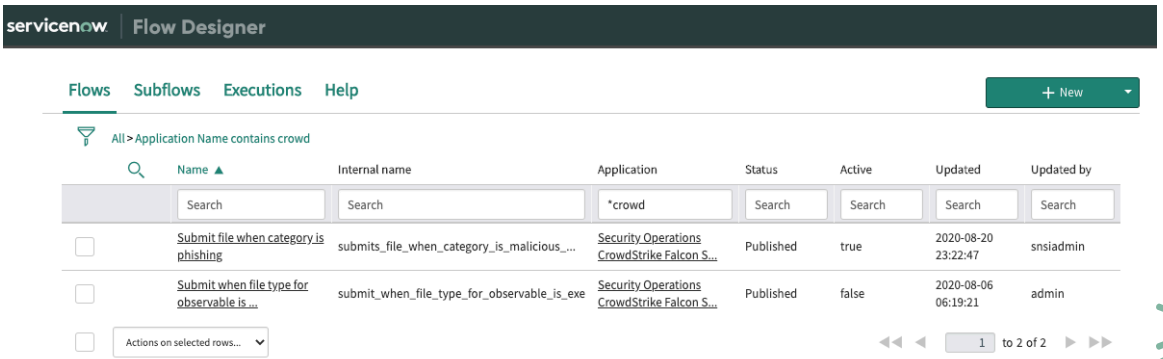




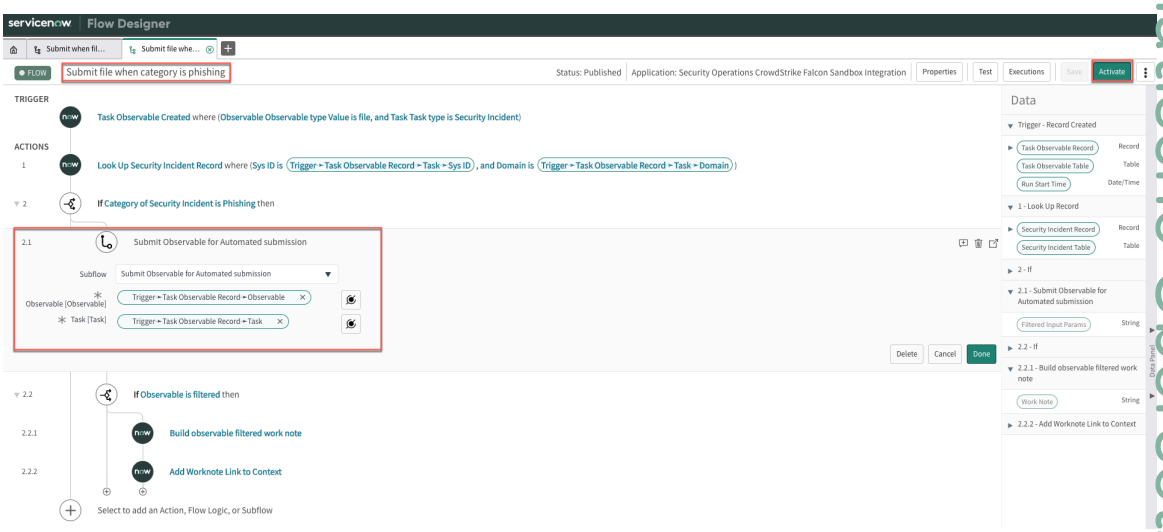

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** > **Flows**.
2. Filtern Sie die Flows nach dem **Anwendungstyp**.
   Zum Beispiel filtert *Crowd die beiden Flows CrowdStrike Falcon X Sandbox.




3. Wählen Sie einen Flow aus, um die Details anzuzeigen.
   Das folgende Beispiel zeigt den Flow Datei senden, wenn die Kategorie „Phishing“ ist.




4. Klicken Sie auf **Aktivieren** und dann auf **OK**, wenn die Bestätigungsmeldung angezeigt wird.

## Nächste Maßnahme

Nachdem Sie automatisierte Übermittlungs-Flows konfiguriert haben, können Sie die Sandbox-Übermittlungsergebnisse anzeigen, um etwaige Bedrohungen zu analysieren.

### Übermittlungsergebnisse in der Sandboxüberwachen

Die Ergebnisse für alle Sandbox-Übermittlungen werden auf der Registerkarte **„Sandbox** -Übermittlungsergebnisse“ für jeden Security Incident angezeigt.

## Vorbereitungen

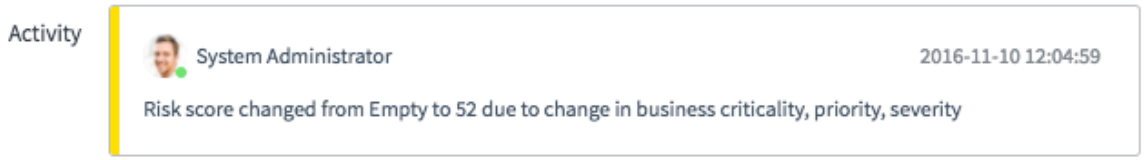
Erforderliche Rolle: sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

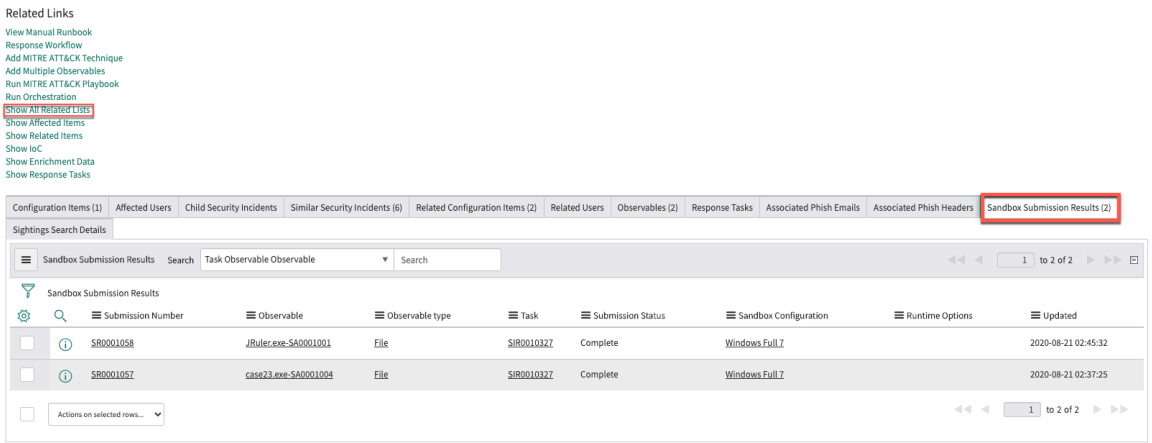
## Prozedur

1. Öffnen Sie den Security Incident , mit dem Sie arbeiten, und vergewissern Sie sich, dass die andbox-Übermittlung von serfolgreich war.




2. Überprüfen Sie die W-Ork -Hinweise auf weitere Informationen, und erfahren Sie, , wie Sie fortfahren können, wenn Sie nicht überprüfen können, ob der Scan erfolgreich war.

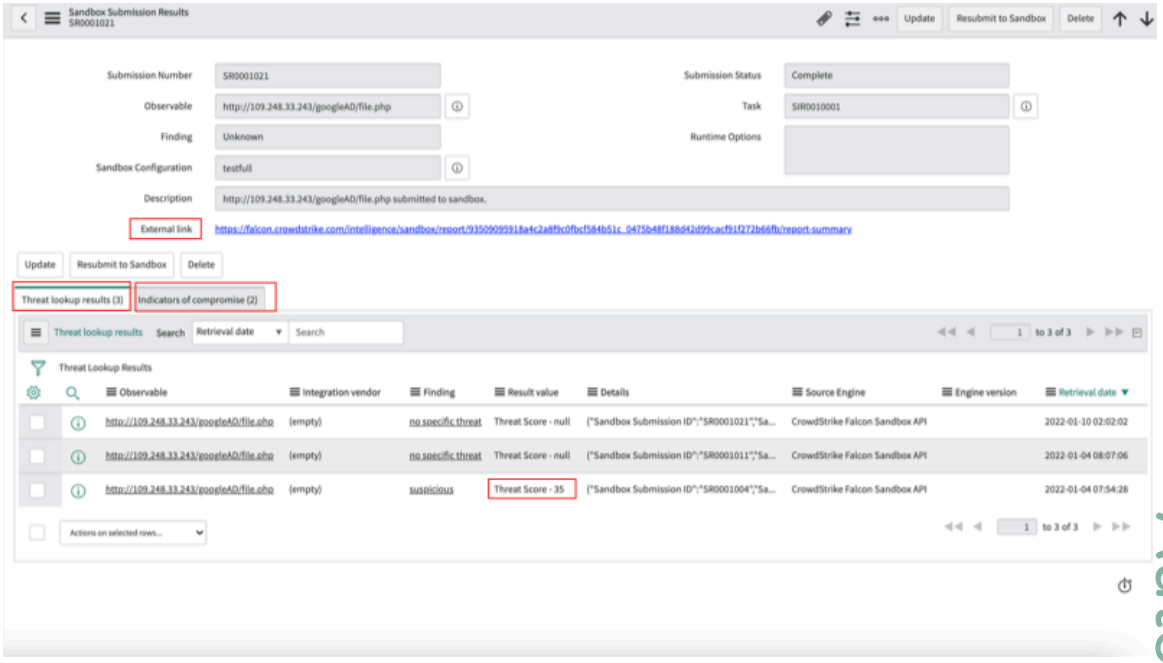
3. Klicken Sie entweder auf den Link zu den vollständigen Ergebnissen in W] oder in der Notizs oder am am Ende des Security Incident, und navigieren Sie zu **Alle zugehörigen Listen**anzeigen > **Sandbox-Übermittlungsergebnisse**.
   Die Ergebnisse werden auf der Registerkarte Sandbox-Übermittlungsergebnisse angezeigt.




4. Klicken Sie auf einen beliebigen Datensatz, um die vollständige andbox-Analyse von sanzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. **Wahlweise:** Klicken **Sie auf Erneut an Sandbox übermitteln,** um das erkennbare Element erneut zu verarbeiten.

## Ergebnisse

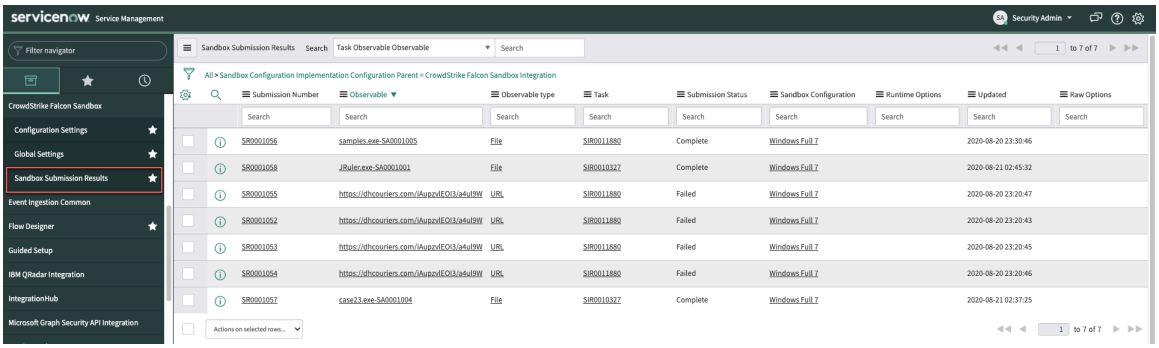
- Die Registerkarte **Ergebnisse** der Bedrohungssuche enthält die Bedrohungsbewertung, einschließlich böswilliger Ergebnisse, Bedrohungsbewertungen und zusätzlicher Details. Diesediese Details werden in der Standardstruktur der Bedrohungssuche für alle ServiceNow Integrationen der Bedrohungssuche bereitgestellt.
- Auf **der** Registerkarte Gefährdungsindikatoren werden die böswilligen oder verdächtigen sund die Box-Ergebnisse mit den Vertrauensbewertungen angezeigt. Die Konfidenzpunktzahlen ähneln anderen Indikatorinformationen, die in der Plattform ServiceNow gespeichert werden. Indikatoren, die als „informativ“ klassifiziert sind, sind auf dieser Registerkartenicht enthalten.
- Klicken Sie auf den **externen Link**, um die Sandbox-ErgebnisseCrowdStrike Falcon X Sandbox im Portal [] anzuzeigen.

> **Hinweis:**
> Diese Option erfordert, dass Sie überCrowdStrike Falcon X Sandbox die Rolle ] verfügen, um die Ergebnisse anzuzeigen.

Sie können auch die Ergebnisse der Übermittlung von sfür alle Security Incidents überwachen, indem Sie zu navigieren **CrowdStrike Falcon Sandbox** > **Sandbox-Übermittlungsergebnisse**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Kennzeichnen Sie Security Incidents mit dem Sandbox-Übermittlungsstatus

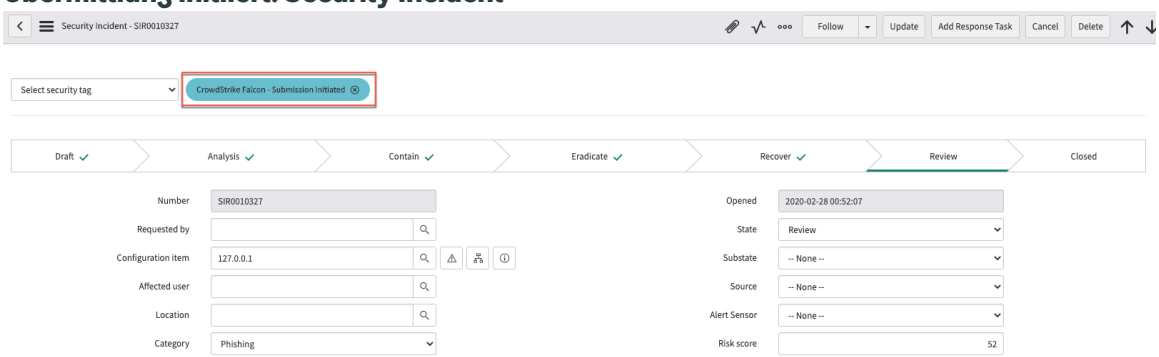
Optional können Sie Security Incidents mit den Tags „Übermittlung initiiert“ und „Übermittlung abgeschlossen“ versehen.

Wenn Sie die Option **Tags anzeigen** in der Sandbox-Übermittlungskonfigurationauswählen, werden Tags angezeigt, um den Status einer Datei- oder URL-Übermittlung anzugeben. Das Überprüfen des Status auf diese Weise ist nützlich, , da die Verarbeitung dersandbox-Analyse mehrere Minuten in Anspruch nehmen kann.

Die Anzeige-Tags sind angerufene Übermittlung initiiert, Übermittlung abgeschlossen und Übermittlung fehlgeschlagen.

Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung initiiert wurde.

### Übermittlung initiiert: Security Incident

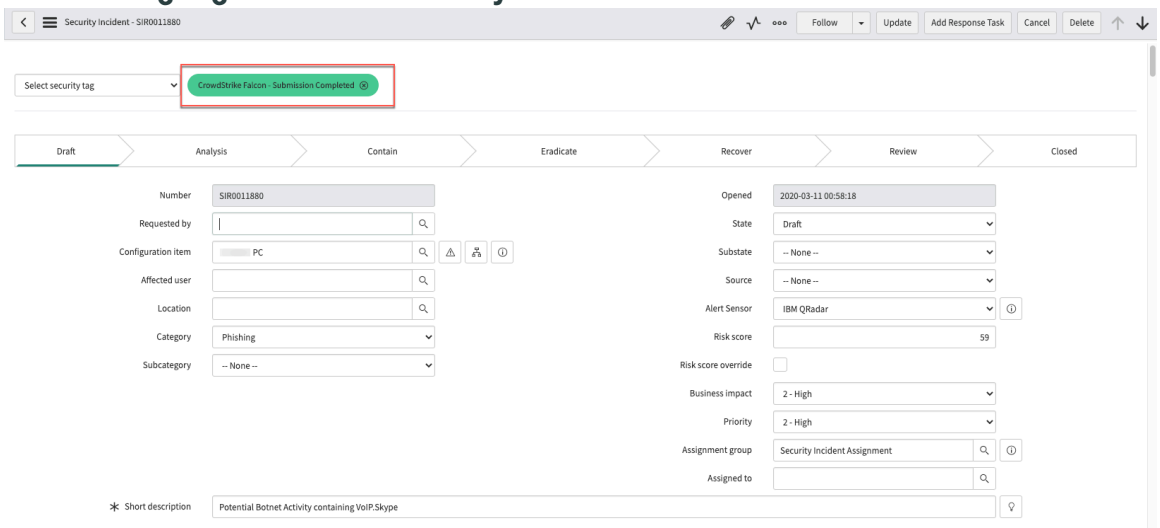



Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung abgeschlossen wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Übermittlung abgeschlossen – Security Incident**




## Überprüfen Sie die globalen Einstellungen von s.

Wenn Probleme mit den Ergebnissen der Datei- oder URL-Übermittlung auftreten, überprüfen und ändern Sie die globalen s-andbox-Einstellungen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Sandbox** > **Globale Einstellungen**.
2. Überprüfen und ändern Sie die Einstellungen nach Bedarf.

| Feld | Beschreibung |
|---|---|
| Dateigrößenbeschränkung (MB) | Sandbox-Upload-Dateigrößenbegrenzung in Megabyte.<br>**Hinweis:**<br>Die Dateigrößenbegrenzung von 256 MB ist standardmäßig konfiguriert. Erhöhen Sie den Wert nicht über 256 MB. Möglicherweise möchten Sie jedoch die maximale Dateigröße reduzieren, um die Übermittlung großer Dateien zu vermeiden. |
| Maximale Zeitüberschreitung für Übermittlungsergebnisse (Minuten) | Maximale Zeitüberschreitung für Übermittlungsergebnisse von den sund Box.<br>**Hinweis:**<br>Die Standardzeitüberschreitung beträgt 30 Minuten. Wenn Ihre Ergebnisse länger als 30 Minuten dauern, können Sie die Zeit erhöhen. Außerdem können Sie die Ergebnisse im andbox-Portal sanzeigen. |

3. Klicken Sie auf **Speichern** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Elasticsearch Incident Enrichment-Integration

Die Integration Elasticsearch – Incident-Ergänzung durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

| | |
|---|---|
| Erkunden<br>Security Incident Response-Integrationen | Einrichten<br>• Beginnen Sie mit der Integration von Elasticsearch – Incident-Ergänzung<br>• Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche |
| Verwenden<br>• Führen Sie eine Sichtungssuche aus<br>• Security Operations Integration - Sichtungs-such-Workflow<br>• Security Operations – Elasticsearch-Sichtungs-such-Workflow | Entwickeln<br>• ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und Hilfe<br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

## Beginnen Sie mit der Integration von Elasticsearch – Incident-Ergänzung

Elasticsearch ist eine verteilte RESTful-Such- und Analyse-Engine, die sich problemlos in Security Operationsintegrieren lässt. Bevor Sie die Integration Elasticsearch – Incident-Anreicherung verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechende API-Basis-URL und Anmeldeinformationen hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

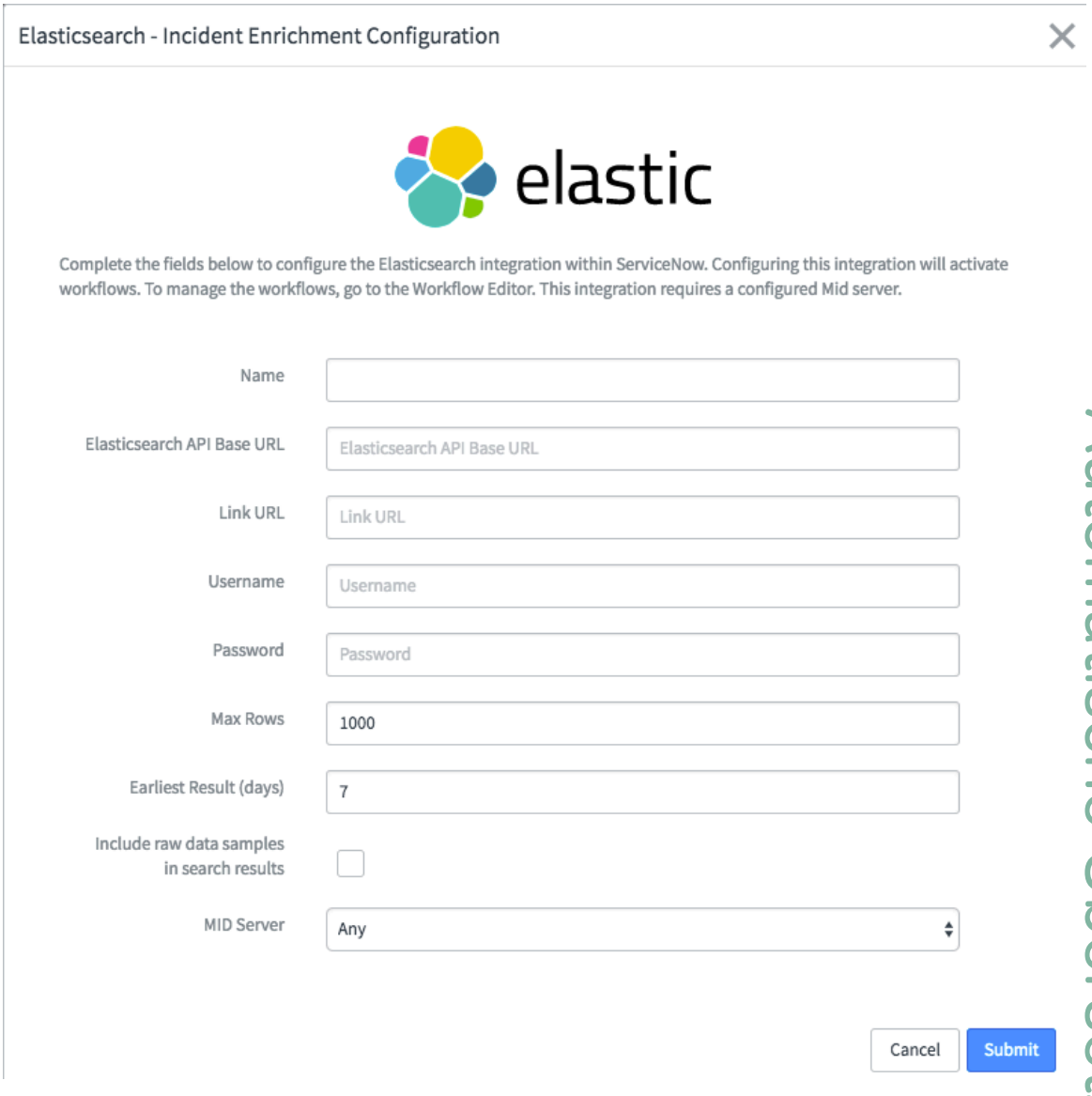
### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf Elasticsearch zu, und rufen Sie die API-Basis-URL unter Ihrem Elasticsearch-Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**4.** Klicken Sie in der Karte Elasticsearch – Incident-Ergänzung auf **Neu**.




**5.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Basis-URL der Elasticsearch-API | Die Basis-URL, die Sie von der Website Elasticsearch erhalten haben. |
| Link-URL | [Optional] Links zu einer Kibana-Instanz, falls verfügbar |
| Benutzername | Ihr Intel Elasticsearch -Benutzername. |
| Passwort | Ihr Intel Elasticsearch -Passwort. |
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Rohdatenmuster in Suchergebnissen berücksichtigen | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

### Ergebnisse
Nach der Konfiguration kann die Integration Elasticsearch - Incident Enrichment für die Veröffentlichung von erkennbaren Elementen in Beobachtungslisten in Security Incident Response ausgewählt werden.

## Integration von FireEye Endpoint Security

FireEye Endpoint Security (HX-Serie) hilft Unternehmen bei der Überprüfung und Analyse von bekannten und unbekannten Bedrohungen auf einem beliebigen Endpunkt.

Erfahrene Angreifer umgehen heute traditionelle Abwehrmaßnahmen, auf die sich die meisten Sicherheitsteams seit Jahren zum Schutz ihrer Endpunkte verlassen. Selbst wenn eine herkömmliche Abwehr eine bekannte Bedrohung stoppt, kann sie nicht feststellen, was diese Bedrohung zu tun versucht hat. FireEye HX Endpunktsicherheit hilft Ihrem Sicherheitsteam, bekannte und unbekannte erweiterte Bedrohungen für Ihre Endpunkte aufzuspüren und zu stoppen.

Die Integration von Gold Standard Security Incident Response mit FireEye HXmacht es Sicherheitsanalysten einfacher und effizienter, Security Incidents sofort zu untersuchen und zu beheben, ohne zwischen Tools navigieren zu müssen. Sie können Netzwerkeinschluss verwenden, um Korrekturaktionen für die Endpunkte auszuführen, Profile zu implementieren, um bestimmte Details zum Host zu erfassen, und bestimmte Abfragen oder Aktionen für den Endpunkt auszuführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Schlüsselfunktionen

- Möglichkeit, Hostanreicherungsaktionen auszuführen, um weitere Details zum Endpunkt zu erfassen, z. B. Hostdetails, Netzwerkstatistiken, Benutzerdetails, Dateidetails, Prozessdetails und Servicedetails.
- Möglichkeit, eine Unternehmenssicherheitssuche durchzuführen, um potenzielle schädliche erkennbare Elemente über Endpunkte hinweg zu erkennen und Korrekturmaßnahmen zu ergreifen.
- Möglichkeit zur Erfassung von Selektierung und Datenerfassung für eine eingehende Endpunktinspektion und -analyse.

## Einschränkungen

Im Folgenden sind die bekannten Einschränkungen dieser Integration aufgeführt:

1. Der Wert für das MID-Anwendungsfeld muss manuell eingegeben werden.
2. „Host isolieren“ und „Auslaufende Services abrufen“ können nicht auf dem Linux-Agent ausgeführt werden.
3. „Isolierung entfernen“ unterstützt den Linux-Agent nicht.
4. Selektierungsakquise bietet keine Unterstützung für Linux-Agent.
5. Benutzer müssen zugehörige Links Ergänzungsdaten anzeigen konfigurieren. Sie ist nicht standardmäßig verfügbar.
6. Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Die verbleibenden werden in die Warteschlange gestellt und beginnen nach Abschluss einer der laufenden Sichtungen.
7. Sichtungen sind sofort einsatzbereit und standardmäßig auf false gesetzt.
8. Hash wird für „Laufende Prozesse abrufen“ nicht unterstützt.

### Richten Sie Ihre NowPlatform-Instanz für die FireEye-Integration ein

Überprüfen und überprüfen Sie das folgende Konfigurationsverfahren, um die NowPlatform-Instanz für die FireEye-Integration einzurichten.

**Vorbereitungen**
Erforderliche Rolle: Now Platform-Administrator (sn_si.admin)

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer NowPlatform-Instanz ausführen müssen, bevor Sie die Anwendung für die FireEye-Integration installieren.

Stellen Sie sicher, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie die Anwendung aus dem ServiceNow Store installieren.

| Aufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen NowPlatform und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind erforderlich:<br>1. Benutzer mit der Rolle „Systemadministrator“ (admin) sind erforderlich, um die Anwendung für die Integration zu installieren.<br>2. Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) sind |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | erforderlich, um die Integration zu konfigurieren und Profile zu erstellen, zu aktivieren und zu entfernen.<br>3. Benutzer mit der Rolle „Security Incident-Analyst“ (sn_si.analyst) sind erforderlich, um mit Security Incidents arbeiten zu können. Benutzer mit dieser Rolle können alle in der Integration verfügbaren Fähigkeiten initiieren. |
| Vergewissern Sie sich, dass Sie einen MID Server installiert und konfiguriert haben. | MID Server konfigurieren: Ein MID Server in Ihrer NowPlatform-Instanz ist erforderlich, um Dateien zu verwalten und eine Verbindung zum FireEye-Service herzustellen, der in Ihrem Unternehmensnetzwerk bereitgestellt wird. Weitere Informationen zu MID Servern finden Sie unter https://docs.servicenow.com |
| Vergewissern Sie sich, dass die zur Unterstützung der Integration erforderlichen ServiceNow-Kernanwendungen installiert und aktiviert sind, bevor Sie die Anwendung installieren. | Die folgenden Anwendungen müssen vor der Installation dieser Anwendung aus dem ServiceNow Store installiert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:<br>1. Security Incident Response-Support<br>2. Security Support Core<br>3. Security Support Common<br>4. Security Incident Response<br>5. Threat Intelligence-Support – Allgemein<br>6. ServiceNow Integration Hub Enterprise Pack-Installationsprogramm |
| Vergewissern Sie sich, dass Sie eine Genehmigungsgruppe erstellt haben, bevor Sie die Genehmigungsoption für Profile aktivieren. | Ein optionaler Genehmigungsworkflow ist verfügbar, um Hostcomputer zu isolieren, sie im Netzwerk wiederherzustellen, Dateien abzurufen und zusätzliche Aktionen für den Endpunkt auszuführen.<br>Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie während der Konfiguration der Profile die Option Genehmigung erforderlich.<br>Wenn kein Profil vorhanden ist und eine Fähigkeit direkt aus der zugehörigen Liste aufgerufen wird, können Genehmigungen über das FireEye-Standardeinstellungsmodul gehandhabt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

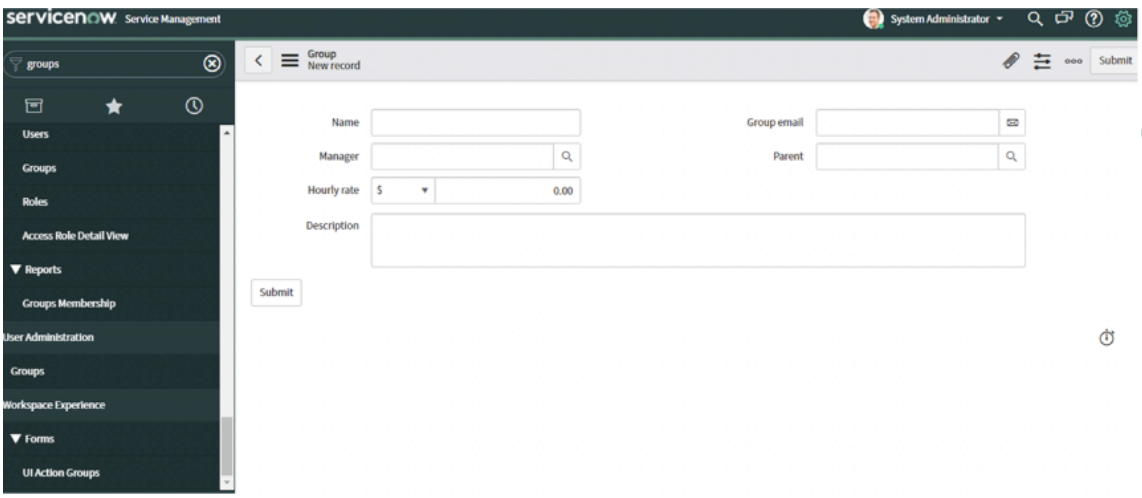
| Aufgabe | Beschreibung |
|---|---|
| | Als Sicherheitsadministrator können Sie die Genehmigung einrichten, während Sie die Profile und die Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in der Gruppenliste in Ihrer Instanz verfügbar sein. |

### Prozedur

1. Navigieren zu **Benutzeradministration** > **Gruppen**.
2. Klicken **Neu** in der Gruppenliste.
3. Füllen Sie das Formular mit den folgenden Details aus:

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppe, die angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird. |
| Gruppen-E-Mail | (Optional) Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers. |
| Manager | (Optional) Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen. |
| Übergeordnet | (Optional) Name der übergeordneten Gruppe, falls einer übergeordneten Gruppe zugeordnet. |
| Stundensatz | (Optional) Betrag, der für jede gearbeitete Stunde bezahlt wird. |
| Beschreibung | (Optional) Zusätzliche Informationen zur Gruppe. |

4. Klicken **Absenden**.




Die neue Gruppe wird in der Gruppenliste angezeigt. Sie haben erfolgreich eine Genehmigungsgruppe erstellt. Fügen Sie Ihrer neuen Gruppe nach Bedarf Benutzer hinzu, die die vom Sicherheitsanalysten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übermittelten Anforderungen genehmigen können. Ein Benutzer erbt Rollen von allen Gruppen, denen er angehört. Sie können Rollen auch direkt einem Benutzer zuweisen.

Um Anforderungen zu überwachen und zu verarbeiten, die von Benutzern mit der Rolle „sn_si.analyst“ übermittelt werden, muss jedes Mitglied der Genehmigungsgruppe in Now Platform zu Meine Genehmigungen navigieren. Alternativ finden Genehmiger die Anforderungen, die speziell für die FireEye-Integration übermittelt wurden, unter „FireEye-Genehmigungen“.

### Nächste Maßnahme

Der nächste Schritt besteht in der Installation und Konfiguration der Anwendung aus dem ServiceNow Store.

## Zeitstempeleinstellungen für Selektierungsakquise konfigurieren

Konfigurieren und überprüfen Sie die Zeitstempeleinstellungen vor dem Installationsverfahren.

### Vorbereitungen

Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

Vor der Installation der FireEye-Anwendung müssen einige Voraussetzungen für FireEye erfüllt sein.

Die Selektierungsakquise kann durch Eingabe in das Feld „Um Zeitstempel“ oder das Feld „Standard“ angefordert werden. Der Zeitstempel fordert Informationen an, die während eines bestimmten Zeitraums vor dem Zeitstempel bis zu einem bestimmten Zeitraum nach dem Zeitstempel erfasst wurden. Der Zeitstempel gibt die Zeit an, zu der das Event aufgetreten ist, von dem die Warnung generiert wurde. Wenn Sie Standard auswählen, fordert die Endpoint Security-Appliance Informationen vom Host für alle Daten rund um ein Event an.

Wenn ein Endpoint Security-Benutzer eine Selektierungssammlung basierend auf einem bestimmten Datum und einer bestimmten Uhrzeit anfordert, gibt der Service Desk-Mitarbeiter Informationen für ein bestimmtes Zeitfenster vor und nach der Warnung zurück. Die Zeitstempeleinstellungen steuern die Länge des Fensters für die Selektierungssammlung. Zeitstempeleinstellungen gelten nur für Agent-URL-Ereignisse (URL-Überwachungsereignisse) und Registrierungsschlüssel-Ereignisse (Reg.-Schlüssel-Ereignisse).

Sie können die Registerkarte Zeitstempeleinstellungen verwenden, um die Zeitspanne vor und nach dem Zeitstempel anzugeben, in der Informationen erfasst werden. Zeitstempeleinstellungen können zwischen 0 und 86.400 Sekunden liegen. Der Standardwert für beide Einstellungen beträgt 600 Sekunden.

Sie können die Registerkarte Zeitstempeleinstellungen auf der Seite „Einstellungen für automatische Selektierung“ verwenden, um die Zeitspanne vor und nach dem Zeitstempel anzugeben, in der Informationen gesammelt werden. Der Zeitstempel gibt die Zeit an, zu der das Event aufgetreten ist, das die Warnung ausgelöst hat.

### Prozedur

1. Navigieren zu **Endpunktsicherheits-Web-UI**.
2. Auswahlvorgang **Administrator** > **Selektierungseinstellungen**.
3. Klicken **Zeitstempeleinstellungen** Registerkarte auf der **Einstellungen für automatische Selektierung** Seite.
4. Geben Sie die Dauer vor und nach dem Zeitstempel an, für den die Informationen benötigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie die Anzahl der Sekunden vor dem angegebenen Zeitstempel ein, für die die Informationen benötigt werden.
6. Geben Sie die Anzahl der Sekunden nach dem Zeitstempel ein, für die die Informationen benötigt werden.
7. Klicken **Speichern**.

**Hinweis:**
Sie können alle Werte auf der Seite auf die Standardeinstellungen zurücksetzen, indem Sie auf klicken **Auf Standardwerte zurücksetzen**, und klicken Sie auf Speichern.

- **Beschaffungsbereich**: Die Seite „Beschaffungen“ zeigt an, wie viel Speicherplatz für Beschaffungen übrig ist.
- **Festlegen von Datenträger-Auslastungsgrenzen für Beschaffungen:**
  - Selektierungen, Dateibeschaffungen und Datenbeschaffungen können sich im Laufe der Zeit ansammeln und immer mehr Speicherplatz verbrauchen. Um dies zu steuern, können Sie ihnen eine bestimmte Menge an Speicherplatz zuweisen. Zehn Prozent des von Ihnen angegebenen Speicherplatzes sind für automatische Selektierungsakquisitionen reserviert. Wenn der insgesamt zugewiesene Erfassungsbereich überschritten wird, werden die ältesten automatischen Selektierungen gelöscht.
  - Wenn die Gesamtdatenträgergröße der abgeschlossenen Erfassungen ein bestimmtes Limit überschreitet, löscht die Endpoint Security-Appliance die ältesten abgeschlossenen Erfassungen, bis genügend Speicherplatz frei ist, um die Gesamtgröße unter das angegebene Limit zu bringen. Akquisitionen, die noch nicht abgeschlossen sind, sind nicht betroffen.
  - Die Endpoint Security-Appliance löscht Erfassungen automatisch, wenn ein Administrator, Analyst oder Ermittler die Endpoint Security-Web-UI verwendet, um den zugeordneten Agent manuell zu löschen.

  So legen Sie Grenzwerte für die Datenträgerauslastung für vollständige Erfassungen mit der Web-UI fest:
- Navigieren Sie zu **Endpunktsicherheit Web-UI**.
- Auswahlvorgang **Grenzwerte für Datenträgerauslastung** aus dem **Administrator** -Menü.
- In der **Platzlimit für Beschaffung** -Bereich geben Sie die maximale Menge an Speicherplatz (in GB) an, der zum Speichern von Selektierung, Datei und Datenerfassungen verwendet werden kann. Gültige Werte und Standardwerte variieren je nach Modell der Endpoint Security-Appliance. Die für Ihr Modell geeigneten Werte werden auf der Seite „Limits für Datenträgerauslastung“ angezeigt.
- Klicken **Speichern**.

**Hinweis:**
Alle genannten Einstellungen werden berücksichtigt. Bei Fehlern gibt Now Platform nur diese Fehler zurück.

### Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration

Installieren und konfigurieren Sie die Anwendung aus dem ServiceNow Store in Ihrer Now Platform-Instanz.

**Vorbereitungen**
Erforderliche Rolle: NowPlatform-Administrator (admin)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

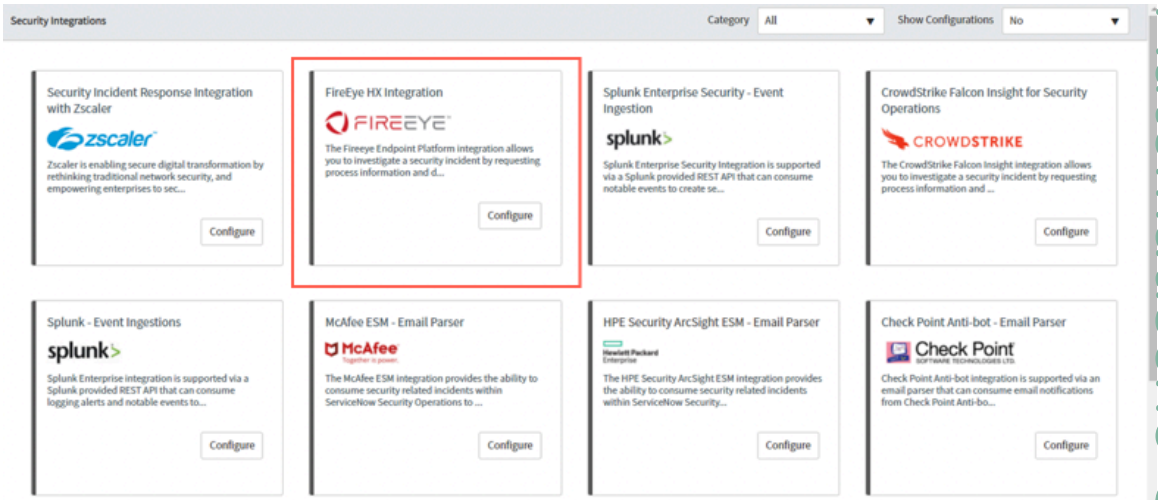
**Hinweis:**
Zum Konfigurieren einer Quelle ist ein aktiver MID Server erforderlich.

Laden Sie die Anwendung Security Incident Response integration with FireEye HX aus dem ServiceNow Store herunter, und installieren Sie sie.

Nachdem Sie die Anwendung erfolgreich installiert haben, führen Sie die folgenden Schritte aus, um sie zu konfigurieren:

### Prozedur

1. Navigieren zu **Integrationen** > **Integrationskonfigurationen**.
2. Rufen Sie die Eigenschaft **Integrationskonfigurationen** -Modul, um die verfügbaren Integrationen anzuzeigen, und suchen Sie nach **FireEye** Kachel.



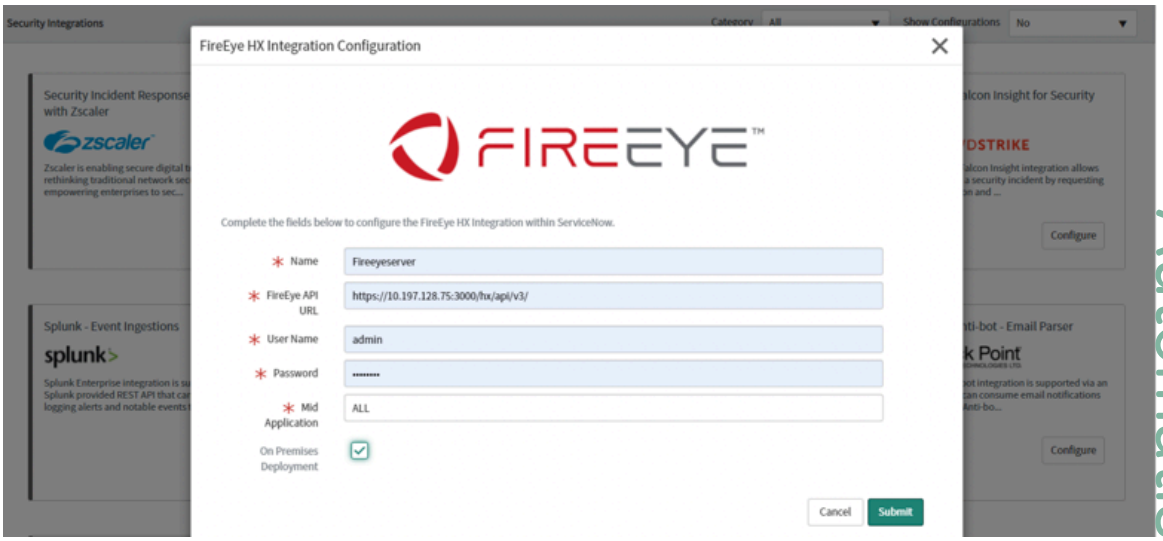

3. Klicken **Konfigurieren** auf der FireEye-Kachel.
4. Geben Sie die folgenden Details an, um die FireEye-Integration einzurichten:

| Feld | Beschreibung |
|---|---|
| Name | Name der FireEye-Konfiguration Dieser Name wird verwendet, um die Quelle und die zugehörigen Anmeldeinformationen und die Konfiguration zu identifizieren. Dieser Name hilft Ihnen, die Anmeldeinformationen und Konten zu unterscheiden und jede Quelle zu identifizieren, um Konflikte mit Profilen zu vermeiden. |
| API-URL | Basis-URL, die die FireEye-API hostet. |
| Benutzername | Geben Sie den Benutzernamen des FireEye-Kontos ein. |
| Passwort | Geben Sie das Passwort des FireEye-Kontos ein. |
| MID-Anwendung | MID-Anwendung, die in Ihrer Umgebung eingerichtet ist. MID-Server ist erforderlich, um ZIP-Dateien für einige der Ergänzungsfunktionen zu verarbeiten. Standardmäßig ist dies ALLE. Benutzer |

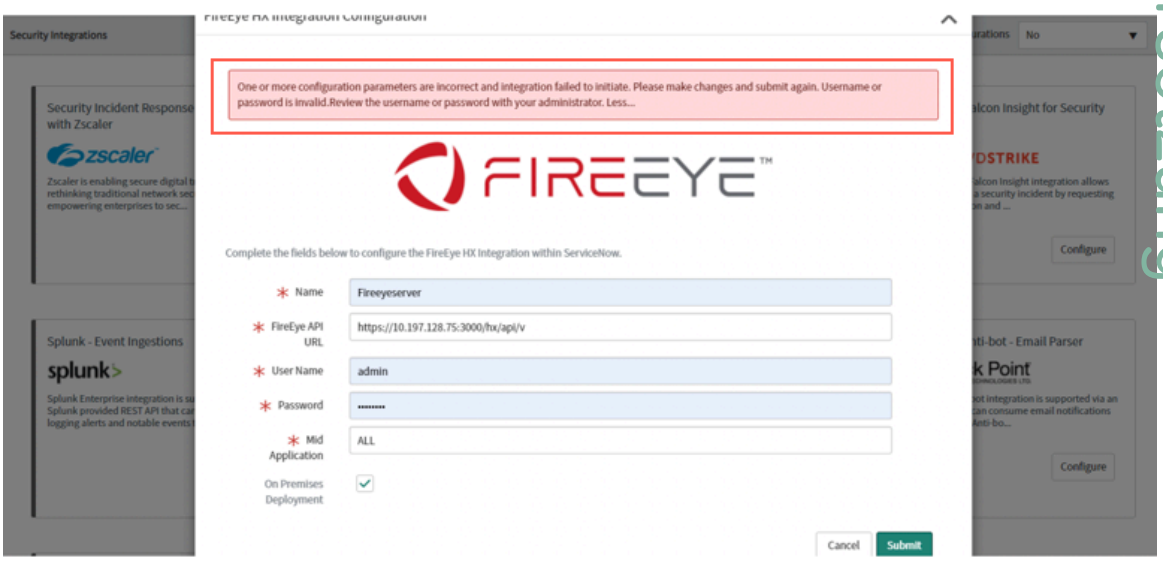
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | müssen einen gültigen Anwendungsnamen manuell angeben. |
| Lokale Bereitstellung | Standardmäßig deaktiviert. Wenn Sie die cloudbasierte Version von FireEye verwenden, vergewissern Sie sich, dass das Kontrollkästchen deaktiviert ist. |




5. Klicken **Absenden**.
   Die Liste „FireEye-Konfigurationen“ wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für einen FireEye-Server abgeschlossen. Wenn Sie keine Verbindung zu FireEye herstellen können oder Ihre Anmeldeinformationen falsch sind, wird eine Validierungsfehlermeldung angezeigt (siehe folgende Abbildung). Vergewissern Sie sich, dass Ihre Anmeldeinformationen korrekt sind, und versuchen Sie es erneut.




### FireEye: Standardeinstellungen

Im Folgenden finden Sie die zusätzlichen Konfigurationseinstellungen nach Abschluss der Installation.

Automatische Übersetzung

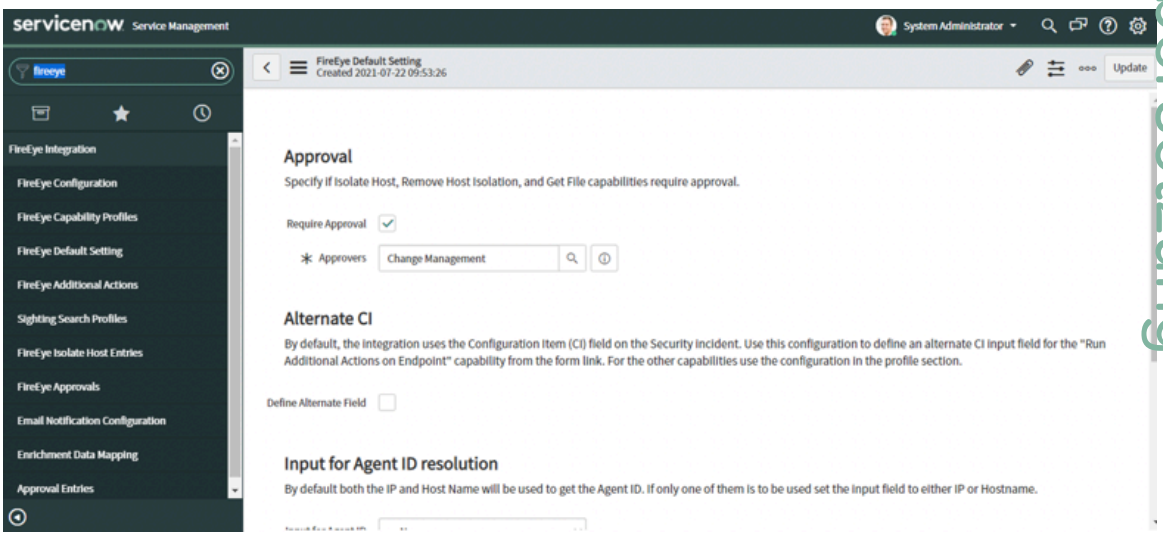
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald Sie die Installation abgeschlossen haben, finden Sie das Modul „FireEye-Standardeinstellungen“ in der linken Navigation. Sie enthält Standardeinstellungen für verschiedene FireEye-Funktionalitäten.

## Zusätzliche Konfigurationen

Im Folgenden sind die zusätzlichen Konfigurationseinstellungen aufgeführt:

1. **Freigabe**: Diese Genehmigung gilt speziell für die Funktionen „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“, wenn sie direkt aus der zugehörigen Liste ausgelöst werden und keine Profile für sie vorhanden sind. Wenn für diese Fähigkeiten Profile vorhanden sind, wird die Genehmigungskonfiguration im Profil berücksichtigt.
   - **Genehmigung erforderlich:** Wenn Sie Genehmigung erforderlich aktivieren, ist das Feld Genehmiger im Formular verfügbar.
   - **Genehmiger**: Liste der Genehmigergruppen. Nachdem Sie eine Anforderung gesendet haben, ist eine Genehmigung durch die Gruppe erforderlich, um die Anforderung abzuschließen.
2. **Alternatives CI**: Wenn Sie dieses Kontrollkästchen aktivieren, wird eine Liste der Felder bereitgestellt, in denen ein alternatives CI an die Fähigkeit übergeben werden kann. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“. Verwenden Sie diese Konfiguration, um ein alternatives CI-Eingabefeld nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Verwenden Sie für die anderen Fähigkeiten die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, wählen die Fähigkeiten das CI-Feld aus dem Security Incident-Formular aus.
3. **Eingabe für die Auflösung der Agent-ID**: Standardmäßig werden IP und Hostname zum Abrufen der Agent-ID verwendet. Wenn nur einer von ihnen verwendet werden soll, legen Sie das Eingabefeld entweder auf IP oder Hostname fest.

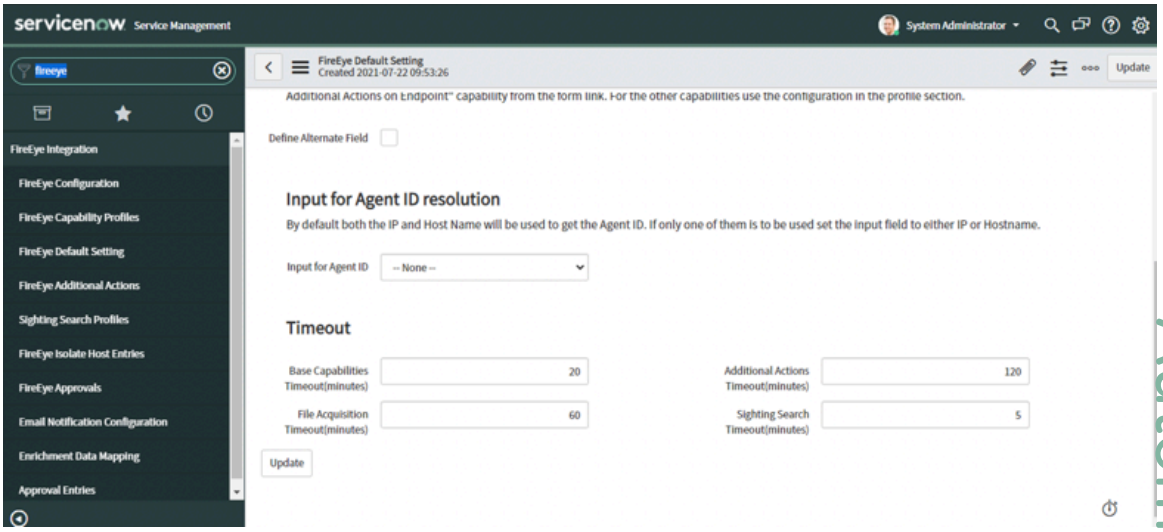



4. **Zeitüberschreitung**:
   - **Zeitüberschreitung für Basisfähigkeiten (Minuten):** Die Funktionen „Anreicherung“, „Host isolieren“ und „Hostisolierung entfernen“ schlagen fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
   - **Zeitüberschreitung für zusätzliche Aktion (Minuten):** Die Funktion „Zusätzliche Aktionen für Endpunkt ausführen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zeitüberschreitung bei Dateierfassung (Minuten):** Die Funktion „Datei abrufen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
- **Zeitüberschreitung für Sichtungssuche (Minuten):** Die Suche wird nach der festgelegten Zeit angehalten.




### Erstellen Sie ein neues Fähigkeitsprofil für die FireEye-Endpunktintegration

Erstellen Sie ein Profil, und wählen Sie die Fähigkeiten FireEye HX aus, die das Profil ausführen soll.

**Vorbereitungen**
Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

**Warum und wann dieser Vorgang ausgeführt wird**
Profile werden erstellt, um Fähigkeiten zusammenzufassen, und helfen Analysten, die Untersuchung/Korrektur einfach durchzuführen.

Im Folgenden finden Sie die Liste der Fähigkeiten, die Sie den Profilen hinzufügen können:

1. Hostdetails abrufen
2. Angemeldete Anwender abrufen
3. Netzwerkstatistiken abrufen
4. Laufende Prozesse abrufen
5. Laufende Services abrufen
6. Datei abrufen
7. Host isolieren
8. Isolation entfernen

Sie können die Funktionen „Datei abrufen“, „Host isolieren“ und „Hostisolierung entfernen“ nicht mit anderen Funktionen verbinden, während Sie ein Profil erstellen. Profile für diese müssen einzeln erstellt werden. Auf der anderen Seite können „Systemdetails abrufen“, „Angemeldete Benutzer abrufen“, „Netzwerkstatistiken abrufen“, „Laufende Prozesse abrufen“ und „Laufende Services abrufen“ zusammengefasst werden. Sie können Profile einzeln erstellen oder sie je nach Bedarf vollständig oder in Teilen zusammenfassen. Sobald eine Fähigkeit in einem Profil enthalten ist, kann sie nicht in ein anderes Profil aufgenommen werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die folgenden Schritte aus, um ein neues Fähigkeitsprofil zu erstellen:

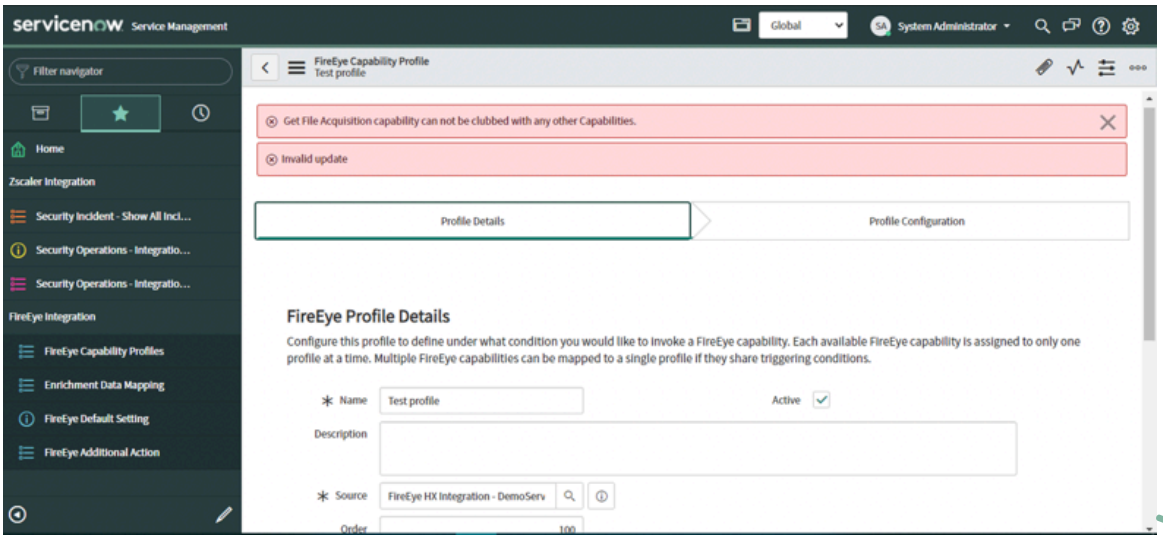
### Prozedur

1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**.
   Die Liste der Fähigkeitsprofile wird angezeigt.
2. Klicken **Neu**.
3. Füllen Sie die Felder im Formular aus.

| | |
|---|---|
| Name | Name für das Fähigkeitsprofil FireEye HX. Anhand dieses Namens können Sie den Profiltyp identifizieren und beschreiben. |
| Beschreibung | Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben. |
| Quelle | Name der Quelle FireEye HX. Nur konfigurierte Quellen sind in der Auswahlliste verfügbar. |
| FireEye HX-Fähigkeiten | Fähigkeiten des Profils FireEye HX. Wählen Sie die gewünschten Fähigkeiten für dieses Profil aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt. |
| Reihenfolge | Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen.<br>Der Flow mit der niedrigsten Nummer hat die höchste Priorität.<br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300, 400. |
| Aktiv | Dies zeigt an, dass das Profil aktiv ist. Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben. |

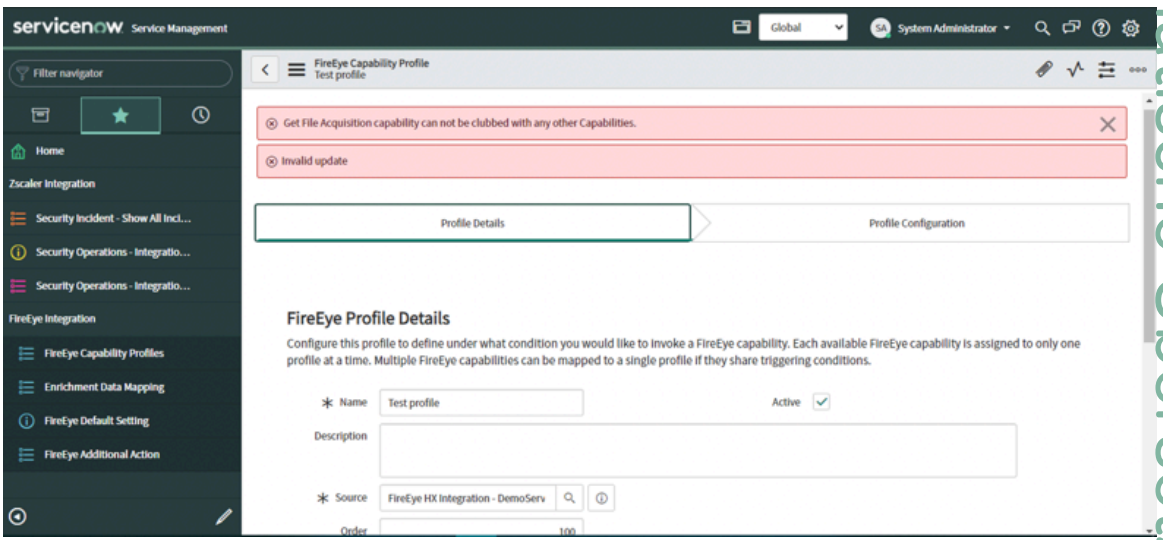


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für Profildetails mit der Fähigkeit „Hostdetails abrufen“.

4. Klicken **Weiter** , um mit Profilkonfiguration fortzufahren.




**Hinweis:**
Die Fähigkeiten „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“ können nicht mit anderen Fähigkeiten verknüpft werden.

## Nächste Maßnahme

Der nächste Schritt besteht in der Konfiguration Ihres Profils. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie sich die Konzepte zum Konfigurieren von Profilen und Auslösebedingungen ansehen. Weitere Informationen finden Sie unter Funktionsweise von Auslöserbedingungen mit einem Konfigurationselement für ein Profil.

### Machen Sie sich mit der Funktionsweise von Auslöserbedingungen für ein Konfigurationselement vertraut

Nachdem Sie ein Profil erstellt und die FireEye-Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass es nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

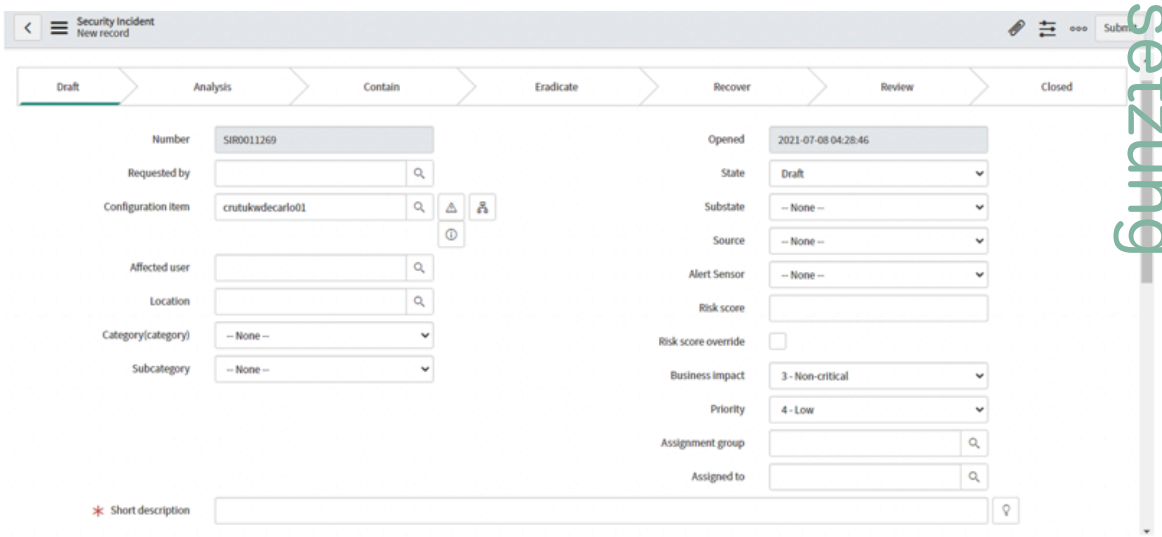
Sie können Auslöserbedingungen festlegen, sodass das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der der Auslöserbedingung entspricht. Wenn die Auslöserbedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie für den Security Incident auf das Formular „EDR-Profil ausführen“ klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in der Now Platform-CMDB gespeicherten Informationen abzugleichen. Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird die CMDB durchsucht, um den Hostnamen und/oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname und/oder die IP wird verwendet, um die Agent-ID auf FireEye HX aufzulösen und den Endpunkt zu identifizieren.

Im Idealfall wird ein übereinstimmender Wert in der Datenbank gefunden, und Daten werden in der Konsole FireEye HX für das übereinstimmende Asset gesammelt. Die Daten für verschiedene Fähigkeiten werden in Ihre Now Platform-Instanz abgerufen und in den zugehörigen Listen von Security Incidents angezeigt. Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt wird, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, das entweder den Hostnamen oder die auszuführende IP enthält die Agent-ID-Auflösung.

Während des Konfigurationsschritts der Profileinrichtung können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt auf FireEye HXidentifizieren können. Sie können ein beliebiges Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich benutzerdefinierter Felder, die Sie erstellen. Wenn Sie dieses alternative CI-Feld als Sicherung auswählen, stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung nicht für den zugehörigen Security Incident ausgefüllt wird.

**Hinweis:**
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Für alle zusätzlichen Aktionen wird das alternative CI auf der Seite mit den Standardeinstellungen ausgewählt.






### Konfigurieren Sie Profile und Security Incidents für die FireEye HX -Integration

Nachdem Sie ein Profil erstellt und die FireEye HX -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den definierten Bedingungen aufgerufen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Wählen Sie bei Bedarf ein alternatives Eingabefeld für das Feld Configuration Item (CI) aus, und legen Sie Filterbedingungen fest, damit das Profil automatisch ausgelöst werden kann, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

**Hinweis:**
Sie können zu folgendem Ort navigieren: **Profilkonfiguration** -Seite erst, nachdem Sie eingegeben haben **Profildetails**.

### Prozedur

1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**.
2. Klicken **Weiter** auf der **Profildetails** Seite, nachdem Sie den Abschnitt „Profildetails“ abgeschlossen haben.
3. Überprüfen und konfigurieren Sie die folgenden Abschnitte:
   - **Incident-Kriterien definieren (Automatisierung)**: Definieren Sie die Bedingungen für Security Incidents, die automatisch die FireEye HX -Fähigkeiten für das Profil auslösen. Wenn Sie nicht auswählen **Definiert Incident-Kriterien** Option, dann können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.
     - Auswahlvorgang **Definiert Incident-Kriterien** Option zum automatischen Auslösen von FireEye HX -Fähigkeiten im Profil.
     - In der **Filterbedingungen**, wählen Sie das erforderliche Feld aus.
     - Sie können hinzufügen **Neues Kriterium** und definieren auch die OR- oder AND-Bedingung.

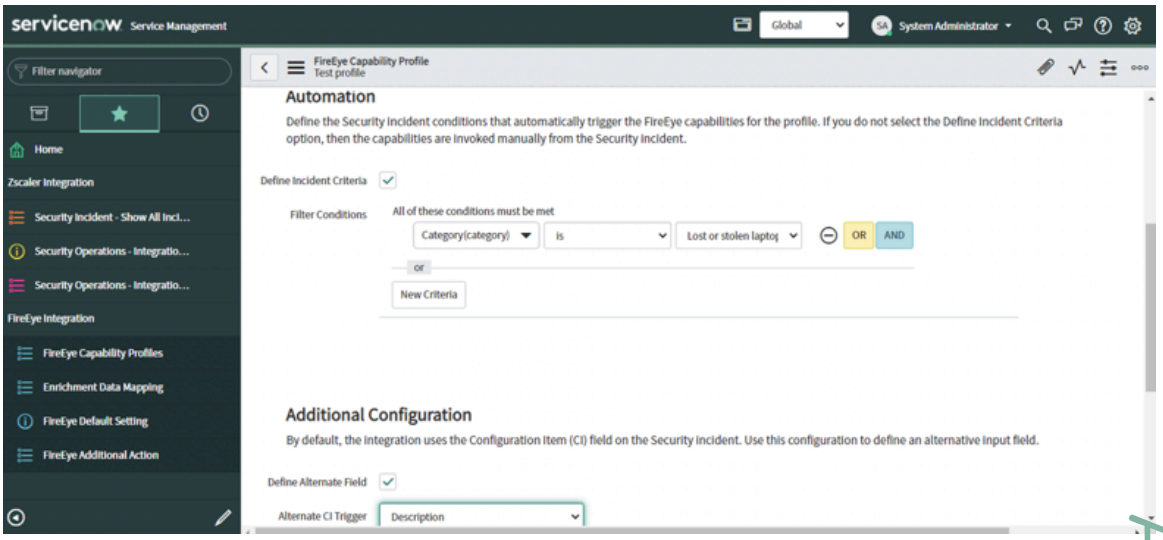
       **Hinweis:**
       „Host isolieren“, „Hostisolierung entfernen“, „Datei abrufen“ kann nicht automatisch ausgelöst werden.

   - **Zusätzliche Konfiguration**: Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um die FireEye HX APIs abzufragen.
     - Rufen Sie die Eigenschaft **Definieren Sie ein alternatives Feld** Option zum Definieren eines alternativen Eingabefelds.
     - Wählen Sie das Eingabefeld aus **Alternatives CI-Auslöserfeld**.

       **Hinweis:**
       Weitere Informationen finden Sie unter Machen Sie sich mit der Funktionsweise von Auslöserbedingungen für ein Konfigurationselement vertraut.

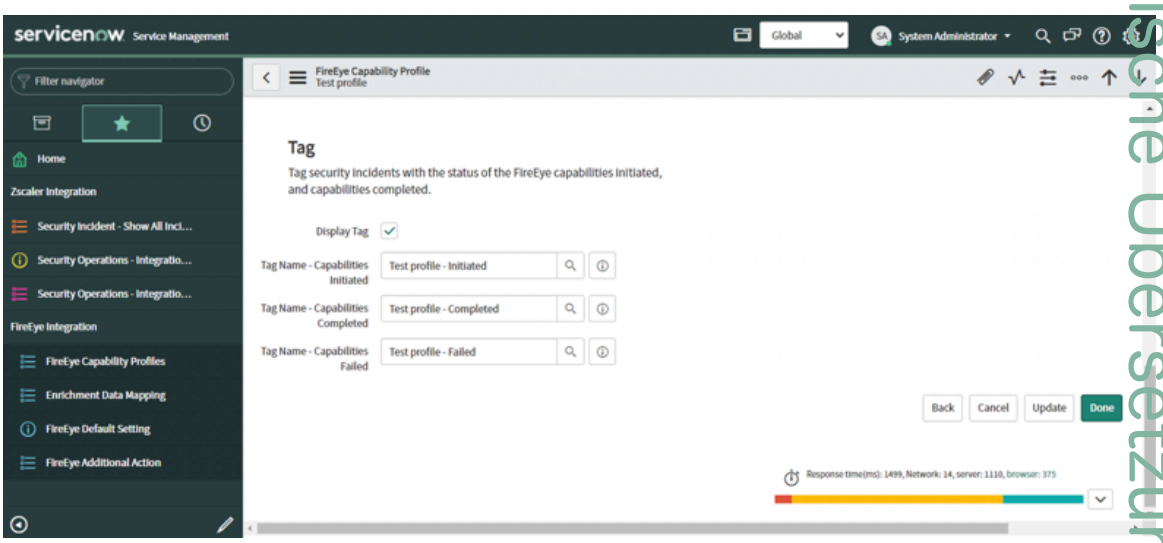


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- **Tags**: Sie können Security Incidents optional mit den Tags FireEye HX Profil initiiert, Profil abgeschlossen und Profil fehlgeschlagen versehen.

  Rufen Sie die Eigenschaft **Tag anzeigen** Kontrollkästchen zum Aktivieren der Kennzeichnung von Security Incidents; Profilname wird bei Aktivierung des Tags vorangestellt. Standardmäßig ist diese Option für alle Profile deaktiviert.

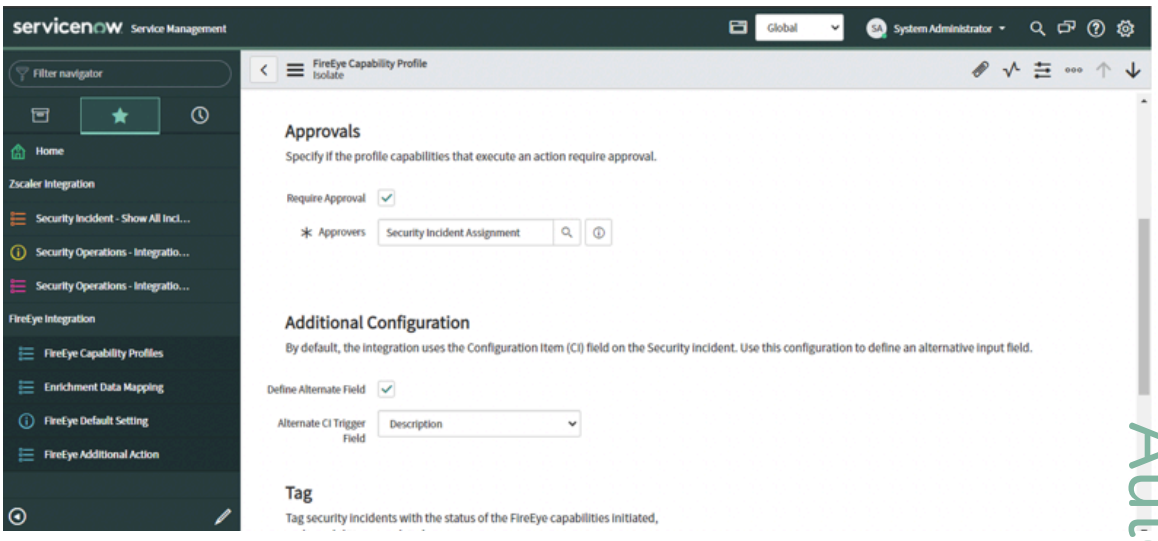



- **Genehmigungen**: Wählen Sie aus **Genehmigung erforderlich** Kontrollkästchen, um eine zusätzliche Steuerungsebene bereitzustellen, wenn die Fähigkeiten FireEye HX zum Isolieren von Hostcomputern, zur Wiederherstellung im Netzwerk und zum Abrufen der Dateien verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Genehmigungsoption in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“, „Hostisolierung entfernen“ und „Datei abrufen“ angezeigt.




4. Klicken Sie auf **Erledigt**.
5. Überprüfen Sie die Auslösebedingungen FireEye HX.

### Überprüfen Sie die Auslöserbedingungsfilter

Testen Sie das Profil, und stellen Sie sicher, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

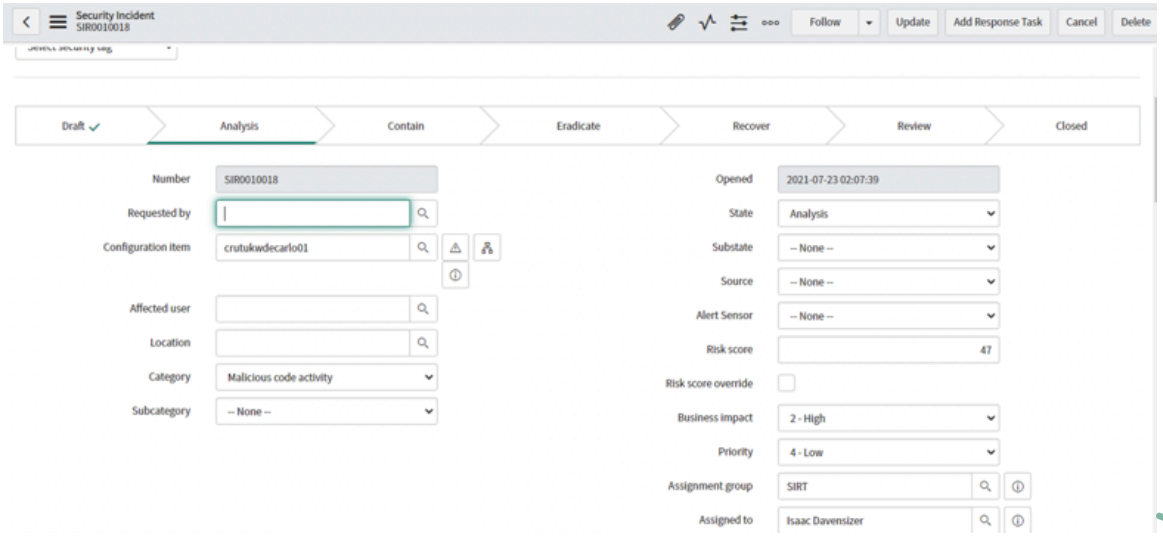
Sobald Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Now Platform Security Incidents anzeigen.

### Prozedur

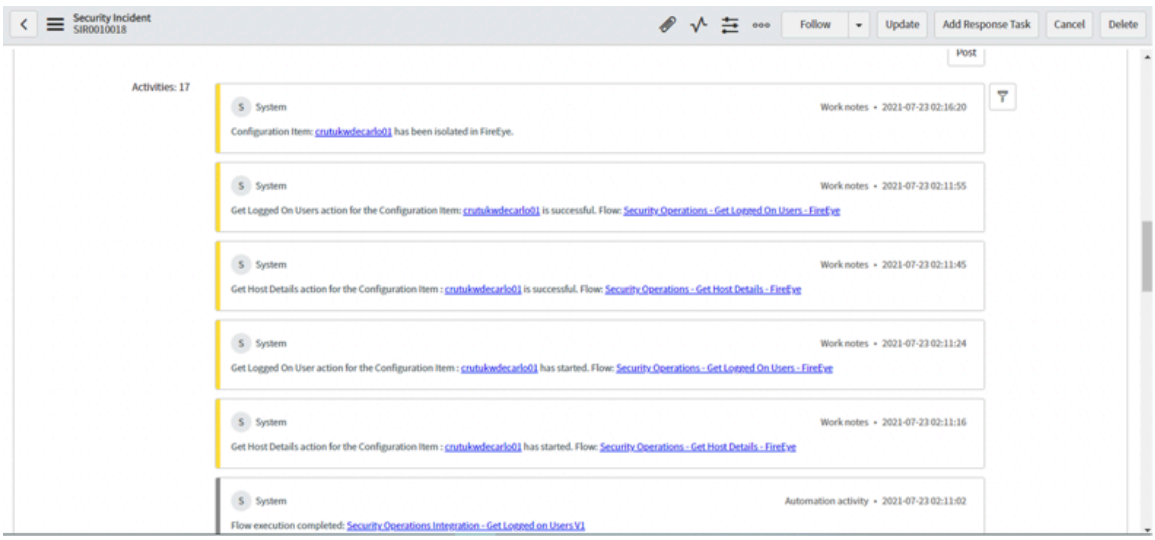
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Auswahlvorgang **Neu** , um einen neuen Security Incident zu erstellen.
3. Geben Sie die im Fähigkeitsprofil angegebenen Filterbedingungen an, um das entsprechende Profil auszulösen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Klicken **Speichern**.




**5.** Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.

**6.** Zeigen Sie die Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ an.

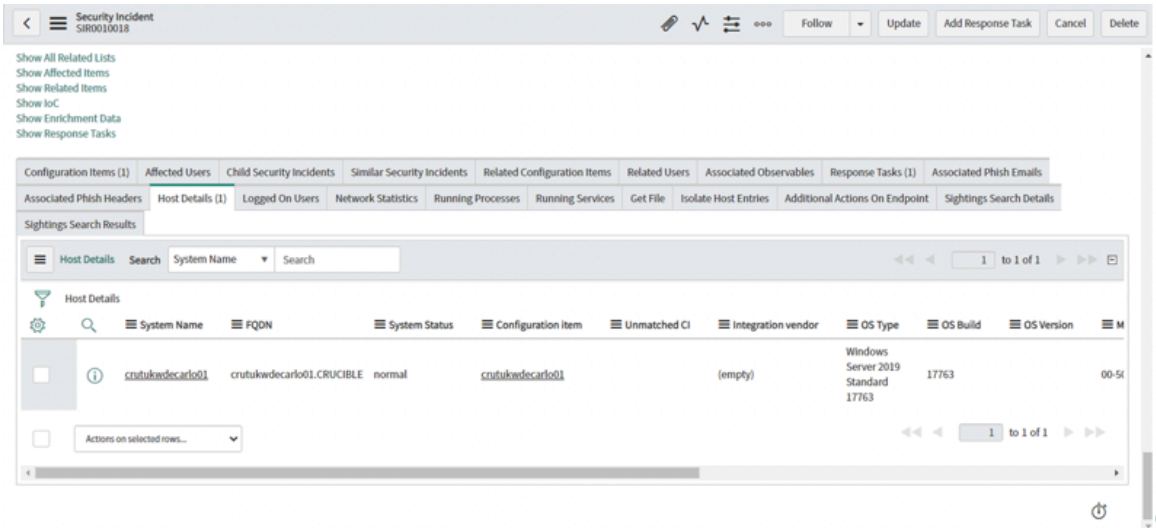
**7.** Klicken **Alle zugehörigen Listen anzeigen**.

**8.** Klicken Sie auf eine beliebige zugehörige Liste (Registerkarte).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Hostdetails.




## Lösen Sie ein FireEye-Fähigkeitsprofil über Zugehörige Links aus

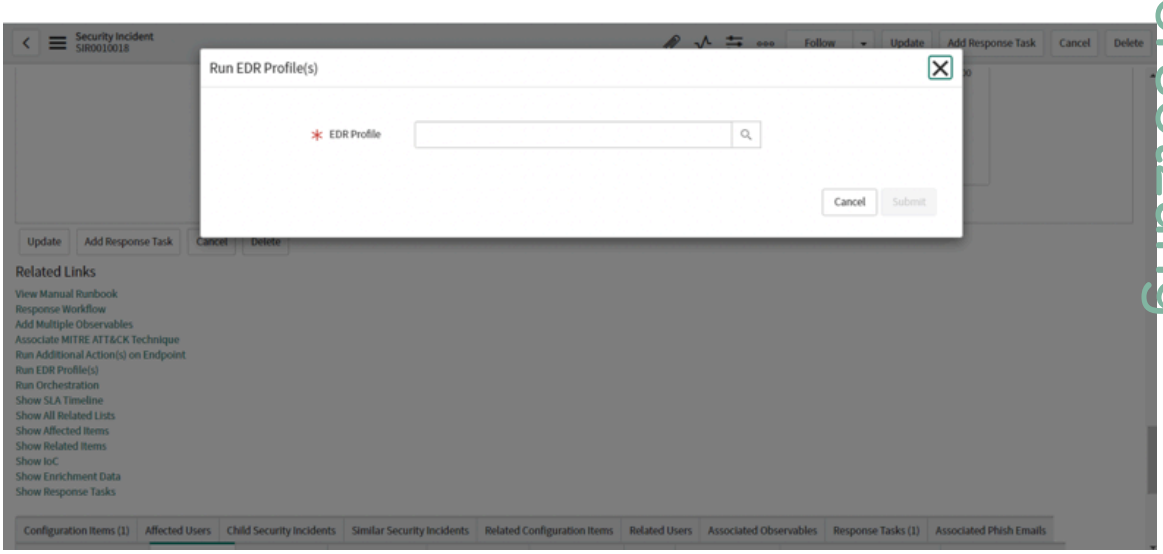
Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

### Prozedur

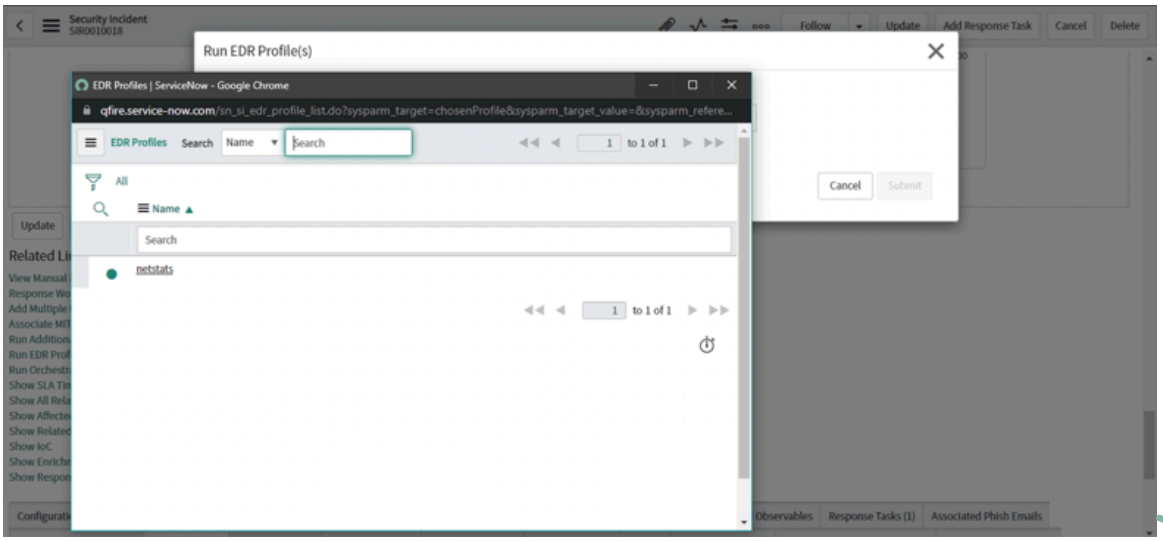
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie überprüfen möchten.
3. Klicken **EDR-Profil(e) ausführen**im Abschnitt „Zugehörige Links“.

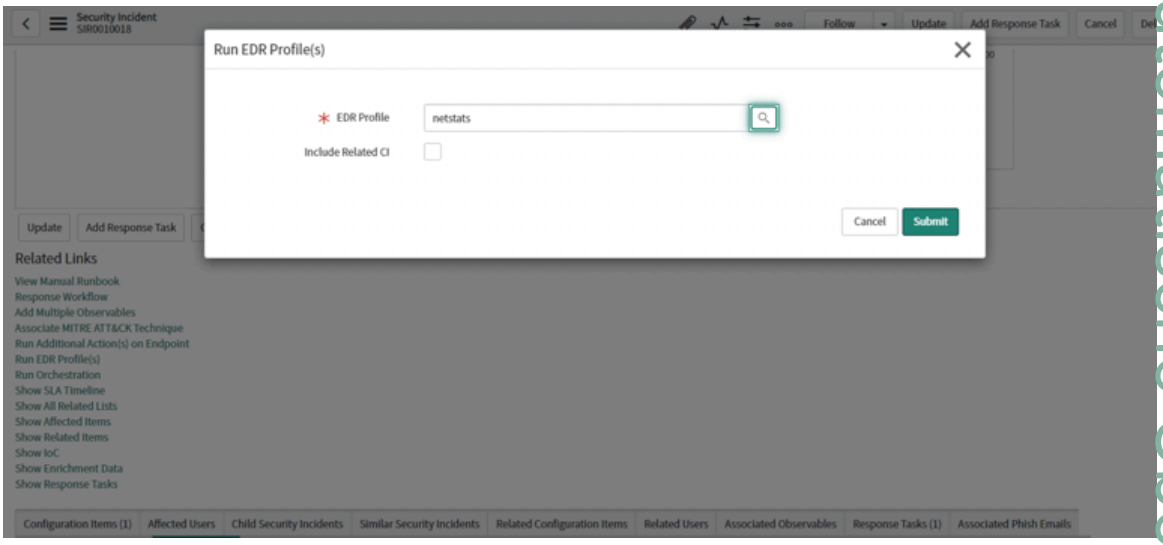



4. Suchen Sie ein Profil, wählen Sie es aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Das ausgewählte Profil wird manuell ausgelöst.
6. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
7. Zeigen Sie die Tags an, und überprüfen Sie die zugehörigen Listen auf die Daten.

**Hinweis:**
Zusätzlich zur Ausführung des Profils für das CI oder das alternative CI des Security Incident können Sie auch das Profil für CI-Werte ausführen, die in der zugehörigen Liste Configuration Item vorhanden sind, indem Sie im Dialogfeld die Option Include Related CI (Zugehöriges CI einbeziehen) aktivieren. Dadurch werden auch Daten für die CI-Werte abgerufen, die in der zugehörigen Liste vorhanden sind. Alternativ können Sie das Profil nur für die in der zugehörigen Liste enthaltenen CI-Werte ausführen.

### Lösen Sie ein FireEye-Fähigkeitsprofil aus der zugehörigen Liste „Konfigurationselement“ aus

Lösen Sie ein Fähigkeitsprofil manuell aus der zugehörigen Liste des Konfigurationselements aus.

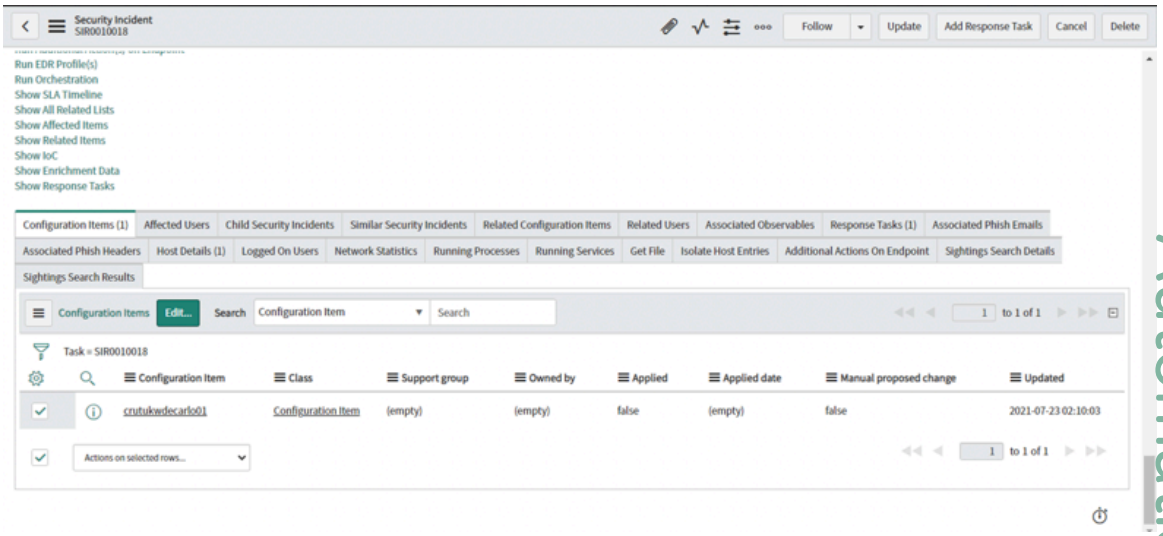
**Vorbereitungen**
Erforderliche Rolle: sn_si.admin, sn_si.analyst

Automatische Übersetzung

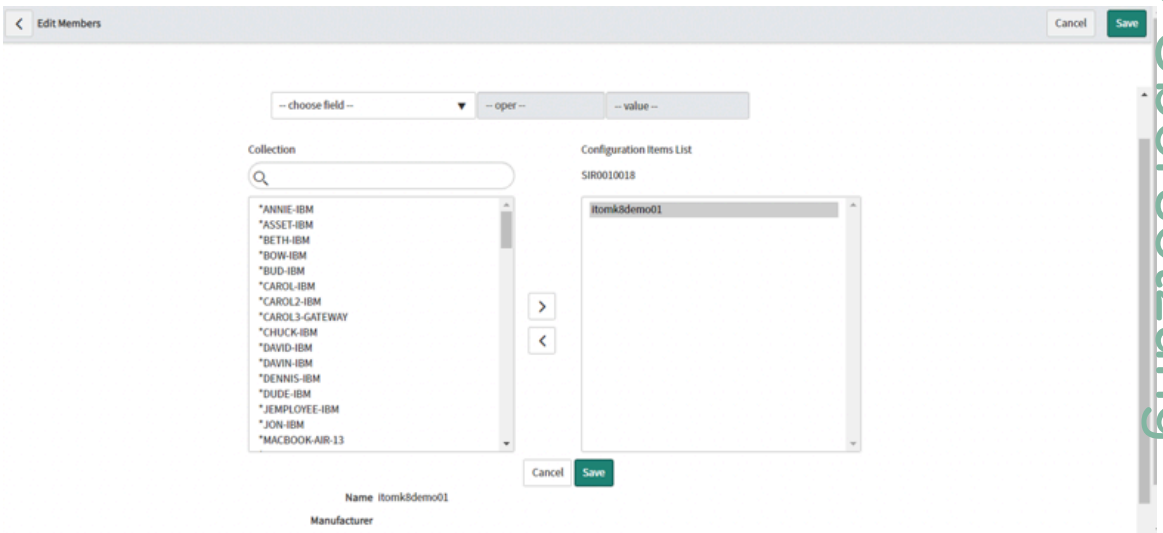
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen FireEye HX.
3. Klicken **Alle zugehörigen Listen anzeigen** im Abschnitt „Zugehörige Listen“
4. Klicken Sie auf die Schaltfläche **Konfigurationselement** Zugehörige Liste.



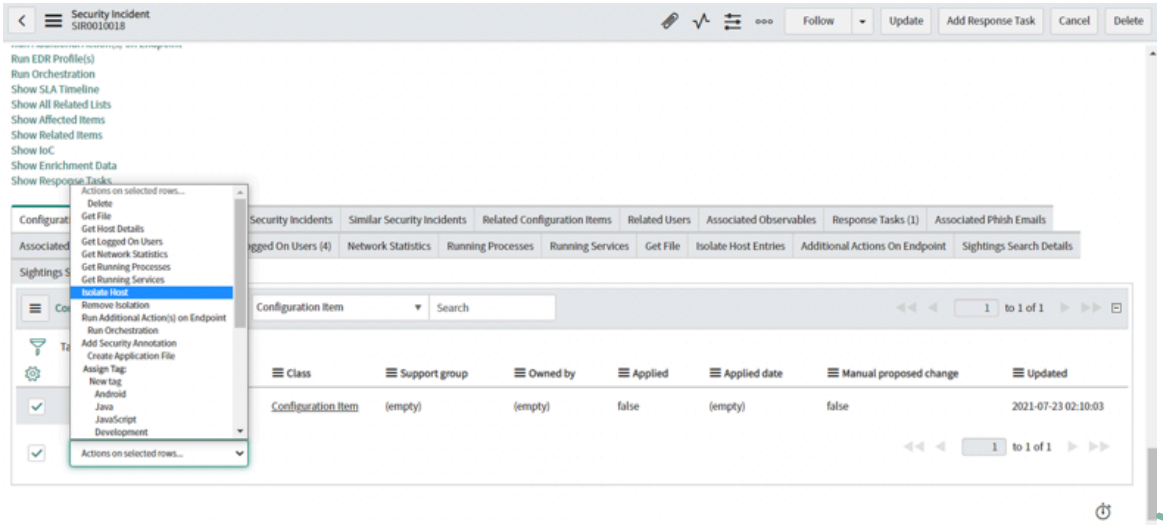

5. Klicken **Bearbeiten** , um die verfügbaren Konfigurationselemente hinzuzufügen, wenn noch keine Werte vorhanden sind, und klicken Sie auf **Speichern**.




6. Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen eine Fähigkeit aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**7.** Die ausgewählte Fähigkeit wird manuell ausgelöst.

**8.** Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.

**9.** Zeigen Sie die Tags an, und überprüfen Sie die Daten in den zugehörigen Listen.

### FireEye – Fähigkeit „Datei abrufen“

Dateierfassungsanforderungen weisen einen Endpoint Security Agent an, eine Datei von seinem Host-Endpunkt abzurufen. Dateibeschaffungen werden für die statische oder dynamische Analyse potenzieller oder verifizierter Gefährdungen sowie für die Aufbewahrung von Nachweisen bei Untersuchungen interner Bedrohungen verwendet. Die Fähigkeit „Datei abrufen“ muss als separates Profil erstellt werden.

#### Vorbereitungen

Erforderliche Rolle: admin

Auslösen von Dateiprofil abrufen und Fähigkeitsprofil FireEye HX erstellen mit **Datei abrufen** -Fähigkeit.

#### Prozedur

**1.** Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.

**2.** Wählen Sie den Security Incident aus, den Sie überprüfen möchten.

**3.** Klicken **EDR-Profil(e) ausführen**im Abschnitt „Zugehörige Links“.

**4.** Durchsuchen und Dateiprofil abrufen aus der Liste der verfügbaren Profile auswählen.

**5.** Geben Sie die an **Dateiname** und **Dateipfad**.

> **Hinweis:**
> Geben Sie den Namen der Datei ein, für die Sie erfassen möchten. Geben Sie einen genauen Pfadnamen oder eine andere geeignete pfadbasierte Windows-Umgebungsvariable an. Sie müssen den Laufwerksbuchstaben oder die Pfadnamen angeben. Verschiedene Endpunkte können unterschiedliche Laufwerkszuordnungen haben. Wenn Sie explizit einen Ordnernamen angeben, können Sie den Pfad mit einem umgekehrten Schrägstrich beenden. Der letzte umgekehrte Schrägstrich ist jedoch nicht obligatorisch.

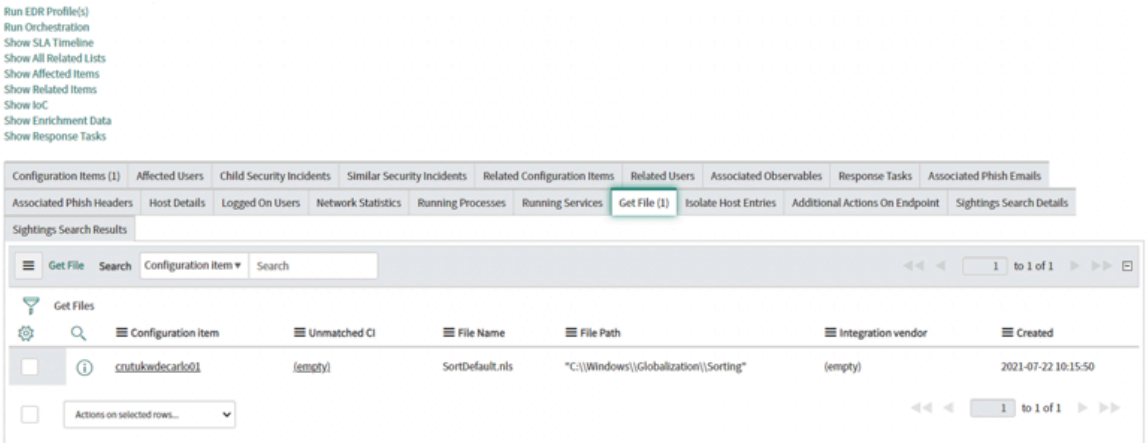
**6.** Klicken **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und überprüfen Sie die Ergebnisse im **Datei abrufen** Zugehörige Liste.

**Hinweis:**
Das Profil „Datei abrufen“ wird jetzt manuell ausgelöst.




**So überprüfen Sie die Beschaffung einer heruntergeladenen Datei:**

- Öffnen Sie die ZIP-Datei für die Dateibeschaffung.
- Geben Sie das zum Öffnen der Datei erforderliche Passwort ein. Das Passwort kann angezeigt werden, indem der Mauszeiger über den Download-Link in der FireEye HX -Konsole bewegt wird. Führen Sie die folgenden Schritte aus, um das Passwort anzuzeigen:
  - Melden Sie sich bei der FireEye HX-Konsole an.
  - Navigieren zu **Akquisitionen** und filtern Sie nach Beschaffungstyp – Datei.
  - Wählen Sie den gewünschten Datensatz aus.

    **Hinweis:**
    Sie können die Details der erfassten Datei auf der rechten Registerkarte anzeigen.

  - Bewegen Sie den Mauszeiger über das **Herunterladen** Link oben verfügbar, um das Passwort zu erhalten.

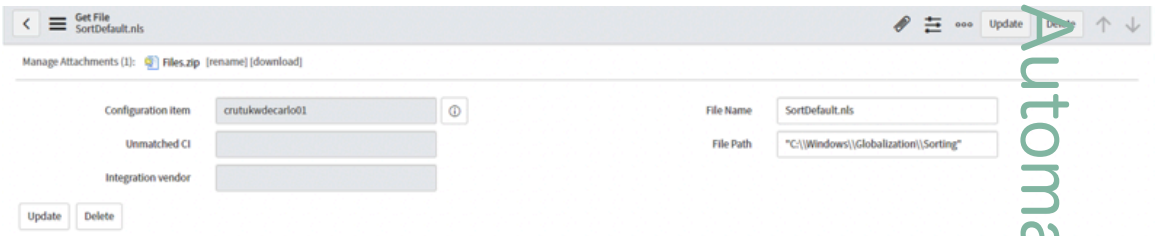


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

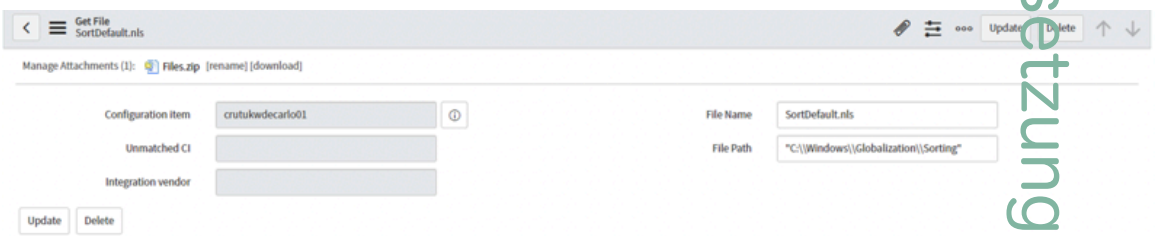
- Öffnen und überprüfen Sie die Dateien in der ZIP-Datei mit einem beliebigen Text- oder XML-Editor.

**Hinweis:**

- Es wird empfohlen, die abgerufene Datei manuell als erkennbares Element hinzuzufügen, damit sie als Beweis für den Security Incident nachverfolgt werden kann. Dies hilft auch, die Dateien in Zukunft anzuzeigen, wenn das Passwort vergessen oder geändert wird.
- Die maximale Dateigröße, die für die Aktion „Datei abrufen“ unterstützt wird, beträgt 1024 MB. Dieser Wert kann durch Ändern von konfiguriert werden **com.glide.attachment.max_size**, und die Standardzeitüberschreitung beträgt 60 Minuten und kann auf der Seite FireEye HX „ Standardeinstellungen“ konfiguriert werden.




- „Datei abrufen“ kann auch über die zugehörige Liste „Configuration Item“ ausgelöst werden.




Automatische Übersetzung

### Zusätzliche FireEye-Aktionen für Endpunkt

Die FireEye-Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Goldstandardaktionen hinausgehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktionen umfassen Selektierungsakquise und Datenakquisitionen. Standardmäßig werden zwei Datenerfassungen unterstützt:

- Umfassendes Skript für Untersuchungsdetails
- Standardskript für Untersuchungsdetails

Darüber hinaus wird Selektierungsakquise ebenfalls standardmäßig unterstützt. Alle diese drei werden standardmäßig zusammen mit der Quelle erstellt. Kunden können auch eigene Aktionen erstellen, z. B. Datenerfassungen aus dem FireEye-Modul „Zusätzliche Aktionen“.[1] Die maximale Dateigröße, die für zusätzliche FireEye-Aktionen unterstützt wird, beträgt 1024. Dieser Wert kann durch Ändern von konfiguriert werden **com.glide.attachment.max_size**, und die Standardzeitüberschreitung beträgt 120 Minuten und kann auf der FireEye-Seite „Standardeinstellungen“ konfiguriert werden.

### Umfassendes Skript für Untersuchungsdetails

Ermöglicht das Sammeln aller forensischen und untersuchenden Artefakte vom Endpunkt, ist jedoch die teuerste Option. Diese Konfiguration ist ideal für Situationen, in denen nur ein Fenster zum Sammeln von Daten vom betreffenden Endpunkt vorhanden ist und die Möglichkeit, weitere Daten zu erfassen, später nicht garantiert werden kann. Verwenden Sie diese Aktion daher mit Vorsicht.

### Standardskript für Untersuchungsdetails

Aktiviert die gängigsten Optionen zum Sammeln forensischer und untersuchender Artefakte von einem Endpunkt. Ist als primäres Antworttool gedacht, wenn Sie den Verdacht haben, dass ein Endpunkt gefährdet sein könnte, und eine eingehende Analyse dieses Endpunkts durchführen müssen. Ziel ist es, ein Gleichgewicht zwischen der Erfassung der relevantesten und wertvollsten Daten zu erreichen und gleichzeitig die kostspieligen Optionen zu vermeiden, die später erfasst werden können, wenn sich weitere Untersuchungen als erforderlich erweisen.

### Selektierung – Akquisition

Selektierungssammlungen enthalten Informationen aus dem Lookback-Cache sowie zusätzliche forensische Audit-Informationen, z. B. URL-Downloadverlauf, Dateidownloadverlauf, Prozess- und Portlisten und Standardsysteminformationen. Möglicherweise möchten Sie solche Informationen untersuchen, wenn anomaler Netzwerkdatenverkehr erkannt wird, und Sie möchten mehr Transparenz in Endpunktaktionen.

### Datenerfassungsskripts in FireEye verwalten

Datenerfassungsanforderungen (manchmal auch als Live-Antwortanforderungen bezeichnet) ermöglichen es Ihnen, alle benötigten Daten von einem einzelnen ausgeführten Endpunkt zu erfassen. Auf der Seite „Datenerfassungsskripts“ in FireEye können Sie die für Datenerfassungsanforderungen verwendeten Datenerfassungsskripts erstellen, bearbeiten, kopieren und löschen.

### Zugriff auf die Seite „Datenerfassungsskripts“ in FireEye

So greifen Sie auf die Seite „Datenerfassungsskripts“ zu:

1. Navigieren Sie zu Endpunktsicherheit Webbenutzeroberfläche.
2. Wählen Sie im Menü „Administrator“ die Option Datenerfassungsskripts aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erstellen eines Skripts in FireEye

So erstellen Sie ein Datenerfassungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** -Menü der Endpoint Security-Webbenutzeroberfläche.
2. Klicken **Skript erstellen**.
3. Geben Sie einen Namen für das neue Skript in ein **Skriptname** an.
4. Geben Sie optional eine Beschreibung des Skripts ein.
5. Wählen Sie das Betriebssystem aus, für das das Skript gilt. Sie können im Dialogfeld „Skript erstellen“ nur ein einzelnes Betriebssystem auswählen.
6. Klicken **Erstellen** , um die Skriptdefinition zu starten.
7. Wählen Sie im einen Beschaffungsdatentyp aus **Fügen Sie einen Beschaffungstyp hinzu**Dropdown-Feld und klicken Sie auf **Hinzufügen**. Optionen für den angeforderten Beschaffungstyp werden rechts neben der Skriptliste angezeigt.
8. Geben Sie Werte für die Optionen des Beschaffungstyps an, oder verwenden Sie die bereits ausgewählten Standardwerte. Die Web-UI warnt Sie nicht und entfernt in Ihren Spezifikationen keine Tabulatoren, Leerzeichen oder unerwünschte Zeichen (z. B. \n).
9. Wiederholen Sie die vorherigen 2 Schritte, um zusätzliche Daten für das Datenerfassungsskript anzufordern. Einige Beschaffungsdatentypen sind nur einmal für ein Skript verfügbar, während andere mehrmals angegeben werden können. Nach dem Hinzufügen eines Beschaffungstyps zu einem Skript wird die Liste der im verfügbaren Beschaffungstypen angezeigt **Fügen Sie einen Beschaffungstyp hinzu**Dropdown-Feld wird entsprechend angepasst.
10. Um einen Beschaffungsdatentyp aus dem Skript zu entfernen, klicken Sie auf der Registerkarte „Beschaffung“ auf der linken Seite der Seite auf das x-Symbol ( ).

**Hinweis:**
Diese Integration unterstützt nicht **Lassen Sie Bearbeitungen vor dem Erfassen zu** Option beim Erstellen von Skripts. Stellen Sie daher sicher, dass das Kontrollkästchen deaktiviert ist.

## Exportieren eines Skripts aus FireEye

Sie können ein Datenerfassungsskript in eine JSON-Datei exportieren. So exportieren Sie ein Datenerfassungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** der Webbenutzeroberfläche von Endpoint Security.
2. Wählen Sie im Menü „Administrator“ die Option Datenerfassungsskripts aus.
3. Wählen Sie links auf der Seite das Skript aus, das Sie exportieren möchten.
4. auswählen **Aktionen** > **Skript exportieren**.
5. Eine JSON-Datei wird auf Ihren Computer heruntergeladen. Der JSON-Dateiname enthält das Betriebssystem, sodass Sie leicht bestimmen können, welche Skripts für welches Betriebssystem gelten.

## Erstellen einer neuen Datenerfassungsaktion in Now Platform

Führen Sie die folgenden Schritte aus, um eine neue Aktion zu erstellen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **FireEye-Integration** > **FireEye: zusätzliche Aktionen**. Die Liste „FireEye – Zusätzliche Aktionen“ wird angezeigt.
2. Klicken **Neu**. Das Formular für die neue Aktion wird angezeigt.
3. Füllen Sie das Formular aus.

| | |
|---|---|
| Aktionsname | Name der ausgeführten FireEye-Aktion. Dieser Name hilft Ihnen, den Aktionstyp zu identifizieren und zu beschreiben. |
| Akquisition | Eine Akquisition erhält die zu analysierenden Daten. Dies ist ein schreibgeschütztes Feld, das standardmäßig auf Datenerfassung festgelegt ist. |
| Quelle | Name der FireEye-Quelle Nur konfigurierte Quellen sind in der Auswahlliste verfügbar. |
| Fähigkeit | Dies ist ein schreibgeschütztes Feld, das mit der Fähigkeit „Zusätzliche Aktion(en) ausführen“ ausgefüllt wird |
| Akquisitionstyp | Typ der Beschaffungsaktion, die abgerufen und analysiert werden muss. |
| Aktiv | Dies zeigt an, dass die Aktion aktiv ist. |
| Genehmigung erforderlich | Wenn Sie die Option Genehmigung erforderlich aktivieren, ist das Feld Genehmiger im Formular verfügbar. Nachdem Sie eine Anforderung gesendet haben, ist eine Genehmigung durch die Gruppe erforderlich, um die Anforderung abzuschließen. |
| Tag anzeigen | Typ des Betriebssystems wie Windows, Mac, Linux zum Hinzufügen von Skripts.<br>**Hinweis:**<br>Derzeit wird nur ein Betriebssystemtyp unterstützt. Sie können eine Aktion pro Betriebssystem erstellen. Erstellen Sie für andere Betriebssysteme nach Bedarf neue Aktionen. |
| Skripts | Das aus FireEye importierte Skript muss für den ausgewählten Betriebssystemtyp bereitgestellt werden. Jedem Betriebssystemtyp kann nur ein Skript hinzugefügt werden. |

4. Klicken **Absenden**.

## Auslösen von Datenerfassungen aus Security Incident

Die erstellten zusätzlichen Aktionen können über den aufgerufenen zugehörigen Link ausgeführt werden **Zusätzliche Aktion(en) für Endpunkt ausführen** für den Security Incident.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
**Lassen Sie Bearbeitungen vor dem Erfassen zu** Die FireEye-Funktionalität wird für „Zusätzliche Aktionen“ für Endpunkt nicht unterstützt.

### Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche mit der FireEye-Integration

Konfigurieren Sie das Sichtungssuchprofil mit dem folgenden Verfahren.

#### Vorbereitungen

Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

Bei jeder Erstellung einer Quelle werden einzelne Sichtungssuchkonfigurationen für fünf Typen (Datei, IPs (v4), MD5, SHA1 und SHA256) erstellt und standardmäßig inaktiv. Sie sollten sie aktivieren, bevor Sie die Sichtungssuche verwenden. Jeder erkennbare Typ hat eine andere Suchabfrage, um Sichtungen abzurufen. Wir würden für jeden erkennbaren Typ eine andere Suche initiieren. Die Suche nach mehreren erkennbaren Elementen für eine Sichtungssuche ist in FireEye nicht möglich, da dies einen UND-Vorgang für die erkennbaren Elemente ausführen würde und das Ergebnis möglicherweise ungenau ist.

**Hinweis:**
Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Die verbleibenden werden in die Warteschlange gestellt und beginnen nach Abschluss einer der laufenden Sichtungen.

Wenn Sie ein neues Sichtungssuchprofil erstellen möchten, führen Sie die folgenden Schritte aus, um eines zu erstellen:

#### Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche – Konfiguration**.
2. Klicken **Neu**.
3. Füllen Sie die Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Name für das Fähigkeitsprofil. |
| Ist gespeicherte Suche | Dadurch wird eine gespeicherte Suche ausgeführt, d. h. das Feld „Name“ muss mit dem Namen der gespeicherten Suche übereinstimmen. |
| Sichtungssuchquelle | Definiert die für die Integration konfigurierte Quelle. |
| Suchen | Fügen Sie eine native Suchzeichenfolge hinzu, um eine Abfrage zu erstellen. |
| Aktiv | Abfrage wird nur ausgeführt, wenn sie aktiv ist. |
| Erkennbarer Typ | Definiert den Typ der erkennbaren Kategorie. |
| Maximale erkennbare Elemente pro Suche | Die Anzahl der erkennbaren Elemente bevor die Suchabfrage in mehrere Abfragen aufgeteilt wird. Legen Sie diesen Wert für diese Integration auf 1 fest. |
| Sichtungssuchparameter | Verwenden Sie Sichtungssuchparameter, um komplexere Abfragen zu definieren, die Logik und |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden. |

4. Klicken **Absenden** , um die Konfiguration abzuschließen.

### Rufen Sie die Sichtungssuche aus einem Security Incident auf

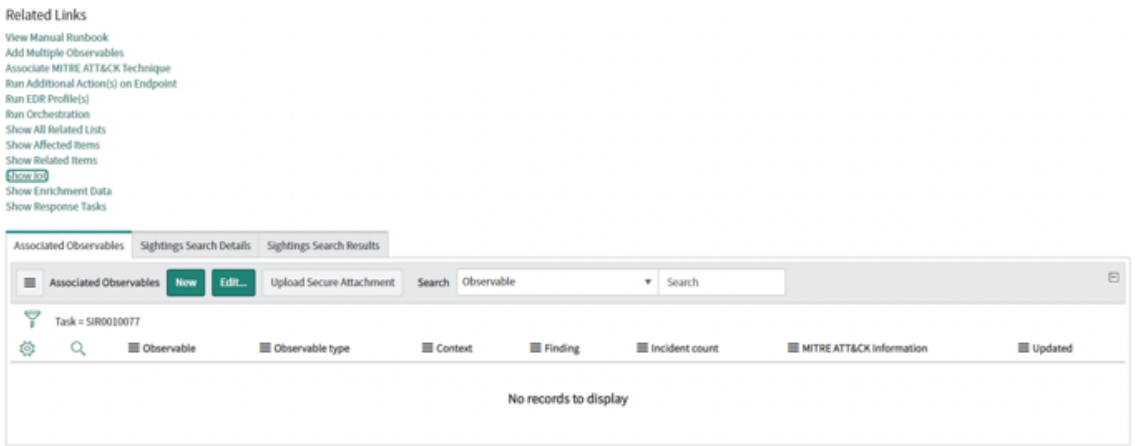
Rufen Sie die Sichtungssuche aus einem SIR-Security Incident auf, indem Sie das folgende Verfahren ausführen.

### Vorbereitungen

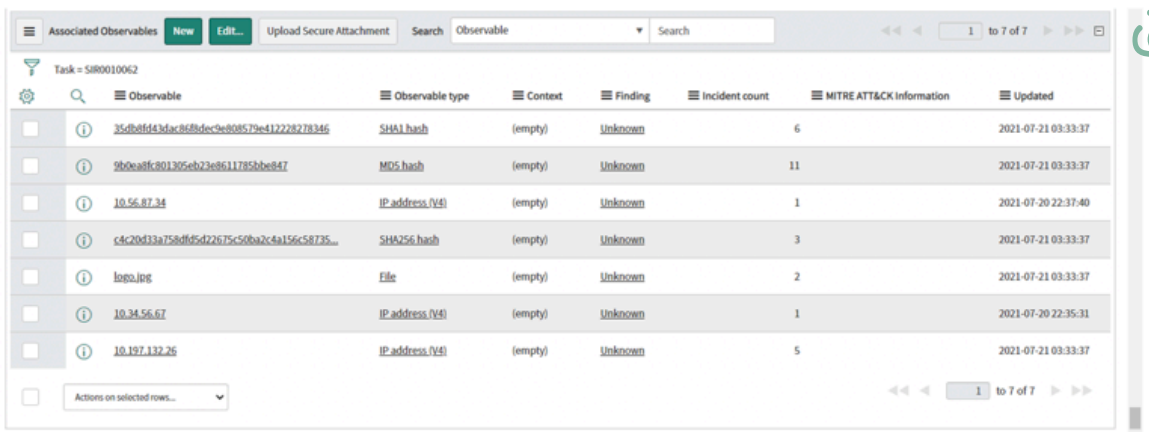
Erforderliche Rolle: Now Platform-Administrator (sn_si.admin)

### Prozedur

1. Navigieren Sie zu Security Incidents.
2. Öffnen Sie eine vorhandene SIR, oder erstellen Sie eine neue SIR.
3. Klicken Sie auf IoC in zugehörigen Links anzeigen.
4. Klicken **Zugehörige erkennbare Elemente** Zugehörige Listen.



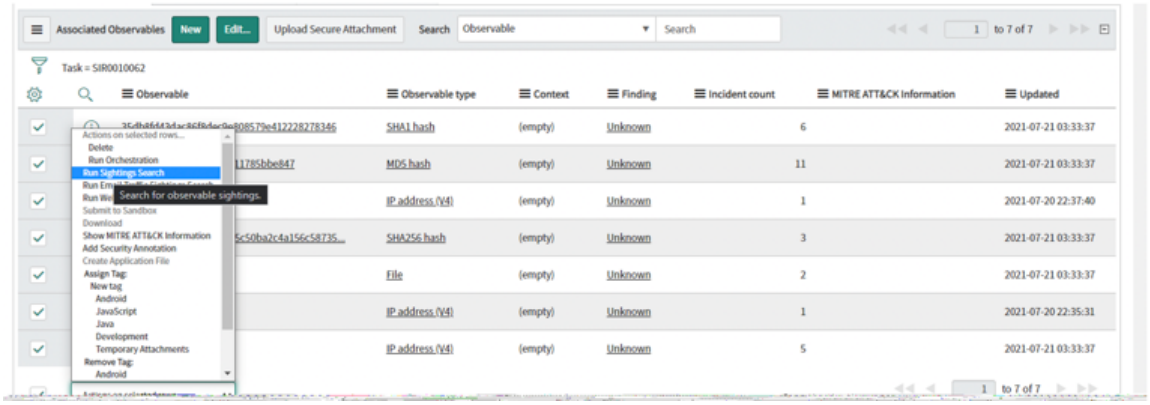

5. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie ein neues erkennbares Element.



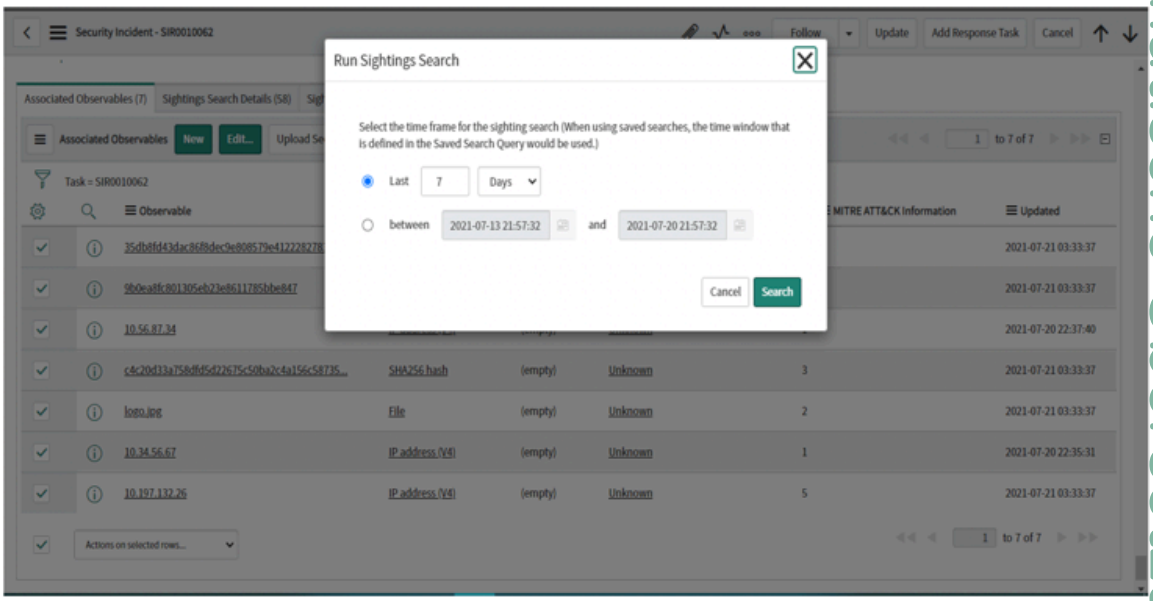

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie die erkennbaren Elemente aus, und klicken Sie unter Aktionen für ausgewählte Zeilen auf **Führen Sie eine Sichtungssuche aus**.



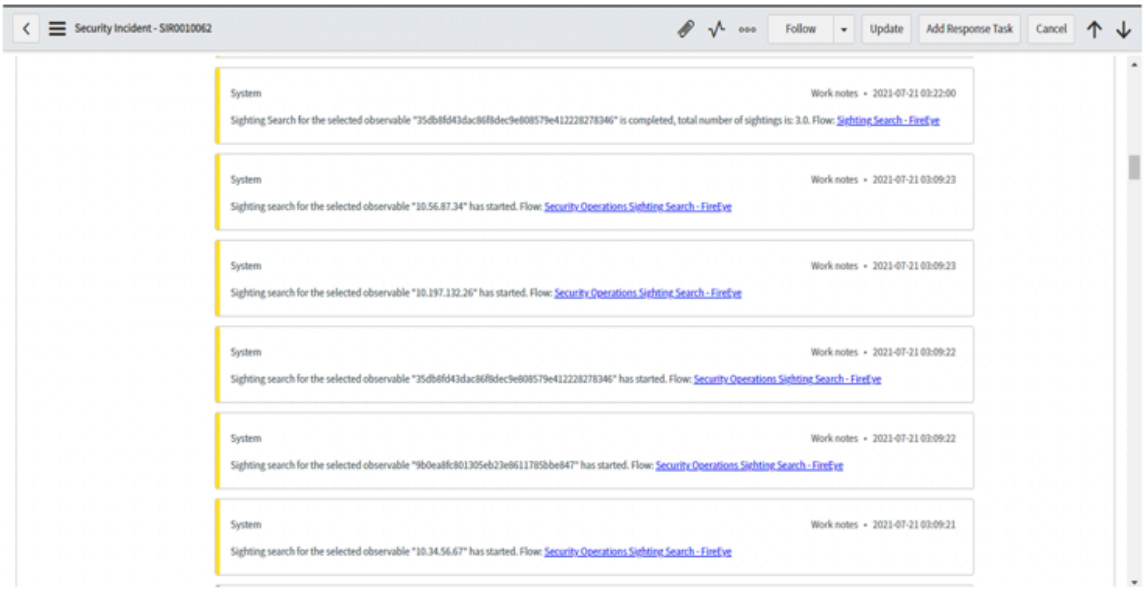

7. Ignorieren Sie die Eingaben im nächsten Dialogfeld, in dem Zeitdaten abgefragt werden.
Es sind Standardwerte ausgefüllt. Die Suche wird jedoch in Echtzeit durchgeführt, und die Zeitwerte werden für diese Integration ignoriert.




8. Überprüfen Sie die Arbeitsnotizen auf den Status.

Automatische Übersetzung

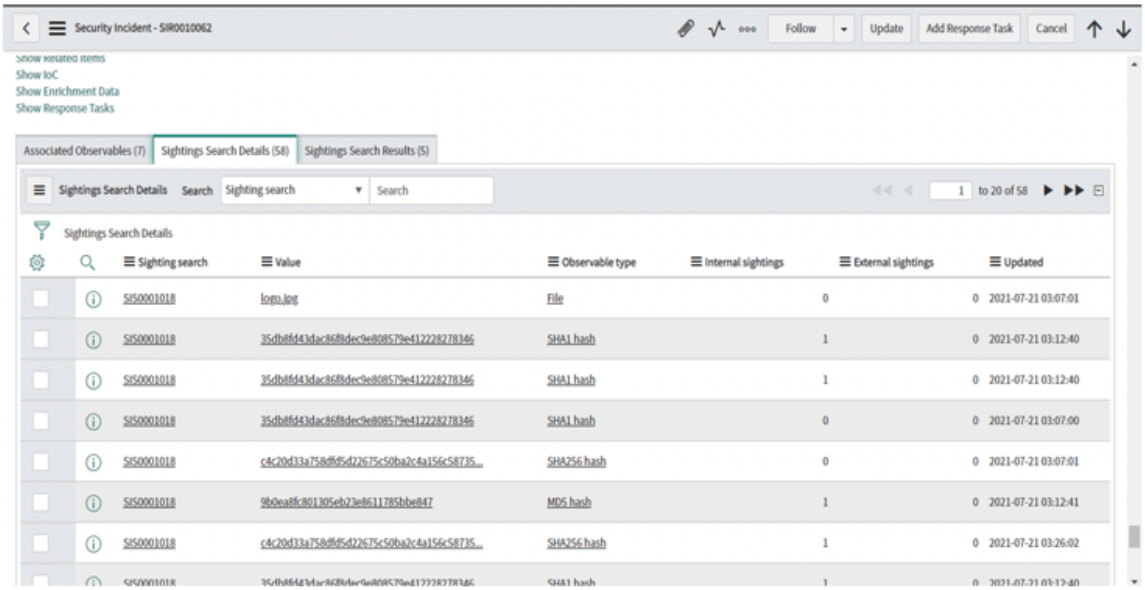
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

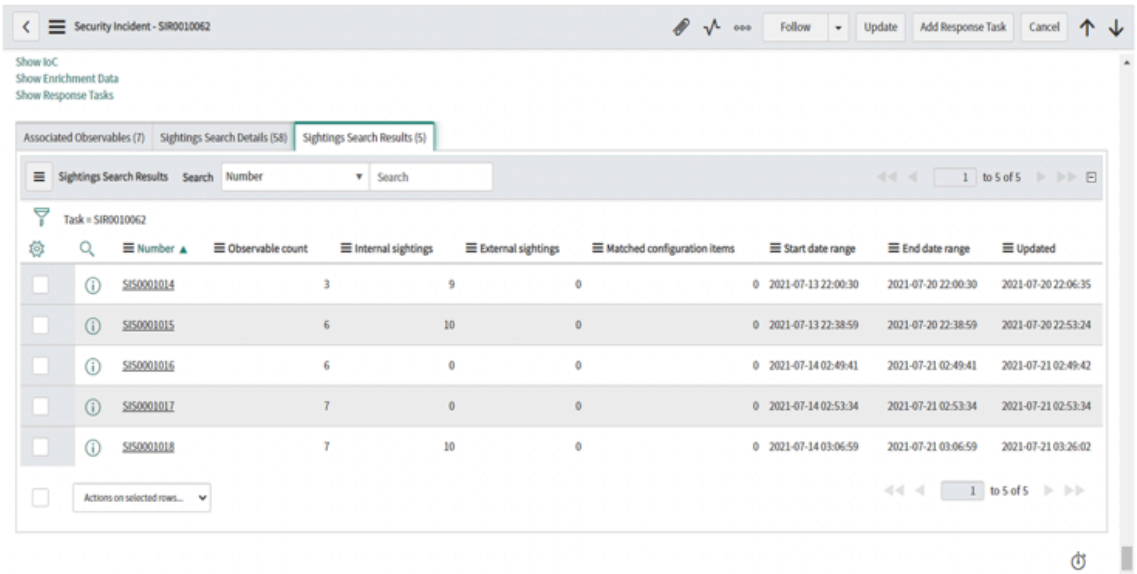



9. Überprüfen Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie auf **Details einer Sichtungssuche** Registerkarte für Details und **Ergebnisse von Sightings Search** Registerkarte für Suchergebnisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Integration „Have I Been Pwned?“

Mit der Security Operations Have I Been Pwned? -Integration können Sie Suchvorgänge für Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob die personenbezogenen Daten von Benutzern durch Datenschutzverletzungen gefährdet wurden.

| | |
|---|---|
| **Erkunden**<br>Security Incident Response-Integrationen | **Einrichten**<br>• Setup der Integration mit Security Operations Have I Been Pwned? .<br>• Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? . |
| **Verwenden** | **Entwickeln** |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| Suchvorgänge für erkennbare Elemente durchführen<br>Workflow „Bedrohungssuche – Have I Been Pwned? “ | • ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer An-wendung installiert wurden |
| **Problembehandlung und Hilfe**<br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Setup der Integration mit Security Operations Have I Been Pwned? .

Have I Been Pwned? ist eine kostenlose Ressource, die verwendet wird, um zu bewerten, ob jemand gefährdet wurde, weil sein Online-Konto bei einer Datenschutzverletzung gefährdet oder „pwned“ war. Die Integration mit Security Operationsist problemlos möglich.

Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509 SSL-Zertifizierung aktualisieren.

Die Plugins Security Incident Response, Threat Intelligenceund Security Operations Have I Been Pwned? sind erforderlich, um die Integration von Security Operations Have I Been Pwned? zu implementieren.

### Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der Security Operations Have I Been Pwned? -Integration, schnell aktivieren und einrichten. Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

### Vorbereitungen

- Das Threat Intelligence -Plugin muss installiert und aktiviert sein, bevor Sie die Security Operations Have I Been Pwned? -Integration verwenden können.

Erforderliche Rolle: sn_si_admin

### Prozedur

Laden Sie die Integration aus dem herunter ServiceNow Store.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? kann jetzt für Suchvorgänge für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zugehörige Informationen**

Suchvorgänge für erkennbare Elemente durchführen

### Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie für die Integration eine SSL-Verbindung benötigen, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.
   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.
   b. Klicken Sie in der Adresszeile auf das Sperrsymbol.
   c. Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.
   d. Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.
   e. Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.
   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
   Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.
2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu**, und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

**Hinweis:**
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .



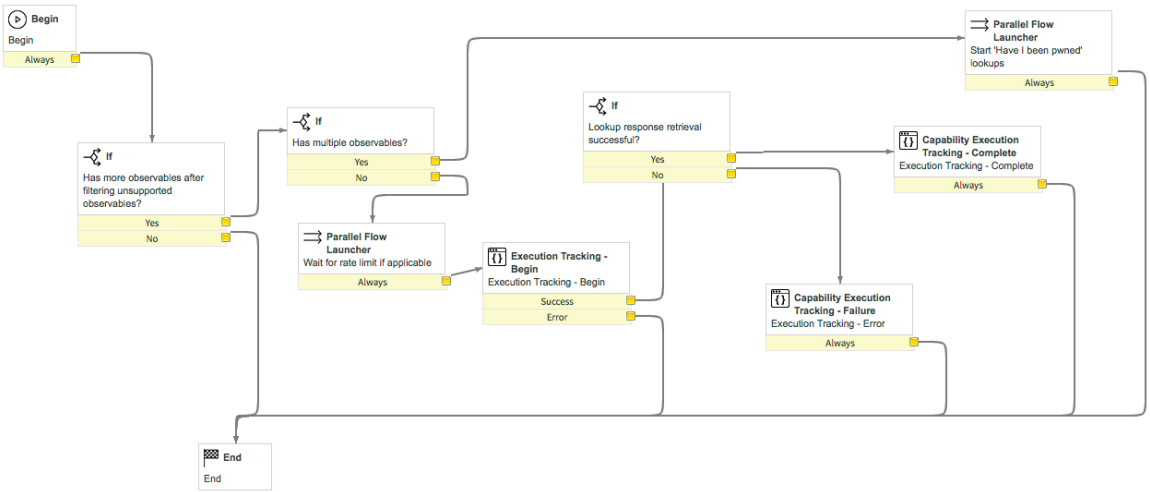
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Workflow „Bedrohungssuche – Have I Been Pwned? “

Der Workflow „Bedrohungssuche – Have I Been Pwned? “ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen um einen von Have I Been Pwned?erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

#### Vorbereitungen
Erforderliche Rolle: sn_si_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von Security Operations-Integration – Funktion „Bedrohungssuche“. ausgelöst, wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen und die Implementierung von Have I Been Pwned? ausgewählt ist. Weitere Informationen finden Sie unter Suchvorgänge für erkennbare Elemente durchführen.




Weitere Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## Integration von HPE Security ArcSight ESM – Email Parser

Die Integration von HPE Security ArcSight ESM - Email Parser wird mithilfe eines E-Mail-Parsers unterstützt, der E-Mail-Benachrichtigungen von ESM verwendet, um Security Incidents zu erstellen.

### Konfigurieren Sie die Integration von HPE Security ArcSight ESM - Email Parser

Die Integration von HPE Security ArcSight ESM – Email Parser verwendet E-Mail-Benachrichtigungen von ESM, um die Ergänzungs- und Antwort-Workflows zu unterstützen.

#### Vorbereitungen
Erforderliche Rolle: sn_si_admin

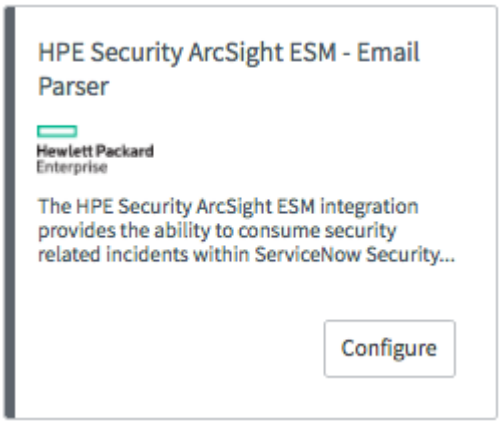
#### Warum und wann dieser Vorgang ausgeführt wird
Für die Integration wird eine Vorlage vom Typ „HPE Security ArcSight ESM – Email Parser“ bereitgestellt. Sie muss vor der Integration konfiguriert und aktiviert werden. Durch Aktualisieren des Parsers wird dieser aktiviert.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




2. Klicken Sie auf der Karte „HPE Security ArcSight ESM – Email Parser“ auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld „ **HPE Security ArcSight ESM – E** -Mail-Analysekonfiguration“ auf den Link **E** -Mail-Analyse konfigurieren.
4. Klicken Sie auf den Link **ArcSight ESM**, um die Einstellungen im bereitgestellten E-Mail-Parser für Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E- Mail ist von aus. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Analyse** “ auf **Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.

## HPE ArcSight Logger -Integration der Incident-Ergänzung

Die Integration HPE ArcSight Logger – Incident-Ergänzung durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

### Erkunden

Security Incident Response-Integrationen

### Einrichten

- Beginnen Sie mit der Integration von HPE ArcSight Logger – Incident-Ergänzung
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

### Verwenden

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungs-such-Workflow
- Security Operations – Arcsight Logger Sichtungs-Workflow
- Sichtungssuchdetails anzeigen
- Sichtungssuchergebnisse anzeigen

### Entwickeln

- ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden

### Problembehandlung und Hilfe



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Beginnen Sie mit der Integration von HPE ArcSight Logger – Incident-Ergänzung

HPE ArcSight Logger streamt Echtzeitdaten, kategorisiert sie in bestimmte Protokolle und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration HPE ArcSight Logger – Incident-Anreicherung verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die API-URL und Anmeldeinformationen hinzufügen.

### Vorbereitungen

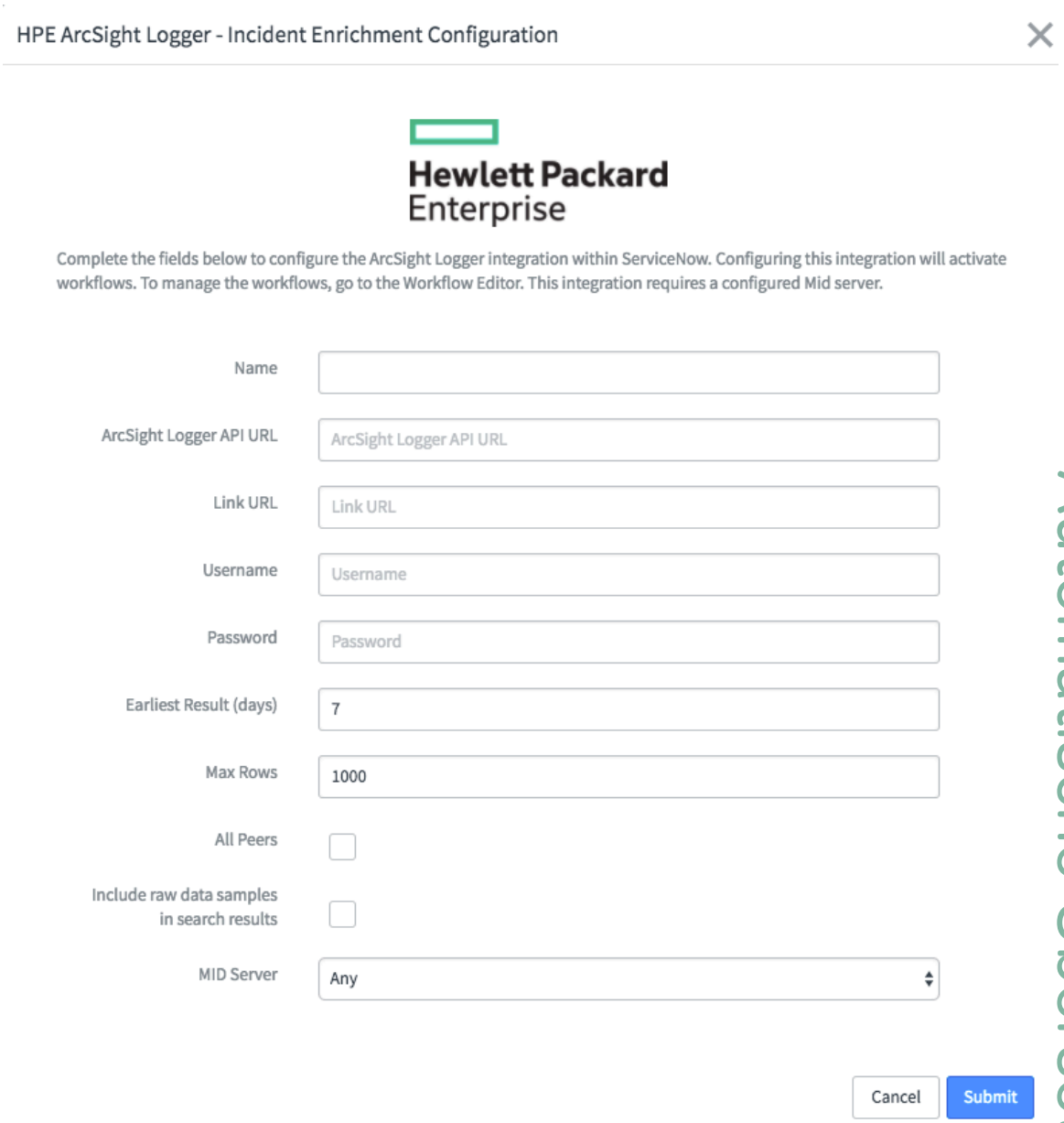
Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie in der Karte HPE ArcSight Logger – Incident-Ergänzung auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Automatische Übersetzung

**4.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Basis-URL der ArcSight Logger-API | Die Basis-URL, die Sie von der HPE Security ArcSight Logger-Website abgerufen haben. |
| Link-URL | [Optional] Die Link-URL, die auf eine HPE Security ArcSight Logger-Instanz verweist, sofern verfügbar. |
| Benutzername | Ihr Intel HPE ArcSight Logger -Benutzername. |
| Passwort | Ihr Intel HPE ArcSight Logger -Passwort. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. |
| Alle Peers | Standardmäßig ist diese Option deaktiviert. Durchsucht wird nur die lokale Protokollierung, mit der Sie verbunden sind. Wenn diese Option aktiviert ist, werden alle Protokollierungen durchsucht, die miteinander verbunden sind. |
| Rohdatenmuster in Suchergebnissen berücksichtigen | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## Integration „Hybrid Analysis“

Die Anwendung Hybrid Analysis ist Teil einer offenen Online-Community, in der Benutzer Dateien und URLs auf Bedrohungen analysieren. Sie teilen Ergebnisse und nutzen Forschungsergebnisse aus der Community, um eine effektivere Reaktion auf Incidents zu ermöglichen. Bei der Integration mit dem Produkt Now Platform Security Operations bietet Ihnen die freigegebene Bedrohungsdaten zusätzliche Einblicke in den Schweregrad bestimmter erkennbarer Elemente.

Die Hybrid Analysis -Integration führt Bedrohungssuchen für die folgenden erkennbaren Elemente durch:

- Datei-Hashes
- IP-Adressen
- URLs

Der Workflow sucht nach neuen erkennbaren Elementen, sobald sie in Security Incidents eintreffen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Als böswillig erkannte erkennbare Elemente werden mit Tags versehen.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von Now Platform®kompatibel.

### Hybrid Analysis installieren und konfigurieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendung Hybrid Analysis ordnungsgemäß in Now Platform Security Operationsintegriert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

| Setupaufgabe | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Administrator (admin) installiert die App und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations und weist die Rolle sn_si.analyst zu. |
| Rufen Sie einen API-Schlüssel ab. | Besuchen Sie die Hybrid Analysis- Website, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: Hybrid Analysis-Website . Die Konfiguration erfordert die Eingabe der API-Schlüssel. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Für das Madrid-Release und spätere Familien-Releases ist das Plugin com.snc.si_dep erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.<br><br>Die folgenden Security Operations Anwendungen müssen über den ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:<br>**1.** Security Integration Framework<br>**2.** Security Support Common<br>**3.** Security Support Orchestration<br>**4.** Security Incident Response<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
|---|---|
| | Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

Erforderliche Rolle: admin

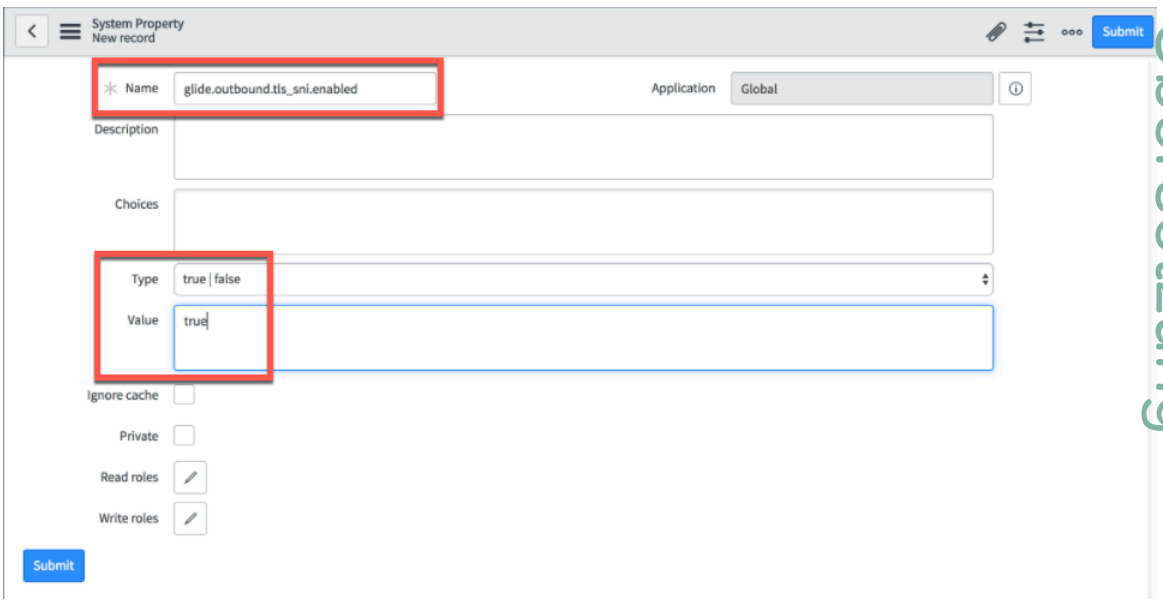
### Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Schritte aus, um die Systemeigenschaften zu aktualisieren und die Integration zu installieren und zu konfigurieren.

### Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein, und drücken Sie die **Eingabetaste**.
   Die Liste **„Systemeigenschaften“** wird angezeigt.
2. Klicken Sie auf **Neu**.
   Ein neuer Datensatz wird angezeigt.
3. Füllen Sie die Felder aus, oder wählen Sie die in der folgenden Tabelle aufgeführten Werte aus, und klicken Sie auf **Absenden**.

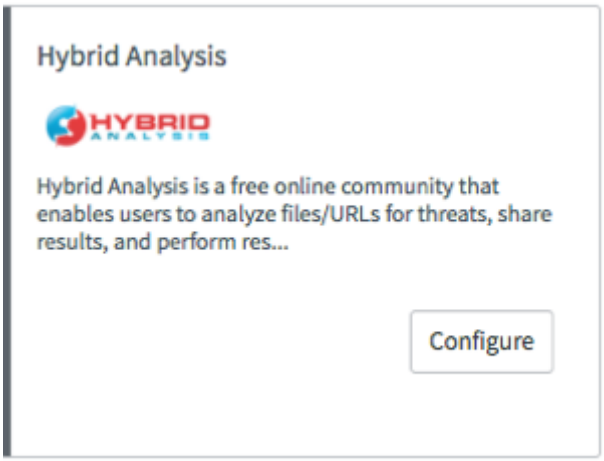
| Feldname | Wert |
|---|---|
| **Name** | glide.outbound.tls_sni.enabled |
| **Typ** | Wählen Sie „ **true“ oder „false“ aus** |
| **Wert** | true |



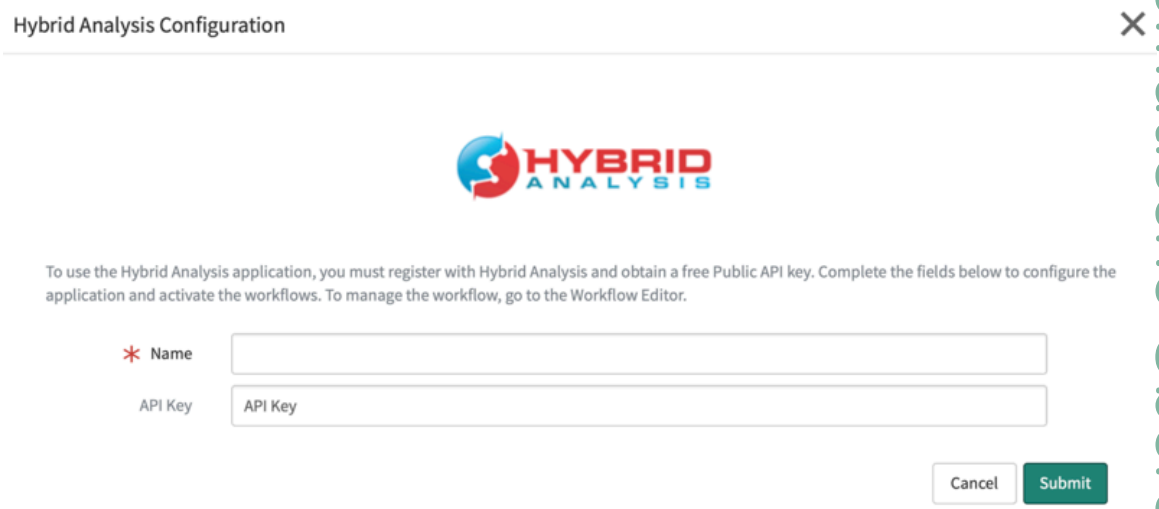

4. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
5. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Hybrid Analysis.
6. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Geben Sie im Dialogfeld „ **Hybrid Analysis Configuration** “ (Konfiguration der Hybridanalyse) den API-Schlüssel ein, den Sie von der Website Hybrid Analysis erhalten haben, und klicken Sie auf **Absenden**.




8. Vergewissern Sie sich, dass die Konfiguration erfolgreich war.
   Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird.

   **Trouble?**

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel Hybrid Analysis möglicherweise ungültig.

### Überprüfen Sie die erwarteten Ergebnisse für Hybrid Analysis

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchen Sie die Suchergebnisse im Security Incident, um sicherzustellen, dass die Bedrohungssuche erfolgreich ausgeführt wurde. Zeigen Sie auch Rohdaten an, und führen Sie Bedrohungssuchen für untergeordnete erkennbare Elemente aus.

### Vorbereitungen

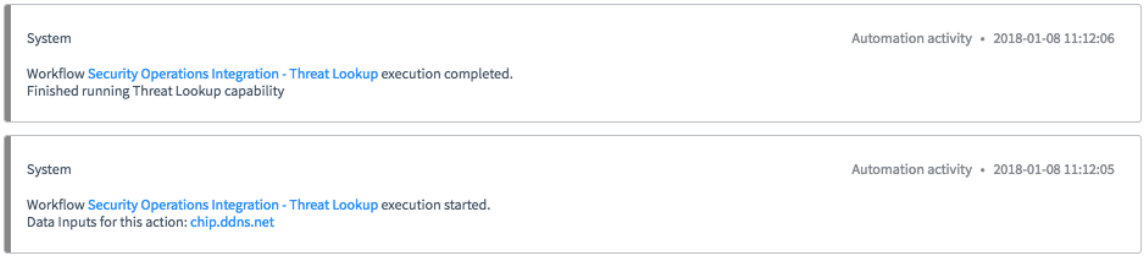
Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

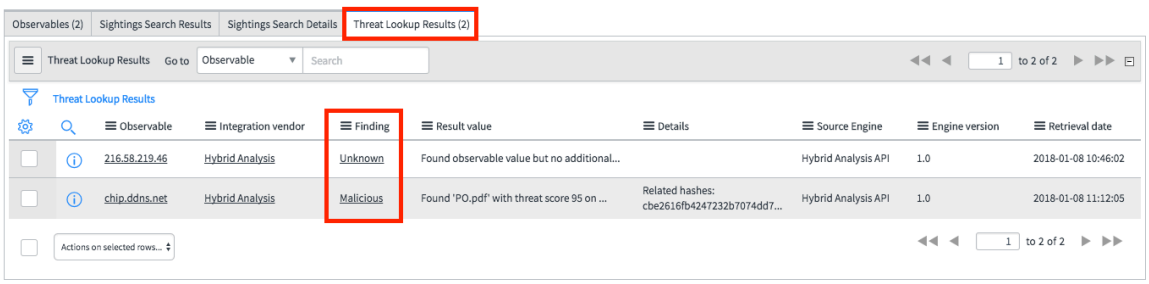



   Nachdem die Anwendung konfiguriert wurde, wird der Workflow automatisch bei der Incident-Erstellung gestartet. Die Ausführung und der Abschlussstatus der Suche werden dann in den Arbeitsnotizen im Security Incident angezeigt.

2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen zum weiteren Vorgehen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen, um die Ergebnisse anzuzeigen.

   **Hinweis:**
   Die Abbildungen in den folgenden Schritten werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt. Klicken Sie in der oberen rechten Ecke des Bannerframes auf das Zahnradsymbol für Einstellungen. Klicken Sie im angezeigten Dialogfeld „ **Systemeinstellungen** “ auf **Formulare**, und überprüfen Sie, ob **Formulare** mit Registerkarten und **Mit dem Formular** ausgewählt sind.

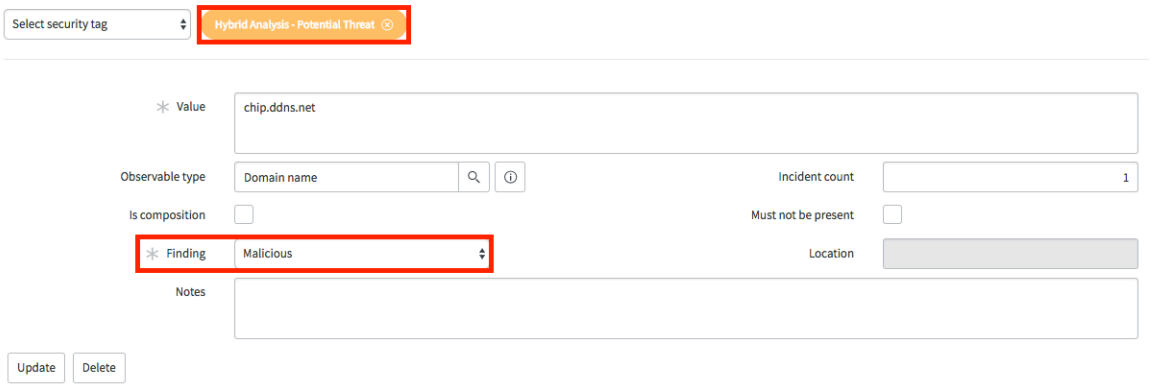



   Auf der Registerkarte Ergebnisse der **Bedrohungssuche** werden die Suchergebnisse am Ende des Security Incident-Datensatzes angezeigt. Beachten Sie, dass in der **Spalte** „Ergebnis“ für Datensätze, die nicht als schädlich eingestuft wurden, Unbekannt angezeigt wird. Bei Ergebnissen, die mit „böswillig“ übereinstimmen, wird in der **Spalte** „Ergebnis“ Böswilligangezeigt.

4. **Klicken** Sie in der Spalte Erkennbares Element auf ein erkennbares Element, um den Datensatz zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

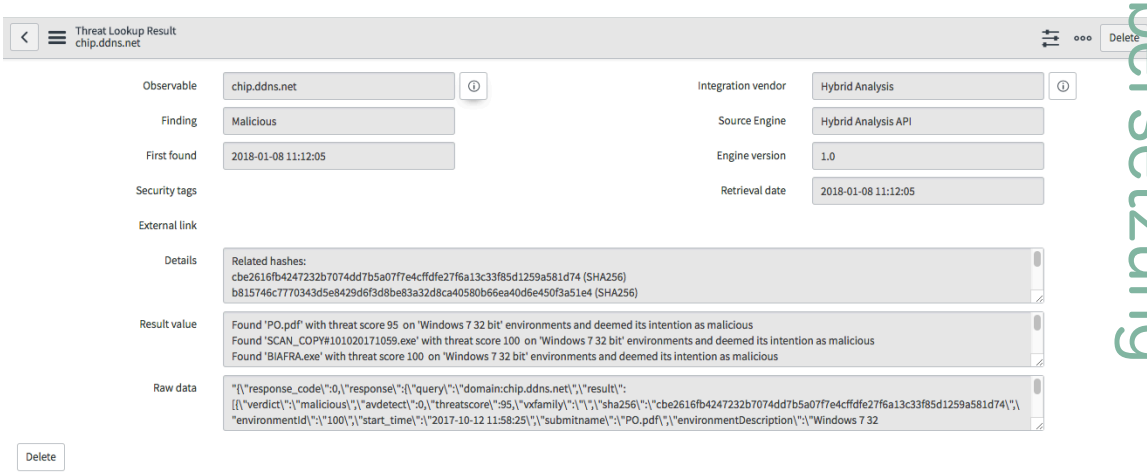



Bei Suchvorgängen, die böswillig übereinstimmen, wird im Feld **Finden**Böswilligangezeigt, und das erkennbare Element wird mit der Quelle Threat Intelligence getaggt, die es als böswillig eingestuft hat, in diesem Fall die Hybrid Analysis -Integration.

5. **Wahlweise:** Führen Sie die Schritte aus, um Rohdaten anzuzeigen, eine Liste der untergeordneten erkennbaren Elemente anzuzeigen und eine Bedrohungssuche für ausgewählte untergeordnete erkennbare Elemente auszuführen.

   a. Navigieren Sie zurück zum Security Incident, und klicken Sie auf der Registerkarte **Ergebnisse der Bedrohungssuche** auf das blaue Informationssymbol neben einem erkennbaren Element.

   b. Klicken Sie im angezeigten Fenster auf **Datensatz öffnen**, um die Daten anzuzeigen.
   Aus allen erkennbaren Elementen, die in den Rohdaten angezeigt werden, die aus der Suche angezeigt werden, erstellt die Hybrid Analysis -Integration auch untergeordnete oder zugehörige erkennbare Elemente.



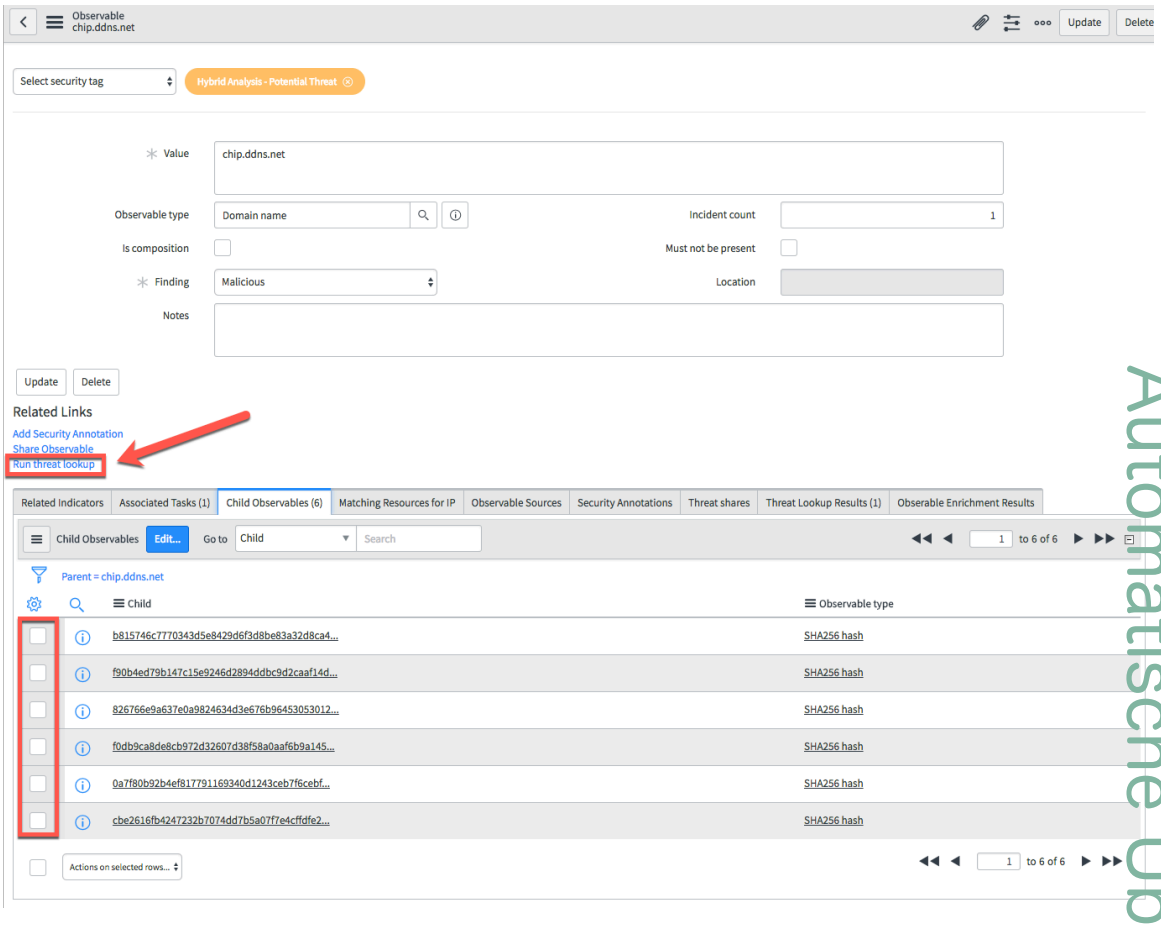

   Der von der API erstellte Link, die Rohdaten und andere Informationen werden angezeigt.

   c. Navigieren Sie zurück zum Security Incident, und klicken Sie auf den zugehörigen Link **IoC anzeigen**.
   Die untergeordneten erkennbaren Elemente werden auf der Registerkarte „ **Untergeordnete erkennbare** Elemente“ des Security Incident angezeigt, da bei der Suche eine vorhandene Verbindung zwischen diesen zugehörigen erkennbaren Elementen und dem ursprünglich übermittelten erkennbaren Element gefunden wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Klicken Sie auf das Feld neben einem erkennbaren Element in der **untergeordneten** Spalte, um es auszuwählen, gefolgt vom zugehörigen Link **Bedrohungssuche** ausführen, um eine Suche durchzuführen.




**e.** Vergewissern Sie sich im angezeigten Dialogfeld, dass die Integration Hybrid Analysis ausgewählt ist, und klicken Sie auf **Absenden**.

**f.** Überprüfen Sie in den Arbeitsnotizen, ob die Suche erfolgreich ausgeführt wurde, und suchen Sie auf der Registerkarte Ergebnisse der **Bedrohungssuche** im Security Incident nach Suchergebnissen für die untergeordneten erkennbaren Elemente.

**Trouble?**
Wenn auf der Registerkarte Ergebnisse der **Bedrohungssuche keine Ergebnisse** angezeigt werden, stellen Sie sicher, dass das erkennbare Element ein Typ ist, der für die Suche von der Integration unterstützt wird.

### (Optional) Hängen Sie ein erkennbares Element für manuell an Hybrid Analysis

Sie können erkennbare Elemente manuell anhängen, wenn Sie eine Bedrohungssuche für erkennbare Elemente durchführen möchten, die beim ersten Event-Auslöser nicht an einen Security Incident angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

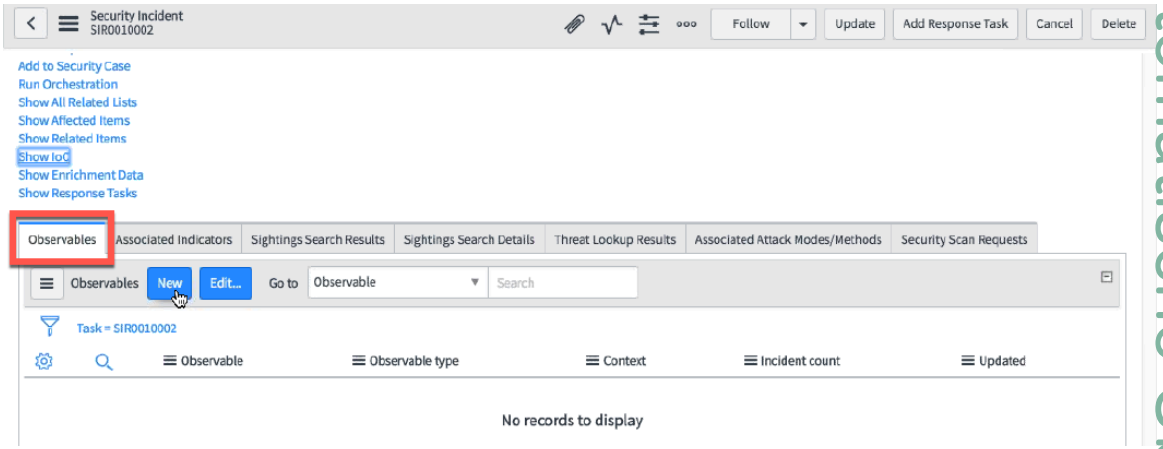
Vergewissern Sie sich, dass das erkennbare Element von einem Typ ist, der von der Integration unterstützt wird. Die Integration führt Suchvorgänge für die folgenden Arten von erkennbaren Elementen durch:

- Datei-Hashes
- IP-Adressen
- URLs

Erforderliche Rolle: sn_si.analyst

### Prozedur

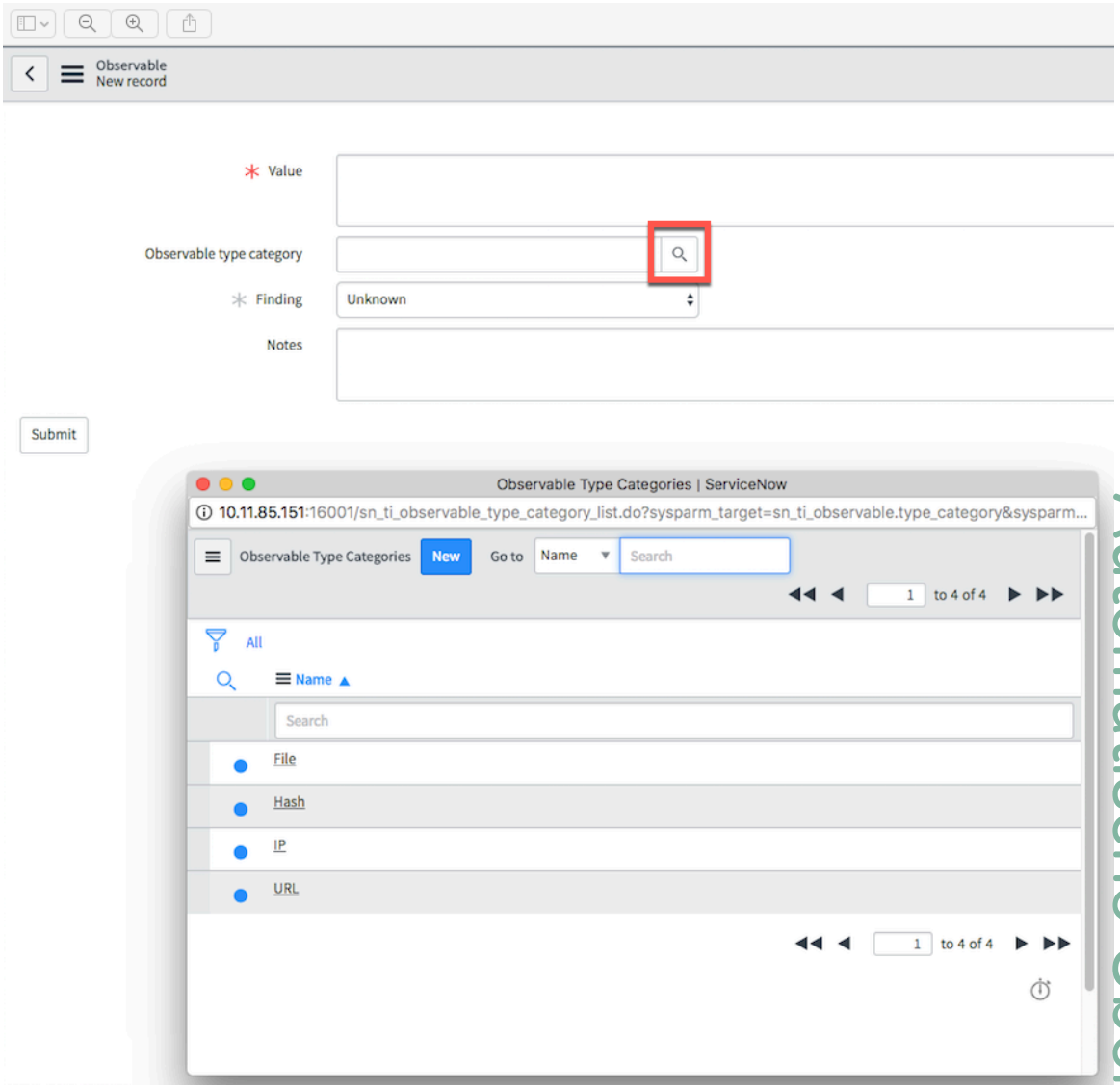
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie im offenen Security Incident auf den Link **IoC anzeigen**unter **Zugehörige Links**.



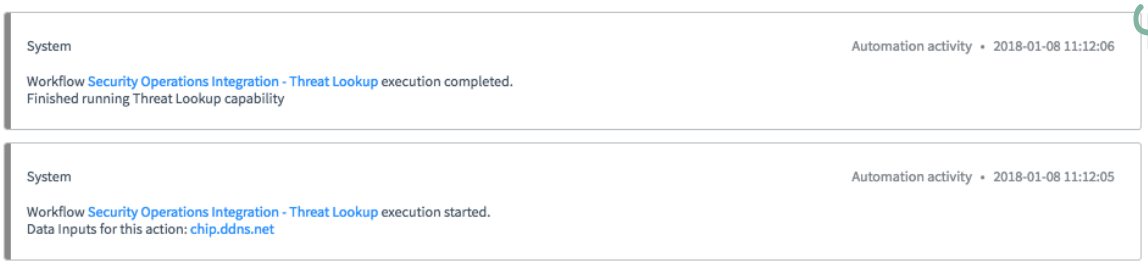

3. Klicken Sie auf der Registerkarte **Erkennbare** Elemente auf **Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** ein erkennbares Element ein (Datei-Hash, IP-Adressen oder URL).
5. Klicken Sie auf das **Suchsymbol**, und klicken Sie im Dialogfeld „Kategorien des erkennbaren Typs“ auf den gewünschten erkennbaren Typ in der Liste, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



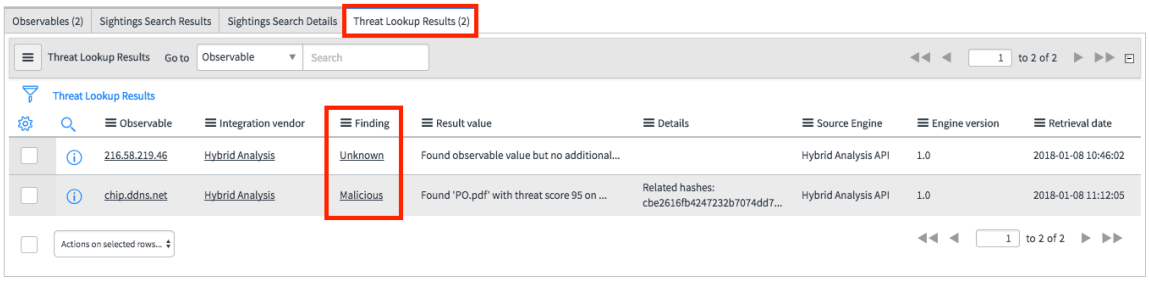

6. Klicken Sie auf **Absenden**.
   Der Workflow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ des Security Incident-Datensatzes angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.



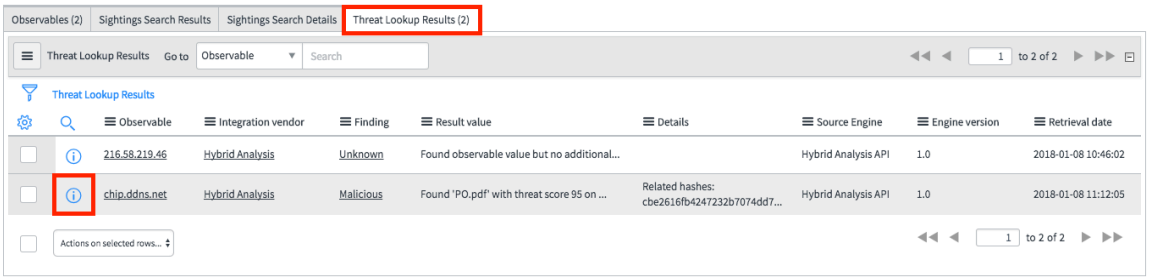

8. Klicken Sie unten im Datensatz auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.
9. Klicken Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche**, um die Ergebnisse anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




10. **Klicken** Sie in der Spalte „Erkennbares Element“ auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.




11. Klicken Sie im angezeigten Dialogfeld auf **Datensatz öffnen**, um die Rohdaten und weitere Details anzuzeigen.
    Alternativ können Sie auch ein vorhandenes erkennbares Element an den Security Incident-Datensatz anhängen.
12. **Wahlweise:** Klicken Sie bei **ausgewählter** Registerkarte Erkennbare Elemente auf **Bearbeiten**.
13. **Wahlweise:** Verschieben Sie im angezeigten Formular „ **Mitglieder bearbeiten** “ ein vorhandenes erkennbares Element aus der **Sammlung** in **die Liste** der erkennbaren Elemente, und klicken Sie auf **Speichern**.
    Sie kehren zum Security Incident zurück.
14. Wählen Sie in der Spalte ganz links die erkennbaren Elemente aus, für die Sie die Suche ausführen möchten, und wählen Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen...** die **Option Bedrohungssuche ausführen**aus.
    Oben im Datensatz wird eine Nachricht angezeigt, die angibt, dass die Anforderung verarbeitet wird. Vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

**Trouble?**
Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweisen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

## IBM QRadar Offense Ingestion Integration

Mit der IBM QRadar Offense Ingestion -Integration können Sie IBM QRadar -Vergehen automatisch abrufen und in Security Incidents umwandeln sowie automatisierte Antwortaktionen aktivieren.

Diese Integration unterstützt Folgendes:

- Discovery von IBM QRadar Straftaten, die Kandidaten für Security Incidents sind.
- Ruft aktuelle Events oder Flows ab, die einem Verstoß zugeordnet sind.
- Verfolgen Sie regelmäßig wichtige Aktualisierungen für Vergehen nach.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuordnung von Vergehen-, Event- und Flow-Feldern zu Security Incident-Feldern
- Vorläufige Ansicht der zugeordneten Felder.
- Richten Sie geplante Erfassungen von Straftaten ein, um regelmäßig Security Incidents zu erstellen.
- Schließen Sie die Vergehen, wenn die Security Incidents geschlossen sind.

### Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration der Straftatenerfassung IBM QRadar .

Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform® ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform integriert wird.

#### Vorbereitungen

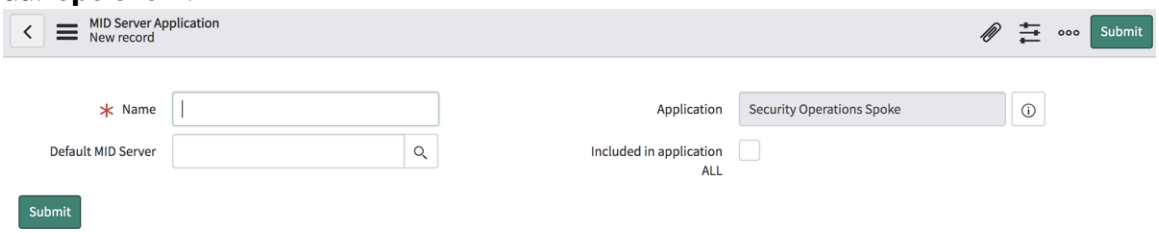
Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Wenn Sie die Anwendung IBM QRadar nicht aus dem ServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel IBM QRadar.
3. Um die Anwendung zu konfigurieren, klicken Sie auf **Neu**.
4. Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld „ **Offense Ingestions Configuration** “ (Angriffserfassungskonfiguration) die Felder aus.

   Führen Sie die folgenden Schritte aus, um eine neue MID Server-Anwendung zu erstellen:

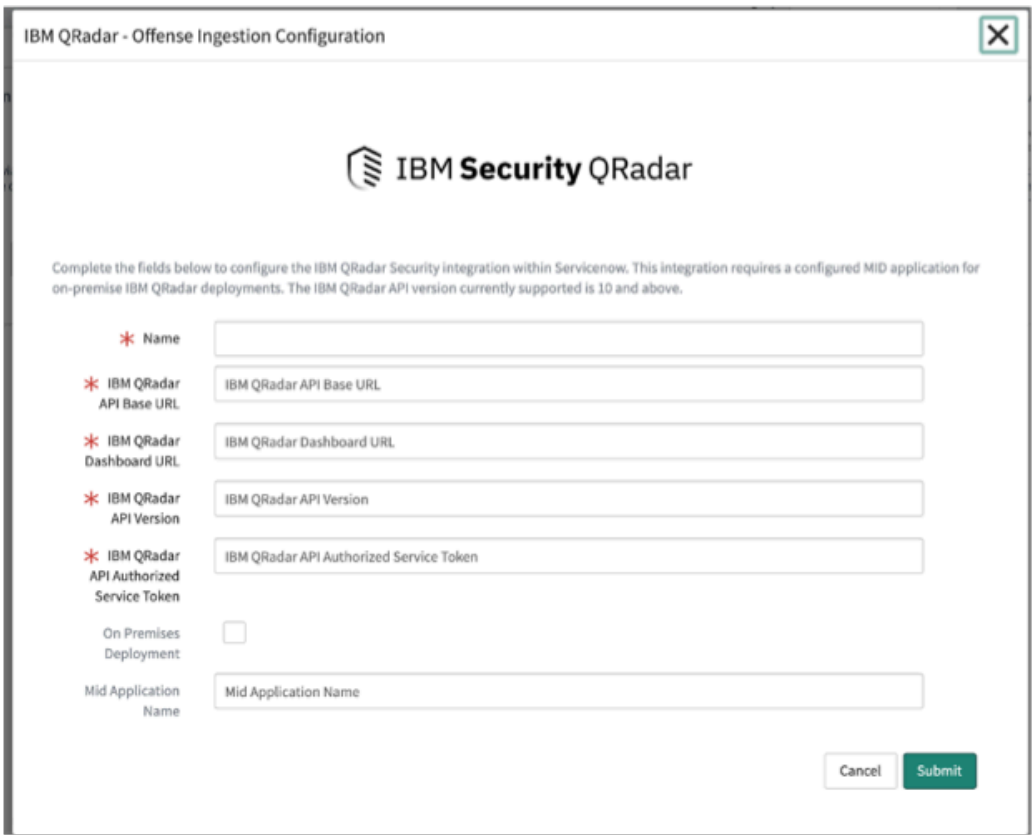
   - Navigieren zu **MID-Server** > **Anwendungen** und klicken Sie auf **Neu**.
   - Geben Sie einen Namen für die MID Server-Anwendung ein, und wählen Sie einen MID Server aus, der als Standard verwendet werden soll.
   - Deaktivieren Sie das Kontrollkästchen In Anwendung ALLE enthalten, und klicken Sie auf **Speichern**.




   - Klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite „ **Mitglieder bearbeiten** “ alle verfügbaren MID Server aus, verschieben Sie sie in die MID Server-Liste, und klicken Sie auf **Speichern**. Je nach Verfügbarkeit wird einer der mit der MID Server-Anwendung konfigurierten MID Server verwendet.
6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID Server-Anwendung an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die Quelle, die Sie im **Formular „IBM QRadar –** Konfiguration der Straftatenerfassung“ konfigurieren, kann für mehrere Now Platform Profile wiederverwendet werden, solange jedes Profil Straftaten erfasst.

7. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration IBM QRadar auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

**Hinweis:**
Wenn Probleme mit der Domänensegmentierungsfunktion IBM QRadar auftreten, wenden Sie sich an den Kundensupport von IBM QRadar.

### Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, das Profil zu erstellen.

### Richten Sie Ihre Now Platform® -Instanz für die Integration der IBM QRadar -Angriffserfassung ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Warum und wann dieser Vorgang ausgeführt wird**
Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

| Setupaufgabe | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform® -Instanz erforderlich.<br>• Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus dem ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform®:<br>○ Benennt, erstellt und bearbeitet Vergehensprofile.<br>○ Wählt die Vergehensdatenfelder IBM QRadar aus und ordnet sie den Security Incident-Feldern zu.<br>○ Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.<br>○ Plant die laufende Erfassung von Vergehen.<br>○ Aktiviert Aktualisierungen von Vergehen, wenn ein SIR-Incident erstellt und geschlossen wird.<br>○ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>○ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.<br>Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der ServiceNow-Website mit Produktdokumentation . |
| Vergewissern Sie sich, dass Sie die folgenden Versionen verwenden:<br>• IBM QRadar Version 7.3.2 oder höher.<br>• IBM QRadar API-Version 10 oder höher.<br>Frühere Versionen werden nicht unterstützt. | Wenn Sie Zugriff auf die Konsole IBM QRadar haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich. |
| Vergewissern Sie sich, dass Sie eine MID Server-Anwendung installiert und konfiguriert haben. | Konfigurierte MID-Server-Anwendung.<br>Ein MID Server in Ihrer Now Platform® -Instanz ist erforderlich, um eine Verbindung zum IBM QRadar |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
|---|---|
| | -Service herzustellen, wenn der IBM QRadar -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Weitere Informationen zu MID Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .<br><br>Wenn Sie den Cloud-Service IBM QRadar verwenden, ist kein MID Server erforderlich. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Event and Alert Ingestion for Security Operations: Diese Anwendung erfordert:<br>○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit<br>○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST<br><br>**Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Event and Alert Ingestion“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport.<br><br>Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

### Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht darin, die Anwendung IBM QRadar aus dem ServiceNow Store für die Integration zu installieren.

#### Erstellen Sie ein Profil für die Integration der Straftatenerfassung IBM QRadar .

Als Benutzer mit der Rolle „sn_si.admin“ erstellen Sie in Ihrer Instanz Now Platform ein Vergehenprofil und bestimmen, welche Vergehen zu Security Incidents führen. Bevor Now Platform Security Incident Response (SIR) Security Incidents aus Vergehen erstellt werden, werden die Feldwerte aus Vergehen in einem Layout eines Now Platform Security Incident angezeigt, sodass Sie eine Vorschau auf die Erstellung des tatsächlichen Security Incident erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Aus Perspektive der Integration mit verfügbaren APIs werden IBM QRadar -Vergehen abhängig vom definierten Profiltyp automatisch in der Security Operations -Umgebung Ihrer Now Platform -Instanz erfasst. Die Integrations-Workflows erfassen verschiedene Arten von Straftaten, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Verstöße werden basierend auf den Profilen erfasst, die Sie in der Security Operations -Umgebung Ihrer Instanz konfigurieren. Alle Vergehen werden anfänglich für einen konfigurierten Vergehenstyp in einem Profil erfasst. Erfasste Vergehen können dann weiter gefiltert werden, um anzugeben, welche Vergehen zu Security Incidents führen. Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für Straftaten erstellen, die als hohes Risiko identifiziert wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Straftaten erstellt, werden einzelne Feldwerte für die Straftaten den entsprechenden Feldern in einem Layout von Security Incidents für eine Vorschau zugeordnet.

Namen für die Vergehensprofile in Ihrer Instanz Now Platform müssen eindeutig sein. Sie können mehrere Konfigurationen für mehrere Quellen erstellen und Sie können auch mehrere Profile für eine einzelne Quelle erstellen.

## Erstellen Sie Profile für die Erfassung von IBM QRadar -Vergehen

Sie können ein Profil einrichten, um Verstöße zu erfassen.

### Vorbereitungen

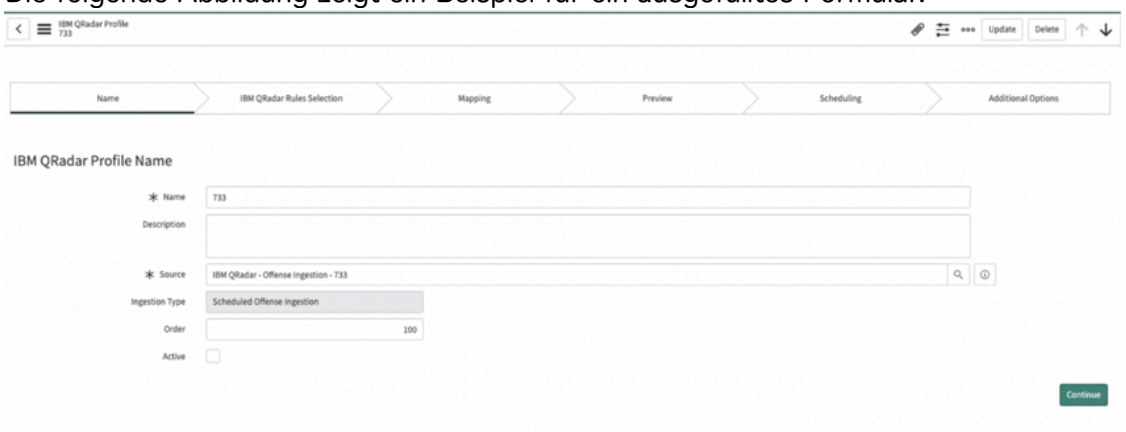
Erforderliche Rolle: sn_si.admin

### Prozedur

1. Um ein Profil für einen Verstoß in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.




### Nächste Maßnahme

Der nächste Schritt besteht darin, die Straftaten für die Erfassung auszuwählen.

## Wählen Sie IBM QRadar Regeln aus

Wählen Sie basierend auf der Quelle IBM QRadar eine oder mehrere IBM QRadar Regeln für das Profil aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

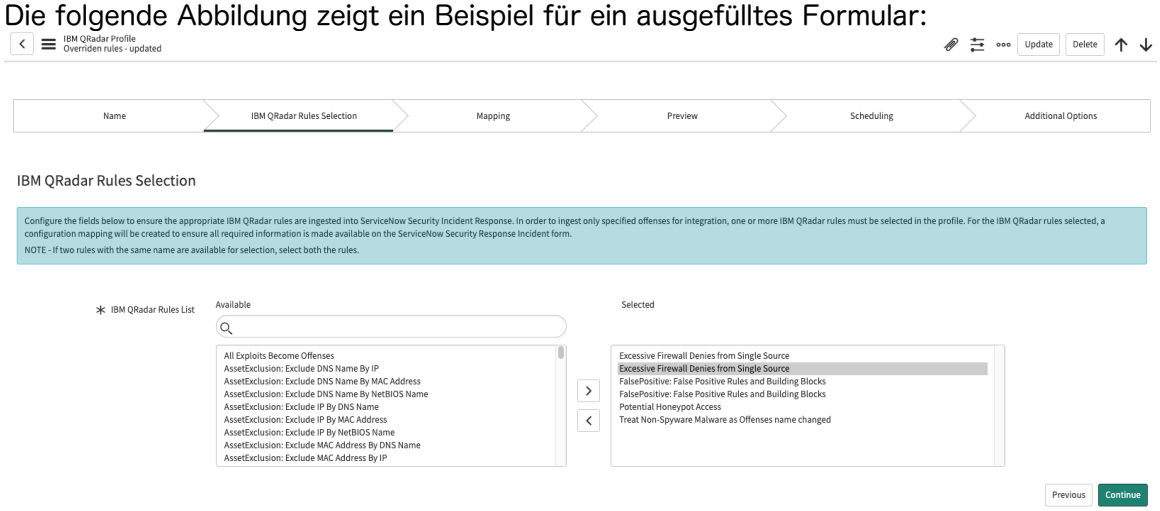
### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie die verfügbaren IBM QRadar -Regeln in Ihrer Now Platform-Instanz an, damit Sie die aktiven IBM QRadar -Regeln kennen, für die Sie Security Incidents erfassen und erstellen möchten.

In IBM QRadarkönnen Sie Regeln anhand ihres Ursprungs als System-, Überschreibungs- und Benutzerregeln identifizieren. Standardmäßig ist der Ursprung einer Regel mit einer Systemregel verknüpft. Wenn Sie eine Systemregel in IBM QRadarändern, wird ihr Ursprung als Überschreiben festgelegt.

Klicken Sie auf die Liste im Feld IBM QRadar Regelliste. Eine Liste der aktiven IBM QRadar Regeln, die in der Konsole IBM QRadar vorhanden sind, wird angezeigt. Wählen Sie eine oder mehrere Regeln aus der Liste aus, und verschieben Sie sie in die Spalte **Ausgewählt**. Vergehen, die durch eine oder mehrere der ausgewählten IBM QRadar Regeln ausgelöst werden, werden in diesem Profil erfasst.

**Regeln mit demselben Namen**: In der Instanz Now Platform wird eine Liste der aktiven oder aktivierten Regeln angezeigt. Wenn Sie eine aktive oder aktivierte Systemregel in IBM QRadarändern, wird eine neue Überschreibungsregel erstellt. Dies führt dazu, dass zwei Regeln mit demselben Namen im Now Platformangezeigt werden. Wenn dieses Szenario auftritt, wählen Sie die Regeln aus, um Security Incidents zu erfassen und zu erstellen.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular:




Klicken Sie auf **Fortsetzen**, um mit dem nächsten Schritt im Assistenten fortzufahren.

#### Zuordnung von Vergehensfeldern für die IBM QRadar -Integration

Nachdem Sie die Regeln ausgewählt haben, besteht der nächste Schritt darin, die Felder für Vergehen, Ereignisse oder Flows den Feldern im Security Incident-Formular zuzuordnen.

## Übersicht

Für den Zuordnungsschritt müssen Sie zuerst Beispielvergehen für eine oder mehrere ausgewählte IBM QRadar -Regeln erfassen. Dann müssen Sie sicherstellen, dass alle relevanten Felddaten für Vergehen der entsprechenden Stelle im Incident-Formular SIR zugeordnet sind, und dann den Incident SIR im Vorschaubereich visualisieren.

Die Zuordnung der Beispielvergehensfelder umfasst Folgendes:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beispieldaten abrufen und ausfüllen: Siehe Beispielvergehen IBM QRadar werden erfasst.
- Vergehensfelder werden dem Security Incident zugeordnet: Siehe IBM QRadar -Angriffsfelder werden Security Incident-Antwortfeldern zugeordnet.

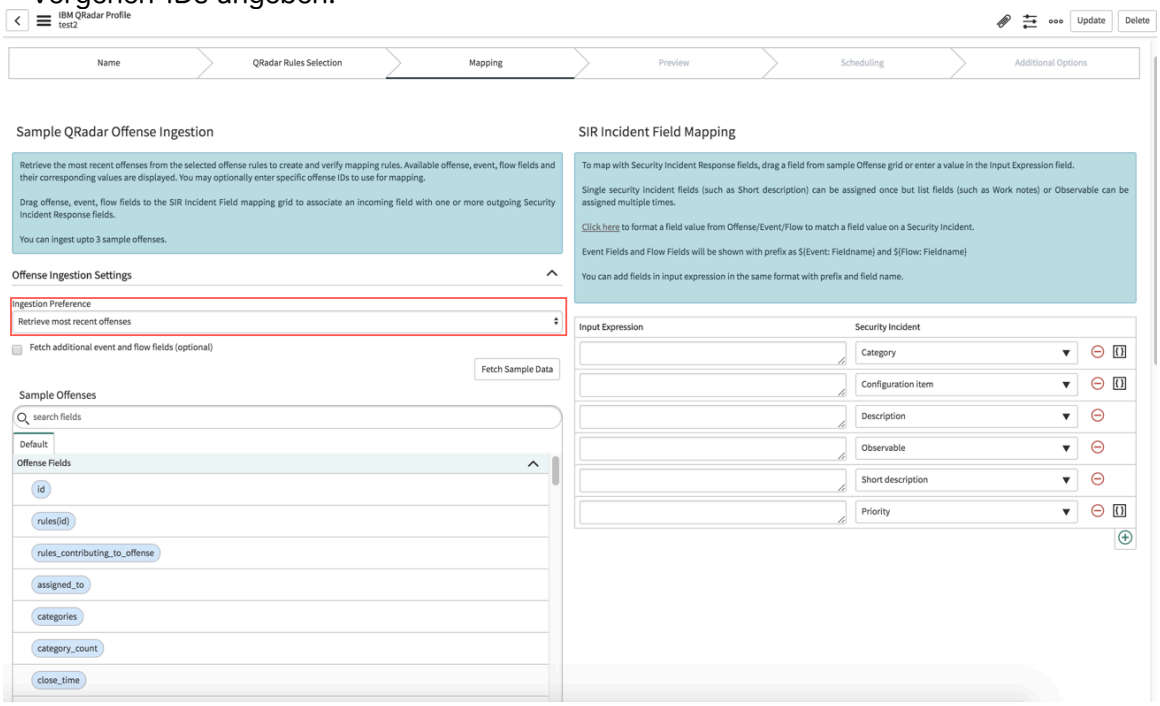
### Beispielvergehen IBM QRadar werden erfasst

Sie können Beispielvergehen für eine oder mehrere ausgewählte IBM QRadar Regeln erfassen.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Prozedur**

1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Sie können entweder die drei letzten Beispielvergehen abrufen oder die eindeutigen Vergehen-IDs für die spezifischen Vergehen angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   **Wählen** Sie in der Auswahlliste „Erfassungseinstellung“ eine der folgenden Optionen aus:
   - Neueste Vergehen abrufen: Die drei letzten Vergehen für die ausgewählten Regeln werden abgerufen.
   - Wählen Sie Straftaten basierend auf Straftaten-ID aus: Geben Sie die Straftat-ID für die abzurufenden Straftaten an. Sie können maximal 3 durch Kommas getrennte Vergehen-IDs angeben.




3. Klicken Sie auf **Beispieldaten abrufen**, um die neuesten Beispiel-Vergehensdaten aus der Konsole IBM QRadar für die ausgewählten Vergehensregeln abzurufen.

   Die Ergebnisse der Straftatfelder und -werte werden als einzelne Registerkarten angezeigt. Ein Vergehen kann durch drei Arten von Regeln ausgelöst werden:



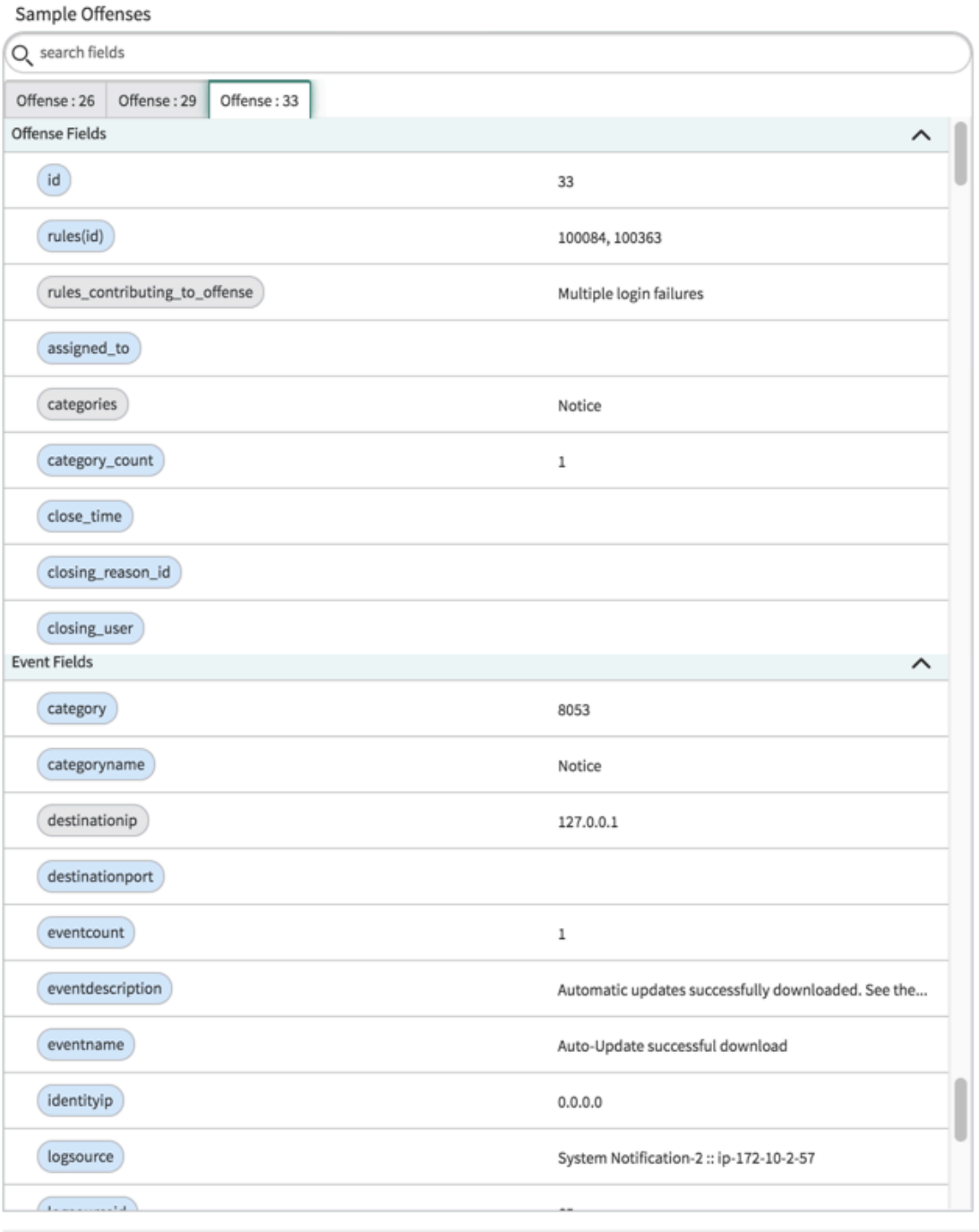
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ereignis: In dieser Regel werden Ereignisprotokolle überprüft, und wenn die angegebenen Kriterien erfüllt sind, wird ein Vergehen erstellt.
- Flow: Netzwerkdaten und -verkehr werden überprüft, und wenn bestimmte Bedingungen erfüllt sind, wird ein Vergehen erstellt.
- Allgemein: In diesem Fall können Sie Bedingungen für Events oder Flows angeben. Wenn eine oder beide Bedingungen erfüllt sind, wird ein Vergehen erstellt.

Der Abruf für Beispielvergehen kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt. Abhängig von der Regel oder den Regeln, die den Vergehen ausgelöst hat, werden zusammen mit den Vergehen-Feldern die Event- oder Flow-Felder ausgefüllt, wie in der folgenden Abbildung dargestellt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






**Hinweis:**
Die angezeigten Event- oder Flow-Felder gehören zum ersten Event- oder Flow-Feld, das den Verstoß basierend auf der entsprechenden Event- oder Flow-Regel ausgelöst hat.

4. Im Folgenden finden Sie benutzerdefinierte Felder für Straftaten, die für diese Integration erstellt wurden. Zusätzlich zu diesen benutzerdefinierten Feldern stehen Standardvergehen-Felder für die Zuordnung zur Verfügung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- rules_contributing_to_offense: IBM QRadar Regeln, die basierend auf der Regel-ID zum Vergehen beigetragen haben.
- users: Benutzernamen für den Verstoß
- remote_destination_ip: Die Remoteziel-IPs für den Verstoß.

  Basierend auf den lokalen Ziel-IDs für den Vergehen sind die folgenden benutzerdefinierten lokalen Zieladressfelder verfügbar:

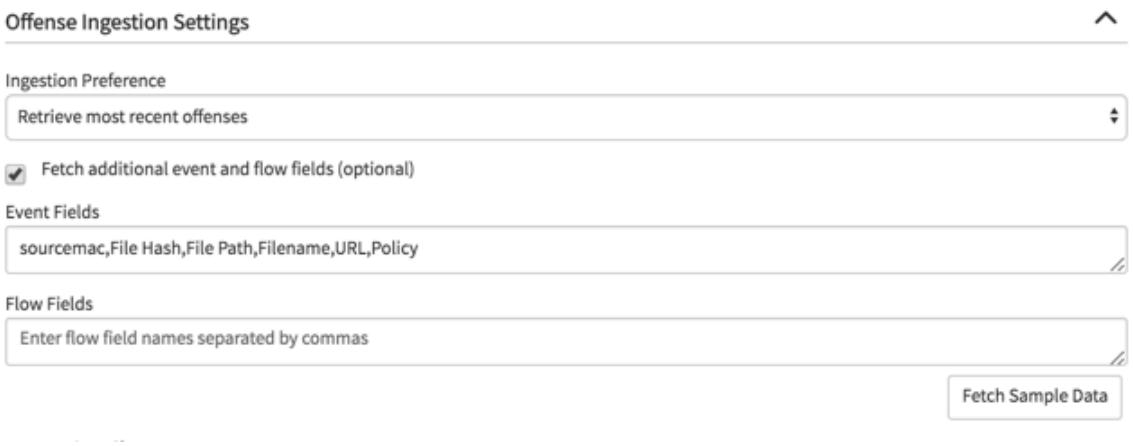
  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (ID)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (Größe)
  - local_destination_address (Netzwerk)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

- Die folgenden Quelladressen sind basierend auf den Quell-IDs des Vergehens verfügbar:
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (ID)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (Größe)
  - source_addresses (Netzwerk)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

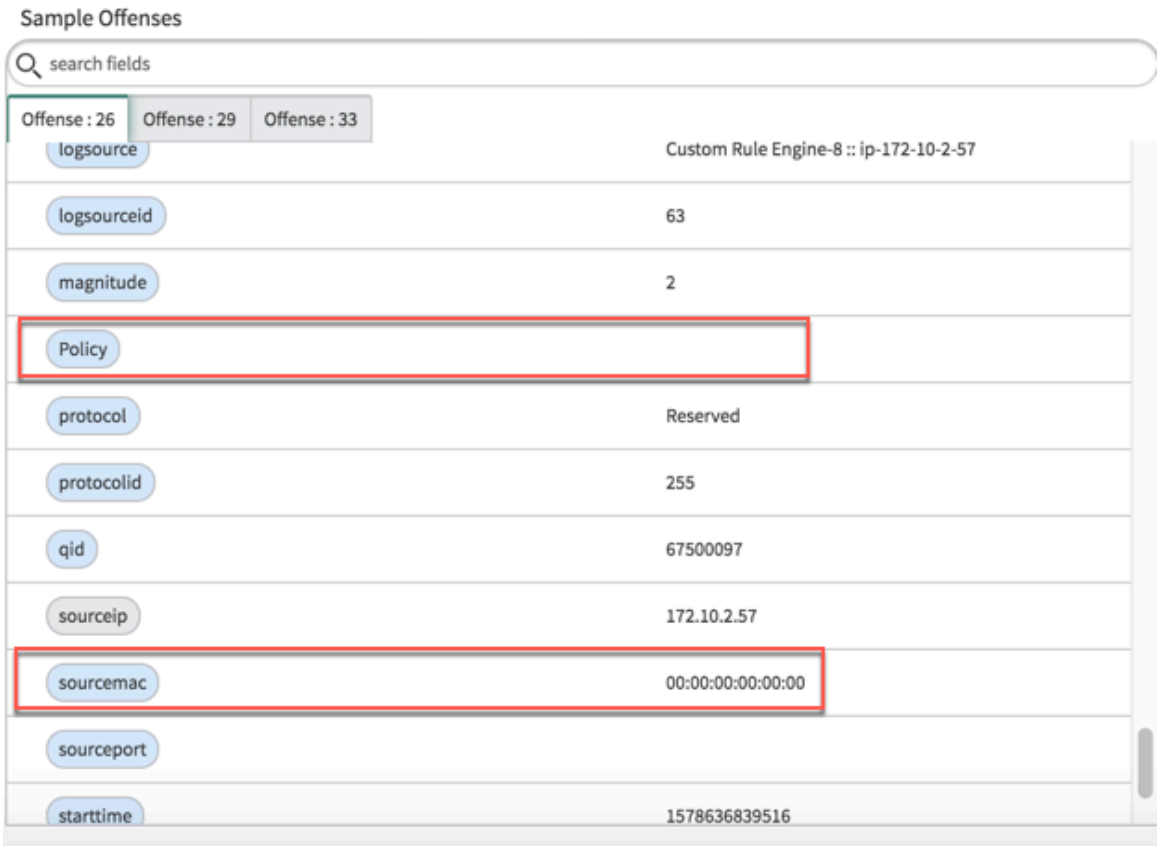
Aktivieren Sie das Kontrollkästchen **Zusätzliche Event- und Flow-Felder abrufen (optional)**. Sie können Beispiel-Event- und Flow-Daten aus allen aktiven, gültigen benutzerdefinierten Event- und Flow-Feldern abrufen. Geben Sie die benutzerdefinierten Felder wie folgt durch Kommas getrennt an:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



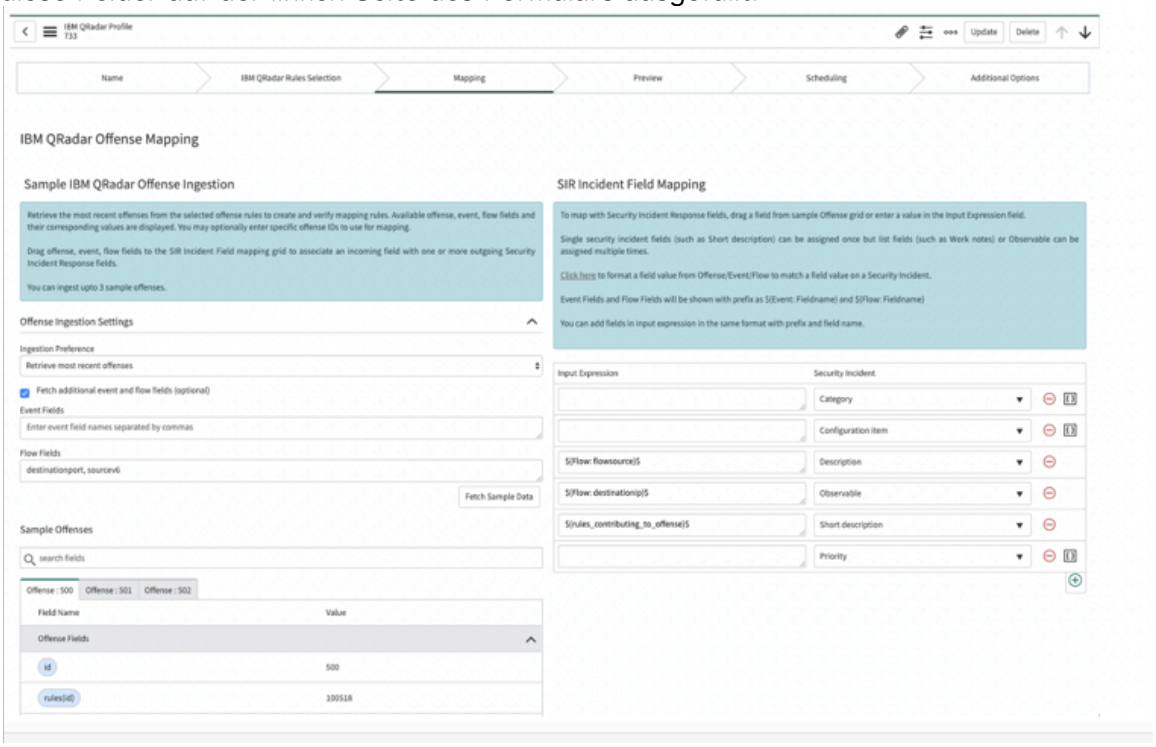

Klicken Sie **auf Beispieldaten abrufen**. Die angegebenen Event- oder Flow-Felder werden zusammen mit ihren Werten (falls verfügbar) wie unten gezeigt an den Event- oder Flow-Abschnitt angehängt:






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Beispieldaten abgerufen haben, werden die entsprechenden Werte für diese Felder auf der linken Seite des Formulars ausgefüllt.




**Nächste Maßnahme**
Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie im nächsten Schritt die Vergehensfelder dem Security Incident zu.

### IBM QRadar -Angriffsfelder werden Security Incident-Antwortfeldern zugeordnet

Ordnen Sie einzelne Vergehens-, Event- und Flow-Felder Feldern in einem Now Platform SIR Security Incident zu.

## Feldzuordnung für Vergehen

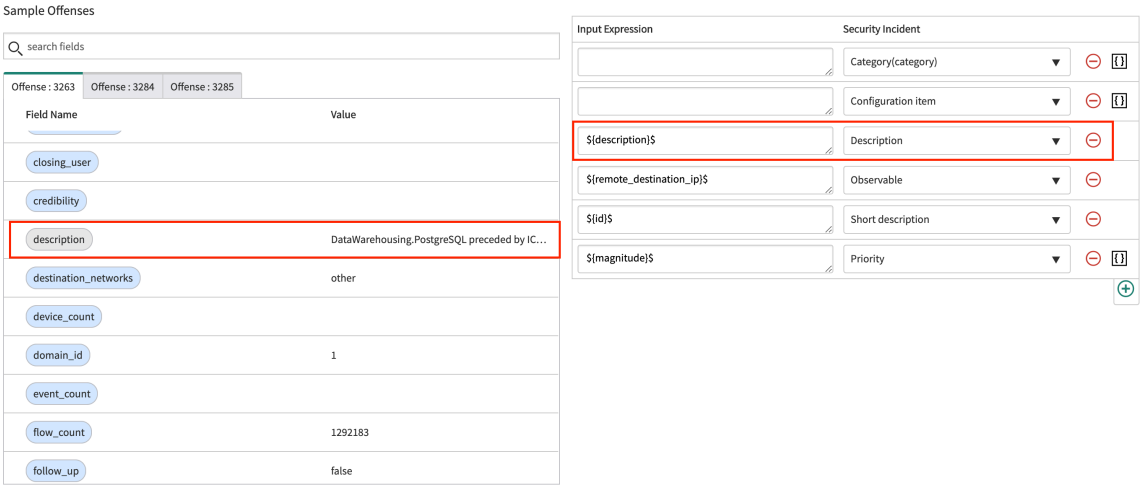
Verwenden Sie als Benutzer mit der Rolle „sn_si.admin“ die Felder aus dem Abschnitt „Beispielvergehen“ auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte SIR-Incident-Feldzuordnung zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Vergehen-, Event- oder Flow-Felder von der linken Seite ziehen und sie im Incident-Zuordnungsabschnitt ServiceNow SIR auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Vergehensfeld einem ausgehenden Security Incident-Feld zu.

1. Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie im nächsten Schritt die Felder für Vergehen, Ereignisse oder Flows dem Security Incident zu. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.
2. Ziehen Sie den Feldnamen, z. B. Beschreibung, in ein Feld in der Spalte Eingabeausdruck neben einem Feldnamen in der Spalte Security Incident.

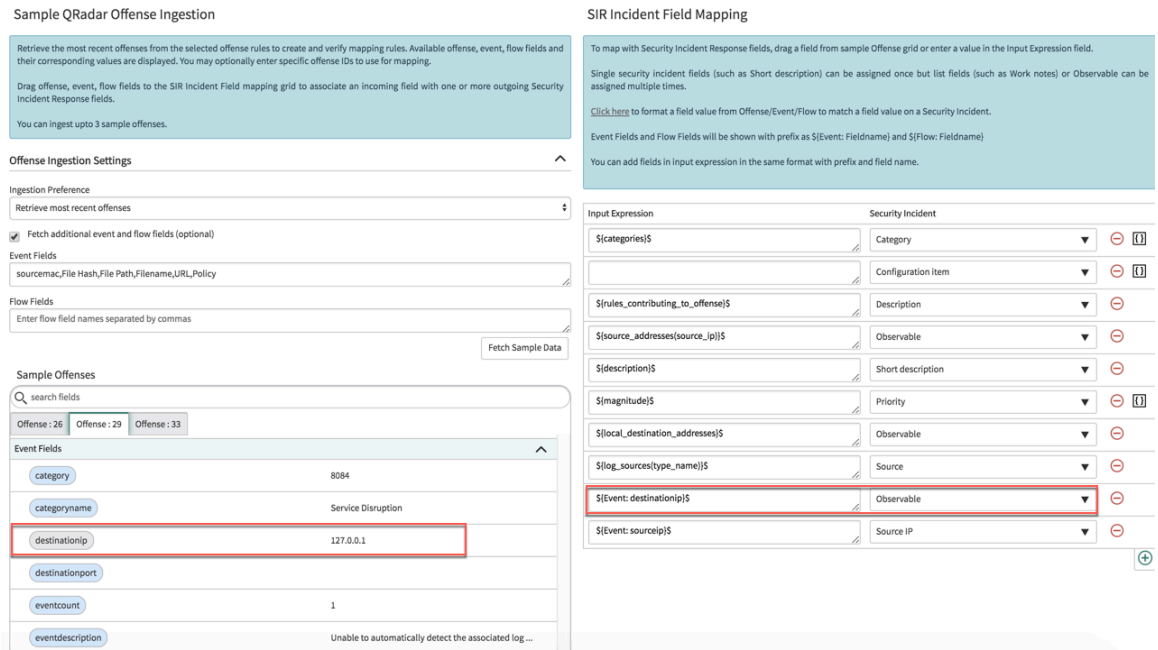
   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Beschreibung dem Feld Beschreibung im Security Incident zugeordnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn Sie den Event- oder Flow-Feldnamen manuell im Abschnitt „Eingabeausdruck“ eingeben, müssen Sie vor dem Namen des zugeordneten Felds ein Präfix wie `${Event:eventfield}$` oder `${Flow:flowfield}$ hinzufügen`.




Damit Sie sicherstellen können, dass keine Vergehen-, Event- oder Flow-Felder im Zuordnungsprozess übersehen oder dupliziert werden, sind die Felder farbcodiert. Die Farbcodierung der Vergehen-Felder hilft Ihnen, die Vergehen-Werte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder in Blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Vergehensinformationen nicht zugeordnet wurden.

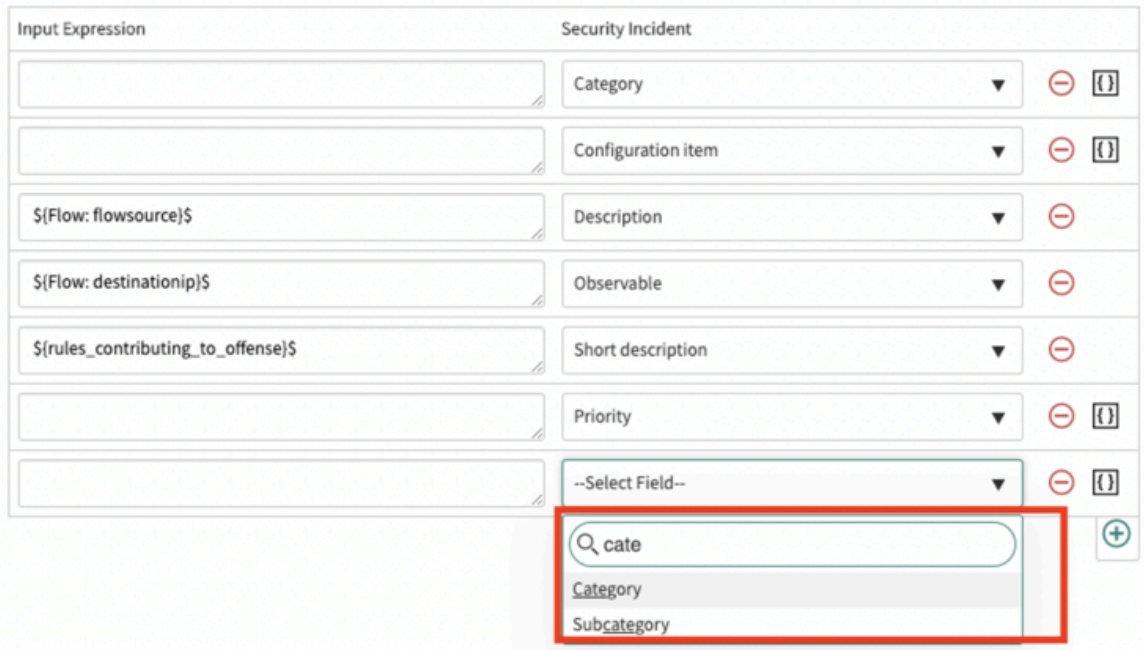
Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Vergehensfeld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie einen eingehenden Verstoß, ein Ereignis oder ein Flow-Feld mehr als einem Feld in einem Security Incident zuordnen. Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ am unteren Rand des Rasters auf das Pluszeichen (+). Ein neues Feld wird angezeigt.
   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat die Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Vergehensfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.




**Hinweis:**
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

   c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.
   d. Wählen Sie auf der linken Seite des Formulars das Feld „Vergehen“ aus, und ziehen Sie es per Drag-and-Drop in ein entsprechendes Feld für Security Incidents auf der rechten Seite.
4. Entfernen Sie Felder mithilfe des Symbols „-“ neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“.
5. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder daraus entfernen.

### Straftatfelder mit mehreren Werten



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident-Felder wie **Kategorie** und **Benutzerfelder** (z. B. Betroffener Benutzer, Zugewiesen an), die mit dem Basisprodukt verfügbar sind, unterstützen nicht mehrere Werte.
- Die folgenden IBM QRadar Felder unterstützen mehrere Werte:
  - *Kategorien*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_offense*
  - *Benutzer*

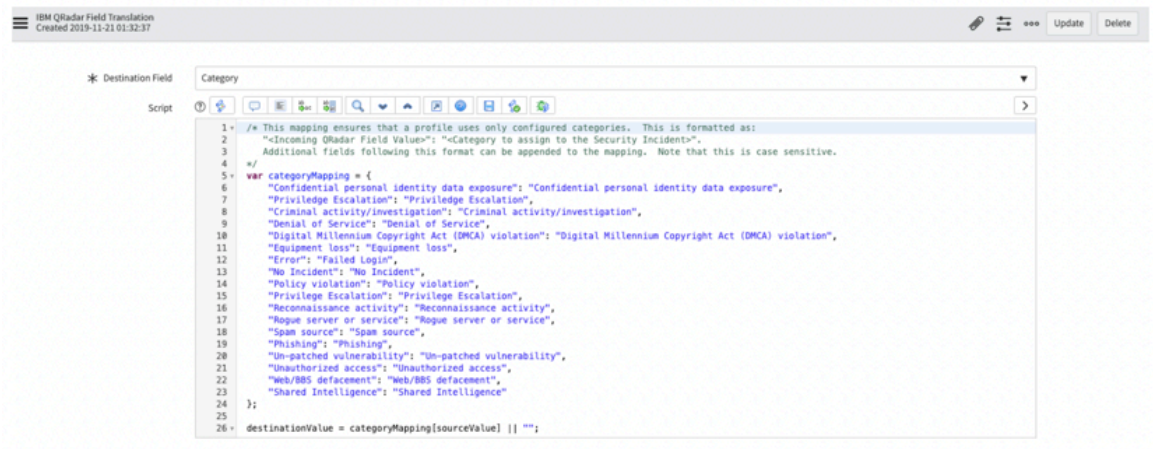
  Wenn Sie die obigen Felder anderen Security Incident Response -Feldern als CI- und erkennbaren Feldern zuordnen müssen, müssen Sie neue Security Incident Response -Felder vom Typ „ **Liste** “ erstellen und für die Zuordnung verwenden.

**Hinweis:**
Standardmäßig werden nur Nicht-Referenzfelder vom Typ **Liste** unterstützt.

### Formatfeldübersetzung

In bestimmten Fällen werden Feldwerte für Vergehen in IBM QRadar möglicherweise nicht direkt in die Felder des SIR-Security Incident übertragen. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Zum Beispiel kann mit dem Skript-Editor ein Kategoriewert von Malware-Warnung und Virusinfection unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können in eine gemeinsame böswillige Codeaktivität im Feld Kategorie des SIR-Security Incident mit Format übersetzt werden Feldübersetzungsfunktion.

Um den Skript-Editor zu verwenden, klicken Sie auf das {} Der Skript-Editor wird angezeigt.




Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Seite „Zuordnung“ zurückzukehren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um anzugeben, welche Vergehen Security Incidents erstellen und welche Vergehen herausgefiltert werden sollen, z. B. Vergehen mit niedriger Priorität. Sie können dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Verstoß erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

1. Scrollen Sie im Formular zum Abschnitt „ **Bedingungen für Incident-Generierung** “, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern, um die Option zu aktivieren.

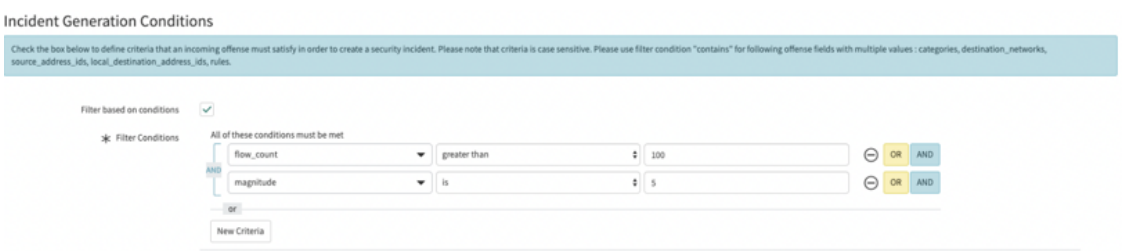
   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Beispiel für QRadar-Offene Ingestion“ für die von Ihnen erfassten Vergehen angezeigt werden. Diese Felder sind dynamisch und ändern sich in Abhängigkeit von den von Ihnen erfassten Straftaten. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Vergehens IBM QRadar übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu Ihrer IBM QRadar -Konsole zurück und überprüfen Ihre Vergehen auf die Stichwörter.

   **Hinweis:**
   Die Felder „ *categories*“, „ *destination_networks*“, *„source_address_ids“*, *„local_destination_address_ids“*, *„remote_destination_ips*“, *„regeln_contributing_to_offense“*und „ *users* “ können mehrere Werte haben (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie für diese Felder die Filterbedingung *Enthält* verwenden, um sicherzustellen, dass die Daten richtig gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**.
   - Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Generierungsbedingungen für Incidents so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Filterung der Incident-Generierungsbedingung hilft Ihnen, die Vergehen einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegenden Regeln oder Filter in IBM QRadarzu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden Incidents nur Vergehen zugeordnet, die allen Kriterien entsprechen.

**Hinweis:**
Wenn einer der Feldnamen für Vergehen Sonderzeichen enthält, z. B. Anführungszeichen (“), Bindestriche ('), Unterstriche (-) oder kaufmännische Und-Zeichen (@), müssen diese Zeichen möglicherweise zu Filterzwecken ersetzt werden, es wird jedoch ein numerisches Suffix angehängt Felder mit doppelten Vergehensnamen unterscheiden. Beispiel: Wenn das erste Vergehensfeld alerts.alert und das zweite Vergehensfeld alerts @alerts ist, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Vergehensfeld ein Suffix hinzugefügt, und das Feld wird in alerts@alert(1) umbenannt, wenn es in der Liste „Filterbedingungen“ angezeigt wird.

## Zusammenfassungskriterien für Straftaten, um ähnliche Straftaten zu behandeln und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Vergehenszusammenfassungskriterien, die einen eingehenden Verstoß zu einem vorhandenen SIR-Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Vergehensdaten auf einem einzigen Security Incident platziert werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

1. Scrollen Sie im Formular zum Abschnitt „Kriterien für die Zusammenfassung von Straftaten“, und aktivieren Sie das Kontrollkästchen „Zusammenfassungsbedingungen“, um diese **Option** zu aktivieren.

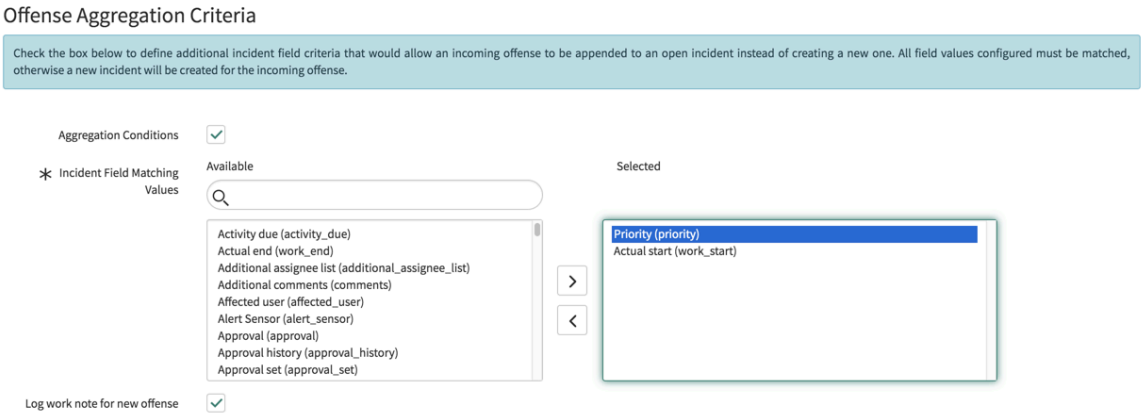
   Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.

2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Now Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Feldwerte für Vergehen zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte abgeglichen wird, sind die Bedingungen für die Zusammenfassung von Verstößen nicht erfüllt, und es wird ein neuer Security Incident erstellt. Im Screenshot unten sehen Sie die Zuordnung von Feldern mit mehreren Werten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn ein neuer Verstoß mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird der neue Verstoß automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Vergehen in einer zugehörigen Liste zu einem Security Incident anzeigen. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum diese Straftaten zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter Zugehörige Links, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.

3. (Optional) Um eine Arbeitsnotiz für einen neuen Verstoß zu protokollieren, der dem Security Incident kürzlich hinzugefügt wurde, aktivieren Sie diese Option. Die Arbeitsnotiz protokolliert, dass ein neuer Vergehen hinzugefügt wurde, zusammen mit einem Link zu den Vergehensdetails und anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben Werte aus einem Vergehen IBM QRadar erfolgreich Feldern in einem Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung zu begrenzen. Sie haben auch Vergehen an vorhandene Security Incidents angehängt, wenn Feldwerte für Vergehen den konfigurierten Zusammenfassungskriterien entsprechen.

4. Klicken Sie auf **Fortsetzen**, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem SIR Security Incident zugeordnet haben

### Zeigen Sie eine Vorschau des Security Incident für die IBM QRadar -Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem SIR Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Vergehensfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie als Benutzer mit der Rolle sn_si.admin eine Vorschau eines Security Incident an und bearbeiten Sie die Zuordnung bei Bedarf erneut, um fehlerhafte Felder zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security

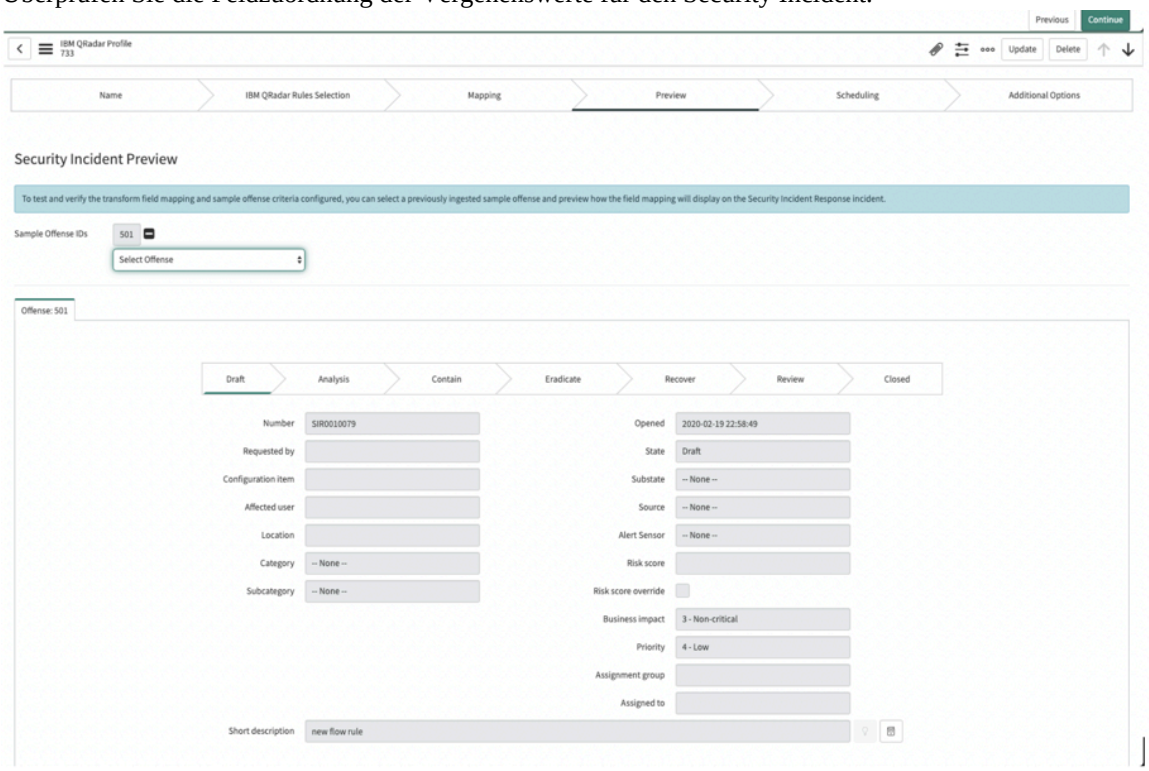


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incidents werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

### Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
2. Wählen Sie in der Auswahlliste Beispiel-IDs für Straftaten ein Element aus.
   Der Security Incident wird angezeigt. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Vergehenswerte für den Security Incident.




Die obige Abbildung zeigt ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

### Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

#### Definieren Sie einen Zeitplan für die Integration von IBM QRadar .

Sie können den Zeitplan für die Erfassung von Straftaten definieren. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf des Vergehens überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Straftaten mithilfe eines Datumsbereichs abrufen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Sie können wählen, ob Sie während des Schritts „Zeitplanung“ historische Verstöße erfassen möchten. Sie können auch auswählen, wie oft zukünftige neue Vergehen und aktualisierte Vergehen, die der Profilkonfiguration entsprechen, abgefragt werden sollen.

Als Benutzer mit der Rolle „sn_si.admin“ konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung der Integration der IBM QRadar -Offenheitserfassung kann durch die unterschiedlichen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrage-Overheads auf dem IBM QRadar -Server gegen den Wunsch ausgleichen, so schnell wie möglich benachrichtigt zu werden, wenn ein Verstoß erstellt oder aktualisiert wird. Für jedes Profil wird ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

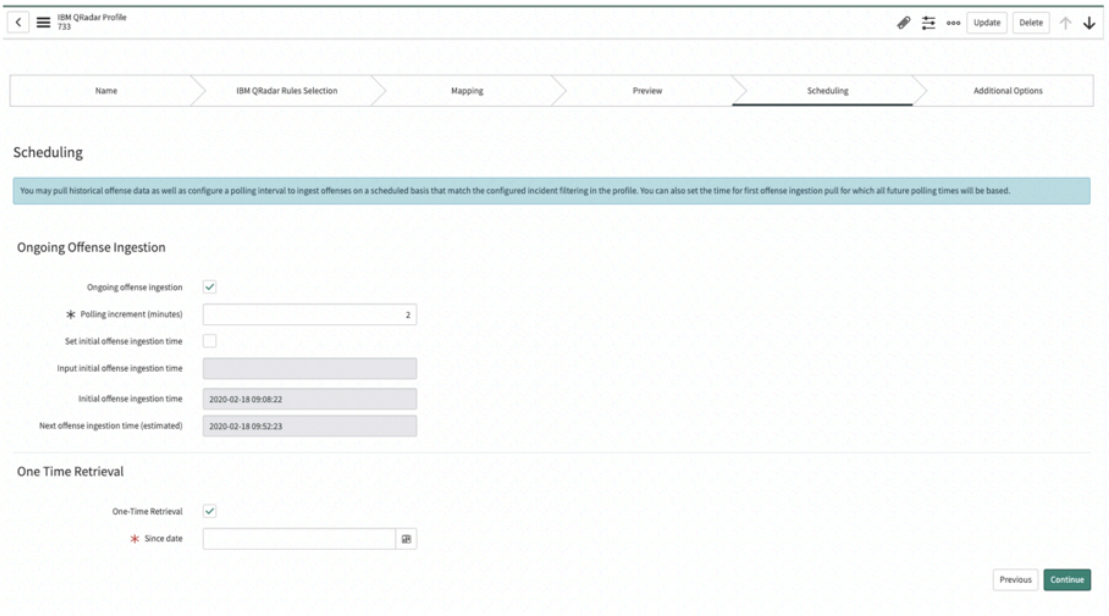
#### Neue und aktualisierte Straftaten werden abgerufen

Wenn der Abfragezeitplan festgelegt ist, ruft die regelmäßige Aufgabe sowohl neue als auch aktualisierte Straftaten ab, die zuvor abgerufen wurden, aber die Incident-Filterkriterien nicht erfüllt haben. Dies bietet Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die bei der ersten Erstellung eines Vergehens möglicherweise nicht vorhanden sind, aber nach einer Aktualisierung verfügbar werden, z. B. während der Untersuchungsphase. Sobald ein Incident für einen bestimmten Verstoß erstellt wurde, werden seine nachfolgenden Aktualisierungen ignoriert, da erwartet wird, dass der Verstoß jetzt als aktiver ServiceNow Security Incident behandelt wird. Alle anderen Straftaten, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Kriterien für die Incident-Generierung überprüft, bis sie Teil eines aktiven Incident werden.

### Prozedur
1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie einen aus, um zu planen, wie und wann Vergehen aus der Konsole IBM QRadar abgerufen werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie auf **Fortfahren**, um zur Seite „Zusätzliche Optionen“ zu navigieren.

### Automatisieren Sie die Aktualisierung und den Abschluss von Vergehen basierend auf dem SIR-Incident-Status

Die IBM QRadar -Integration verfügt über eine bidirektionale Schnittstelle, die die Erstellung von Security Incidents durch Vergehen ermöglicht, sowie über die Möglichkeit, die Vergehen zu aktualisieren, sobald der Security Incident mit relevanten Incident-Details wie Security Incident-Nummer und -Zuweisung erstellt und/oder geschlossen wurde -Gruppe, Security Incident-URL usw.

### Vorbereitungen

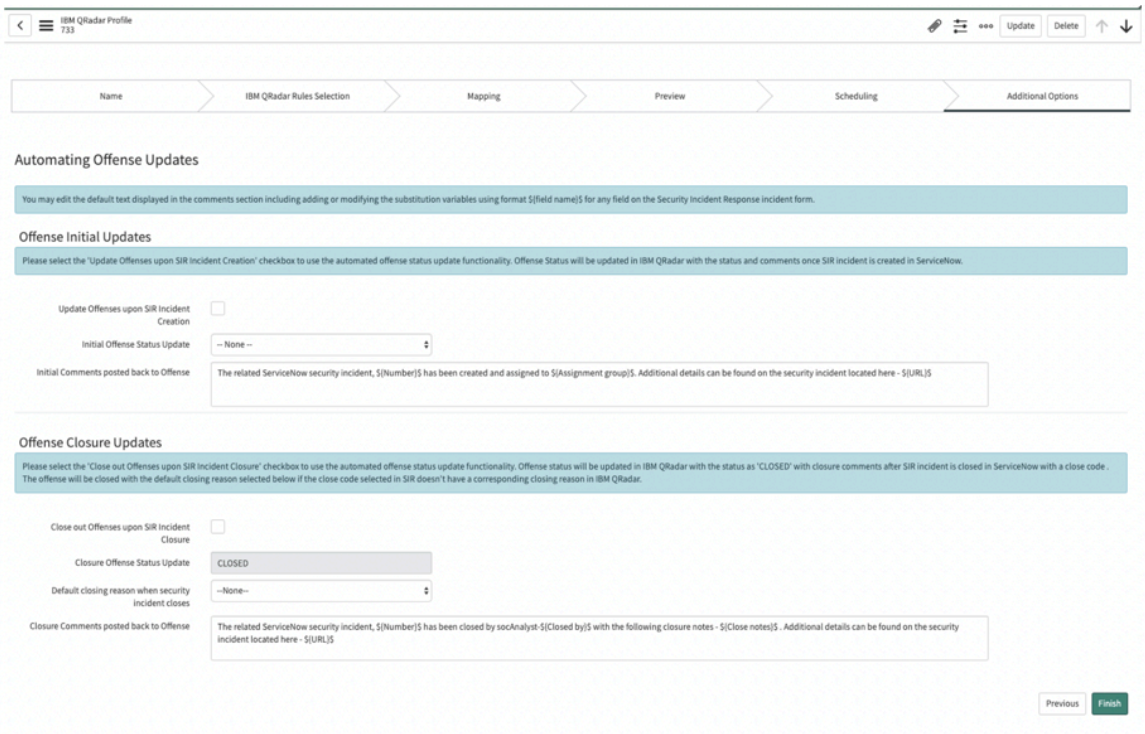
Erforderliche Rolle: sn_si.admin

### Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung von Verstößen abzuschließen, wenn der Security Incident erstellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu verschieben.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um basierend auf Ihrer Planung Vergehen aus der Konsole IBM QRadar abzurufen.

### IBM QRadar Konfigurationseinstellungen für -Integrationen

Verwenden Sie diese Option, um die Standardsystemeigenschaften der Erfassungsintegration IBM QRadar zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen**.

#### IBM QRadar-Integrationseinstellungen

| Eigenschaftsname | Beschreibung |
|---|---|
| Grenzwert für die Anzahl von Security Incidents erzwingen, die innerhalb von 24 Stunden erstellt werden können.<br><br>sn_sec_qradar.max_si_per_day | Gibt die maximale Anzahl von Security Incidents an, die innerhalb von 24 Stunden erstellt werden können.<br>• Typ: Ganzzahl<br>• Standardwert: 1000 |
| Erzwingen Sie eine Begrenzung der Anzahl von Verstößen, die zu einem einzelnen Incident zusammengefasst werden können.<br><br>sn_sec_qradar.max_aggregation_per_si | Der Grenzwert für die Zusammenfassung von Verstößen für einen Security Incident. Beispiel: Wenn es 102 Vergehen gibt, werden die ersten 100 Vergehen zu Security Incident_1 und die verbleibenden 2 zu Security Incident_2zusammengefasst. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**IBM QRadar-Integrationseinstellungen (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| | • Typ: Ganzzahl<br>• Standardwert: 100 |
| Diese Eigenschaft legt den Zeitraum von AQL fest, um die letzten Ereignisse/Flows für einen bestimmten Verstoß abzurufen.<br><br>sn_sec_qradar.on_demand_recent_days_limit | Gibt die Anzahl der Tage an, um aktuelle Events oder Flows für einen bestimmten Verstoß abzurufen.<br>• Typ: Ganzzahl<br>• Standardwert: 7 |
| Diese Eigenschaft begrenzt die Anzahl der aktuellen Ereignisse, die für einen bestimmten Verstoß abgerufen werden.<br><br>sn_sec_qradar.on_demand_event_limit | Gibt die Anzahl der Ereignisse an, die für einen Verstoß abgerufen werden. Die neuesten Events werden basierend auf dem Event-Zeitstempel zuerst abgerufen.<br>• Typ: Ganzzahl<br>• Standardwert: 100 |
| Diese Eigenschaft begrenzt die Anzahl der aktuellen Flows, die für einen bestimmten Verstoß abgerufen werden.<br><br>sn_sec_qradar.on_demand_flow_limit | Gibt die Anzahl der Flows an, die für einen Verstoß abgerufen werden. Die neuesten Flows werden basierend auf dem Flow-Zeitstempel zuerst abgerufen.<br>• Typ: Ganzzahl<br>• Standardwert: 100 |
| Diese Eigenschaft legt den Zeitüberschreitungswert (Sekunden) für die AQL fest, die aktuelle Flows/ Ereignisse für einen bestimmten Verstoß abruft.<br><br>sn_sec_qradar.on_demand_timeout | • Typ: Ganzzahl<br>• Standardwert: 300 |
| Zeitüberschreitung für Such-IDs (Sekunden) für Datensätze in der Warteschlange für die Abfrage von AQLs eines Verstoßes.<br><br>sn_sec_qradar.sid_ttl | Die Zeitüberschreitung der AQL für einen Verstoß in der Warteschlange, bevor ein Security Incident erstellt wird. Wenn beispielsweise 90 Vergehen vorliegen, werden die ersten 50 Vergehen für AQL-Daten im ersten Batch und die verbleibenden 40 Vergehen im nachfolgenden Batch im selben Abfrageintervall verarbeitet.<br>• Typ: Ganzzahl<br>• Standardwert: 300 |
| Schwellenwert zur Steuerung der Anzahl der Suchvorgänge, die in IBM QRadar gleichzeitig ausgeführt werden können, was | Gibt die Anzahl der Vergehen an, die Sie in einem einzelnen Batch in einem Abfrageintervall abrufen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**IBM QRadar-Integrationseinstellungen (Fortsetzung)**

| Eigenschaftsname | Beschreibung |
|---|---|
| durch die geplante Integration ausgelöst wird<br><br>job.sn_sec_qradar.records_threshold_in_que_for_aql | • Typ: Ganzzahl<br>• Standardwert: 50 |
| Dies ist die Anzahl der Tage für die Bereinigung von Integrationstabellen.<br><br>sn_sec_qradar.queue_item_expire | Im Folgenden sind die Integrationstabellen aufgeführt:<br>• sn_sec_qradar_events: IBM QRadar-Ereignisse<br>• sn_sec_qradar_flows: IBM QRadar-Flows<br>• sn_sec_qradar_offense_updates: IBM QRadar-Aktualisierungen für Straftaten<br>• sn_sec_qradar_offense_to_task – IBM QRadar-Angriff auf Aufgabe<br>• Typ: Ganzzahl<br>• Standardwert: 30 |
| Grenzwert für Straftaten pro geplanter Aufgabe, die pro Profil ausgeführt wird, entweder beim einmaligen Abruf oder bei laufender Erfassung.<br><br>sn_sec_qradar.max_offense_limit_per_run | Gibt die Anzahl der Straftaten an, die Sie bei einem einzigen Abruf in die Now Platform abrufen.<br>• Typ: Ganzzahl<br>• Standardwert: 1000 |
| Legen Sie diese Eigenschaft fest, um die Funktion „Aktualisierungen von Straftaten“ zu aktivieren.<br><br>sn_sec_qradar.get_offense_updates | **Hinweis:**<br>Das Aktivieren dieser Einstellung kann zu einer Verzögerung beim Erstellen eines Security Incident führen.<br>• Typ: true \| false<br>• Standardwert: falsch |

Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

### Optional: Kopieren Sie ein IBM QRadar -Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Profile zu kopieren, um Zeit zu sparen.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Warum und wann dieser Vorgang ausgeführt wird**
Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor Abschluss der Konfiguration nicht versehentlich

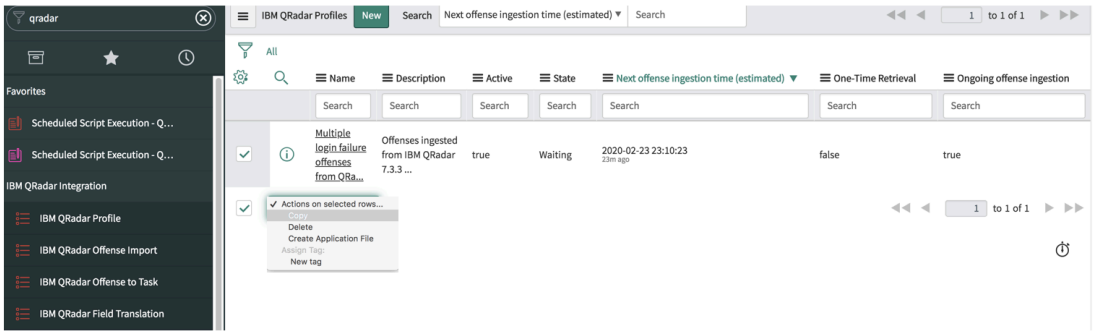


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

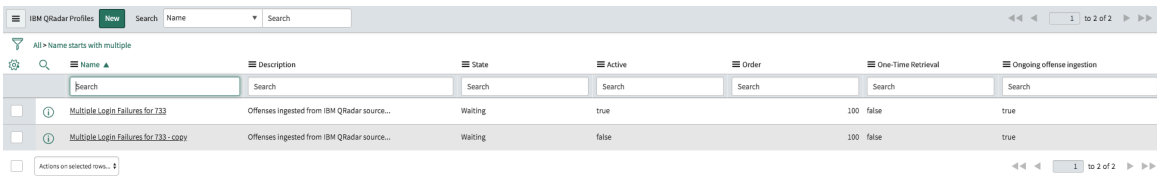
### Prozedur

1. Navigieren zu **Alle** > **Integration mit IBM QRadar** > **IBM QRadar-Profil**.
2. Wählen Sie in der angezeigten Liste „IBM QRadar-Profile“ ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.




Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält copy. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.

**Hinweis:**
Wenn Sie eine andere Quelle für das Profil auswählen, müssen Sie neue Regeln (Wählen Sie IBM QRadar Regeln aus) für das Profil auswählen. Wenn Sie jedoch dieselbe Quelle verwenden und neue Regeln auswählen, werden die Beispielvergehen gelöscht.




Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **Aktiv** auf „false“ gesetzt ist, da das Profil aktiviert werden muss.

### Nächste Maßnahme

Nachdem Sie die Konfigurationsschritte abgeschlossen haben, werden Sie aufgefordert, das neue Profil zu aktivieren.

## Domänentrennung und IBM QRadar Erfassung von Straftaten

Domänentrennung wird bei der Erfassung von IBM QRadar -Angriffen unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

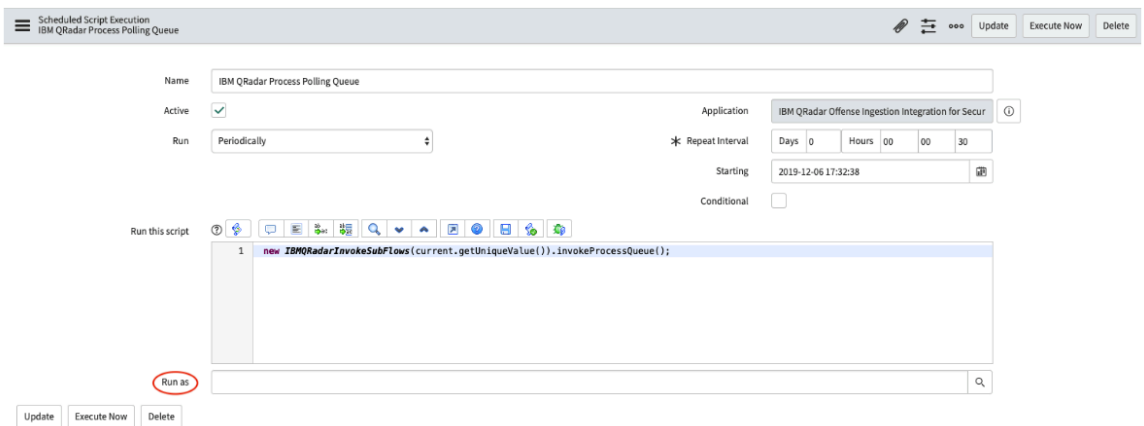
## Funktionsweise der Domänentrennung in IBM QRadar Offense Ingestion

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der Rolle `sn_si.admin` in der entsprechenden Domäne.

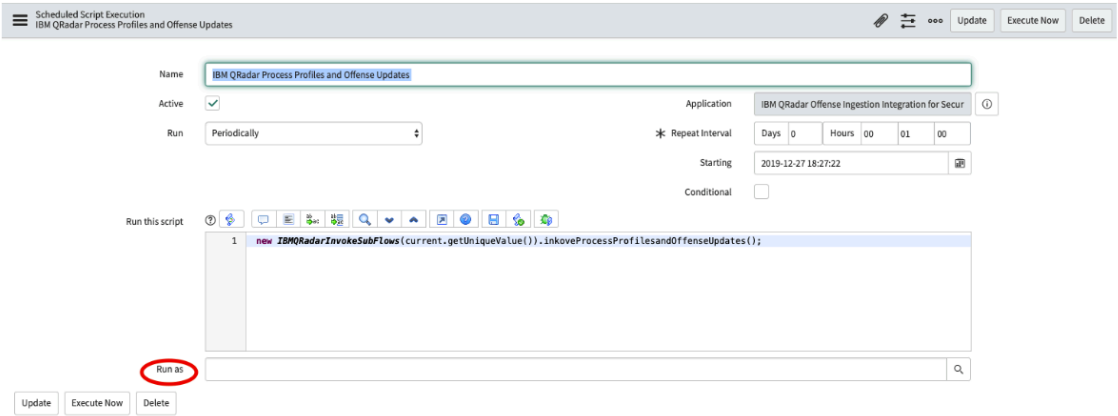
> **Hinweis:**
> Verwenden Sie beim Erstellen des Profils die Domänenauswahl, um die spezifische Domäne auszuwählen. Erstellen Sie den Benutzer nicht in der übergeordneten Domäne und ändern Sie später die Domäne des Profils. Sie sollten einen bestimmten Benutzer für jede Domäne für Ihr Profil mit der Rolle `sn_si.admin haben`. Verwenden Sie diesen Benutzer, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie die geplanten Aufgaben „ IBM QRadar Prozessabfragewarteschlange“, IBM QRadar „ Prozessprofile“ und „Aktualisierungen von Offensiven“ für jede Domäne.
- Ändern **Sie Ausführen als** vom Systembenutzer in den Benutzer mit der Rolle `sn_si.admin` in der entsprechenden Domäne, und führen Sie die geplante Aufgabe aus.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Zugehörige Informationen**

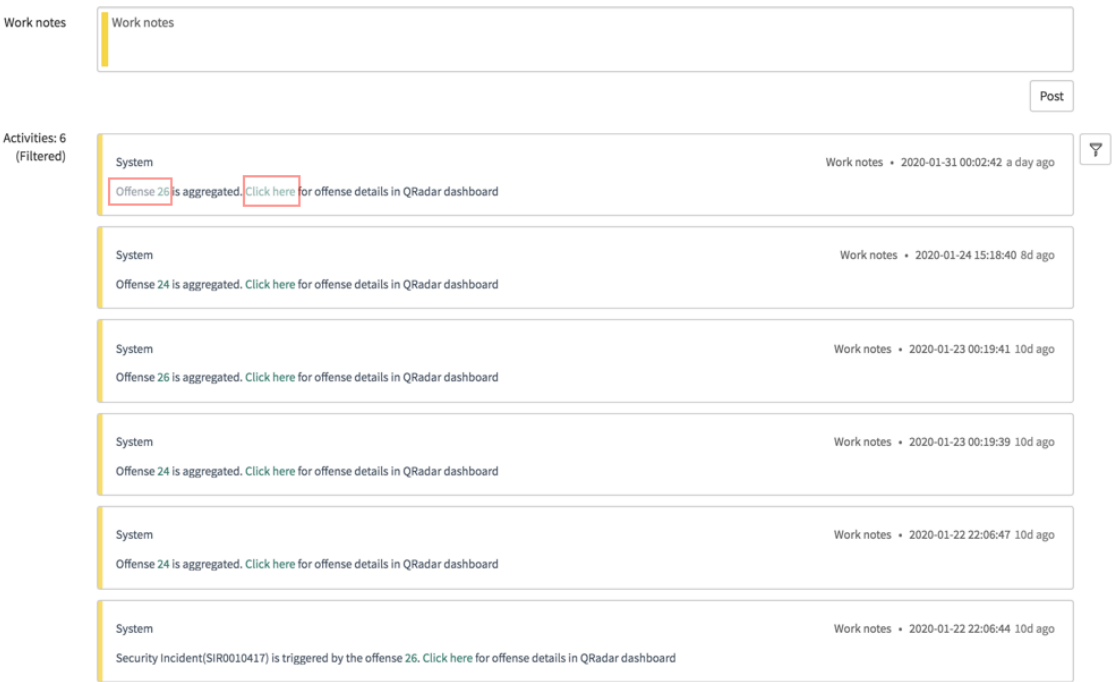
Domänentrennung für Service Provider

### Security Incident Response-Formular nach Erfassung von Sicherheitsvorfällen

Nachdem ein IBM QRadar -Vergehen erfasst wurde, wird ein Security Incident erstellt und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

## Arbeitsnotiz

Eine Arbeitsnotiz mit Details zu dem Vergehen, das den Security Incident ausgelöst hat, wird veröffentlicht.

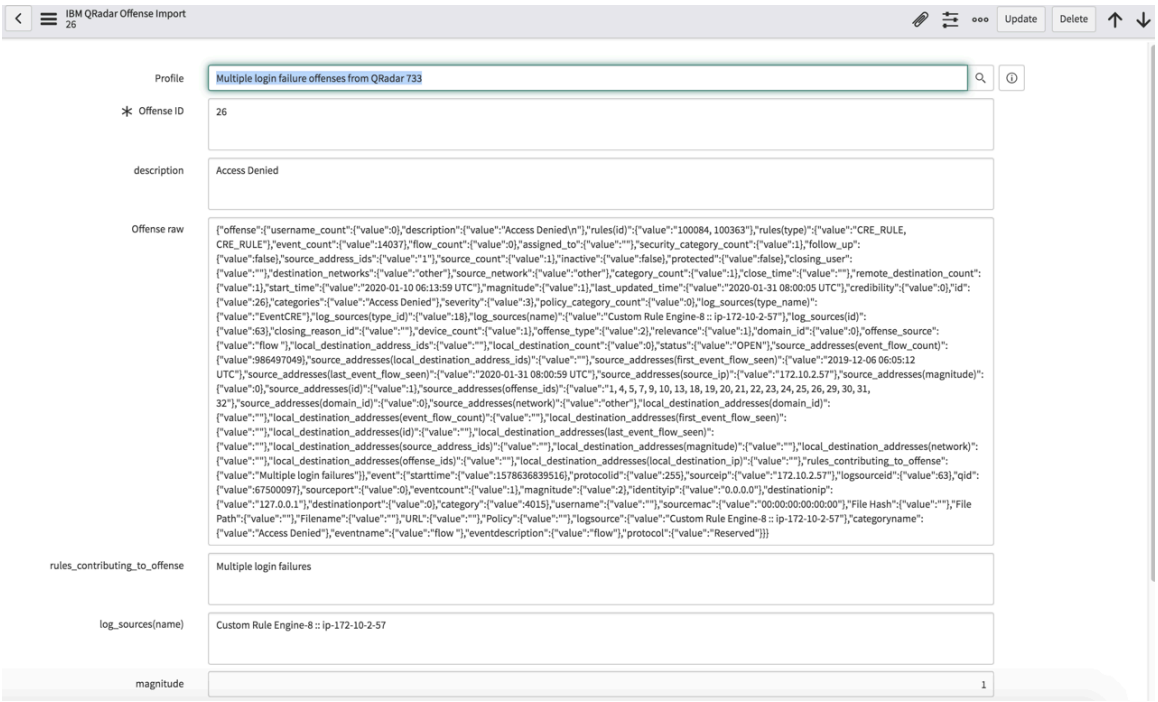



Klicken Sie auf den Link für den Verstoß, um zum internen Security Incident-Datensatz zu navigieren. Der Hyperlink Hier **klicken** führt Sie zum Dashboard IBM QRadar, in dem Sie die Vergehensdetails anzeigen können.

Wenn Sie die Option **Arbeitsnotiz für neuen Verstoß** protokollieren in den Kriterien für die Zusammenfassung von Straftaten ausgewählt haben, wie in IBM QRadar -Angriffsfelder werden Security Incident-Antwortfeldern zugeordnetbeschrieben, wird bei der Zusammenfassung des Vergehens eine Arbeitsnotiz veröffentlicht.

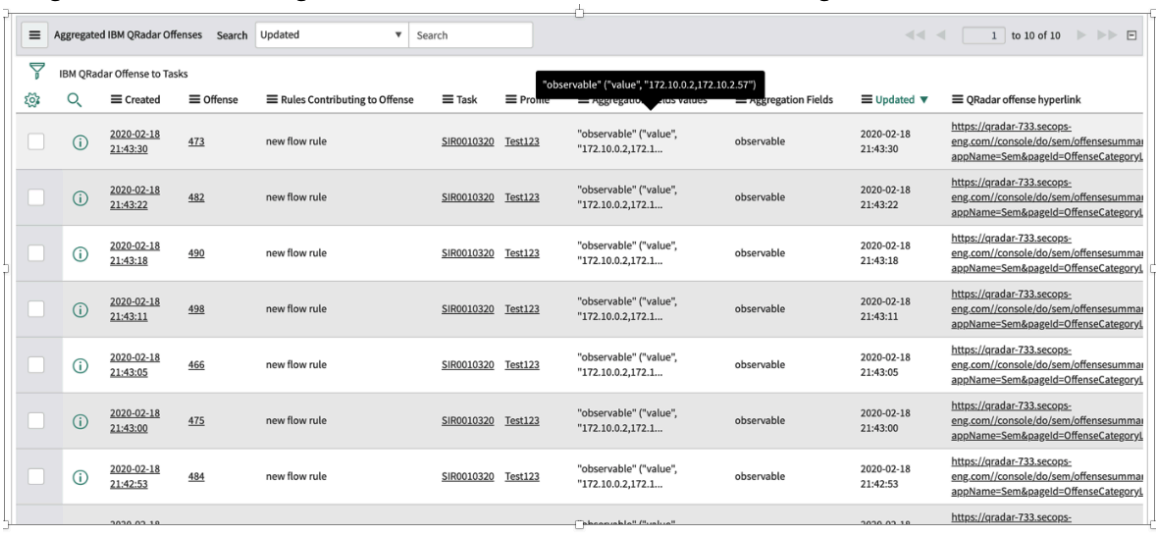


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Zusammengefasste Straftaten

Klicken **Zugehörige Listen** > **Zusammengefasste IBM QRadar-Vergehen** , um die zum Security Incident zusammengefassten Straftaten anzuzeigen. Klicken Sie auf den Hyperlink QRadar-Vergehen, um den Vergehen im Dashboard IBM QRadar anzuzeigen.

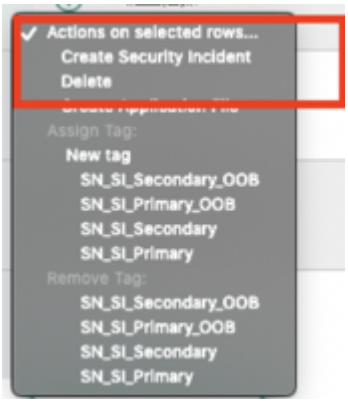



Security Incident erstellen: Wählen Sie einen Verstoß aus der Liste aus, klicken Sie auf das Menü **Aktionen** und dann auf **Security Incident erstellen**. Diese Option erstellt einen Security Incident für den Vergehen, und dieser Vergehen wird vom übergeordneten Security Incident getrennt.

Verstoßdatensatz löschen: Wählen Sie einen Verstoß aus der Liste aus, klicken Sie auf das Menü **Aktionen** und dann auf **Löschen**. Mit dieser Option wird der Vergehensdatensatz gelöscht.

Automatische Übersetzung

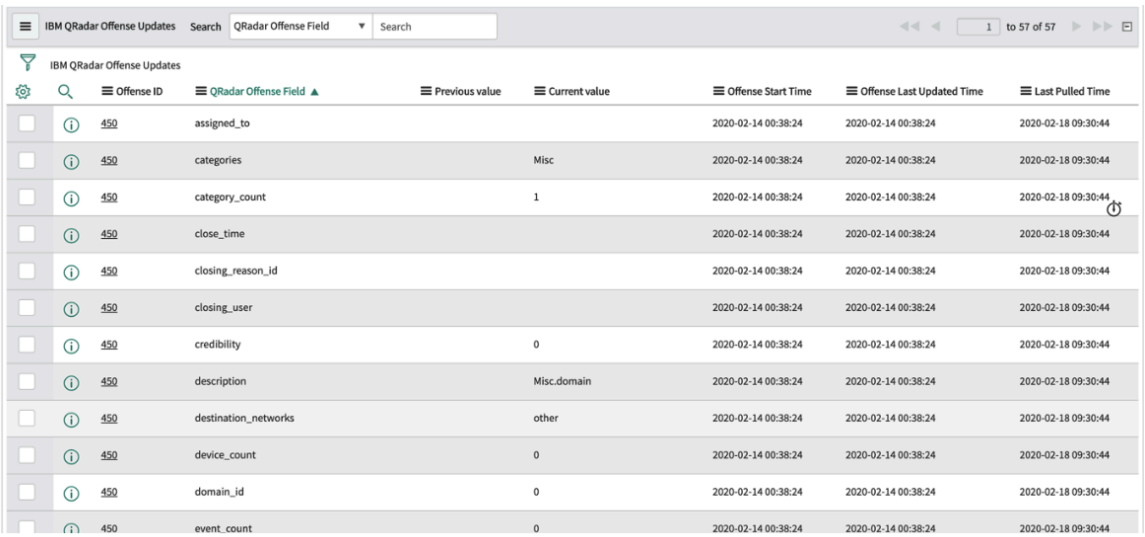
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Aktualisierungen für IBM QRadar-Vergehen

Dies zeigt die standardmäßigen und benutzerdefinierten Vergehensfelder und verfolgt Änderungen am Vergehen während jedes Abfrageintervalls. Dies ist hilfreich, da Sie Aktualisierungen von Vergehen direkt anzeigen können, ohne zum Dashboard IBM QRadar navigieren zu müssen. Alle Änderungen an den Werten werden in den Feldern Vorheriger Wert und Aktueller Wert angezeigt.

Um die Funktion „Aktualisierungen von Straftaten“ zu aktivieren, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen** und aktivieren **Legen Sie diese Eigenschaft fest, um die Funktion „Aktualisierungen von Straftaten“ zu aktivieren**. Standardmäßig ist diese Einstellung deaktiviert.

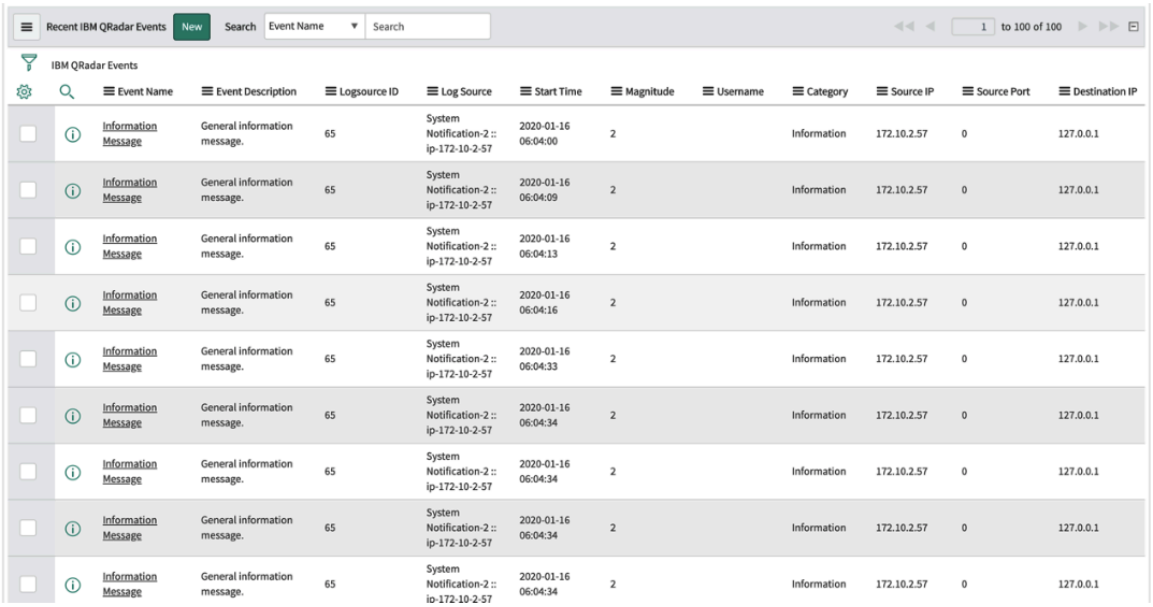



## Aktuelle IBM QRadar-Events

Klicken Sie unter **Zugehörige Links** auf die Option **Recent IBM QRadar Events abrufen**, um die neuesten IBM QRadar Events anzuzeigen.

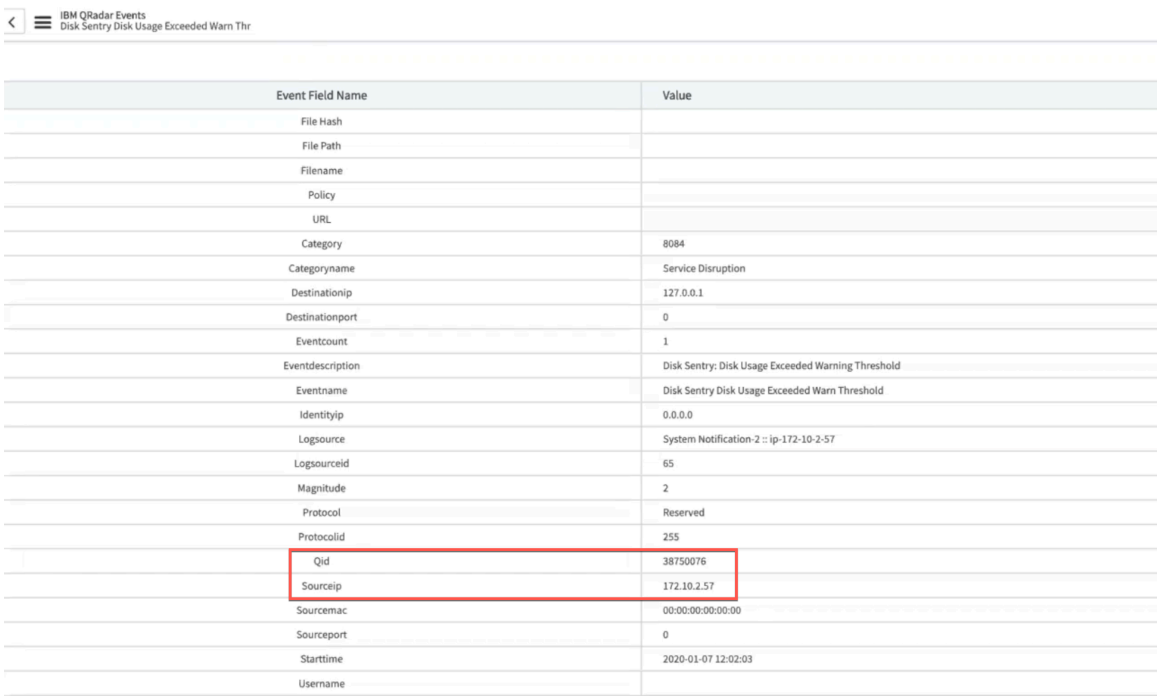


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Standardmäßig werden maximal 100 Events angezeigt. Sie können diese Standardeinstellung in IBM QRadar Konfigurationseinstellungen für -Integrationenändern.

**Hinweis:**
Die obige Abbildung zeigt die standardmäßigen Event-Felder, die dem Vergehen zugeordnet sind. Wenn Sie benutzerdefinierte Event-Felder konfiguriert und zugeordnet haben (siehe IBM QRadar -Angriffsfelder werden Security Incident-Antwortfeldern zugeordnet), können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Event-Name klicken.



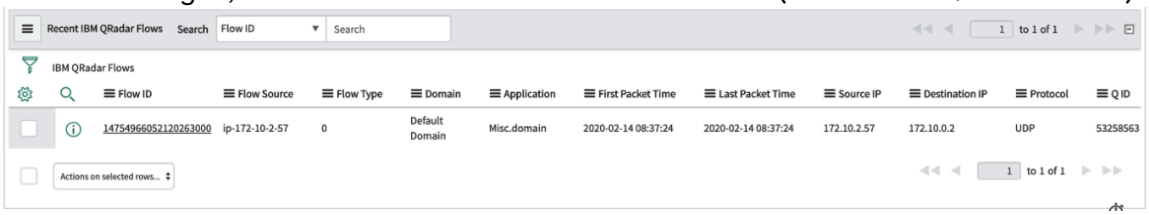

## Aktuelle IBM QRadar-Flows

Mit Integration Hub und Flow Designer sind mehrere Flows, Subflows und Aktionen mit der IBM QRadar -Integration verfügbar. Wenn Sie unter den zugehörigen Links auf die Option



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Recent IBM QRadar Flows abrufen** klicken, werden die neuesten Flows abgerufen. Um diese Flows anzuzeigen, klicken Sie auf **Recent IBM QRadar Flows**(Letzte IBM QRadar-Flows).




Standardmäßig werden maximal 100 Flows angezeigt. Sie können diese Standardeinstellung in IBM QRadar Konfigurationseinstellungen für -Integrationenändern.

**Hinweis:**
Die obige Abbildung zeigt die Standard-Flow-Felder, die dem Vergehen zugeordnet sind. Wenn Sie benutzerdefinierte Flow-Felder konfiguriert und zugeordnet haben (siehe IBM QRadar -Angriffsfelder werden Security Incident-Antwortfeldern zugeordnet), können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Flow-ID klicken.

### Verwendung von Flow Designer und Integration Hub mit IBM QRadar-Integration der Straftatenerfassung

Mit der Funktionalität von Flow Designer und Integration Hub wurden mehrere Subflows und Aktionen als Teil der Integration der IBM QRadar -Angriffserfassung erstellt.

Die folgenden IBM QRadar Subflows sind verfügbar:

- Validierung von Verbindungen und Anmeldeinformationen: Wird in der Konfigurationskachel zur Validierung des Hosts und der Anmeldeinformationen beim ersten Setup verwendet.
- IBM QRadar-Regelabruf: Dies wird im Abschnitt „Regeln“ des Profil-Setups verwendet, um alle aktiven Regeln in IBM QRadarabzurufen. Dieser Subflow wird asynchron ausgelöst.
- Beispieldaten zu Straftaten aus IBM QRadar abrufen: Wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.
- IBM QRadar-Angriffsstatusaktualisierungen: Wird jede Minute durch eine geplante Aufgabe ausgelöst und aktualisiert den Vergehen in IBM QRadar, wenn der Security Incident erstellt oder geschlossen wird.
- Profile ausgeplanter Aufgabe und Verstößen in der Warteschlange verarbeiten: Wird jede Minute durch eine geplante Aufgabe ausgelöst, um Verstöße pro Profil basierend auf dem Abfrageintervall abzurufen. Dadurch werden Verstöße abgerufen und zur weiteren Verarbeitung in die Abfragetabelle eingereiht.
- Abfragewarteschlange verarbeiten und in Batches abfragen: Wird alle 30 Sekunden durch eine geplante Aufgabe ausgelöst, um die Abfragetabellenwarteschlange zu verarbeiten.
- Aktuelle IBM QRadar-Flows abrufen: Wird über den Link des Security Incident-Formulars ausgelöst, um die neuesten Flows des Vergehens abzurufen.
- Letzte IBM QRadar-Ereignisse abrufen: Wird über den Link des Security Incident-Formulars ausgelöst, um die neuesten Verstoßereignisse abzurufen.

Um diese Subflows anzuzeigen, melden Sie sich als Benutzer mit der Rolle `sn_si.admin` an, und navigieren Sie zu **Flow Designer** > **Designer**. Klicken Sie auf den Link Name eines der oben aufgeführten Subflows, um den Subflow im Detail anzuzeigen.



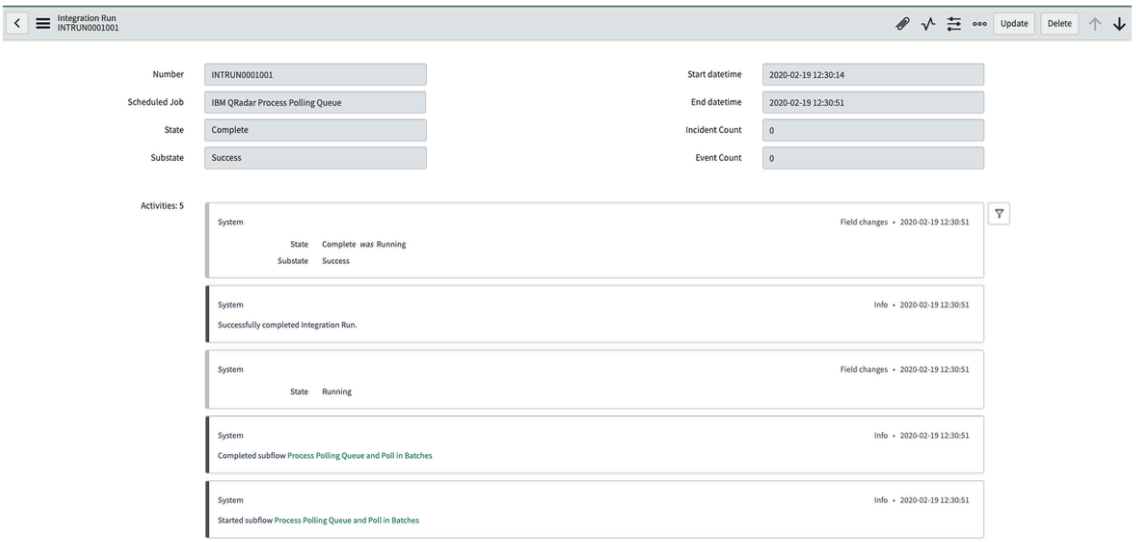
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Problembehandlung bei der Integration der IBM QRadar -Offenheitserfassung

In diesem Abschnitt werden wichtige Tipps zur Problembehandlung und häufig gestellte Fragen im Zusammenhang mit der Erfassung von IBM QRadar -Angriffen behandelt.

- Integrationsausführung: Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Integrationsausführungsdatensatz mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der gezogenen Straftaten und die Anzahl der Incidents, die in einer geplanten Aufgabe erstellt wurden, werden ebenfalls angezeigt. Benutzer mit der Rolle sn_si.analyst können sehen, ob während der Integrationsausführung Fehler/Profilabrufe fehlgeschlagen sind.

  Arbeitsnotizen in der Integrationsausführung enthalten Links zu den ausgeführten Subflows. Benutzer mit der Rolle sn_si.analyst können die Tabelle sn_event_ingestion_integration_run auf aufgetretene Fehler überprüfen. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Integrationsausführungsdatensätzen für jede Ausführung einer geplanten Aufgabe protokolliert.




- SSL-Probleme: Stellen Sie beim Herstellen einer Verbindung mit IBM QRadar Cloud-Instanzen sicher, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in die -Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Details siehe https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 .
- Unvollständiges Profil: Während der Konfiguration des Profils müssen Sie im Abschnitt „Zusätzliche Optionen“ (Automatisieren Sie die Aktualisierung und den Abschluss von Vergehen basierend auf dem SIR-Incident-Status) auf die Schaltfläche **Fertig** stellen klicken, um sicherzustellen, dass das Profil in den Status Warten verschoben wird, um anzuzeigen, dass es auf die Erfassung wartet.
- Profil validieren: Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die Profilstatus, das Datum des letzten Abrufs des Profils, die Importtabelle für Vergehen und die Datensätze der Tabelle „Vergehen zu Aufgabe“.
- MID-Server-Konfiguration: Wenn Sie die Anwendung IBM QRadar lokal installieren, müssen Sie nach der Konfiguration des MID-Servers eine MID-Server-Anwendung erstellen. Der MID-Server-Anwendungsname sollte in der Kachel „Integrationskonfigurationen“ anstelle des MID-Server-Namens verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die standardmäßige Zeitüberschreitung für MID-Server beträgt 30 Sekunden. Anweisungen zum Deaktivieren der Zeitüberschreitung finden Sie unter <link>. Beachten Sie, dass dies eine systemweite Änderung ist, die sich auf andere Integrationen auswirken kann.

- Updates für Offenses: Wenn Sie die Eigenschaft *sn_sec_qradar.get_offense_updates* aktiviert haben und eine Verzögerung bei der Erstellung von Security Incidents feststellen, deaktivieren Sie die Eigenschaft. Aktivieren Sie diese Eigenschaft nicht, wenn das Abfrageintervall niedrig und die Last der Vergehen in QRadar hoch ist, da dies die Last der Warteschlange erhöht.
- Event, Flow-Daten, remote_ip oder Benutzerdaten in einem Security Incident fehlen: Wenn Sie feststellen, dass Event, Flow-Daten, remote_ip oder Benutzerdaten in einem Security Incident fehlen, erhöhen Sie die Zeitüberschreitung (Sekunden) für den Parameter *sn_sec_qradar.sid_ttl*. Durch Erhöhen der Dauer wird die Erstellung des Security Incident verzögert, bis die AQLs die Analyse jedes Verstoßes abgeschlossen haben.
- Zeitüberschreitungen: Wenn Sie Zeitüberschreitungsfehler in den Anwendungsprotokollen anzeigen, überprüfen und ändern Sie die folgenden Flow Designer-Aktionen:

**Flow Designer-Aktionen**

| Parameter | Aktion |
|---|---|
| **Rufen Sie Beispielvergehen ab**<br>`var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);` | Überprüfen und aktualisieren Sie die Dauer in Millisekunden. |
| **Rufen Sie Beispielvergehen ab**<br>`var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);` | Fügen Sie einen Parameter für *executeAction hinzu*, und geben Sie die Dauer in Millisekunden ein. |
| **Ruft Vergehen für Profil- und Warteschlangendatensätze in der Abfragetabelle ab**<br>`var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);` | Überprüfen und aktualisieren Sie die Dauer in Millisekunden. |
| **Wrapper zum Testen der Verbindung REST**<br>`var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);` | Fügen Sie einen Parameter für *executeAction hinzu*, und geben Sie die Dauer in Millisekunden ein. |
| **Wrapper zum Validieren von API-Anmeldeinformationen REST** | Fügen Sie einen Parameter für *executeAction hinzu*, und geben Sie die Dauer in Millisekunden ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Parameter | Aktion |
| --- | --- |
| `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);` | |
| **REST-Schritt für IBM QRadar-Angriffsaktualisierungen**<br>`var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);` | Überprüfen und aktualisieren Sie die Dauer in Millisekunden. |

## IBM QRadar – Integration der Incident-Ergänzung

Die Integration IBM QRadar – Incident-Ergänzung durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

### Erkunden

Security Incident Response-Integrationen

### Einrichten

- Beginnen Sie mit der Integration von IBM QRadar – Incident-Ergänzung
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

### Verwenden

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungs-such-Workflow
- Workflow „Security Operations – QRadar-Sichtungssuche“.
- Sichtungssuchdetails anzeigen
- Sichtungssuchergebnisse anzeigen

### Entwickeln

- ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

### Problembehandlung und Hilfe

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Beginnen Sie mit der Integration von IBM QRadar – Incident-Ergänzung

IBM QRadar ist ein SIEM-Produkt (Enterprise Security Information and Event Management), das sich problemlos in Security Operationsintegrieren lässt. Bevor Sie die Integration IBM



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

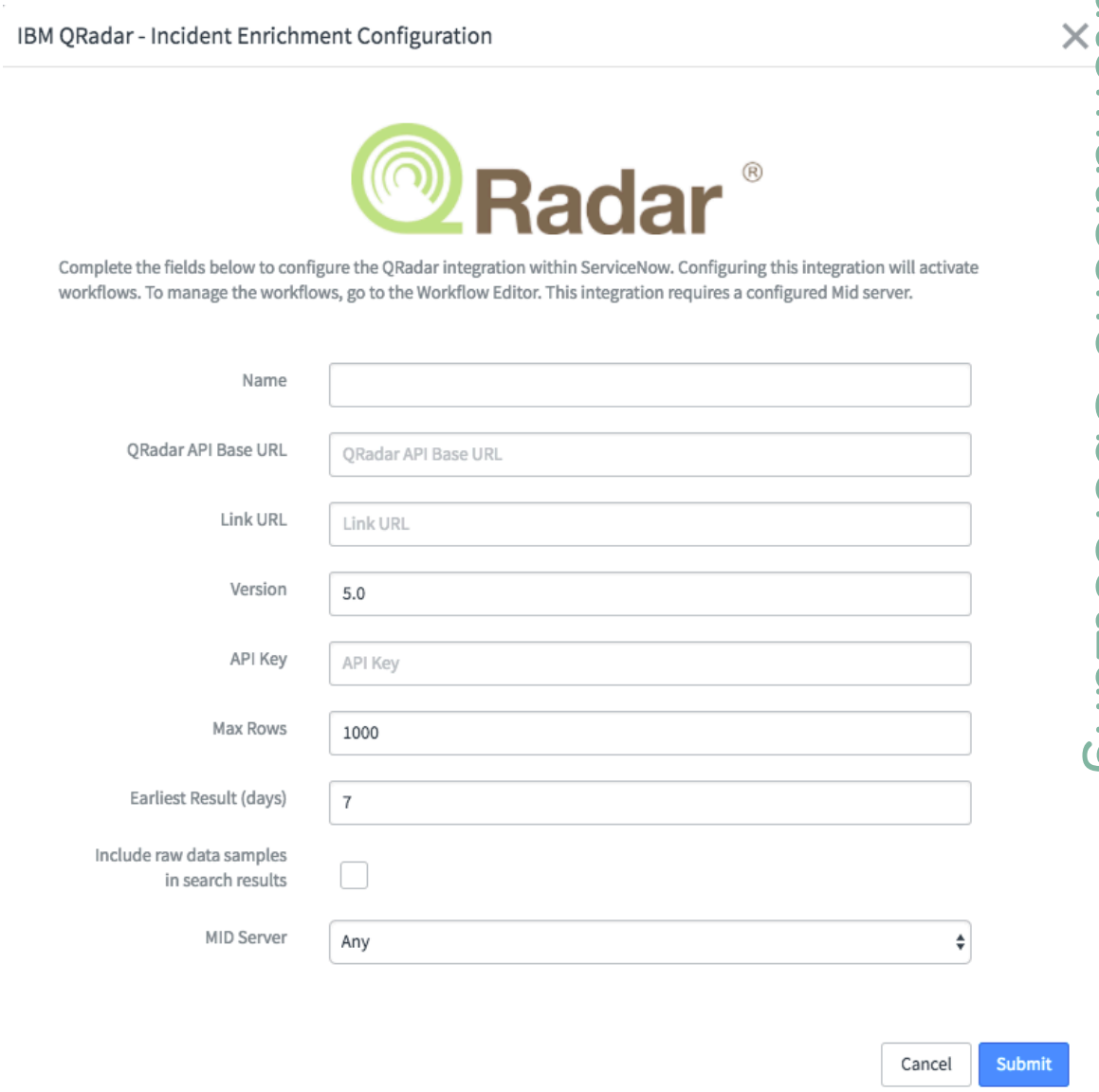
QRadar - Incident Enrichment verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechende API-Basis-URL und den API-Schlüssel hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf IBM QRadar zu, und rufen Sie die API-Basis-URL und den API-Schlüssel unter Ihrem IBM QRadar -Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie in der Karte IBM QRadar – Incident-Ergänzung auf **Neu**.




5. Füllen Sie die Felder nach Bedarf aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Basis-URL der QRadar-API | Die Basis-URL, die Sie von der Website IBM QRadar erhalten haben. |
| Link-URL | [Optional] Die Link-URL, die auf eine IBM QRadar -Instanz verweist, sofern verfügbar. |
| Version | Die Version IBM QRadar ; 5.0 ist der Standardwert. |
| API-Schlüssel | Der API-Schlüssel, den Sie von der Website IBM QRadar erhalten haben. |
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |
| Rohdatenmuster in Suchergebnissen berücksichtigen | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## LogRhythm-Übersicht

Die Zuordnungsflexibilität dieser Integration bietet einem Analysten Einblick in Events und zugehörige Alarmdaten, die zur weiteren Untersuchung und Korrektur in Now Platform Security Incidents integriert werden können.

Alarmprofile werden in Ihrer Instanz Now Platform erstellt, um anzupassen, wie verschiedene LogRhythm Alarmfelder in einem Security Incident von Now Platform angezeigt werden. Eine Standardzuordnung von Alarmfeldern wird bereitgestellt, die entsprechend den kundenspezifischen Anforderungen bearbeitet werden kann.

Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. Wenn ein Event die Erstellung eines Security Incident in der Now Platform® -Instanz auslöst, wird von Ihrer Now Platform® -Instanz eine Anforderung gesendet, Alarme aus der LogRhythm -Client-Konsole entweder über einen MID-Server oder sogar ohne MID-Server abzurufen.

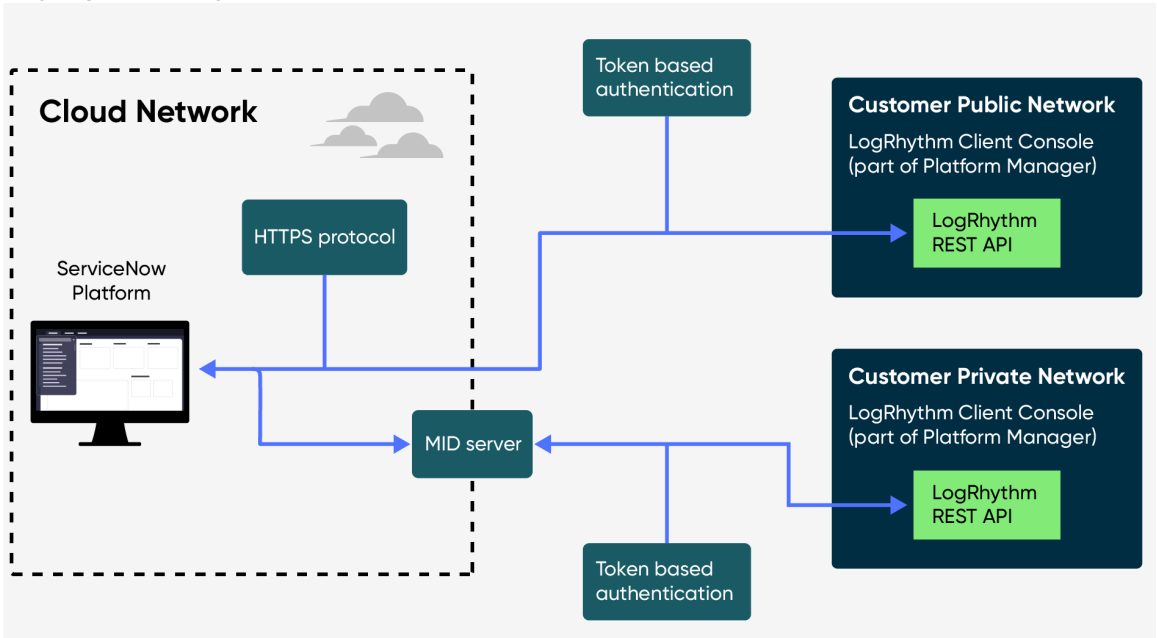
Der REST-API-Schlüssel wird von Now Platform® zur Authentifizierung bei der Clientkonsole von LogRhythm verwendet. Über diese Verbindung kann Ihre Instanz Now Platform einzelne LogRhythm -Alarme basierend auf konfigurierten Profilen abrufen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die REST-API wird verwendet, um Nachrichtendetails zu erfassen, auf die die REST-API nicht zugreift.

**LogRhythm-Integration**




## Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Flexibilität zum Erstellen mehrerer Alarmprofile für verschiedene Alarmtypen wie Phishing und Malware.
- Drag-and-Drop-Zuordnung von LogRhythm Alarmfeldwerten zu zugeordneten SIR Security Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf LogRhythm Beispielalarmen.
- Erfassen Sie historische Alarme sowie laufende zukünftige Alarme in konfigurierbaren Intervallen.
- Automatisierter LogRhythm Alarmabschluss nach Incident-Abschluss von SIR. Eine URL zum Incident SIR sowie eine Incident-ID werden als Referenz bereitgestellt.

## Unterstützte Releases von Now Platform

Diese Integration ist mit Quebec oder späteren Releases von Now Platform®kompatibel.

## Unterstützte Versionen von LogRhythm

Diese Integration ist mit LogRhythm 7.8 oder höher kompatibel. Die früheren Versionen werden aufgrund von API-Einschränkungen nicht unterstützt.

**Hinweis:**
Die folgenden Themen sind nummeriert. Um eine reibungslose Installation zu gewährleisten und die erwarteten Ergebnisse zu überprüfen, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie die REST-API für ein LogRhythm

Sie verwenden den REST-API-Schlüssel LogRhythm, um zusätzliche Event-Details für einzelne Alarmfelder zu erfassen. Der API-Schlüssel enthält Details, die mit der REST-API LogRhythm nicht verfügbar sind.

## Vorbereitungen

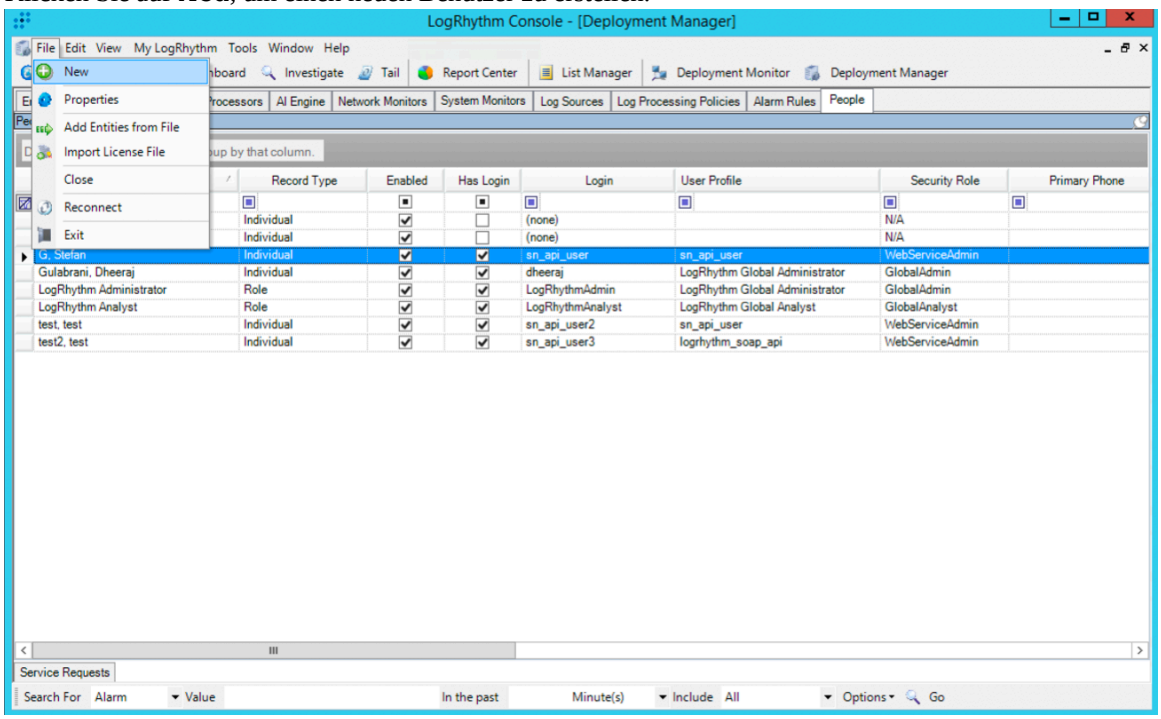
Erforderliche Rolle: LogRhythm Clientkonsole/Platform Manager-Administrator

## Warum und wann dieser Vorgang ausgeführt wird

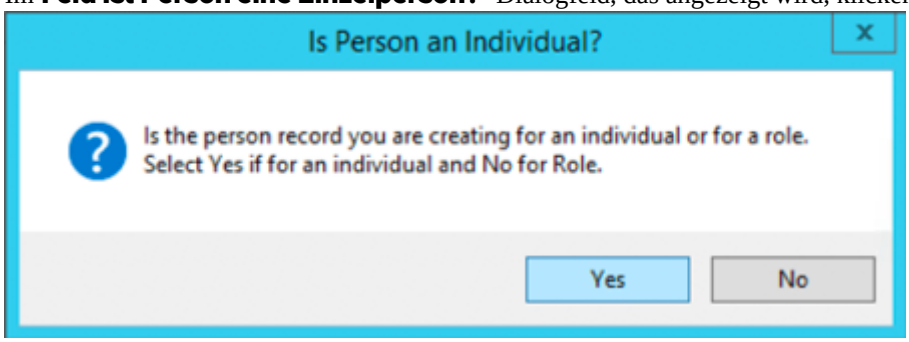
Diese Aufgabe wird in der Clientkonsole LogRhythm ausgeführt. Richten Sie die REST-API LogRhythm ein, bevor Sie das Plugin aus dem ServiceNow Storeinstallieren.

## Prozedur

1. Navigieren Sie zur LogRhythm Clientkonsole, und wählen Sie das Menü **Datei** aus.
2. Klicken Sie auf **Neu**, um einen neuen Benutzer zu erstellen.




3. Im **Feld Ist Person eine Einzelperson?** -Dialogfeld, das angezeigt wird, klicken Sie auf **Ja**.

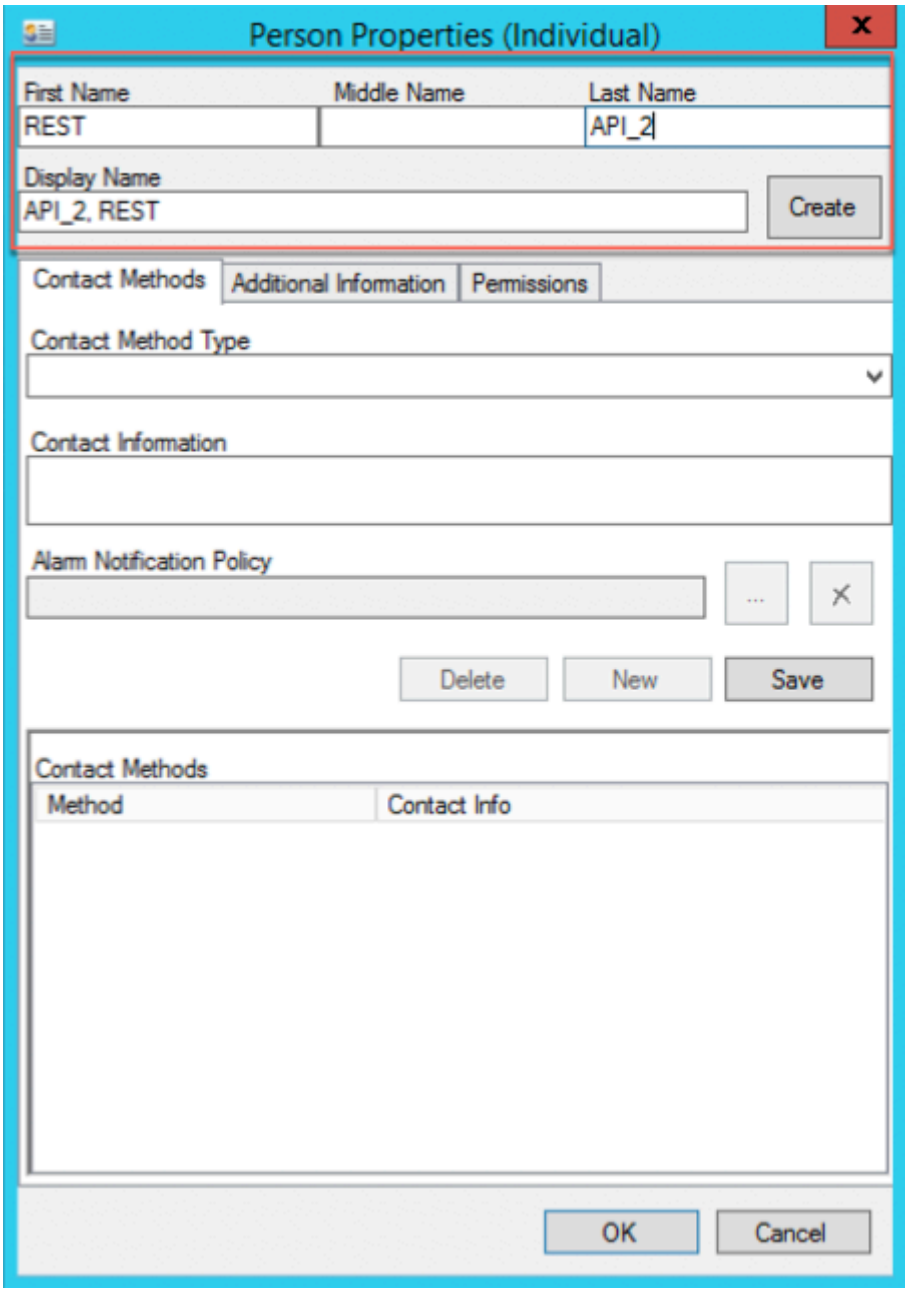



4. Füllen Sie im angezeigten Dialogfeld „Personeneigenschaften“ die Felder Name aus.

   Verwenden Sie einen anderen Namen für die REST-API LogRhythm als den, den Sie zum Erstellen der REST-API verwendet haben, z. B. REST API_2.

Automatische Übersetzung

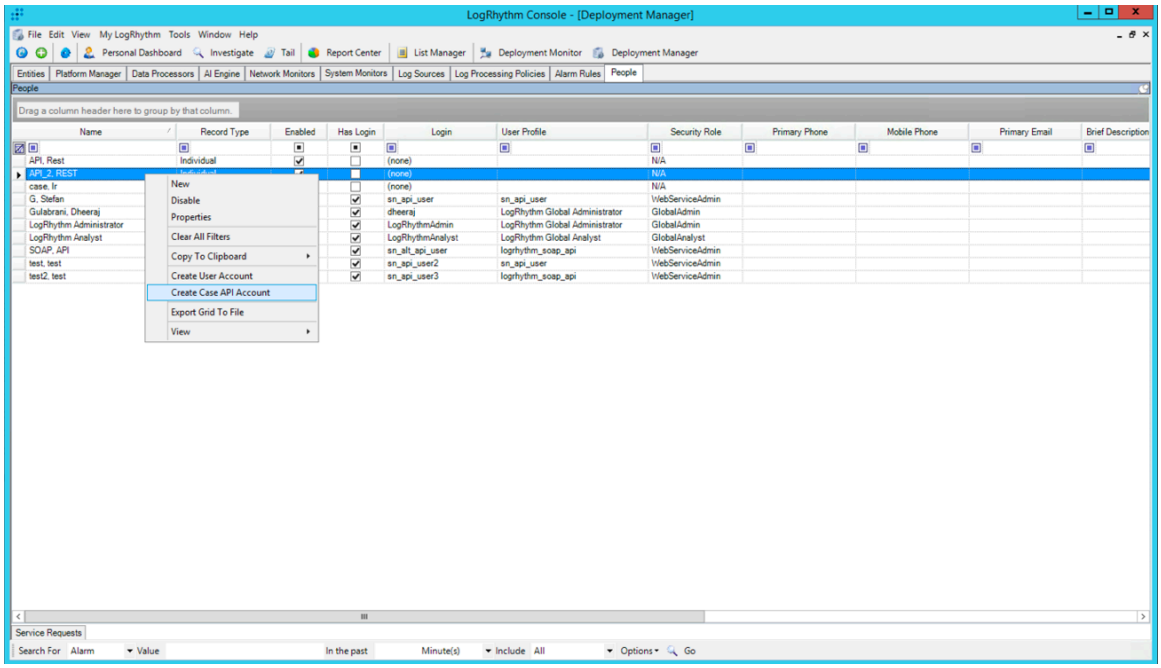
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf den neuen Eintrag in der Spalte Name (**API_2_REST**), und wählen Sie in der Auswahlliste **API-Account für Fall erstellen**aus.

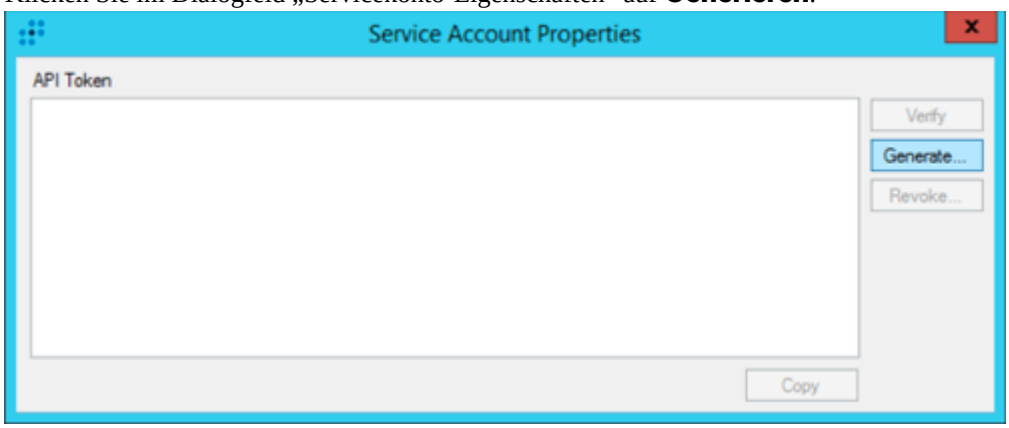


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

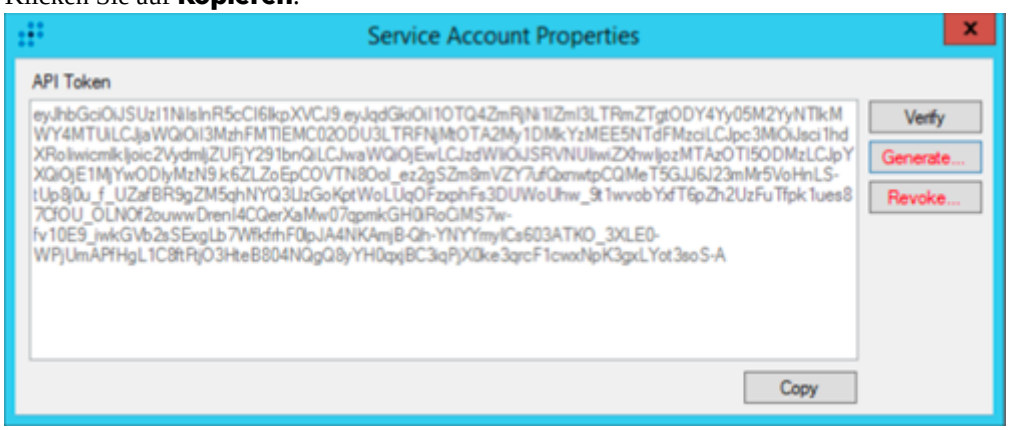



**Hinweis:**
Die Fall-API wird nicht verwendet, aber die Anmeldeinformationen für das Fall-API-Konto und die LogRhythm REST API sind identisch.

7. Klicken Sie im Dialogfeld „Servicekonto-Eigenschaften“ auf **Generieren**.




8. Klicken Sie auf **Kopieren**.




Sie haben jetzt die LogRhythm REST API eingerichtet. Fügen Sie die Zeichenfolge, die Sie im vorherigen Schritt kopiert haben, in Ihre Instanz [ Now Platform im Feld LogRhythm REST-API-Token während der in Installieren Sie das Plugin, und konfigurieren Sie LogRhythmaufgeführten Konfigurationsschritte ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie das Plugin, und konfigurieren Sie LogRhythm.

#### Installieren Sie das Plugin, und konfigurieren Sie LogRhythm

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendung ordnungsgemäß mit Security Operations auf dem Now Platform®integriert wird.

### Vorbereitungen

Erforderliche Rolle: admin

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich. Die neueste Version von LogRhythm ist 7.8 oder höher.

**Hinweis:**
Ihre vorhandenen Alarmprofile werden in der aktuellen Version LogRhythm nicht mehr unterstützt. Daher müssen Sie neue Alarmprofile erstellen und die erforderlichen Konfigurationen vornehmen.

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Systemadministrator (admin) installiert das Anwendungs-Plugin und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• (sn_si.admin) überwacht die folgenden Aufgaben:<br>◦ Benennt, erstellt und bearbeitet Alarmprofile.<br>◦ Ordnet Alarme zu und filtert sie – identifiziert bestimmte LogRhythm Alarme, die Security Incidents erstellen, und konfiguriert, wie diese Alarmfelder einem Now Platform® Security Incident zugeordnet werden.<br>◦ Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.<br>◦ Erfasst historische Alarme und plant abgerufene Alarme.<br>◦ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>◦ Diese Rolle hat auch Zugriff auf das Modul Security Operations. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | • Der Security Incident-Analyst (sn_si.analyst) reagiert auf Security Incidents, die basierend auf den Alarmprofileinstellungen erstellt werden. |
| Rufen Sie einen API-Benutzernamen und ein Passwort von LogRhythm ab, und vergewissern Sie sich, dass Sie Version LogRhythm 7.8 oder höher verwenden. | Besuchen Sie die Produktwebsite, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: LogRhythm Enterprise-Website . Die Benutzerkonten, Anmeldeinformationen und Zertifikate müssen vor der Installation der Anwendung ordnungsgemäß konfiguriert werden.<br><br>Die Integration erfordert LogRhythm Version 7.8 oder höher und die LogRhythm REST APIs.<br><br>Weitere Informationen finden Sie unter Richten Sie die REST-API für ein LogRhythm. |
| Vergewissern Sie sich, dass Sie einen MID Server installiert und konfiguriert haben. | In Ihrer Now Platform -Umgebung ist ein MID Server erforderlich. Auf der Website der ServiceNow-Produktdokumentation finden Sie Informationen zum Einrichten und Konfigurieren von MID Servern. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Für das Rome-Release und spätere Familien-Releases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration |



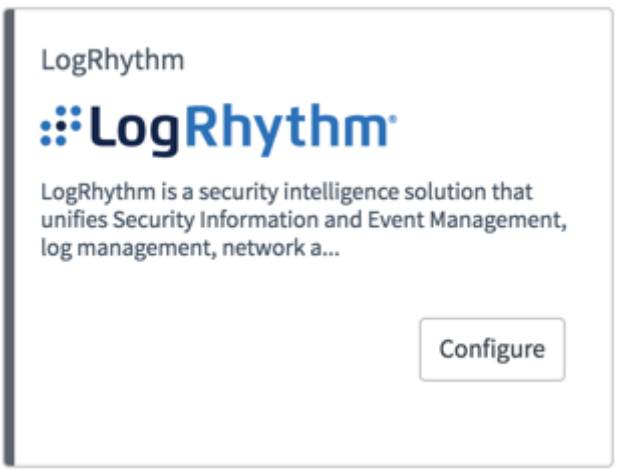
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

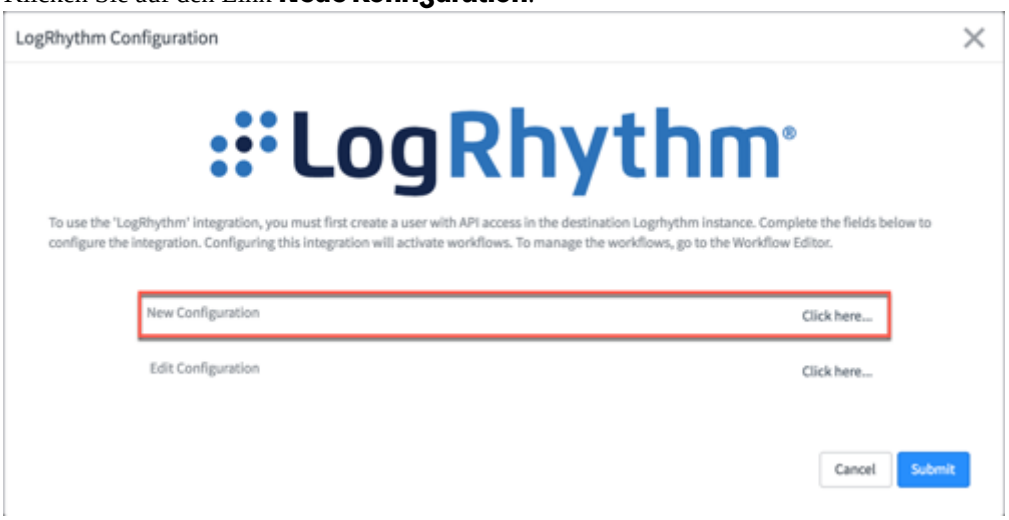
**Wichtig:**
Bei Konnektivitätsproblemen mit der Clientkonsole LogRhythm finden Sie weitere Informationen unter Überprüfen Sie die Konnektivität für LogRhythm.

### Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel LogRhythm.
3. Klicken Sie auf **Konfigurieren**.




4. Klicken Sie auf den Link **Neue Konfiguration**.




5. Füllen Sie die Felder im Formular aus.

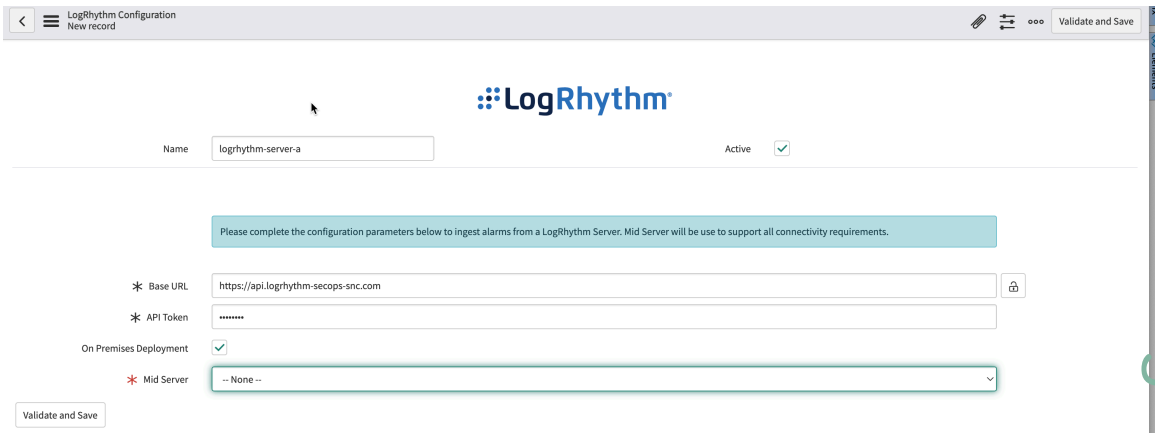


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### LogRhythm-Konfiguration

| Feld | Beschreibung |
|---|---|
| Name | LogRhythm Servername, z. B. logrhythm-server-a. |
| Basis-URL | Basis-URL, die die REST-API LogRhythm hostet.<br><br>Der MID Server ermöglicht den Zugriff auf das Netzwerk, in dem die LogRhythm-Clientkonsole gehostet wird. Diese URL ist der Ort, an dem der Server LogRhythm in diesem Netzwerk gehostet wird. Klicken Sie rechts auf das Schlosssymbol, um das Feld zu bearbeiten und Text für eine URL einzugeben, z. B. https://logrhythm.secops-eng.com:8501/. |
| API-Token | Geben Sie das Token ein, das Ihrer REST API zugeordnet ist, die Sie in der Clientkonsole LogRhythm erstellt haben. |
| Lokale Bereitstellung | Option zur Auswahl, ob es sich um eine LogRhythm lokale Bereitstellung handelt. |
| MID-Server | Spezifischer MID Server, der in Ihrer Umgebung eingerichtet ist. Nur die aktiven und validierten MID Server sind in dieser Auswahlliste verfügbar. |

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.




6. Klicken Sie **auf Validieren und speichern**.
   Nachdem die Validierung erfolgreich abgeschlossen wurde, wird eine Meldung angezeigt, und die Seite LogRhythm „ Konfigurationen“ wird neu geladen. Der nächste Schritt besteht darin, ein Alarmprofil zu erstellen.

### Nächste Maßnahme

Nachdem Sie die Validierung erfolgreich abgeschlossen haben, ist der nächste Schritt Erstellen eines Alarmprofils für LogRhythm.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen eines Alarmprofils für LogRhythm

In einem Alarmprofil, das Sie erstellen und benennen, geben Sie an, welche Alarme Sie aus der LogRhythm Client-Konsole abrufen möchten. Sie definieren auch, wie sie Feldern in einem Now Platform Security Incident zugeordnet werden.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

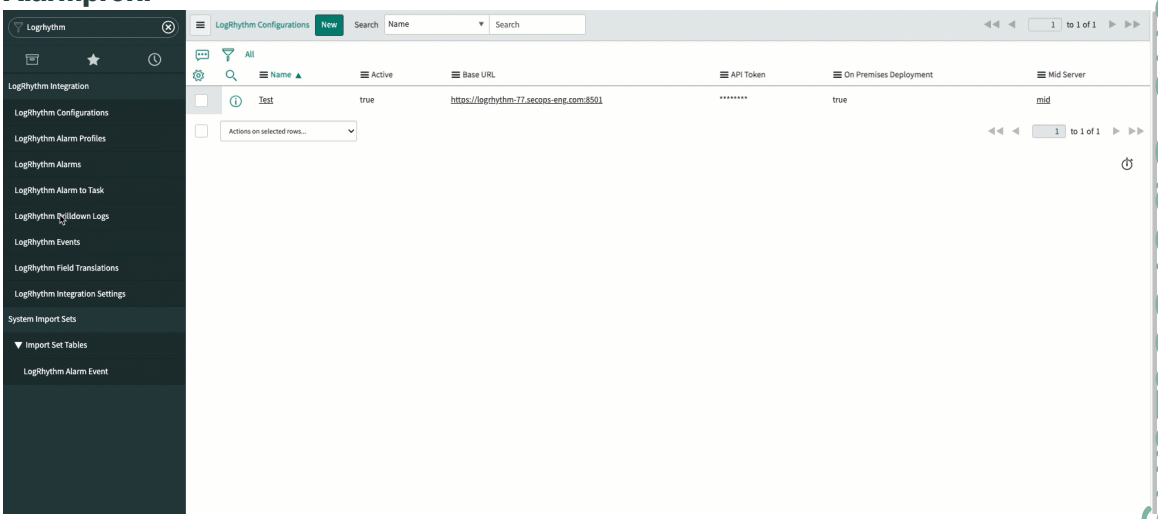
## Warum und wann dieser Vorgang ausgeführt wird

Basierend auf dem konfigurierten Alarmprofil kann ein Alarmprofil standardmäßig alle Arten von Alarmen erfassen. Sie können jedoch Filterkriterien verwenden, um bestimmte Alarmtypen zu erfassen. Mit dieser Now Platform -Integration werden alle konfigurierten Alarmregeln oder bestimmte Alarmregeln basierend auf dem erstellten Profil erfasst. Alarmregeln, z. B. nur Alarme mit hoher Risikostufe, können dann gefiltert werden, um anzugeben, welche Alarme Security Incidents erzeugen sollen. Bevor Security Incidents erstellt werden, werden einzelne Feldwerte in den gefilterten Alarmen den entsprechenden Feldern im Security Incident Now Platform zugeordnet. Diese Konfiguration erfolgt über ein Alarmprofil in Ihrer Now Platform -Instanz.

## Prozedur

1. Navigieren zu **Alle** > **LogRhythm Integration**.
2. Wählen Sie das Modul **„LogRhythm** - **Alarmprofile** “ aus, um die Liste der Alarmprofile anzuzeigen.

**Alarmprofil**




3. Um ein neues Alarmprofil zu erstellen, klicken Sie auf **Neu**.
   Ein neues Alarmprofilformular wird angezeigt. Oben auf der Seite wird in der Fortschrittsleiste **Name** ausgewählt. Diese Leiste verfolgt Ihren Fortschritt während der Konfiguration.
4. Füllen Sie die Felder im Formular aus.

**Alarmprofil**

| Feld | Beschreibung |
|---|---|
| Name | Name für das Alarmprofil. Anhand dieses Namens können Sie die Alarmtypen identifizieren, z. B. *Nicht autorisierter Zugriff* (*VPN*), *Malware*oder *Phishing*. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Kurzbeschreibung | Kurztext für zusätzliche Informationen zum Alarmprofil, die den Typ der Alarme oder eine Alarmkategorie enthalten können. Eine Beispielbeschreibung: Alle Alarme, die nicht autorisierten PowerShell- und Sudo-Zugriffsversuchen zugeordnet sind. |
| Quelle | Quellserver aus der Auswahlliste. Die Liste besteht aus LogRhythm Konfigurationen, die Sie bereits eingerichtet haben, z. B. `logrhythm-server-a`. Weitere Informationen finden Sie unter Installieren Sie das Plugin, und konfigurieren Sie LogRhythm. |
| Reihenfolge | Priorität des Alarmprofils. Dieses Feld gibt die Reihenfolge an, in der die Alarmprofile ausgeführt werden, wenn zwei oder mehr Alarmprofile die Auslösebedingungen gemeinsam nutzen. |
| Aktiv | Standardmäßig ist diese Option nicht ausgewählt. Nachdem Sie alle Schritte zum Einrichten von Alarmprofilen abgeschlossen und auf Fertigstellen **geklickt**haben, werden Sie aufgefordert, dieses Kontrollkästchen zu aktivieren, um das Alarmprofil zu aktivieren. Wenn das Alarmprofil aktiv ist, werden Alarme automatisch aus der LogRhythm Client-Konsole abgerufen. |

5. Klicken Sie auf **Fortsetzen**, um Ihre Daten zu speichern und mit dem Zuordnungsformular fortzufahren.

   Wenn die Validierung erfolgreich ist, wird die Seite neu geladen, und das **Zuordnungsformular** wird angezeigt. Sie können erst mit der Konfiguration fortfahren, nachdem Sie Ihre Verbindung und Ihre Anmeldeinformationen erfolgreich validiert haben.

**Zugehörige Informationen**

LogRhythm Alarme werden dem Security Incident zugeordnet

### LogRhythm Alarme werden dem Security Incident zugeordnet

Nachdem Sie die Quelle LogRhythm ausgewählt haben, die Sie erfassen möchten, müssen Sie einzelne LogRhythm Alarmfelder den Security Incident-Feldern von Now Platform zuordnen.

Die Zuordnung von Alarmen umfasst die folgenden Aufgaben:

- Ordnen Sie LogRhythm Alarme zu. Für diese Aufgabe werden Beispielalarme anhand der Alarm-IDs oder der letzten Alarme aus der LogRhythm -Client-Konsole aufgelistet und erfasst (Abruf).
- Die Beispielalarmfelder sind in drei Gruppen unterteilt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alarmfelder: Die verfügbaren Alarmfelder und ihre entsprechenden Werte werden angezeigt.
- Event-Felder: Die verfügbaren Event-Felder und ihre entsprechenden Werte werden angezeigt.
- DrillDownLog-Felder: Die verfügbaren Drilldown-Protokollfelder und ihre entsprechenden Werte werden angezeigt.

- Jede abgerufene Alarm-ID wird als Registerkarte angezeigt. Vergewissern Sie sich, dass auf den Registerkarten „Alarm ID“ (Alarm-ID) alle kritischen Alarmfelder aus dem Abschnitt „ Alarm Sample Ingestion “ (Erfassung von Alarmbeispielen) auf der linken Seite des Formulars dem Abschnitt „ SIR-Incident-Feldzuordnung “ auf der rechten Seite des Formulars zugeordnet sind.
- Nachdem Sie die Alarme dem Feld SIR-Incident-Feldzuordnung zugeordnet haben, wird die Alarmkategorie auch im Feld Eingabeausdruck angezeigt. Beispiel: `${Alarm: alarmid}$`.
- Sie können die Konfiguration ändern, indem Sie Felder im Security Incident hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder anhand der bereitgestellten Farbcodierung nach.
- Sie können Alarme filtern, um anzugeben, welche Alarme in die SIR-Anwendung erfasst werden. Sie können die Alarme entweder direkt filtern oder die Alarmkategorien verwenden, um Ihre Suche basierend auf Alarme, Events oder DrillDownLogs aufzuschlüsseln.
- Verwenden Sie den Skript-Editor, wenn Sie Werte für die Felder Priorität und Kategorie im Security Incident formatieren möchten.

Der nächste Schritt ist Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu.

**Zugehörige Informationen**

Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu

Verwenden Sie den Skript-Editor, um LogRhythm -Werte zu formatieren

Filtern Sie Alarme nach LogRhythm

### Ordnen Sie LogRhythm Alarmfelder Security Incident-Feldern zu

Sie ordnen den Security Incident-Feldern einzelne Alarmfelder zu. Die vorkonfigurierte Zuordnung kann bearbeitet werden, und die für die Felder bereitgestellte Farbcodierung hilft Ihnen, bereits zugeordnete Alarme zu überwachen. Dieser Schritt hilft Ihnen zu visualisieren, wie sich Ihre Änderungen auf die Felder des Security Incident auswirken.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Wenn Sie mit den LogRhythm -Alarmen nicht vertraut sind, navigieren Sie zur LogRhythm Client-Konsole, und überprüfen Sie einige Beispiel-Alarm-IDs. Im folgenden Beispiel wurden LogRhythm Alarme 9468 und 9474 verwendet, um die Alarme dem Security Incident zuzuordnen.

#### Warum und wann dieser Vorgang ausgeführt wird

Mit diesem Formular ordnen Sie die Alarmregeln LogRhythm auf der linken Seite den Security Incident-Feldern auf der rechten Seite zu.

Die folgende Abbildung zeigt die Standardzuordnung von Alarmen, die für jedes Alarmprofil vorkonfiguriert ist. Diese Standardzuordnung kann bearbeitet werden, und mit diesem Formular passen Sie die Felder an, die den Security Incident ausfüllen. Nachdem Sie



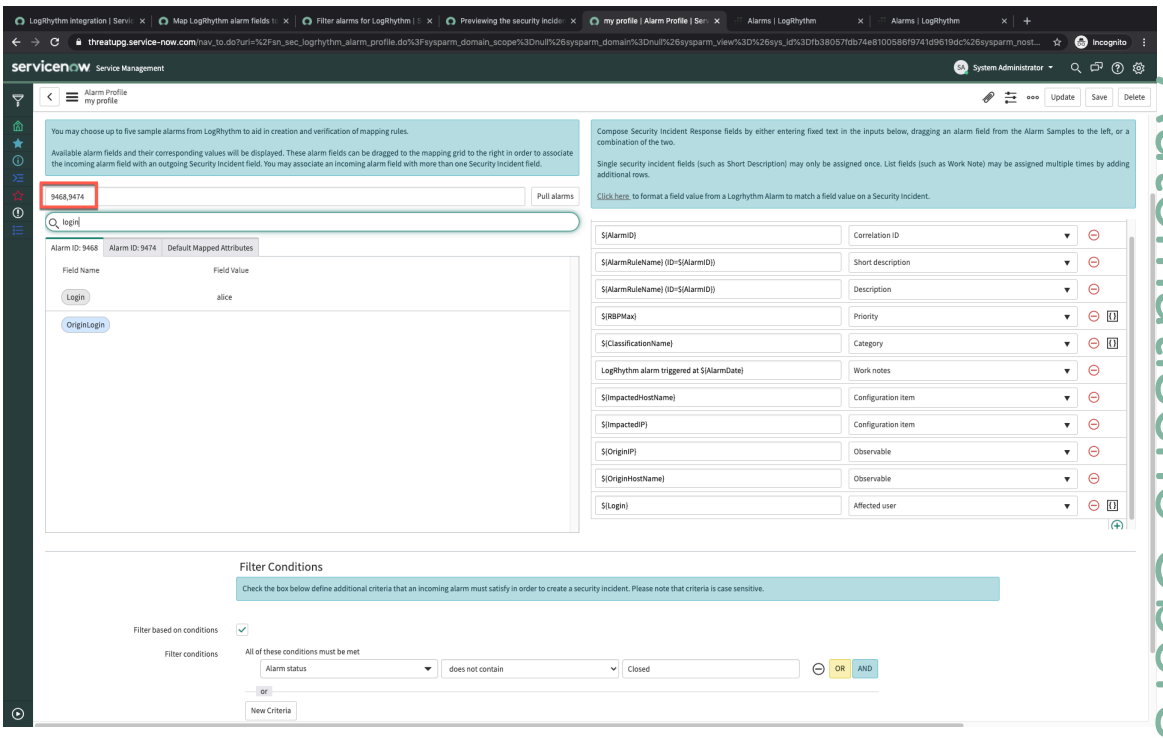
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Zuordnung abgeschlossen haben, können Sie sehen, wie sich das Hinzufügen oder Entfernen von Alarmfeldern potenziell auf die Feldwerte im Security Incident auswirkt.

Auf der linken Seite dieses Formulars sind in der folgenden Abbildung die Alarmregeln LogRhythm dargestellt. Die Werte dieser Alarmregeln werden den Security Incident-Feldern auf der rechten Seite des Formulars zugeordnet.

## Prozedur

1. Klicken Sie nach dem Erstellen eines Alarmprofils für **LogRhythm** in der Fortschrittsleiste auf Zuordnung.
2. Geben Sie im Feld **Alarm-Sample** -Erfassung bis zu fünf Beispiel-Alarm-IDs LogRhythm durch Kommas getrennt ein (9468,9474).




3. Klicken Sie neben dem **Alarmfeld auf Alarme abrufen**.

   Der Abruf für Beispielalarme kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   Nachdem die Beispielalarm-IDs übermittelt und erfolgreich vom Server LogRhythm abgerufen wurden, werden die Alarmfelder und ihre entsprechenden Werte in Registerkarten angezeigt.

### Hinweis:

Nachdem eine Alarm-ID erfolgreich abgerufen wurde, gibt Now Platform möglicherweise die folgende Meldung zurück: Die folgenden neuen Felder sind in Kürze zum Filtern verfügbar. Laden Sie dieses Profil in einigen Minuten neu, wenn eine Filterung basierend auf diesen Feldern erforderlich ist. itemspacketsin, itemspacketsout.

Diese Nachricht wird angezeigt, wenn der einzelne abgerufene Alarm Feldnamen enthält, die zuvor nicht von Now Platformverarbeitet wurden. Diese Felder sind für die Zuordnung verfügbar. Wenn jedoch diese Nachricht angezeigt wird, laden Sie das Formular neu, damit diese Felder angezeigt werden und in den Filterauswahllisten des Bedingungsgenerators verfügbar sind, wenn Sie bereit sind, Filterbedingungen festzulegen.

Automatische Übersetzung

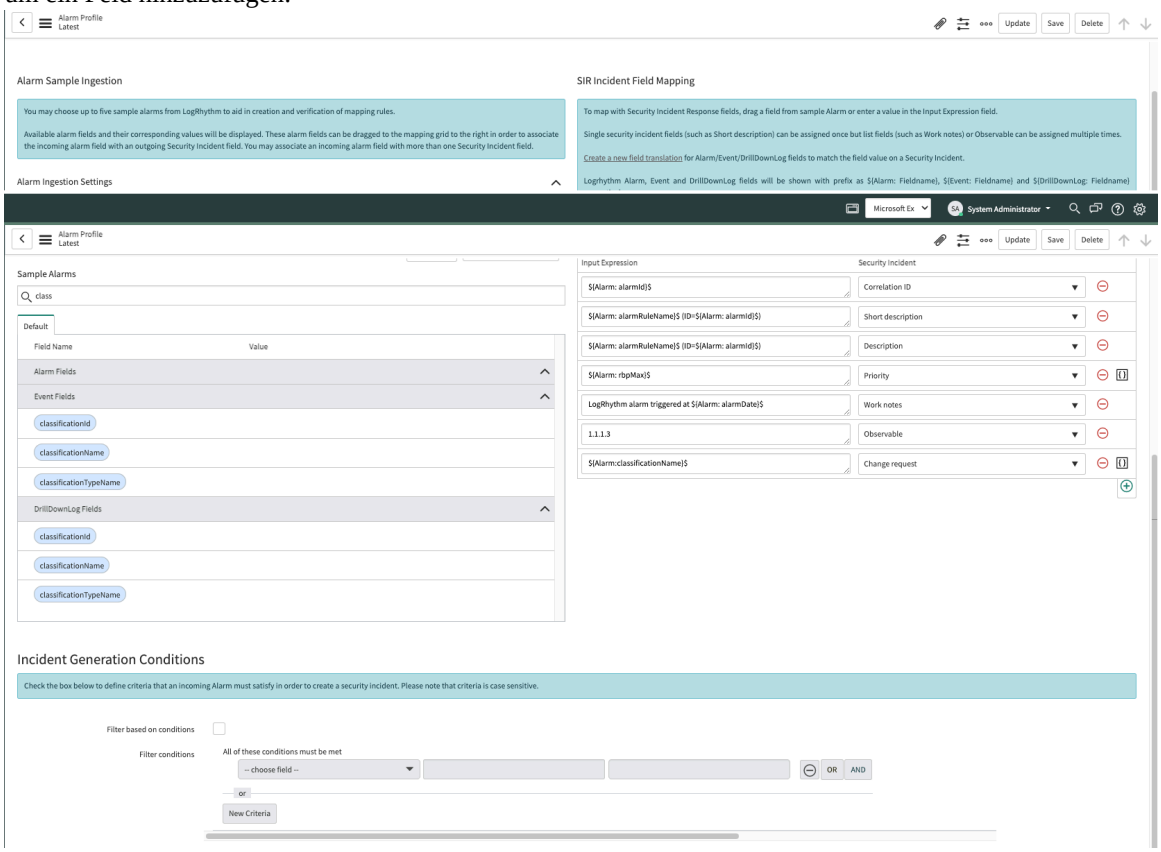
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die Erfassung dieser Beispielalarme in der Alarmprofilkonfiguration können Sie die Zuordnung von Alarmfeldern zu Security Incidents verhindern, die keine Werte enthalten. Außerdem werden Alarmfelder mit Werten an den entsprechenden Feldern im Security Incident ausgerichtet. Dieser Schritt stellt sicher, dass alle kritischen Alarmfelder zugeordnet werden und keine Feldwerte im Security Incident fehlen.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Alarme übersehen oder dupliziert werden, sind Alarmfelder farbcodiert. Ein hellblaues Alarmfeld (Account, AlarmRuleID, AlarmStatususw.) zeigt an, dass ein Feld noch nicht für die Zuordnung zu einem Security Incident ausgewählt wurde.

Ein graues Feld (AlarmDate, AlarmIDund AlarmRuleName) zeigt an, dass bereits ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen, da in bestimmten Fällen ein Alarmfeld mehr als einem Feld in einem Security Incident zugeordnet werden kann. Beispielsweise können die Felder „ Erkennbare Elemente “ und „Arbeitsnotiz“ mehr als einen Wert haben.

4. Um die Beispielalarmdaten zu löschen, klicken Sie auf **Beispielalarmdaten**löschen.
5. Um die Standardkonfiguration für den Security Incident zu bearbeiten, führen Sie die folgenden Schritte aus, um ein Feld hinzuzufügen:




   a. Klicken Sie rechts unten im Formular auf das Plus-Symbol.
   Ein neues Feld wird angezeigt.

   b. Wählen Sie in der Spalte Security Incident ein verfügbares Feld aus der Auswahlliste aus.

   In der erweiterten Auswahlliste sind einige der Felder schattiert dargestellt. Zum Beispiel hat die Kategorie einen grauen Hintergrund, was darauf hinweist, dass sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für LogRhythm Alarmfelder stellt diese Farbcodierung für die Security Incident-Felder sicher, dass



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Werte aus den Alarmfeldern nicht versehentlich demselben Security Incident-Feld zugeordnet werden.

In der obigen Abbildung ist die Alarmregel ${Alarm:classificationName}$ bereits dem Feld Kategorie im Security Incident in diesem Profil zugeordnet.

**Hinweis:**
Das Feld „Erkennbares Element“ kann mehreren Feldern desselben Security Incident zugeordnet werden, sodass mehrere erkennbare Elemente angezeigt werden können. Ebenso können die Felder Konfigurationselement und Arbeitsnotizen so zugeordnet werden, dass mehrere Werte angezeigt werden.

Auf der Seite „Erfassung von Alarmbeispielen“ des Formulars zeigt Blau an, dass kein Alarmregelfeld zugeordnet wurde. Grau zeigt an, dass sie zugeordnet wurde. In der Auswahlliste auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zeigt Weiß an, dass kein Feld zugeordnet wurde. Grau zeigt an, dass ein Feld zugeordnet wurde. Verwenden Sie diese Farbcodierung, um die Feldzuordnung nachzuverfolgen.

In der obigen Abbildung wurde Betroffener Benutzer aus der Auswahlliste als neues Feld für den Security Incident ausgewählt.

**c.** Klicken Sie im Abschnitt „Erfassung von Alarmbeispielen“ auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte Alarm-ID im Feld Eingabeausdruck auszuwählen.

In der Abbildung oben wurde „ Anmeldung “ ausgewählt.

**d.** Ziehen Sie es in das leere Feld, und lassen Sie es los.
In der linken Spalte im Abschnitt SIR-Incident-Feldzuordnung wird der neue Wert für das Feld Betroffener Benutzer angezeigt. In diesem Fall wird der Wert für Login aus dem Alarm LogRhythm im Feld Betroffener Benutzer des Security Incident angezeigt.

**6.** Alternativ können Sie manuell einen Wert für Felder in der Spalte Eingabeausdruck eingeben, indem Sie den Cursor in das Feld Eingabeausdruck setzen und den gewünschten Alarmwert eingeben.

Beispiel: In der obigen Abbildung wurde dem Security Incident-Formular ein weiteres Feld (Zuweisungsgruppe) hinzugefügt, und Security Incident-Zuweisung wurde manuell in das Feld eingegeben.

**7.** Setzen Sie die Bearbeitung der vorkonfigurierten Zuordnung nach Bedarf fort.
Wenn Sie Werte aus LogRhythm Alarmfeldern in Werte übersetzen müssen, die von den Feldern im Security Incident unterstützt werden, können Sie den Skript-Editor verwenden. Weitere Informationen finden Sie unter Verwenden Sie den Skript-Editor, um LogRhythm -Werte zu formatieren.

### Nächste Maßnahme
Nachdem Sie die Feldzuordnung abgeschlossen haben, führen Sie den nächsten Schritt zu Filtern Sie Alarme nach LogRhythm.

#### Filtern Sie Alarme nach LogRhythm

Durch das Festlegen von Filterkriterien für Alarme nach der Zuordnung von Feldern können Sie bestimmen, welche Alarme in die SIR-Anwendung erfasst werden sollen. Durch das Filtern von Alarmen können Sie die Anzahl der Alarme, die Sie erfassen, wenn das Alarmprofil aktiviert ist, erheblich reduzieren.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

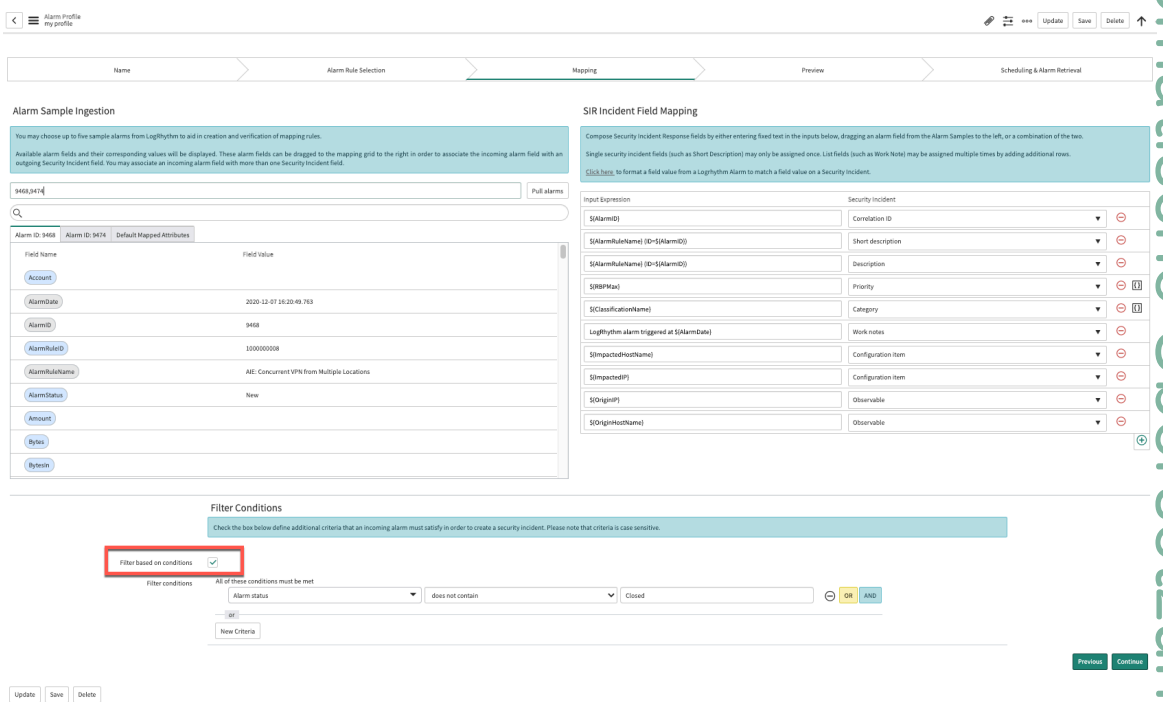
Verwenden Sie die Filterbedingungen am unteren Rand des Zuordnungsformulars, um bestimmte Alarme herauszufiltern oder die Erfassung auf Alarme zu beschränken, die bestimmte Kriterien auf Feldebene erfüllen. Durch das Filtern wird die Anzahl der erfassten Alarme erheblich reduziert, nachdem das Alarmprofil aktiviert wurde. Verwenden Sie die Filterung, um eine überschaubare Menge von Alarmen zu erfassen, die Ihre Mitarbeiter im Security Operations Center (SOC) unterstützen können.

**Hinweis:**

Das folgende Beispiel zeigt eine Standardfiltereinstellung, in der „Alarm status-does-not-Contain-Closed“ die Standardeinstellung ist. Dieser Filter ruft nur aktive Alarme ab, und diese Einstellung reduziert die Anzahl der abgerufenen Alarme. Die folgenden Schritte zeigen, wie Sie einen weiteren nützlichen Filter hinzufügen, der nur Alarme mit den höchsten Schweregrad- oder Prioritätswerten enthält.

### Prozedur

1. Um die Filterkriterien zu bearbeiten, aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern.

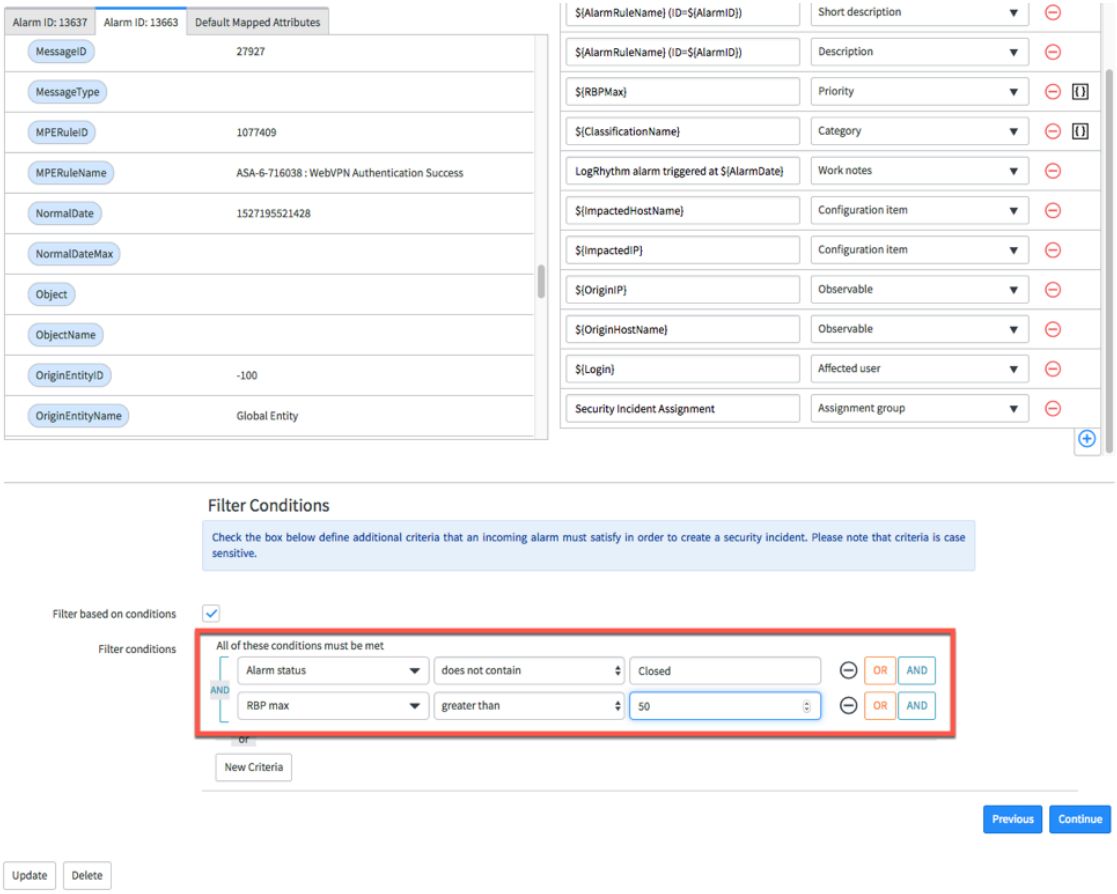



2. Klicken Sie rechts neben dem Feld **Filterbedingungen** auf **ODER** oder **UND**.
3. Wählen Sie in der neuen Zeile, die angezeigt wird, die Filterbedingungen aus den Auswahllisten aus.

Die folgende Abbildung zeigt einen zusätzlichen Filter, der den Kriterien hinzugefügt wurde, bei denen die risikobasierte Priorität (RBP max. ) größer als 50ist. Mit dieser Filtereinstellung werden nur LogRhythm Alarme mit einem risikobasierten Prioritätswert größer als 50 abgerufen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Nachdem Sie sich vergewissert haben, dass alle kritischen LogRhythm Alarmfelder dem Security Incident Now Platform zugeordnet sind, und Filterkriterien festgelegt haben, um die Alarmerfassung zu begrenzen, wählen Sie eines aus, um mit der Konfiguration fortzufahren.

### Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau der zugeordneten Felder im Security Incident anzuzeigen. Weitere Informationen finden Sie unter Vorschau des Security Incident mit zugeordneten LogRhythm Alarmwerten anzeigen.

### Vorschau des Security Incident mit zugeordneten LogRhythm Alarmwerten anzeigen

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie den Feldern im Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle kritischen LogRhythm Alarmfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Erforderliche Rolle: sn_si.admin.

## Sicherheitsvorfall

Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.

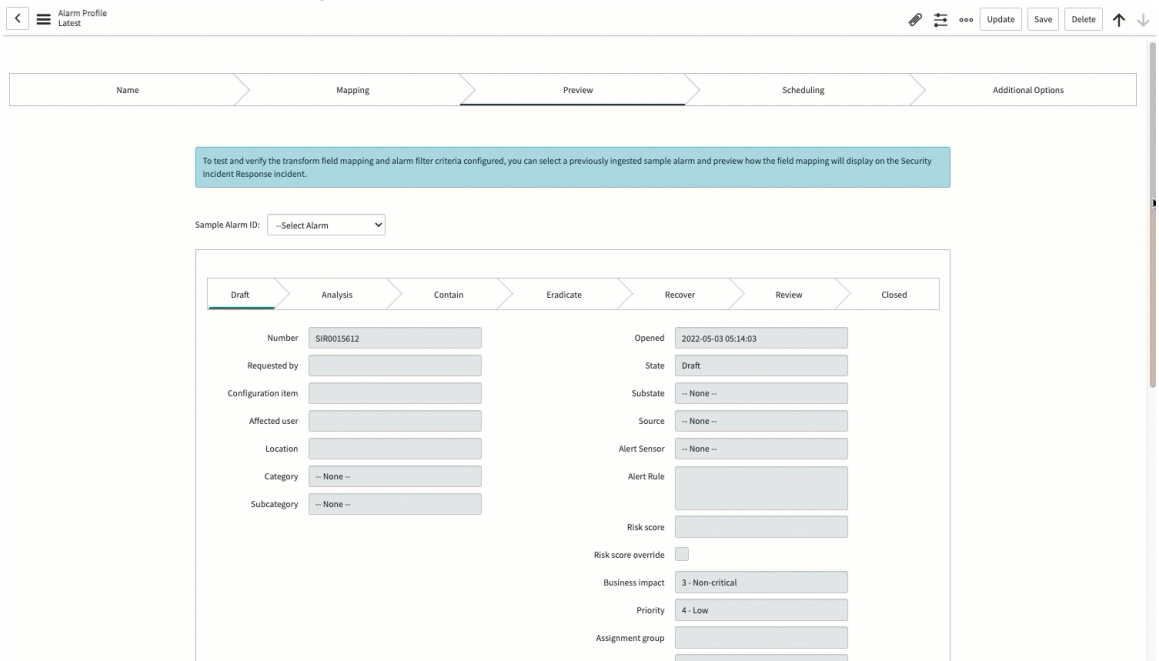
Ein Beispiel für die Vorschau für den gesamten Security Incident Now Platform ist in den folgenden beiden Abbildungen dargestellt. Dieses Beispiel der Vorschau des Security Incident wird mit den LogRhythm Alarmfeldern ausgefüllt, die aus dem Beispielalarm 13663 zugeordnet wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sind die Felder Konfigurationselement, Betroffener Benutzer, Priorität, Zuweisungsgruppeund Kurzbeschreibung des Security Incident ausgefüllt.

**Obere Hälfte des Security Incident**




In der unteren Hälfte des Security Incident-Formulars wird das Feld Beschreibung ausgefüllt. Im Abschnitt Zugehörige Elemente werden die Felder Konfigurationselement, ErkennbaresElement und Arbeitsnotiz mit Werten ausgefüllt. Wenn mehrere Werte für diese Felder zugeordnet werden, wird jeder Wert im Security Incident angezeigt, da jedes dieser Felder mehr als einen Wert akzeptieren kann.

## Fehlerbedingungen in der Vorschau

Die folgenden Warnmeldungen werden möglicherweise angezeigt, wenn Sie eine Vorschau des Security Incident anzeigen. Wenn ein Beispielalarm die Filterkriterien nicht erfüllt, wird der gesamte Security Incident nicht ausgefüllt.

## Eingabewert nicht gefunden

Wenn die Alarm-ID in den Filterbedingungen enthalten ist, wird möglicherweise weiterhin eine Warnmeldung angezeigt, wenn für bestimmte zugeordnete Felder keine bestimmten Eingabewerte gefunden werden. Im folgenden Beispiel wird in der Vorschau des Datensatzes davon ausgegangen, dass das Feld Zugewiesen an keinen Wert enthält, obwohl es zugeordnet wurde.

Überprüfen Sie für diesen Nachrichtentyp im Zuordnungsdatensatz, ob der Eingabewert korrekt ist. In diesem Fall ist die Person im Feld Zugewiesen an im Security Incident in der Instanz Now Platform falsch. Wenn dieser Alarm erfasst wird und einen Security Incident mit dieser Bedingung erstellt, werden Felder mit diesem Eingabewert (Abel Tuter) im Security Incident leer gelassen.

Die verbleibenden blauen Nachrichten dienen der Information und weisen darauf hin, dass diese Felder keinen Wert haben, der in der Vorschau angezeigt werden kann. Mit dieser Vorschau kann der Security Incident-Administrator, der das Alarmprofil konfiguriert, überprüfen, ob diese Felder in der ersten Erstellungsphase keinen Wert haben sollten, da in bestimmten Fällen Security Incident-Felder später automatisch ausgefüllt werden können. Andere Zuordnungsfehler werden ebenfalls angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie mit der Zuordnung und der Security Incident-Vorschau zufrieden sind, wählen Sie eine aus, um mit der Konfiguration fortzufahren.

| Option | Beschreibung |
|---|---|
| Klicken Sie in der Fortschrittsleiste auf **Fortsetzen** oder **Zeitplanung**. | Fahren Sie mit dem Formular **„Zeitplanung und Alarmabruf" fort**.<br><br>**Zeitplanung und Alarmabruf** auf der Fortschrittsleiste ausgewählt ist. Der nächste Schritt besteht in der Planung des Alarmabrufs. |
| Klicken Sie auf **Zurück**. | Kehren Sie zum Alarmprofil zurück, und setzen Sie die Zuordnung fort. |
| Geben Sie eine andere Alarm-ID in die **Auswahlliste Beispielalarm** -ID oben im Vorschauformular ein. | Die **Auswahlliste Beispielalarm-ID wird für jede von Ihnen eingegebene Alarm-ID** angezeigt. Sie können bis zu fünf Alarme auswählen.<br><br>Mit dieser Option können Sie eine Vorschau einer weiteren LogRhythm Alarm-ID für einen Security Incident anzeigen. |

Nachdem Sie eine Vorschau des Security Incident angezeigt haben und mit den Ergebnissen zufrieden sind, führen Sie den nächsten Schritt zu LogRhythm Alarme planen und abrufen.

### LogRhythm Alarme planen und abrufen

Nachdem Sie eine Vorschau des Security Incident mit den von Ihnen ausgewählten und zugeordneten LogRhythm Alarmen angezeigt haben, können Sie den Alarmabruf planen. Nachdem Sie diesen Schritt abgeschlossen haben, kann das Alarmprofil aktiviert werden.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

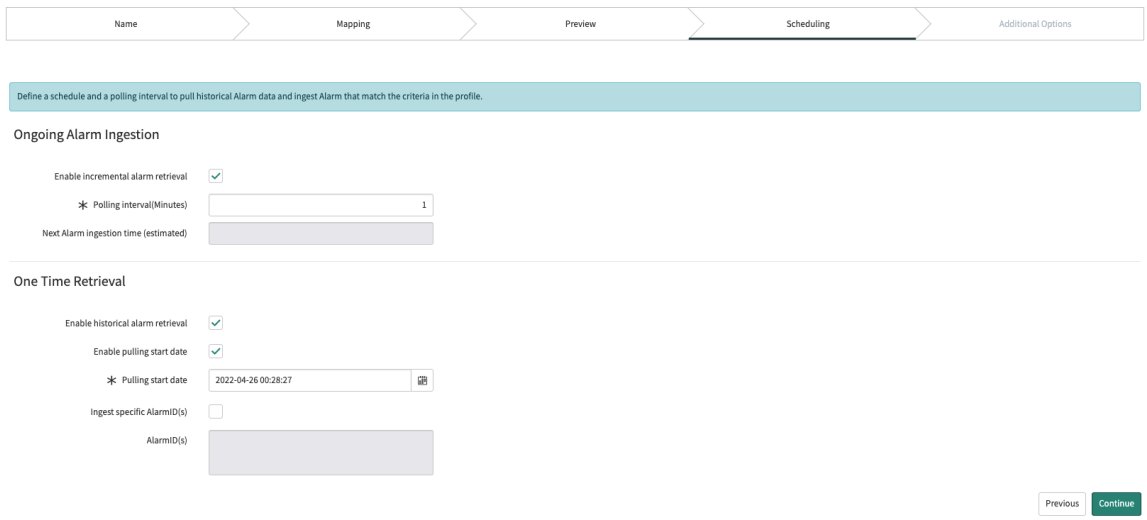
**Warum und wann dieser Vorgang ausgeführt wird**
Mit der Zeitplanung können Sie die Zeitplanung und die für den Abruf ausgewählten Alarmtypen ändern. Sie filtern die erfassten Alarme basierend auf einem Datumsbereich oder bestimmten Alarm-IDs. Mit diesem Schritt legen Sie fest, ob Sie historische Alarme erfassen möchten und wie oft Sie zukünftige Alarme abfragen, die der Alarmprofilkonfiguration entsprechen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Klicken Sie in der Fortschrittsleiste auf den Schritt **Zeitplanung**.

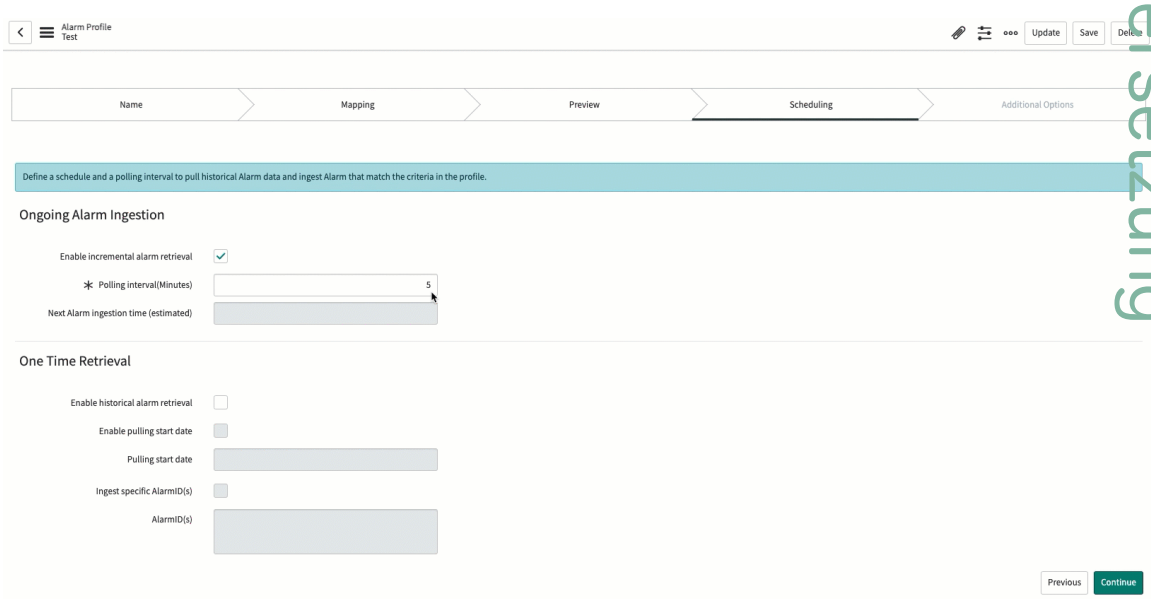



2. Wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.

3. Führen Sie die folgenden Schritte aus, um den historischen Alarmabruf zu bearbeiten, um ein Datum für den Alarmabruf oder eine bestimmte Alarm-ID einzugeben.

   a. Wählen Sie **Abrufstartdatum aktivieren**und dann **Abrufstartdatum aus**.

   b. Klicken Sie im Feld **Abrufstartdatum** auf den angezeigten Kalender, wählen Sie das Datum aus, gefolgt vom grünen Häkchen, um Ihren Eintrag zu speichern.




   Das Datum wird angezeigt.

   c. Alternativ können Sie die Option **Spezifische Alarm-ID(s)** erfassen auswählen und im Feld Alarm-ID(s) die spezifischen Alarm-IDs für die **Verlaufsdaten** eingeben, um bestimmte Alarm-IDs abzurufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können bis zu fünf durch Kommas getrennte Alarme eingeben.

**d.** Klicken Sie auf **Aktualisieren**.

**4.** Wählen Sie eine der folgenden Optionen aus, um mit der Bearbeitung fortzufahren oder die Konfiguration abzuschließen.

### Nächste Maßnahme

Nachdem Sie die Details für „Laufende Alarmerfassung“ und „Einmaliger Abruf“ konfiguriert haben, führen Sie den nächsten Schritt zu Zusätzliche Optionen für LogRhythm Alarme.

#### Zusätzliche Optionen für LogRhythm Alarme

Die LogRhythm Enterprise-Integration bietet Ihnen die Möglichkeit, die LogRhythm -Warnungen basierend auf den Security Incidents automatisch zu aktualisieren oder zu schließen.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Option Anfängliche Alarmaktualisierungen aktivieren, werden die Alarme in den LogRhythm-Kommentaren automatisch mit den ersten Alarmaktualisierungen aktualisiert. Wenn Sie analog dazu die Option „Aktualisierungen des Alarmabschlusses“ aktivieren, werden die Alarme in LogRhythm automatisch zusammen mit dem SIR-Abschlusscode und den Abschlusskommentaren geschlossen.

Die Alarm-ID LogRhythmNow Platform wird während des gesamten Lebenszyklus des Incident mit der ID des Security Incident [] verbunden. Diese Korrelation ermöglicht das gleichzeitige und automatisierte Schließen von Security Incidents/Alarmen. Wenn der Security Incident-Datensatz Security Incident Response (SIR) geschlossen wird, wird in der Warnung in der Webkonsole von LogRhythm ein Kommentar veröffentlicht. Dieser Kommentar gibt an, dass der Alarm basierend auf dem Abschluss des Security Incident Now Platform geschlossen wurde. Die Incident-Nummer und eine URL, die als Referenz auf den Security Incident verweist, sind auch im Kommentarbereich im LogRhythm -Alarm enthalten.

### Prozedur

**1.** Klicken Sie in der Fortschrittsleiste auf den Schritt **Zusätzliche Optionen**.

**2.** Um die automatisierte Alarmaktualisierung für die SIR-Incident-Erstellung zu verwenden, wählen Sie eine der folgenden Optionen aus, um den Alarmabruf zu konfigurieren.

**3.** Um die automatisierte Alarmaktualisierung für den SIR-Incident-Abschluss zu verwenden, wählen Sie eine der folgenden Optionen aus, um den Alarmabruf zu konfigurieren.

**4.** Klicken Sie auf **Fertigstellen**, um das Alarmprofil zu speichern.

### Trouble?

Wenn Sie keine Notizen sehen, die darauf hinweisen, dass der Alarm im Security Incident erfolgreich geschlossen wurde, überprüfen Sie die Arbeitsnotizen auf weitere Informationen darüber, wie Sie das Problem beheben können. Überprüfen Sie auch Ihre Serververbindung. Wenn Sie bestätigen, dass der Security Incident



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Platform geschlossen wurde und der Server keine Zeitüberschreitung aufweist, müssen Sie den Alarm möglicherweise in der Webkonsole von LogRhythm manuell schließen.

### Zusätzliche Konfigurationen für die LogRhythm -Integration

Verwenden Sie die LogRhythm Integrationseinstellungen, um die voreingestellten System- und Fehlerbehebungseigenschaften gemäß Ihren Anforderungen zu ändern.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Prozedur

1. Navigieren zu **Alle** > **LogRhythm Integration** > **LogRhythm-Integrationseinstellungen**.
2. Konfigurieren Sie die Systemeigenschaften gemäß Ihren Anforderungen.
3. Füllen Sie die Felder im Formular aus.

### LogRhythm Eigenschaften des Integrationssystems

| Feld | Beschreibung |
|---|---|
| Dadurch wird der Filter angewendet, bevor die Daten in ServiceNow-Tabellen gespeichert werden. | Option, um zu bestimmen, ob Sie den Filter anwenden möchten, bevor die Daten in den ServiceNow-Tabellen gespeichert werden.<br><br>Standardmäßig ist der Wert auf Ja festgelegt. |
| Max. Security Incident kann an einem Tag erstellt werden | Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können.<br><br>Standardmäßig ist der Wert auf 2000 festgelegt. |
| LogRhythm Die regelmäßige Erfassung kann 1000+ Alarme umfassen, daher wird Paginierung verwendet, um die Alarme zu erfassen. Limit pro Seite, das zum Abrufen der Anzahl von Alarmen pro Seite zulässig ist. | Option zum Definieren der maximalen Anzahl von Alarmen, die auf einer einzelnen Seite abgerufen werden sollen.<br><br>Standardmäßig ist der Wert auf 100 festgelegt. |
| Löschen Sie Datensätze der Tabelle „Quelle für Aufgabe“, die älter als die angegebene Anzahl von Tagen sind. | Option zum Löschen von Datensätzen der Tabelle „Quelle zu Aufgabe“, wenn die angegebene Anzahl von Tagen nicht eingehalten wurde.<br><br>Standardmäßig ist der Wert auf 30 festgelegt. |

4. Konfigurieren Sie die Problembehandlungseigenschaften gemäß Ihren Anforderungen.
5. Füllen Sie die Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Problembehandlungseigenschaften für LogRhythm-Integration**

| Feld | Beschreibung |
|---|---|
| Geplante Erfassung debuggen: Aktiviert Systemprotokolle auf Debug-Ebene für die Erfassung durch eine geplante Aufgabe. Dadurch werden alle Nachrichten/Ausnahmen protokolliert, die durch die geplante Erfassung beim Abrufen von Alarmen/Drilldown-Protokollen/Ereignissen aus LogRhythmgeneriert werden. | Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Erfassung durch die geplante Aufgabe.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |
| Debug-Transformationszuordnung: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Transformationszuordnung. Dadurch werden alle Nachrichten protokolliert, die von Transformationszuordnungen beim Erstellen eines Security Incident aus dem Alarmimport generiert wurden. Dadurch wurde auch die UI-Aktion in der Alarmimporttabelle aktiviert, um die Transformationszuordnung erneut auszuführen. | Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Transformationszuordnung.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |
| Beispielerfassung in Alarmprofil debuggen: Aktiviert Systemprotokolle auf Debug-Ebene für die Beispielerfassung. Dadurch werden alle Nachrichten protokolliert, die während der Erfassung von Beispielen generiert werden. | Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Beispielerfassung.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |
| Vorschau in Alarmprofil debuggen: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Alarmprofilvorschau. Dadurch werden alle Meldungen protokolliert, die beim Rendern der Vorschau für den Beispielalarm generiert werden. | Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Alarmprofilvorschau.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |
| Ausgehende REST-Aufrufe debuggen: Durch Aktivieren dieser Eigenschaft wird die Protokollierung auf Debug-Ebene in der Systemprotokolltabelle für alle REST-Aufrufe (Anforderung und Antwort) mit oder ohne MID-Server von LogRhythmermöglicht. | Option zum Aktivieren der Protokollierung auf Debug-Ebene in der Systemprotokolltabelle für alle REST-Aufrufe mit oder ohne MID-Server von LogRhythm.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |

6. Klicken Sie auf **Speichern**.

### Verwenden Sie den Skript-Editor, um LogRhythm -Werte zu formatieren

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Alarmwerten und den manuell eingegebenen Alarmwerten können Sie den Skript-Editor verwenden, um Feldwerte im Security Incident während des optionalen Zuordnungsschritts zu formatieren.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

Der Skript-Editor ändert die Werte eines LogRhythm -Alarms, sodass die Werte unterstützt werden, die den Feldern Priorität und Kategorie des Security Incident zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen, wenn LogRhythm Alarmwerte den Feldern Priorität und Kategorie des Security Incident zugeordnet sind, sollten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert eines LogRhythm -Alarms in einen Wert übersetzen möchten, der von den Feldern „ Priorität “ oder „ Kategorie “ des Security Incident unterstützt wird, verwenden Sie den Skript-Editor.

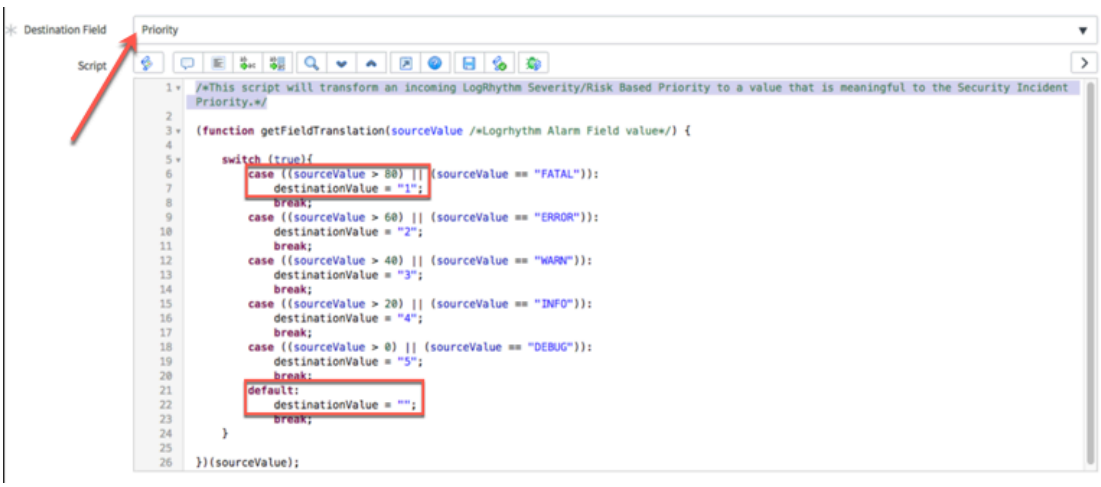
### Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular im Abschnitt „SIR-Incident-Feldzuordnung“ auf das Klammersymbol [{}], um den Skript-Editor zu öffnen.

   Die Standardwerte sind für die Felder Priorität und Kategorie im Security Incident enthalten. Sie können diese Werte bearbeiten.

   Überprüfen Sie für dieses Beispiel im geöffneten Editor, ob **Priorität** in der **Auswahlliste** Zielfeld angezeigt wird, wie in der folgenden Abbildung dargestellt. Beachten Sie, dass dieses Feld die Security Incident- *Priorität*und nicht die risikobasierte LogRhythm*Priorität*ist.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Priorität geeignet sein. Für einen LogRhythm -Alarm wird beispielsweise einer risikobasierten Prioritätspunktzahl ein Wert zwischen 0 und 100 zugewiesen. In Now Platformunterstützt das Prioritätsfeld eines Security Incident jedoch Werte zwischen 1 und 5. Wie in der vorherigen Abbildung dargestellt, übersetzt eine Skripteinbindung die Alarmfeldwerte LogRhythm in die entsprechenden Werte, die vom Feld im Security Incident in Now Platformunterstützt werden.

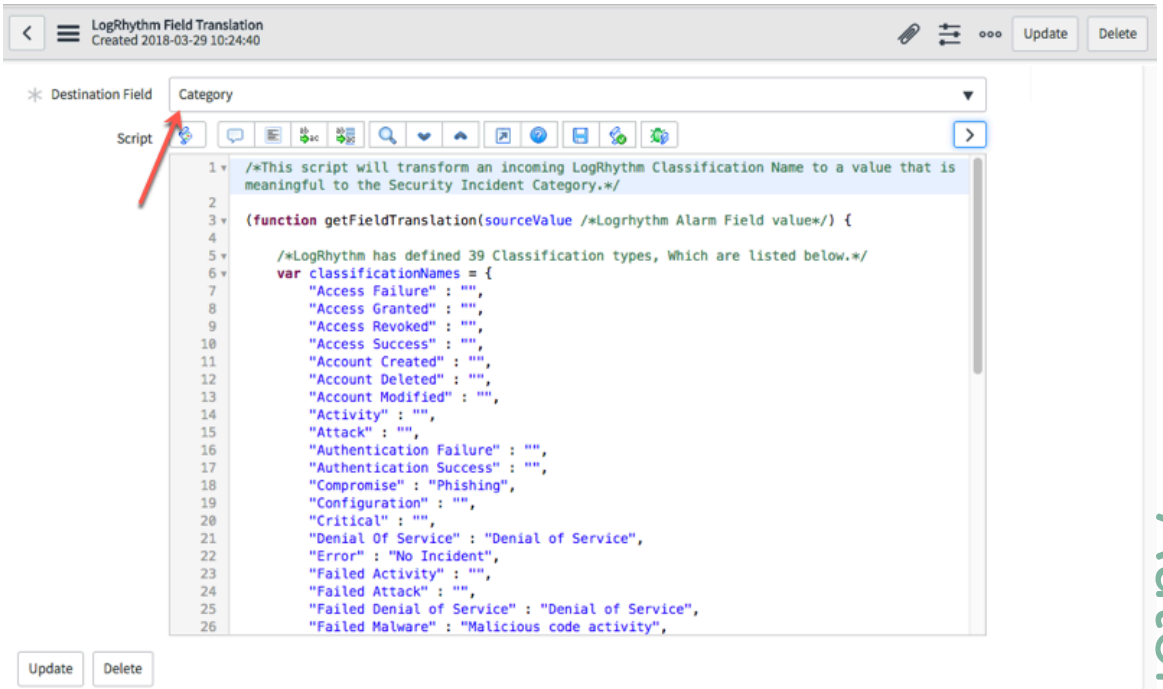
   Wenn in diesem Beispiel für das Feld Priorität der Alarmwert LogRhythm80 oder größer ist, wird im Security Incident-Feld (Priorität ) 1angezeigt. Dieser Wert wird im Security Incident in eine kritische Priorität übersetzt. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null gesetzt.

2. Geben Sie Änderungen ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern. Die Tabelle LogRhythm „ Feldübersetzungen“ wird angezeigt.
3. Schließen Sie die Tabelle, um zum Formular „Zuordnung“ zurückzukehren.

   Die folgende Abbildung zeigt den Skript-Editor mit Kategorie, die in der Auswahlliste Zielfeld ausgewählt ist.

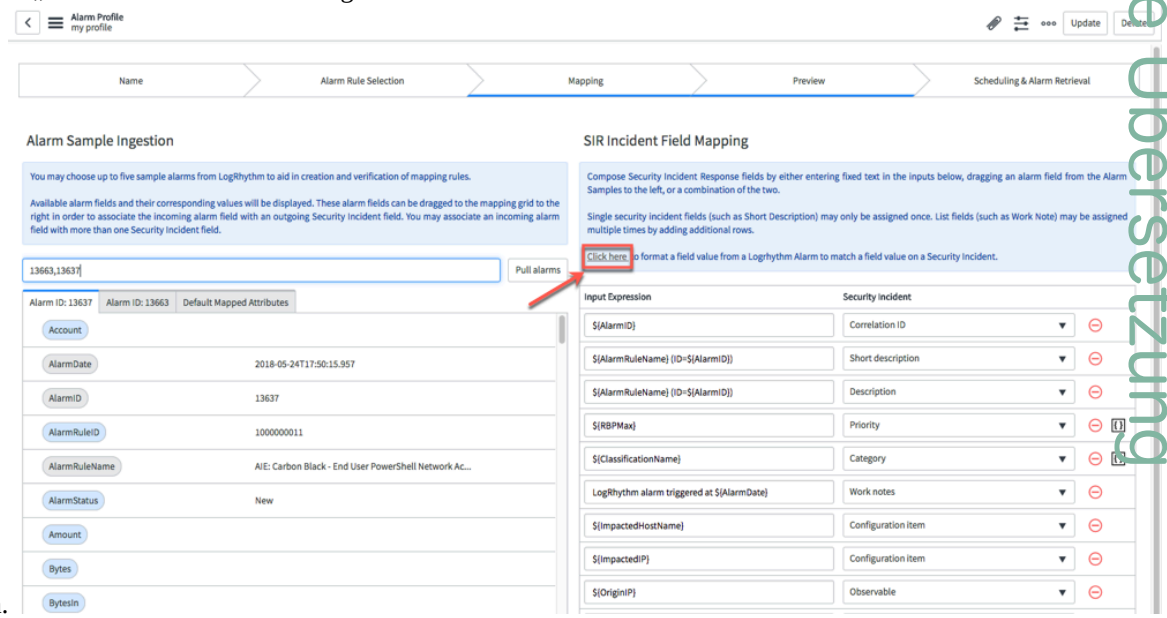


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Wenn Sie der Liste „Feldübersetzungen“ ein neues Feld hinzufügen möchten, führen Sie die folgenden Schritte aus, um einen neuen Datensatz hinzuzufügen.

**a.** Wenn das Zuordnungsformular angezeigt wird, klicken Sie im Abschnitt „SIR-Incident-Feldzuordnung“ auf den Link **Hier**



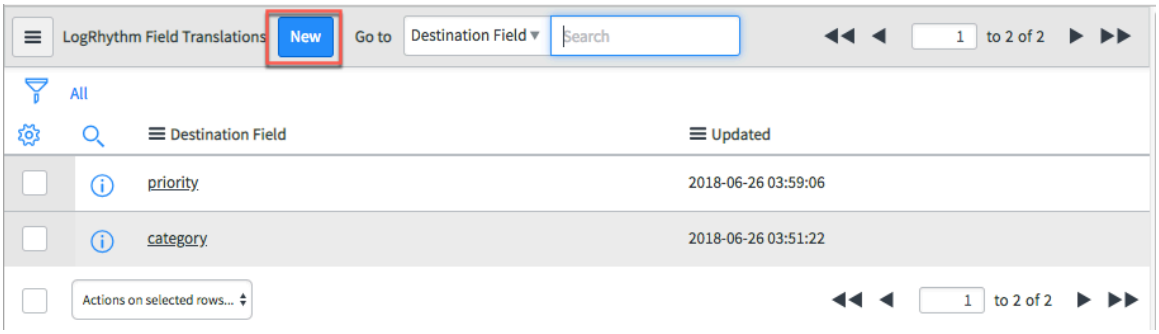

klicken.

Die Liste LogRhythm Feldübersetzung mit den Feldern „ Priorität “ und „Kategorieziel“ wird angezeigt.

**b.** Klicken Sie auf „Neu“.

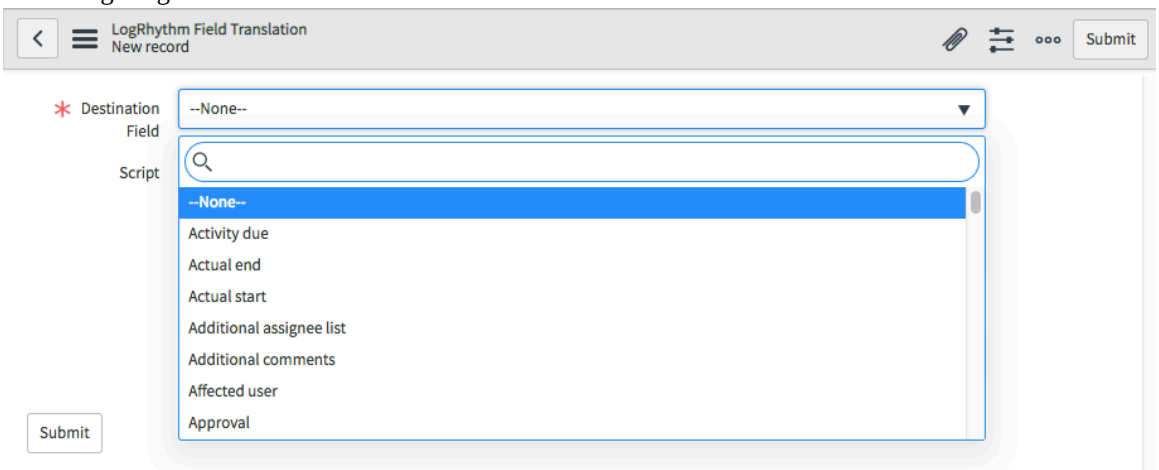
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Ein neuer Datensatz wird angezeigt.

**c.** Wählen Sie in der Auswahlliste Zielfeld ein Zielfeld im Security Incident aus, in dem Ihre geskripteten Werte angezeigt werden sollen.




**d.** Klicken Sie auf **Absenden**.
Der Skript-Editor wird angezeigt.

**e.** Geben Sie Änderungen in den Editor ein, und klicken Sie auf **Absenden**, um Ihre Änderungen zu speichern.
Die Tabelle LogRhythm „ Feldübersetzungen“ mit Ihrem neuen Datensatz wird angezeigt.

**5.** Schließen Sie die Tabelle, um zum Formular „Zuordnung“ zurückzukehren.

### Kopieren Sie ein Alarmprofil für LogRhythm

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein neues Alarmprofil zu erstellen. Wenn Sie mehrere Alarmprofile für verschiedene Alarmtypen erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, können Sie Alarmprofile kopieren, um Zeit zu sparen. Dieser Prozess ist optional.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Warum und wann dieser Vorgang ausgeführt wird**
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus wird das kopierte Profil auf inaktiv gesetzt, damit es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird.

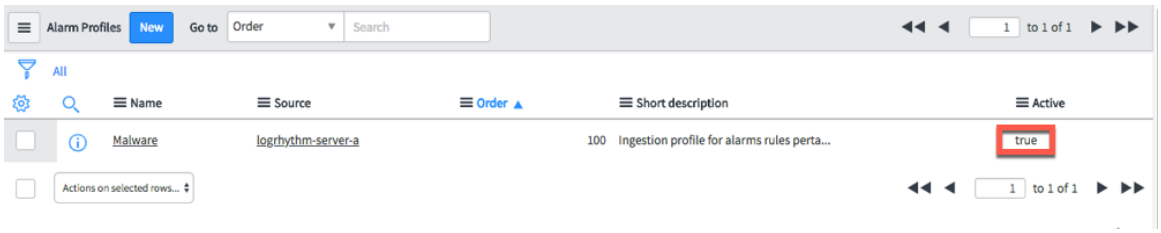


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

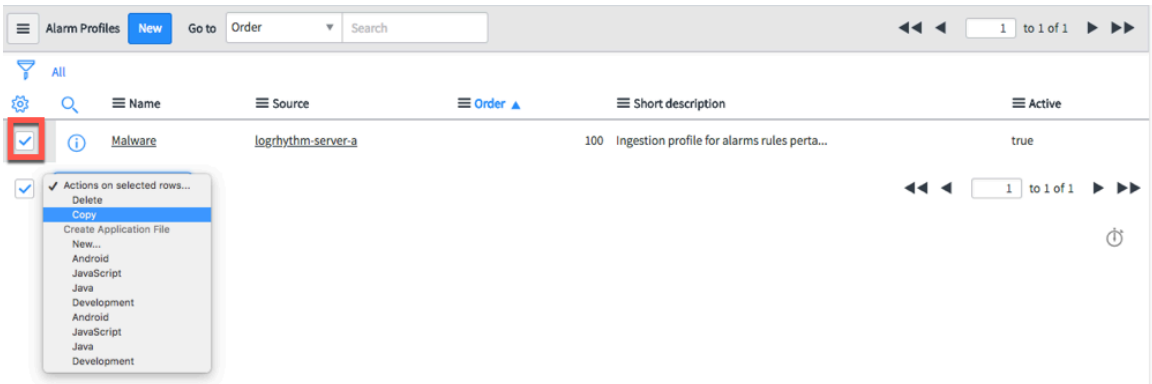
### Prozedur

1. Navigieren zu **Alle** > **LogRhythm Integration** > **LogRhythm-Alarmprofile**.

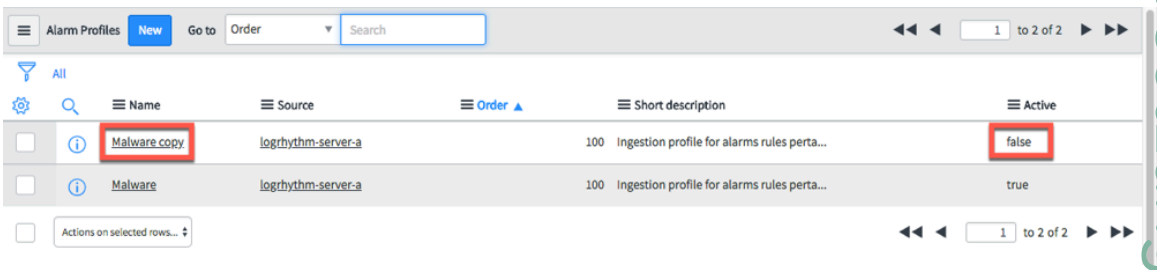
   Beachten Sie in der angezeigten Liste, dass die Spalte Aktiv angibt, ob das Profil aktiv ist (true).




2. Wählen Sie im Feld links neben der Spalte **Name** den Namen des Datensatzes aus.
3. Wählen Sie in der **Auswahlliste Aktionen für ausgewählte Zeilen** die Option **Kopieren**aus.




In der Liste **„Alarmprofile“** werden sowohl die Kopie als auch das ursprüngliche Profil angezeigt. Obwohl der ursprüngliche Datensatz aktiv ist, ist die Kopie zu diesem Zeitpunkt inaktiv (false). Nachdem Sie es konfiguriert haben, aktivieren Sie dieses kopierte Profil.




Sie können die Werte des kopierten Profils bearbeiten und es umbenennen, sodass abgerufene Alarmregeln für das neue Profil gelten. Sie werden aufgefordert, das neue Profil zu aktivieren, sobald die Konfigurationsschritte abgeschlossen sind.

## Deaktivieren Sie den automatisierten Alarmabschluss für LogRhythm

Deaktivieren Sie die Funktion zum automatischen Schließen von Alarmen, wenn Sie die Abschlussinformationen für Security Incidents nicht mehr in der LogRhythm Webkonsole anzeigen möchten. Nach der Deaktivierung schließt Now Platform keine Alarme mehr in der Webkonsole von LogRhythm. Dieser Prozess ist optional.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

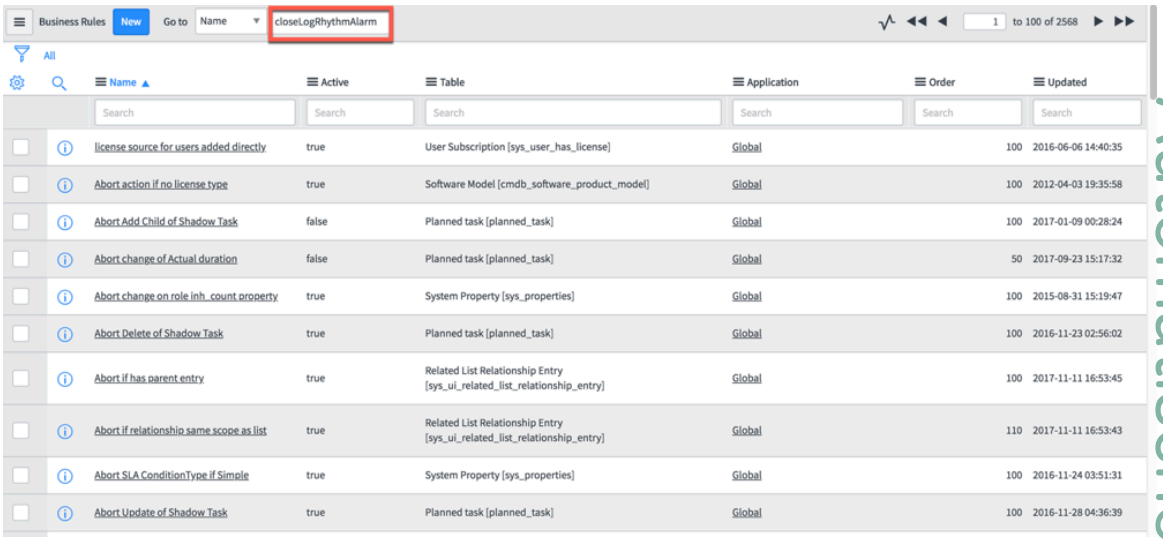
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Nach der Deaktivierung werden die Statusnotizen und andere Abschlussinformationen zum Security Incident nicht mehr in der LogRhythm Webkonsole angezeigt.

### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln** und wählen Sie das Modul **„Business Rules“** aus.
2. Wenn dies nicht in der Liste „ **Business Rules** “ angezeigt wird, geben Sie im Suchfeld **LogRhythm Close Alarm On SI Close** (LogRhythm-Alarm bei SI-Abschluss schließen) ein, und drücken Sie die **Eingabetaste**.




3. Klicken Sie in der Spalte **Name** auf den **Link LogRhythm-Alarm bei SI** -Abschluss schließen, um den Datensatz zu öffnen.
4. Deaktivieren Sie im angezeigten Datensatz das Kontrollkästchen **Aktiv**.
5. Klicken Sie auf **Aktualisieren**.
   Die Funktion zum automatischen Schließen von Alarmen ist jetzt deaktiviert.

## Zeigen Sie LogRhythm Drilldown-Ereignisse an

Zeigen Sie die zugehörigen Roh- oder Basis-Events für einen LogRhythm -Alarm im Security Incident an.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Als Sicherheitsanalyst können Sie die zugehörigen Roh- oder Basis-Events für einen LogRhythm -Alarm anzeigen, ohne zur LogRhythm -Konsole zurückkehren zu müssen. Sie können dazu zu einer zugehörigen Liste wechseln, die alle Drilldown-Ereignisse für den Incident SIR enthält.

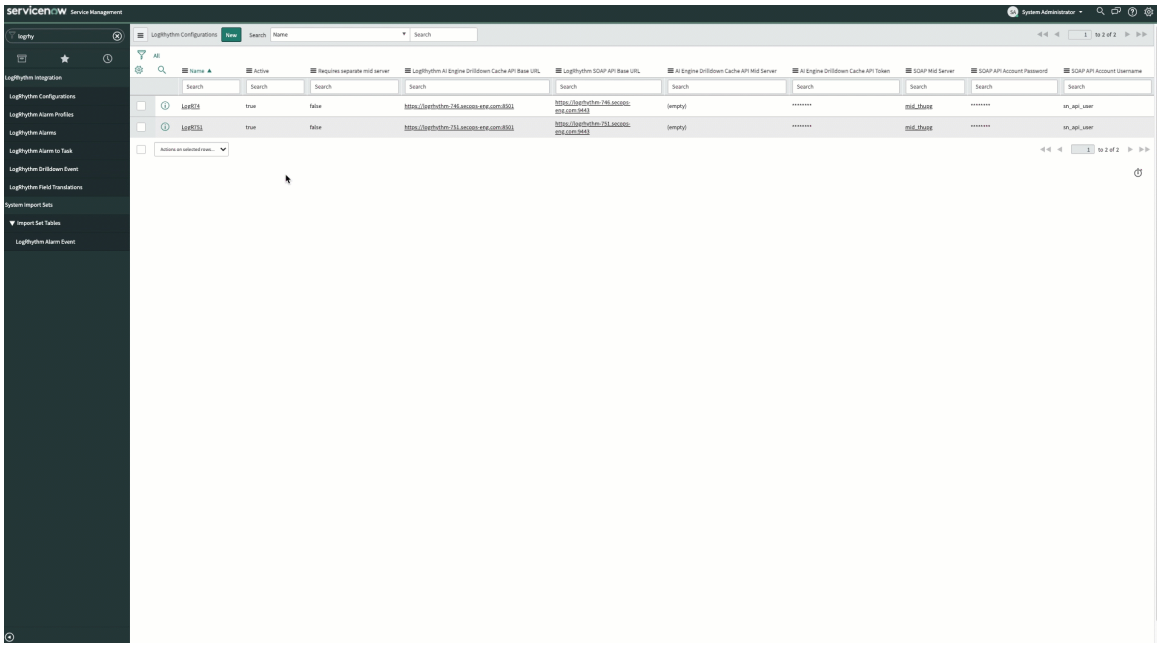
### Prozedur

Navigieren zu **Alle** > **LogRhythm Integration** > **LogRhythm-Drilldown-Ereignisse**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie zum Modul **LogRhythm Drilldown Events** navigieren, die Liste der Events nach „Gruppieren **nach Alarm-ID"**sortieren und auf den zugehörigen Security Incident klicken. Im Security Incident finden Sie die Registerkarte **LogRhythm-Drilldown-Ereignisse** unter den zugehörigen Links.



### Problembehandlung bei der LogRhythm-Integration

Beheben Sie Konnektivitäts- und Alarmerfassungsprobleme.

Informationen zur Problembehandlung finden Sie in den folgenden Themen:

- Überprüfen Sie die Konnektivität für LogRhythm
- Skriptausführung und Systemprotokoll für LogRhythm

### Überprüfen Sie die Konnektivität für LogRhythm

Überprüfen Sie Ihre Verbindung zur LogRhythm Client-Konsole, indem Sie Curl-Anforderungen senden, um die LogRhythm REST API zu testen. Der Verifizierungsprozess ist optional.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Um sicherzustellen, dass die Verbindung zur LogRhythm Client-Konsole nach dem Einrichten der LogRhythm REST APIs ordnungsgemäß funktioniert, senden Sie zwei Curl-Anforderungen vom Computer, auf dem sich der in Installieren Sie das Plugin, und konfigurieren Sie LogRhythmkonfigurierte MID Server befindet.

Die LogRhythm REST API verwendet WSSE für die Authentifizierung, was einige externe Skripts erfordert, um mit Curl und Postman zu funktionieren.

Die LogRhythm REST API verwendet ein Token für die Authentifizierung, sodass Sie den tatsächlichen Validierungsaufruf ausführen können, den die Integration verwendet. Die „0" am Ende der URL ist eine LogRhythm Alarm-ID. Die LogRhythm REST API mit einer Standardkonfiguration erfordert Port 8501. Diese Portnummer sollte in der URL enthalten sein, die Sie für den Test verwenden möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

Aktualisieren Sie die URL<LogRhythm REST url> und Token<api token> in der folgenden curl-Anforderung, und senden Sie sie an die Validierung der LogRhythm REST API: **curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Authorization: Bearer** „ “https://<cache drilldown url> /lr-drilldown-cache-api/drilldown/0"
Für eine erfolgreiche Verbindung mit der LogRhythm REST API sollten Sie HTTP 404 erhalten, aber der Antworttext enthält Alarm ID: 0 not found(Alarm-ID: 0 nicht gefunden).

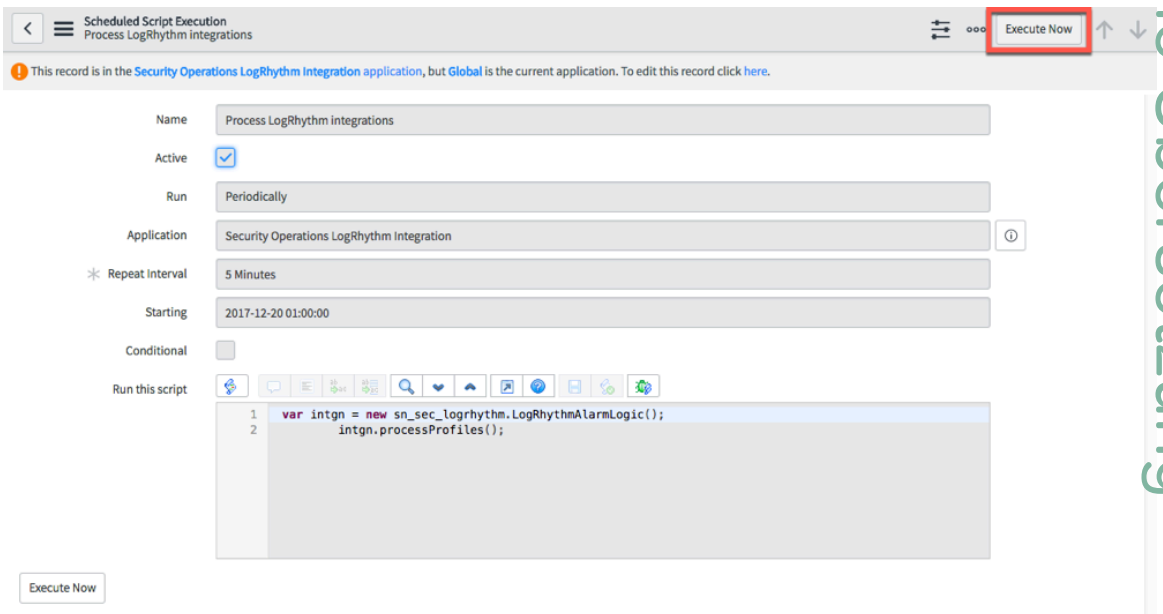
### Skriptausführung und Systemprotokoll für LogRhythm

Wenn Sie ein Problem bei der Alarmerfassung beheben, können Sie das standardmäßige Abfrageintervall von fünf Minuten überschreiben, um die Ergebnisse sofort anzuzeigen. Rufen Sie in diesem Szenario die Skriptausführung manuell auf, um die Abfrage auszuführen. Diese Ausführung ist optional.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Regelmäßige Aufgabe** > **Geplante Aufgaben** und wählen Sie das Modul „ **Geplante Aufgaben** “ aus.
2. Klicken Sie auf den Integrationsaufgaben-Datensatz „Process LogRhythm “ .
3. Klicken Sie im angezeigten Datensatz „Geplante Skriptausführung“ auf **Jetzt ausführen**.




Wenn Sie weitere Hilfe bei der Fehlerbehebung benötigen, können Sie auf das Systemprotokoll für die LogRhythm -Abfragen zugreifen.

4. Führen Sie bei anderen allgemeinen Problembehandlungsproblemen diese Schritte aus, um auf die Systemprotokolle zuzugreifen.

   a. Navigieren zu **Systemprotokoll** > **Alle** und wählen Sie **Alle**.

   b. Legen Sie den Filter (Wechselnzu) auf **Quelle** fest, und geben Sie sn_sec_logrhythmein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**c.** Drücken Sie die **Eingabetaste**.
Alle von der Integration generierten Nachrichten werden in dieser Tabelle angezeigt. Die aufgelisteten Nachrichten können Einblicke in die laufenden Prozesse der Integration geben und Sie bei der weiteren Problembehandlung unterstützen.

## Integration „McAfee ePO“

Die EDR-Fähigkeit (Integrationsendpunkterkennung und -reaktion) von McAfee ePO, mit der SOC-Analysten (Security Operations Center) Cyberbedrohungen identifizieren und den durch schädliche Dateien verursachten Schaden beheben können.

## Übersicht

In dieser Integration werden zwei Sätze von McAfee ePO -Fähigkeiten verwendet: die Fähigkeiten, die Aktionen aufrufen, z. B. das Isolieren eines Hosts und das Initiieren eines Malware-Scans, und die Fähigkeiten, die Abfragen ausführen, um Systemdetails und Bedrohungsereignisse zu erfassen. Beide Arten von Fähigkeiten, die Aktionen und die Abfragen, werden von Ihrer Now Platform® -Instanz aus aufgerufen. Sie können diese Fähigkeiten gruppieren, sodass sie automatisch ausgeführt werden, wenn eine bestimmte Art von Sicherheitsereignis auftritt, oder Sie können sie manuell aus einem Now Platform® Security Incident aufrufen.

Die folgenden McAfee ePO -Fähigkeiten sind für diese Integration verfügbar.

**Ruft Systemdetails ab**

Erfasst Systemdetails, einschließlich Details zum Betriebssystem.

**Initiiert einen Malware-Scan**

Initiieren Sie basierend auf der Scan-Konfiguration und -Zeitplanung einen Scan eines betroffenen Endpunkts.

**Host isolieren/nicht isolieren**

Entfernen Sie ein System zu Untersuchungszwecken aus dem Netzwerkzugriff, und stellen Sie den Zugriff auf das Netzwerk wieder her.

**Listet Bedrohungsereignisse auf**

Erfassen Sie den Compliance-Status und die aktuellen Bedrohungsereignisse.

## Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen.

- Unterstützt die automatisierte Auslösung von McAfee ePO Abfragen, die auf Incident-Bedingungen basieren.
- Unterstützt das manuelle Starten von McAfee ePO -Fähigkeiten aus Now Platform® Security Incident Response (SIR) Security Incidents, die bei Bedarf Aktionen ausführen.
- Die Flexibilität, mehrere Profile zum Auslösen verschiedener Arten von McAfee ePO - und Now Platform® Security Operations -Fähigkeiten zu erstellen. Diese Profile sammeln Informationen zu Bedrohungsereignissen oder führen Aktionen basierend auf den Bedingungen bestimmter Incident-Kategorien wie Malware aus.
- Validieren Sie Ihre Profilkonfiguration mit einer Vorschau der McAfee ePO -Ergebnisse für SIR Security Incidents.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Tagging aktiviert ist, identifizieren Sicherheits-Tags, welche McAfee ePO -Fähigkeiten anfänglich von einem Workflow gestartet werden und wann die Abfragen oder Aktionen erfolgreich abgeschlossen sind.
- Ein vollständiger Audit-Pfad der McAfee ePO -Abfragen und -Aktionen wird in den Arbeitsnotizen zu SIR Security Incidents veröffentlicht, und Befehle von Now Platform® werden in der McAfee ePO -Konsole protokolliert.
- Unterstützt mehrere McAfee ePO -Konsolen.

## ServiceNow Plugins

Das Plugin „com.snc.si_dep“ ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations Anwendungen müssen über den ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response
5. Arbeitsbereich für Security Incident Response

Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Richten Sie Ihre Now Platform -Instanz für die McAfee ePO -Integration ein.

## Das Erweiterungs-Plugin ServiceNow

Das Plugin „ServiceNow Security Operations Extension for McAfee ePO“# ist für diese Integration erforderlich. Sie installieren dieses ServiceNow -Plugin in Ihrer McAfee ePO -Konsole. Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die McAfee ePO -Integration ein.

## MID-Server

Für diese Integration muss ein installierter und konfigurierter MID Server in Ihrer Now Platform® -Instanz eine Verbindung zum McAfee ePO -Server (Konsole) herstellen. Weitere Informationen zu MID Servern finden Sie auf der Website der ServiceNow-Produktdokumentation .

## Unterstützte Versionen von McAfee

Die Integration unterstützt Version 5.9.1 und 5.10 von McAfee ePO. Sie unterstützt McAfee Agent: MA 5.5.1.388. Weitere Informationen zu McAfee-Produkten und dem ePolicy Orchestrator finden Sie auf der McAfee-Produktwebsite .

Die Integration unterstützt Version 10.5 des Produkts McAfee Endpoint Security Threat Prevention. Wenn Sie Version 10.5 nicht ausführen, wenden Sie sich an Ihren McAfee ePO -Administrator, um zu erfahren, ob Ihre Version On-Demand-Scans über Tag-Aktionen unterstützen kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

McAfee ePO Sicherheits-Tags werden in dieser Integration verwendet. Sie müssen diese Tags in Ihrer McAfee ePO -Konsole erstellen. Weitere Informationen zu diesen Tags finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..

## Referenzen

| Referenz | Dokumentbezeichner | Dokumententitel |
|---|---|---|
| 1 | McAfee-Produktwebsite | McAfee-Produktwebsite |
| 2 | McAfee-Geschäftsproduktdokumentation für ePolicy Orchestrator Cloud | McAfee-Produktdokumentation |
| 3 | ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |

Eine Prüfliste, um Ihren Fortschritt beim Einrichten, Installieren und Überprüfen der Ergebnisse für die Integration nachzuverfolgen, finden Sie unter Prüfliste für die McAfee ePO -Integration.

Um eine reibungslose Installation der Anwendung zu gewährleisten und die erwarteten Ergebnisse zu überprüfen, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

**Zugehörige Informationen**

Integrationsarchitektur für McAfee ePO

### Integrationsarchitektur für McAfee ePO

Das folgende Thema bietet einen Überblick über die Systemarchitektur und listet die wichtigsten Funktionen der Integration auf. Dieser Abschnitt enthält auch Informationen zu den Setup-Schritten, die Sie in Ihrer Instanz Now Platform und in der Konsole von McAfee ePolicy Orchestrator (McAfee ePO) ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

## Wichtige Begriffe für die McAfee ePO -Integration

Die folgenden Begriffe werden in der gesamten Installations- und Konfigurationsdokumentation für die -Integration verwendet.

**Now Platform**

Ein Unternehmensprodukt ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere Produkte basieren.

**Security Incident Response (SIR)**

Eine Now Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und dem Abschluss nach Incidents nachverfolgt.

**Plugin**

Plugins sind Softwarekomponenten, die bestimmte Features und Funktionalitäten in Ihrer Now Platform -Instanz bereitstellen. Weitere Informationen zur Installation und Konfiguration der Integrations-Plugins finden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration.

**ePolicy Orchestrator (McAfee ePO)**

Die Benutzerkonsole, in der Sie die McAfee-Services, -Produkte und -Einstellungen verwalten.

**McAfee-Erweiterungs-Plugin**

Dieses ServiceNow Erweiterungs-Plugin ist für diese Integration erforderlich. Dieses Plugin befindet sich in Ihrer McAfee ePO -Konsole und verbindet Ihre McAfee ePO -Konsole mit Ihrer Now Platform -Instanz.

**Fähigkeit**

Eine automatische Aktivität, die von Ihrer Instanz Now Platform initiiert und in der Konsole McAfee ePO ausgeführt wird, um Ergänzungsabfragen durchzuführen und Aktionen für Ihre Assets auszuführen.

**Profil**

Einstellungen für McAfee ePO -Fähigkeiten, die Sie konfigurieren, um anzugeben, wann und unter welchen Bedingungen Fähigkeiten Ergänzungsabfragen und Aktionen für Ihre Assets ausführen.

**MID-Server verwenden**

Eine Anwendung, die die Kommunikation und die Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services erleichtert.

**ServiceNow -Administrator (admin)**

Benutzer mit dieser Rolle laden die Plugins SIR und McAfee ePO herunter und installieren sie in Ihrer Instanz Now Platform. Benutzer mit dieser Rolle weisen bei Bedarf auch die Rolle „Security Incident-Administrator“ zu.

**ServiceNow Security Incident-Administrator (sn_si.admin)**

Benutzer mit dieser Rolle führen die Konfiguration der McAfee ePO -Integration mit dem Produkt Security Incident Response (SIR) in Ihrer Instanz von Now Platform nach Bedarf durch. Benutzer mit dieser Rolle weisen bei Bedarf auch die Rolle „Security Incident-Analyst“ zu.

**ServiceNow Security Incident-Analyst (sn_si.analyst)**

Benutzer mit dieser Rolle interagieren mit und analysieren Security Incidents im SIR-Produkt.

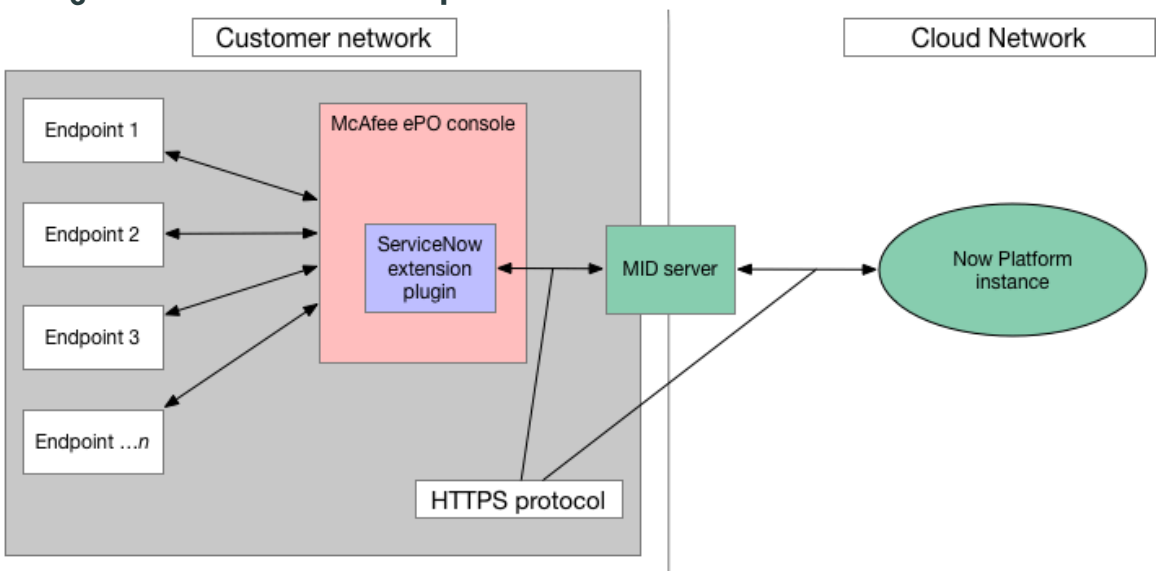
## Systemverbindung und Datenfluss

Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. Ein Now Platform MID-Server ist erforderlich, damit Ihre Now Platform -Instanz über ein ServiceNow -Erweiterungs-Plugin eine Verbindung zu einem McAfee ePO -Server (Konsole) herstellen kann. Nachdem Sie eine Verbindung hergestellt haben, rufen Sie Fähigkeiten von Ihrem Now Platform auf, um Malware-Scans zu initiieren, Hostcomputer zu isolieren und in Ihrem Netzwerk wiederherzustellen, die letzten Scan-Ergebnisse abzurufen und Systemdetails zu Ihren Assets zu erfassen. Wenn diese Fähigkeiten Ergebnisse aus Ihren Assets zurückgeben, die Ihren Suchkriterien entsprechen, werden Daten über den MID Server in Ihre Now Platform -Instanz abgerufen. Daten werden in den zugehörigen Listen eines Now Platform Security Incident Response (SIR) Security Incidents angezeigt. Die folgende Abbildung zeigt den Datenfluss für eine Gruppe von Endpunkten, die von einer McAfee ePO -Konsole verwaltet werden.



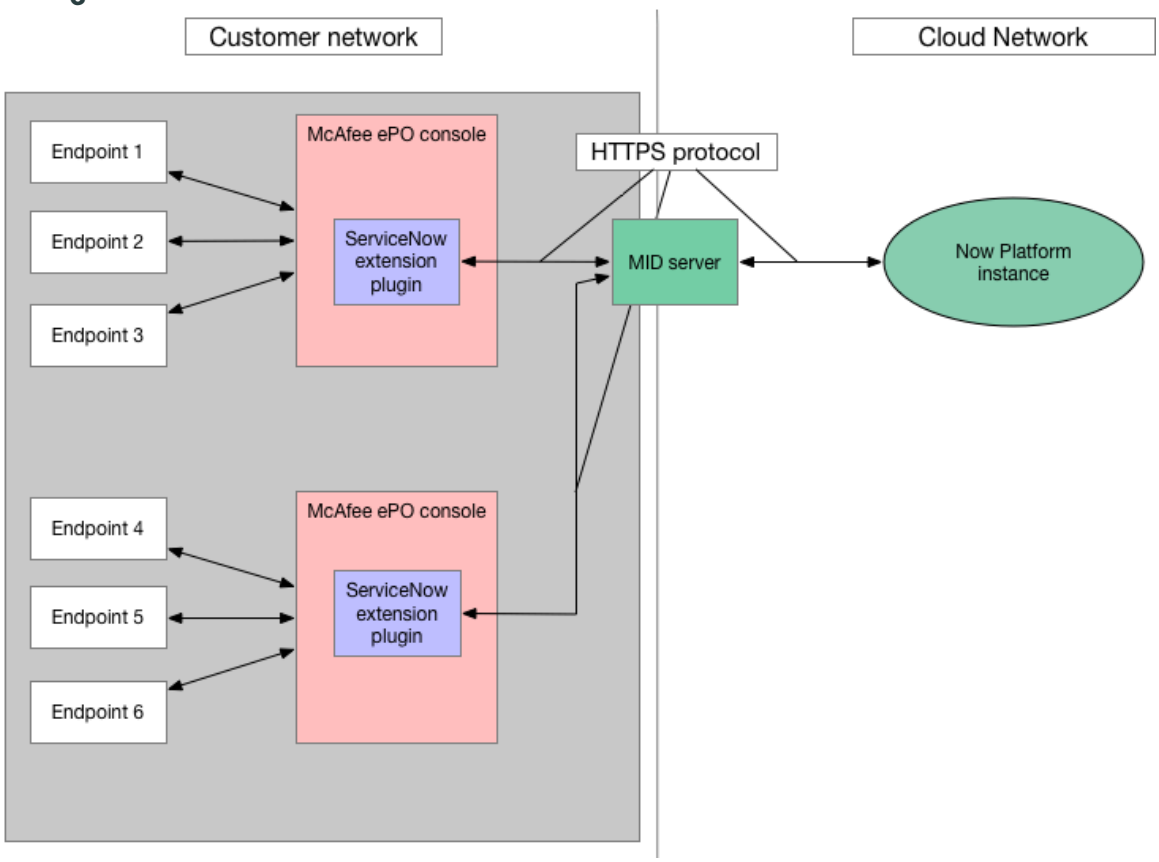
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfiguration eines einzelnen Endpunkts




Wie in der folgenden Abbildung dargestellt, kann diese Integration mehr als eine McAfee ePO -Konsole unterstützen. Sie können eine Gruppe von Endpunkten von einer McAfee ePO -Konsole und eine andere Gruppe von Endpunkten von einer anderen McAfee ePO -Konsole verwalten lassen. Daten aus mehreren McAfee ePO -Konsolen werden über einen einzelnen MID-Server abgerufen. Sie können jedoch auch mehrere MID-Server konfigurieren, wenn dies für Ihre Organisation erforderlich ist.

### Konfiguration der MID-Server




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Workflows für die McAfee ePO -Integration

Diese Integration umfasst die folgenden Workflows. Diese Workflows sind vorkonfiguriert und wurden speziell für diese Integration entwickelt. Sie können diese Workflows nach Bedarf bearbeiten, um die Anforderungen Ihrer Organisation zu erfüllen. Weitere allgemeine Informationen zu Workflows und zur Verwendung des Workflow-Editors finden Sie unter Erste Schritte mit Workflows .

- Security Operations McAfee ePO-Integration – Hostdetails abrufen
- Security Operations McAfee ePO-Integration – Malware-Scan initiieren
- Security Operations McAfee ePO-Integration – Host isolieren
- Security Operations McAfee ePO-Integration – Bedrohungsereignisse auflisten
- Security Operations McAfee ePO-Integration – Isolierung entfernen

## Verbindung mit externen Systemen

Die Integration erfordert, dass der MID Server über eine HTTPS-Protokollverbindung mit der McAfee ePO -Konsole kommuniziert.

### Prüfliste für die McAfee ePO -Integration

Verwenden Sie diese Prüfliste, um alle Aufgaben der Integration zu durchlaufen.
Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

**Vorbereitungen**
Erforderliche Rolle: Für jeden Schritt werden Rollen aufgelistet.

**Warum und wann dieser Vorgang ausgeführt wird**
Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration mit der folgenden Tabelle nach. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. In jeder Zeile der Tabelle werden Aufgaben aufgelistet und die Rollen angegeben, die zum Ausführen der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

**Prozedur**

Führen Sie die Schritte in der Tabelle in der Reihenfolge aus, in der sie angezeigt werden.

**Prüfliste**

| Element | Beschreibung |
|---|---|
| ☐ | Richten Sie als Benutzer mit der Administratorrolle Now Platform® ] Ihre Now Platform® -Instanz ein.<br>**a.** Weisen Sie die Rollen Now Platform® und Security Incident Response zu.<br>**b.** Vergewissern Sie sich, dass ServiceNow Security Incident Response und andere Plugins, die die Integration unterstützen, für Ihren Release von Now Platforminstalliert und aktiviert sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
|---|---|
| | **c.** Installieren und konfigurieren Sie einen MID-Server in Ihrer Now Platform® -Instanz.<br>**d.** Erstellen Sie eine Genehmigungsgruppe, wenn Sie vom Security Incident-Analysten übermittelte Anforderungen für den Isolationshost verarbeiten und Malware-Scan-Aktionen initiieren möchten.<br>Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die McAfee ePO -Integration ein. |
| ☐ | Richten Sie als McAfee ePO ]-Administrator Ihre McAfee ePO -Konsole ein.<br>**a.** Vergewissern Sie sich, dass Sie Version 5.9 von McAfee ePOverwenden.<br>**b.** Installieren Sie das Erweiterungs-Plugin [ ServiceNow in Ihrer Konsole McAfee ePO.<br>**c.** Vergewissern Sie sich, dass Sie Sicherheits-Tags in Ihrer McAfee ePO -Konsole für den isolierten Host erstellt haben, und initiieren Sie Malware-Scan-Aktionen.<br>Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..<br>Um weitere Informationen zu erhalten und die Erweiterungs-Plugin-Datei zu erhalten, navigieren Sie in Ihrer Now Platform -Instanz zu **Wissen** > **Artikel** > **Alle** und geben Sie im Feld Suche ServiceNow Security Operations Extension for McAfee ePO ein. |
| ☐ | Installieren Sie als Benutzer mit der Administratorrolle Now PlatformMcAfee ePO die Anwendung [] aus dem ServiceNow Store, konfigurieren Sie einen Server, und stellen Sie eine Verbindung zur Konsole McAfee ePO her.<br>Weitere Informationen finden Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration. |
| ☐ | Bearbeiten Sie als Benutzer mit der Rolle Now Platform Security Incident-Administrator die Sicherheits-Tag-Namen in Ihrer Instanz von Now Platform® so, dass sie den Tag-Namen entsprechen, die Sie in der Konsole McAfee ePO erstellt haben.<br>Weitere Informationen finden Sie unter Bearbeiten Sie Sicherheits-Tags in Now Platform für die McAfee ePO -Integration. |
| ☐ | Erstellen Sie als Benutzer mit der Rolle „Security Incident-Administrator“ ein Profil für McAfee ePO -Fähigkeiten.<br>Weitere Informationen zu Profilen finden Sie unter McAfee ePO Integrationsfähigkeitsprofile. Informationen zu den Schritten zum Erstellen eines Profils finden Sie unter Erstellen Sie ein Fähigkeitsprofil für die McAfee ePO -Integration. |
| ☐ | Konfigurieren Sie als Benutzer mit der Rolle „Security Incident-Administrator“ ein Profil, und testen Sie Security Incidents. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
|---|---|
| | **a.** Überprüfen Sie die Informationen zu Auslöserbedingungen und -einstellungen.<br>**b.** Konfigurieren Sie ein Profil.<br>**c.** Testen Sie Security Incidents, und zeigen Sie eine Vorschau an.<br>**d.** Suchen Sie Suchergebnisse und andere Details in den zugehörigen Listen zum Security Incident.<br>**e.** Erstellen und konfigurieren Sie verschiedene Arten von Profilen, und testen Sie Security Incidents für jeden Typ.<br><br>Weitere Informationen zu Auslöserbedingungen und dem Feld „Alternatives CI“ finden Sie unter Definieren von Auslöserbedingungen mit einem Konfigurationselement (CI)-Feld für ein McAfee ePO -Profil. Die Schritte zum Konfigurieren eines Profils, zum Testen und zur Vorschau von Security Incidents und Beispiele für Profiltypen finden Sie in den Beispielen nach Profile für die McAfee ePO -Integration konfigurieren. |
| ☐ | Senden Sie als Benutzer mit der Rolle Now Platform „ Security Incident-Analyst“ zusätzliche Anforderungen für Malware-Scans und Listen-Bedrohungsevents. Weitere Informationen finden Sie unter Lösen Sie das Profil McAfee ePO manuell aus einem Security Incident aus<br><br>In Now Platformkönnen Sie als Benutzer mit einer Genehmigungsrolle oder als Mitglied einer Genehmigungsgruppe Anforderungen für die Isolierung der Hostisolierung genehmigen und die Isolierung entfernen.<br><br>Weitere Informationen zur Verarbeitung von Genehmigungsanforderungen finden Sie unter Erstellen Sie eine Genehmigungsgruppe. |

Sie haben die Setup-Schritte erfolgreich abgeschlossen, die Anwendung installiert und konfiguriert und die erwarteten Ergebnisse für die Integration überprüft.

### Richten Sie Ihre Now Platform® -Instanz für die McAfee ePO -Integration ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz von Now Platform® ausführen müssen, bevor Sie die Anwendung für die Integration von McAfee ePO installieren.

## Richten Sie Anforderungen ein

Erforderliche Rolle: Now Platform Administrator (admin). Überprüfen Sie die folgenden Informationen vor Ihrer Now Platform® -Instanz für die McAfee ePO -Integration.

Die folgende Tabelle enthält eine Liste der Setup-Anforderungen für die Anwendung. Vergewissern Sie sich, dass Sie diese Aufgaben abgeschlossen haben, bevor Sie die Anwendung für die -Integration aus dem ServiceNow Storeinstallieren.

| Richten Sie die Aufgabe ein | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind erforderlich: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Richten Sie die Aufgabe ein | Beschreibung |
| --- | --- |
| | • Ein Benutzer mit der Systemadministratorrolle (admin), um die Anwendung zu installieren.<br>• Ein Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) konfiguriert die Anwendung und erstellt, aktiviert und entfernt Profile.<br>• Ein Benutzer mit der Rolle „Security Incident-Analyst“ (sn_si.analyst) arbeitet mit Security Incidents. Zu den Aufgaben gehört das manuelle Starten von Profilen aus Security Incidents. Wenn die Genehmigungsoption in einem Profil während des Konfigurationsschritts ausgewählt wird, senden Benutzer mit dieser Rolle auch Anforderungen zum Isolieren von Hosts und zum Zurückgeben an das Netzwerk. |
| Vergewissern Sie sich, dass Sie Version 5.9 von McAfee ePOverwenden. | Die Integration unterstützt Version 10.4.3 von McAfee ePolicy Orchestrator. |
| Vergewissern Sie sich, dass Sie das Erweiterungs-Plugin [ ServiceNow in Ihrer Konsole McAfee ePO ] installiert haben. | Installieren Sie das Plugin ServiceNow in Ihrer Konsole McAfee ePO.<br><br>Um weitere Informationen zu erhalten und die Plugin-Datei zu erhalten, navigieren Sie in Ihrer Now Platform -Instanz zu **Wissen** > **Artikel** > **Alle** und geben Sie im Feld Suche ServiceNow Security Operations Extension for McAfee ePO ein. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Das Plugin „Security Incident Response Dependency“ (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Richten Sie die Aufgabe ein | Beschreibung |
| --- | --- |
| | **1.** Security Incident Response<br>**2.** Arbeitsbereich für Security Incident Response<br>**3.** Security Integration Framework<br>**4.** Security Support Common<br>**5.** Security Support Orchestration<br><br>Weitere Informationen zur Installation der Security Operations-Kernanwendungen finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |
| Vergewissern Sie sich, dass Sie einen MID Server installiert und konfiguriert haben. | In Ihrer Now Platform® -Instanz ist ein installierter und konfigurierter MID Server erforderlich. Weitere Informationen zu MID Servern finden Sie auf der Website der ServiceNow-Produktdokumentation . |
| Wenn Sie den Genehmigungsprozess für Profile aktivieren möchten, stellen Sie sicher, dass Sie eine Genehmigungsgruppe zur Verarbeitung von Anforderungen erstellt haben. | Für die Isolierung von Hostcomputern und deren Wiederherstellung im Netzwerk ist ein optionaler Genehmigungsprozess verfügbar.<br><br>Wenn diese Option aktiviert ist, ist eine vorherige Genehmigung erforderlich, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden.<br><br>Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie die Option **Genehmigung** erforderlich während des Konfigurationsschritts für ein Profil.<br><br>Standardmäßig wird die Genehmigungsberechtigung dem Now Platform® Security Incident-Administrator (sn_si.admin) zugewiesen. Diese Berechtigung kann einer Genehmigungsgruppe neu zugewiesen werden. Innerhalb der Gruppe hat jedes Mitglied die Berechtigung, Anforderungen zu genehmigen oder abzulehnen.<br><br>Sie wählen während des Konfigurationsschritts Ihrer Profileinrichtung eine aktive Genehmigungsgruppe aus. Weitere Informationen finden Sie unter Erstellen Sie eine Genehmigungsgruppe. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.

Im folgenden Abschnitt werden die Setup-Schritte aufgelistet, die Sie in der Konsole McAfee ePO ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Store für die -Integration installieren.

#### Vorbereitungen

Erforderliche Rolle: McAfee ePO Administrator

Vergewissern Sie sich als Benutzer mit McAfee ePO-Administratorberechtigung, dass Sie das Erweiterungs-Plugin „ServiceNow.zip“ in Ihrer McAfee ePO -Konsole installiert haben. Dieses Erweiterungs-Plugin ist für die Integration erforderlich. Um weitere Informationen zu erhalten und das Plugin zu erhalten, navigieren Sie in Ihrer Now Platform -Instanz zu **Wissen** > **Artikel** > **Alle**. Geben Sie im Feld Suche ServiceNow Security Operations Extension for McAfee ePO ein.

#### Warum und wann dieser Vorgang ausgeführt wird

Das Erweiterungs-Plugin [ ServiceNow verbindet Ihre Now Platform -Instanz mit Ihrer McAfee ePO -Konsole. Über diese Verbindung können Sie auf die Sicherheits-Tags verweisen, die Sie in Ihrer McAfee ePO -Konsole für den Isolationshost erstellen und Malware-Scan-Aktionen für die Fähigkeitsprofile in Ihrer Now Platform -Instanz initiieren.

Die Sicherheits-Tags in Ihrer McAfee ePO -Konsole müssen mit den Sicherheits-Tags in den Fähigkeitsdatensätzen in Ihrer Now Platform ]-Instanz übereinstimmen.

Die folgenden Schritte zeigen, wie Sie das Erweiterungs-Plugin installieren, ein Sicherheits-Tag in Ihrer McAfee ePO -Konsole erstellen und dem Tag eine Aktion zuweisen. Weitere Informationen zu den Sicherheits-Tags in der Konsole McAfee ePO finden Sie auf der McAfee-Website mit Produktdokumentation .

**Hinweis:**
Die Abbildungen im folgenden Abschnitt stammen aus der Konsole McAfee ePO.

#### Prozedur

1. Wenn Sie das Erweiterungs-Plugin [ ServiceNow nicht auf Ihrer Konsole McAfee ePO installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren.

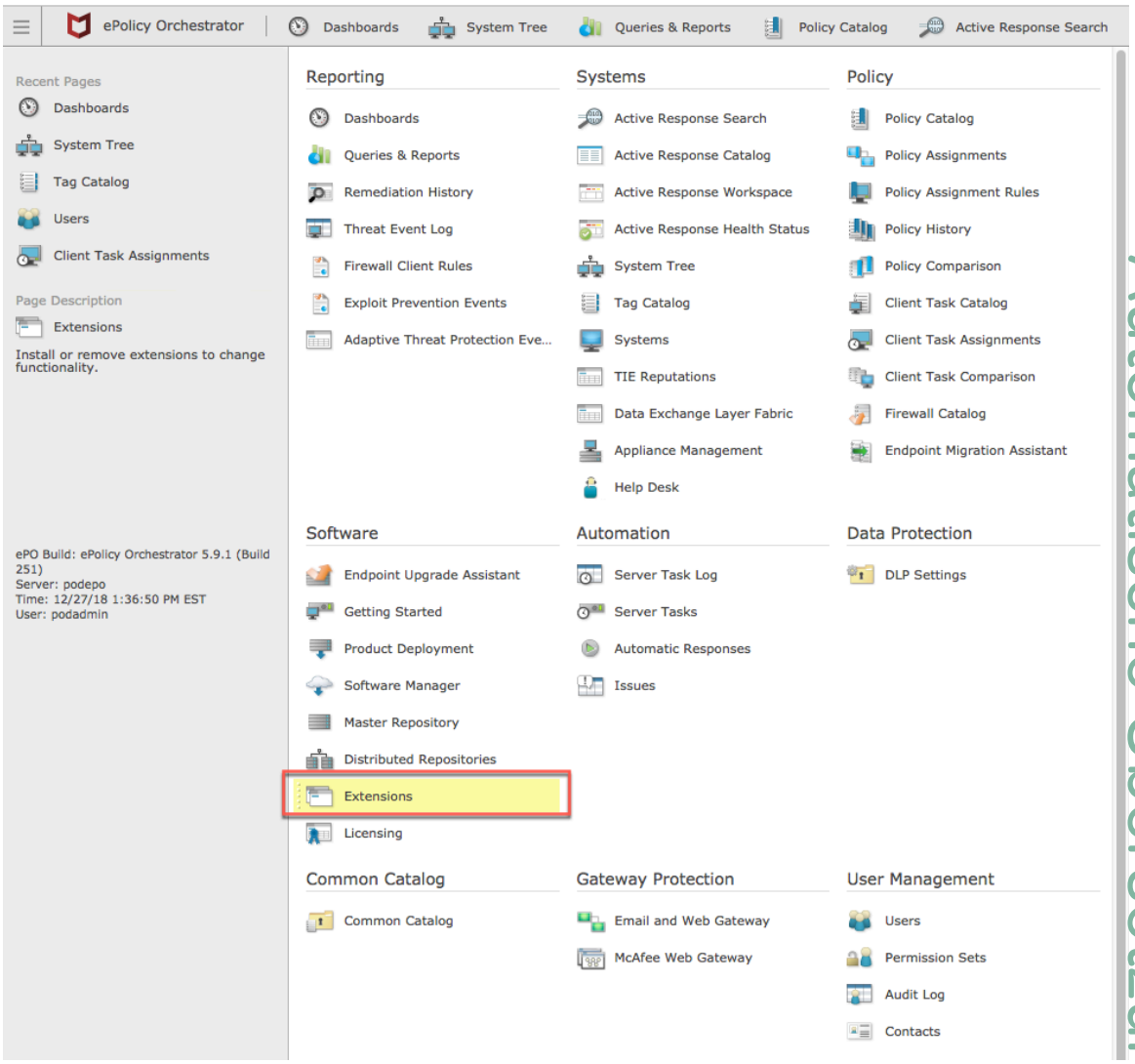
   a. Melden Sie sich bei Ihrer McAfee ePO -Konsole mit Ihrem McAfee-Benutzernamen und Passwort an.

Automatische Übersetzung

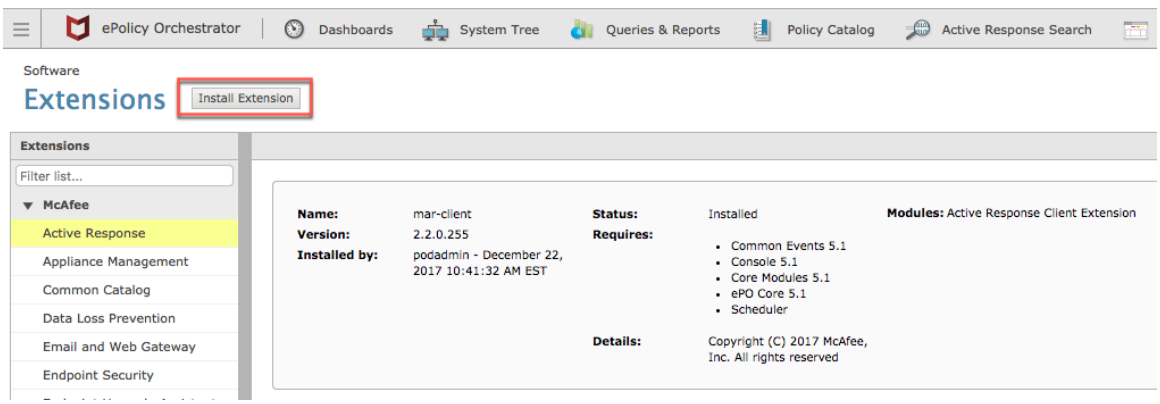
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wenn die in der folgenden Abbildung gezeigte Seite nicht angezeigt wird, klicken Sie oben links im Banner der Homepage auf das Menüsymbol, um sie anzuzeigen.

3. Klicken Sie im Abschnitt „Software“ auf den Link **Erweiterungen**.



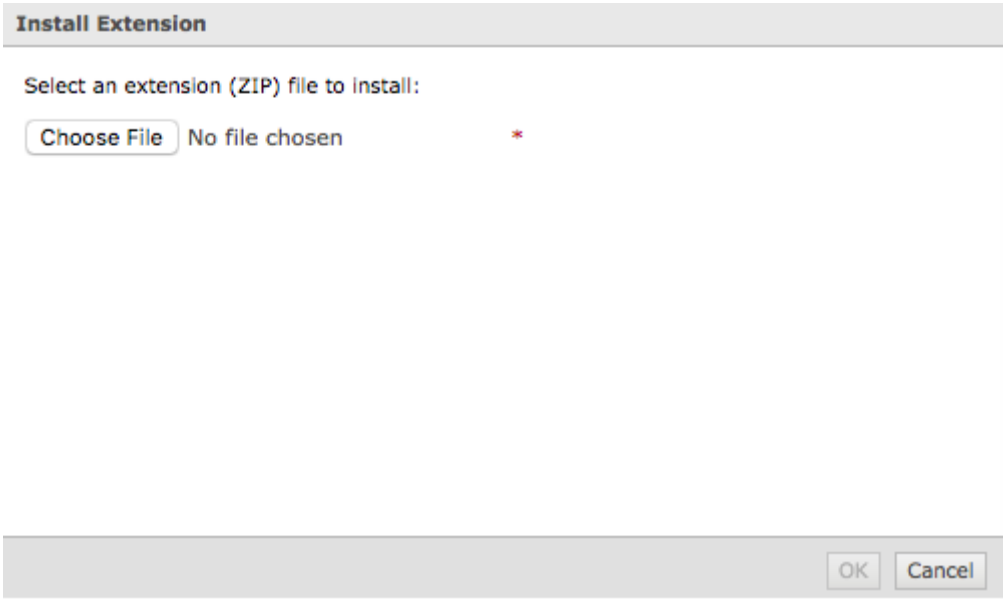

4. Klicken Sie auf der angezeigten Seite „Erweiterungen“ auf **Erweiterung installieren**.



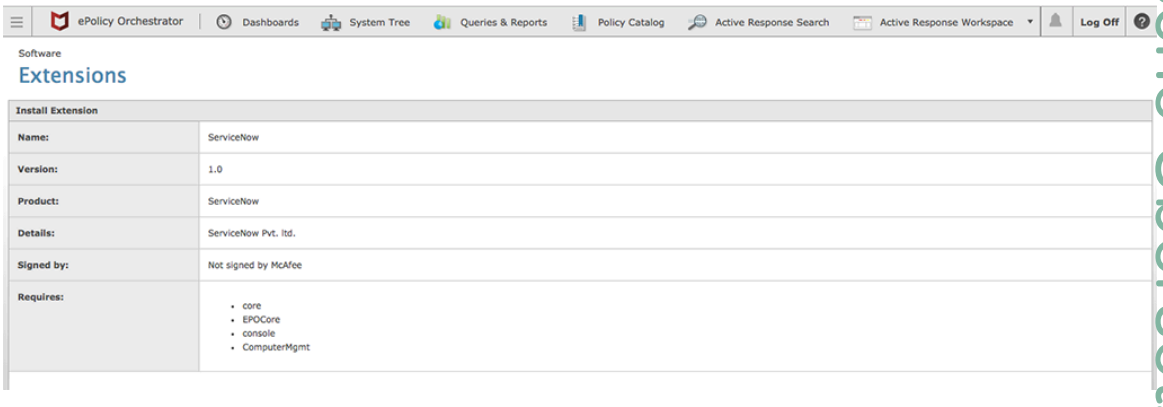

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie im Dialogfeld „Erweiterung installieren“ auf **Datei wählen**, navigieren Sie zur Datei Servicenow.zip auf Ihrem System, und klicken Sie auf **OK**, um sie herunterzuladen.




Nach Abschluss des Downloads wird die Seite „Softwareerweiterungen“ mit dem aufgeführten Erweiterungs-Plugin ServiceNow angezeigt.



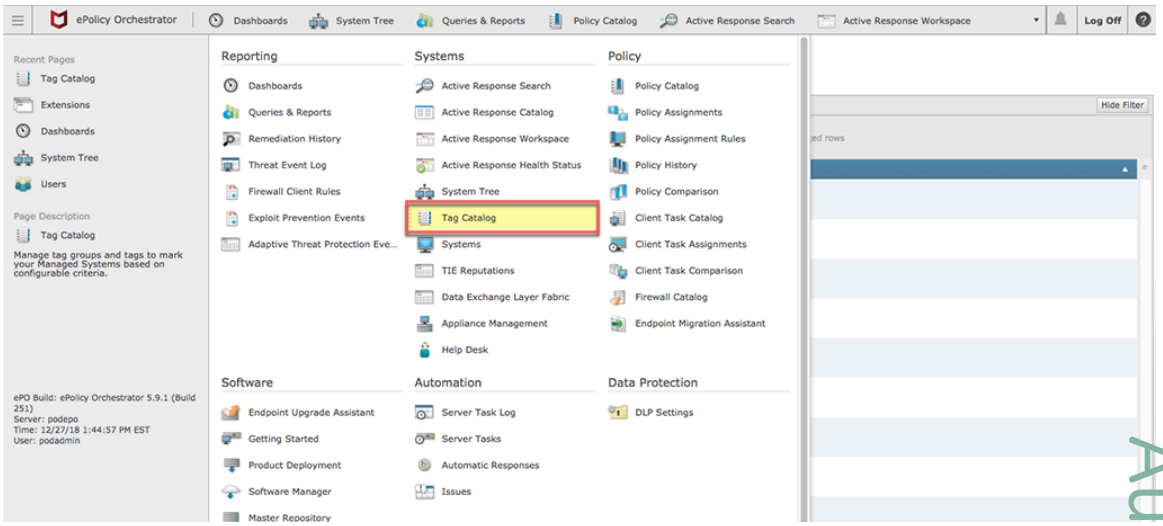

Sie haben die Plugin-Erweiterung [] erfolgreich auf Ihrer Konsole McAfee ePOServiceNow installiert.

6. Wenn Sie in der Konsole McAfee ePO keine Sicherheits-Tags für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ erstellt haben, führen Sie die folgenden Schritte aus.

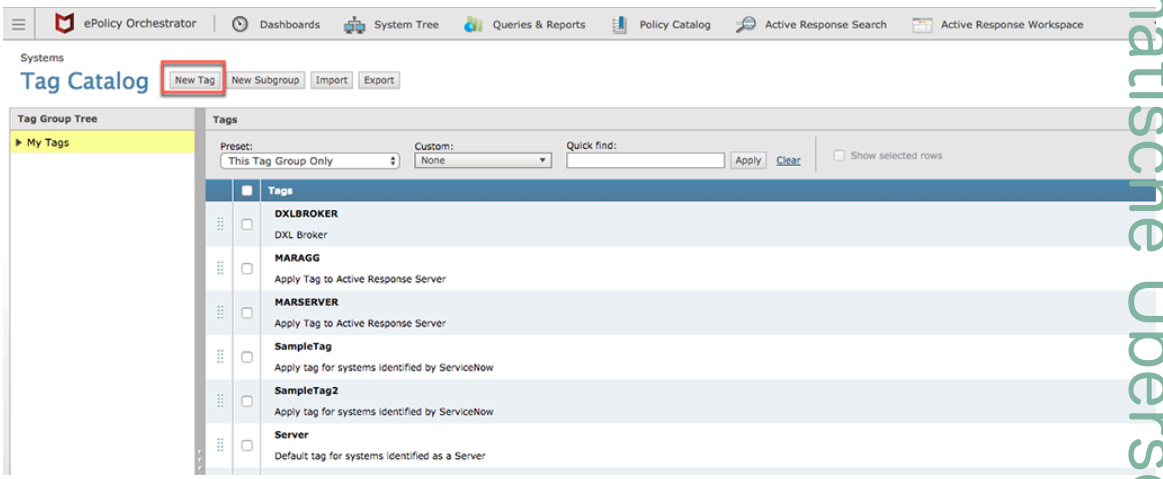


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Navigieren Sie zur -Homepage, und klicken Sie auf den Link **Tag Catalog** (Tag-Katalog).

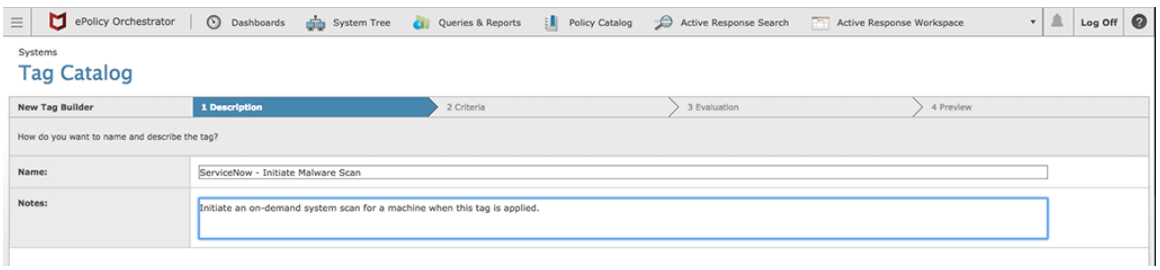



**b.** Klicken Sie auf der angezeigten Seite „Tag Catalog“ (Tag-Katalog) auf **Neues Tag**.




**c.** Wählen Sie im angezeigten Fortschrittsbalken den Schritt Beschreibung aus, und geben Sie einen Namen und eine Beschreibung für das Tag ein.

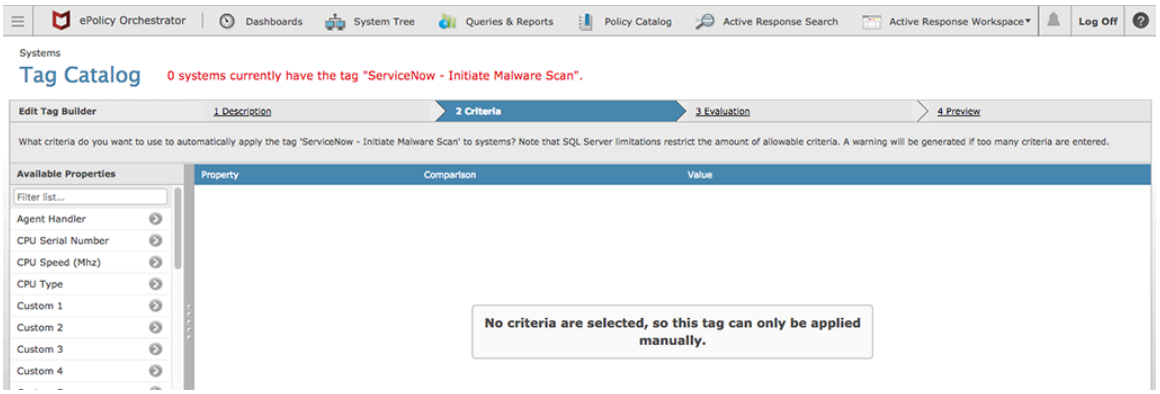
In diesem Beispiel wird ein Tag mit einem Namen und einer Beschreibung für die Fähigkeit „Malware-Scan initiieren“ angezeigt. Dieser Tag-Name wird in Ihrer Now Platform -Instanz abgeglichen und referenziert.



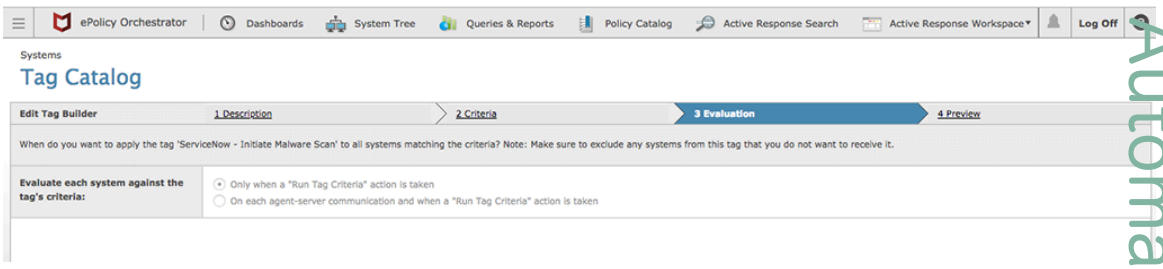

**d.** Um zum Schritt „Kriterien“ zu gelangen, klicken Sie in der Fortschrittsleiste auf **Kriterien**.
Die angezeigten Nachrichten weisen darauf hin, dass diesem Tag derzeit keine Aktionen zugewiesen sind und dass das Tag nur manuell angewendet werden kann.

Automatische Übersetzung

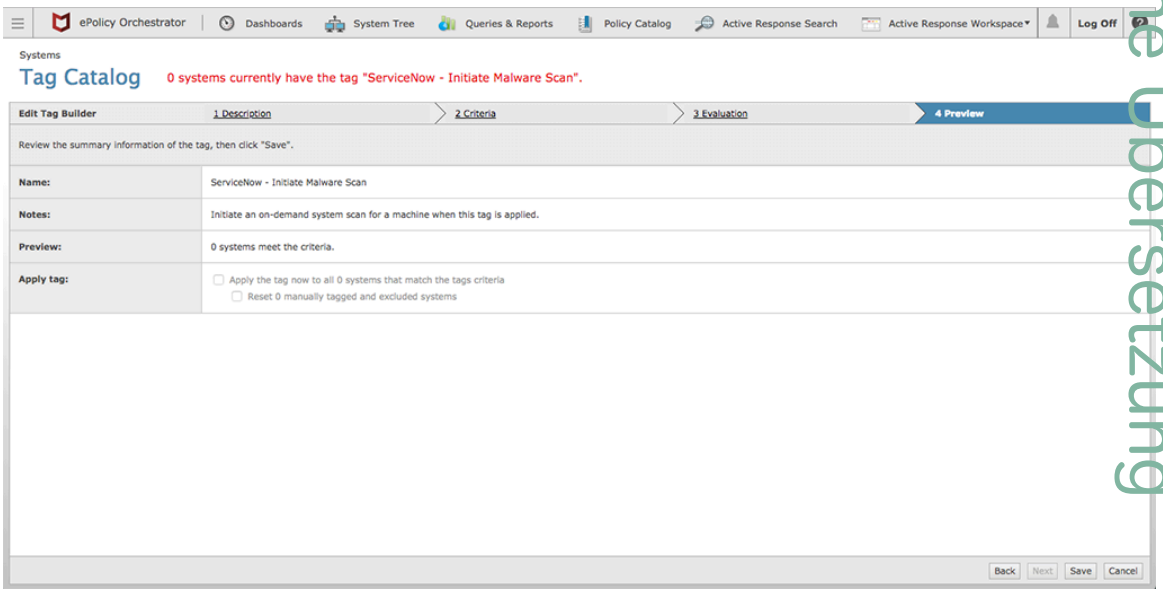
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**e.** Klicken Sie in der Fortschrittsleiste auf **Auswertung**, um fortzufahren.




**f.** Wenn die Seite „Tag-Katalog“ des Schritts „Auswertung“ angezeigt wird, belassen Sie die Einstellungen auf dieser Seite in ihren Standardwerten und klicken Sie in der Fortschrittsleiste auf **Vorschau**.

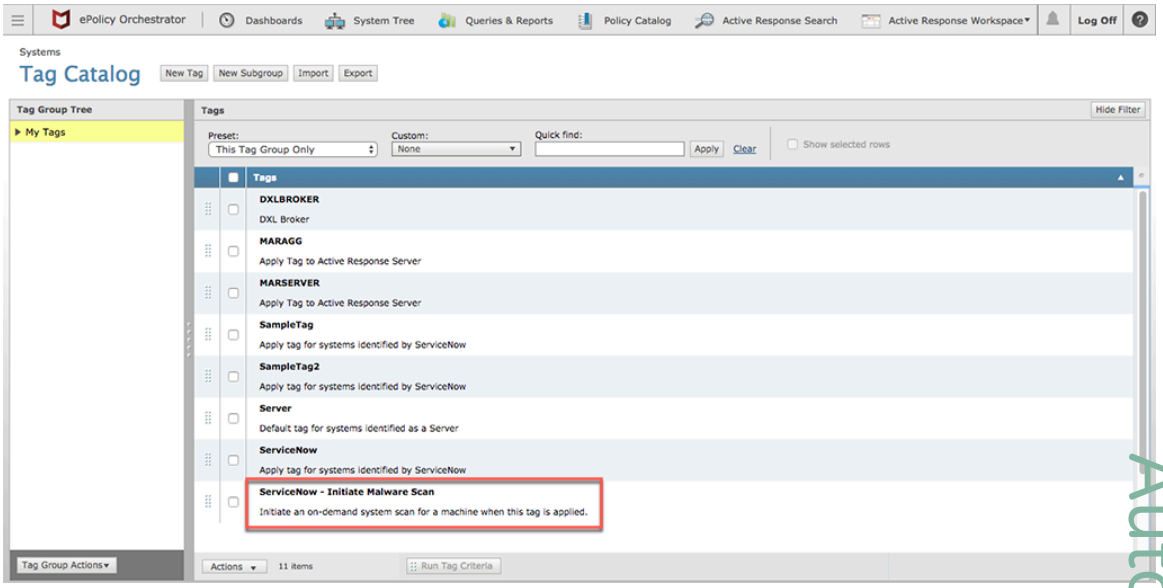



**g.** Wenn die Vorschauseite angezeigt wird, klicken Sie unten rechts auf der Seite auf **Speichern**, um den Datensatz zu speichern.

Automatische Übersetzung

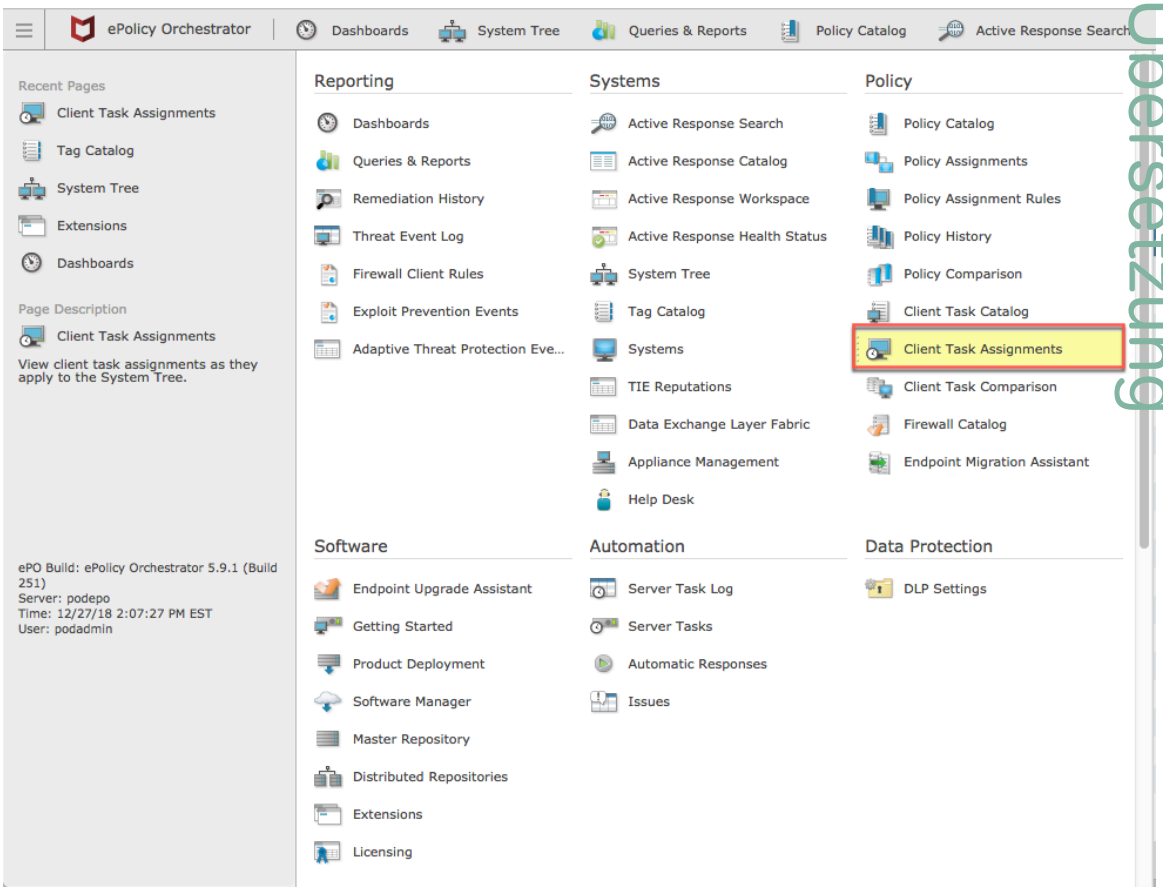
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das neue Tag wird im Tag-Katalog angezeigt (siehe folgende Abbildung).




7. Erstellen Sie ein Sicherheits-Tag für die Host-Isolationsaktion, indem Sie die vorherigen Schritte wiederholen.
   Nachdem Sie beide Tags erstellt haben, können Sie den neuen Tags Aktionen zuweisen.
8. Führen Sie die folgenden Schritte aus, um Ihrem neuen Tag eine Aktion hinzuzufügen.

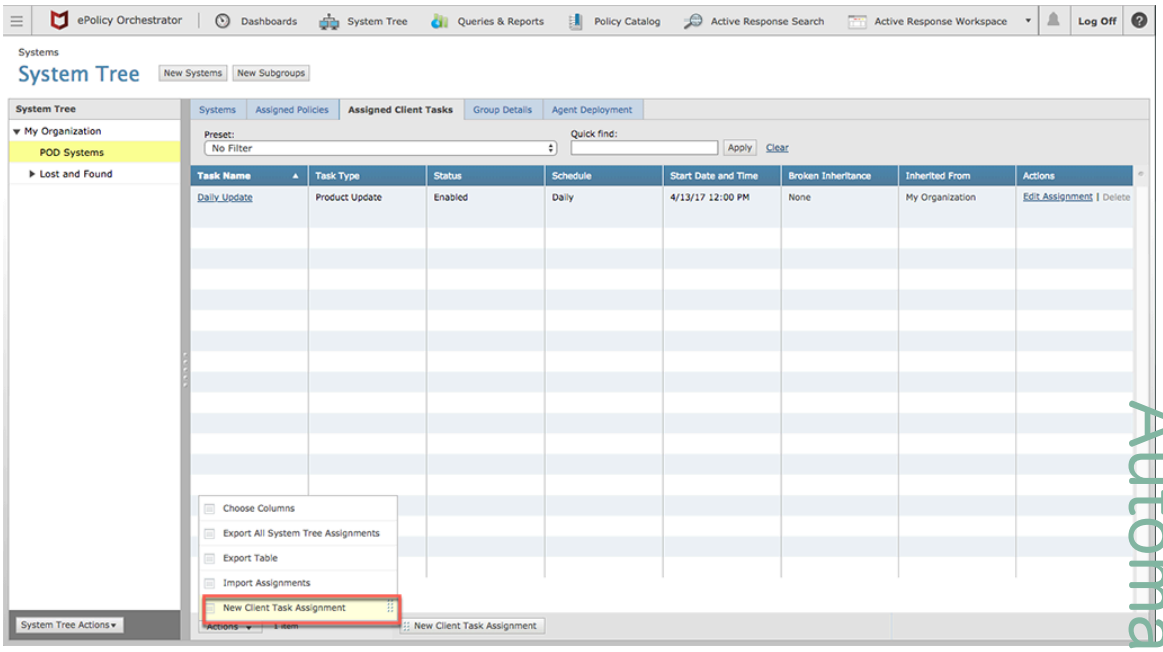
   a. Navigieren Sie zur Homepage, und klicken Sie im Abschnitt „Richtlinie“ auf den Link **Client-Aufgabenzuweisungen**.



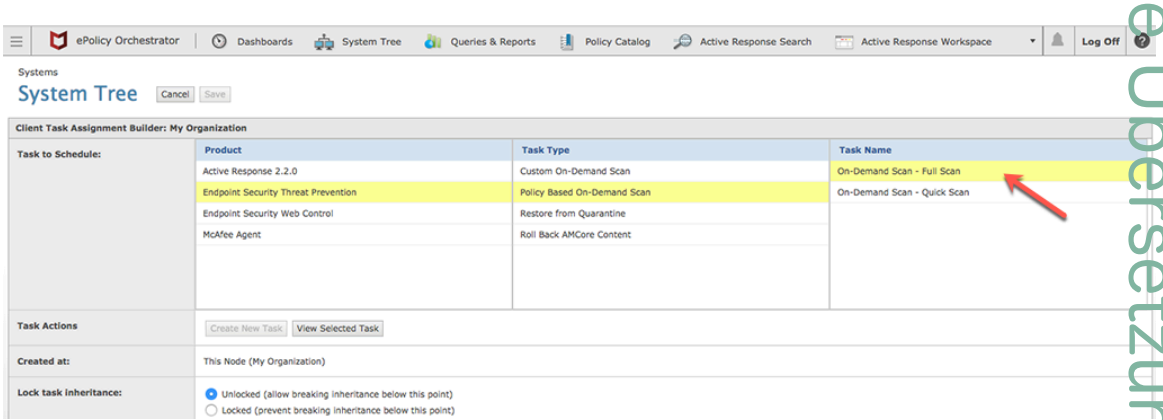

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**b.** Erweitern Sie auf der angezeigten Seite „Systemstruktur“ am unteren Rand der Seite das Menü **Aktionen**, und wählen Sie **Neue Client-Aufgabenzuweisung**aus.



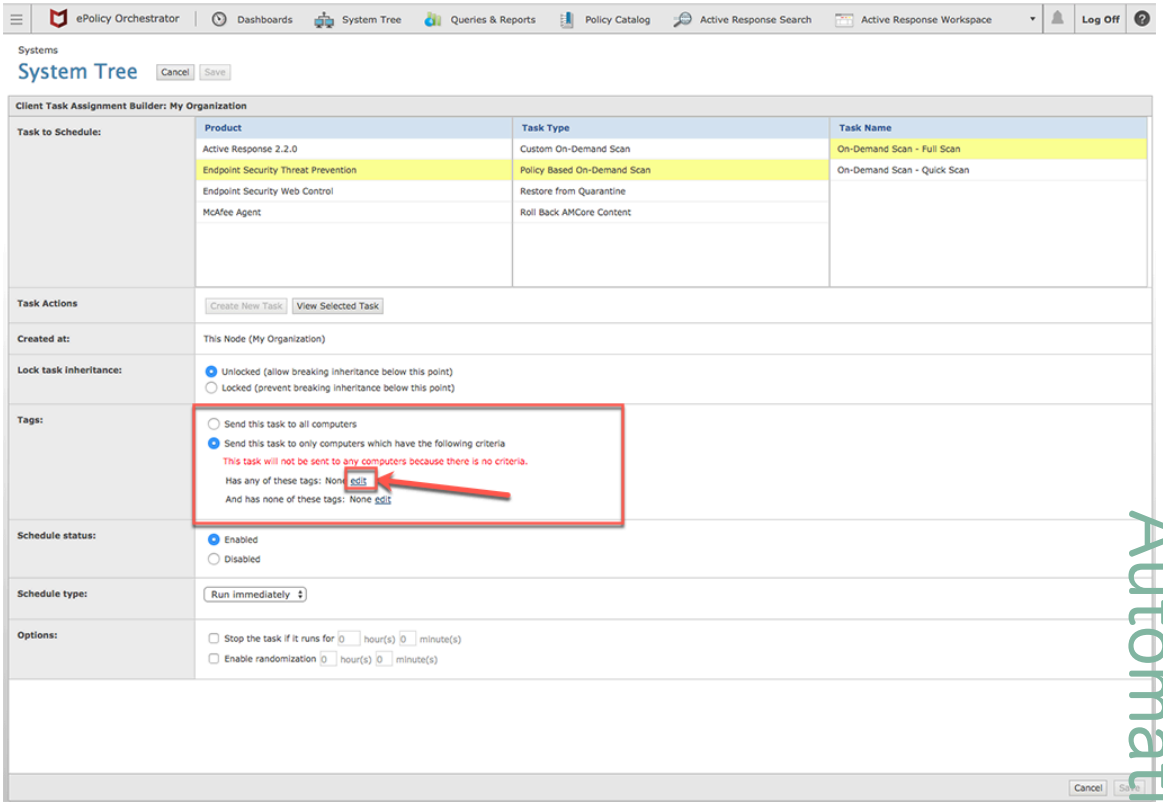

**c.** Navigieren Sie auf der angezeigten Seite zu **Endpunktsicherheits-Bedrohungsabwehr** > **Richtlinienbasierter Scan bei Bedarf** > **On-Demand-Scan – Vollständiger Scan** indem Sie den Pfad wie in der folgenden Abbildung auswählen.



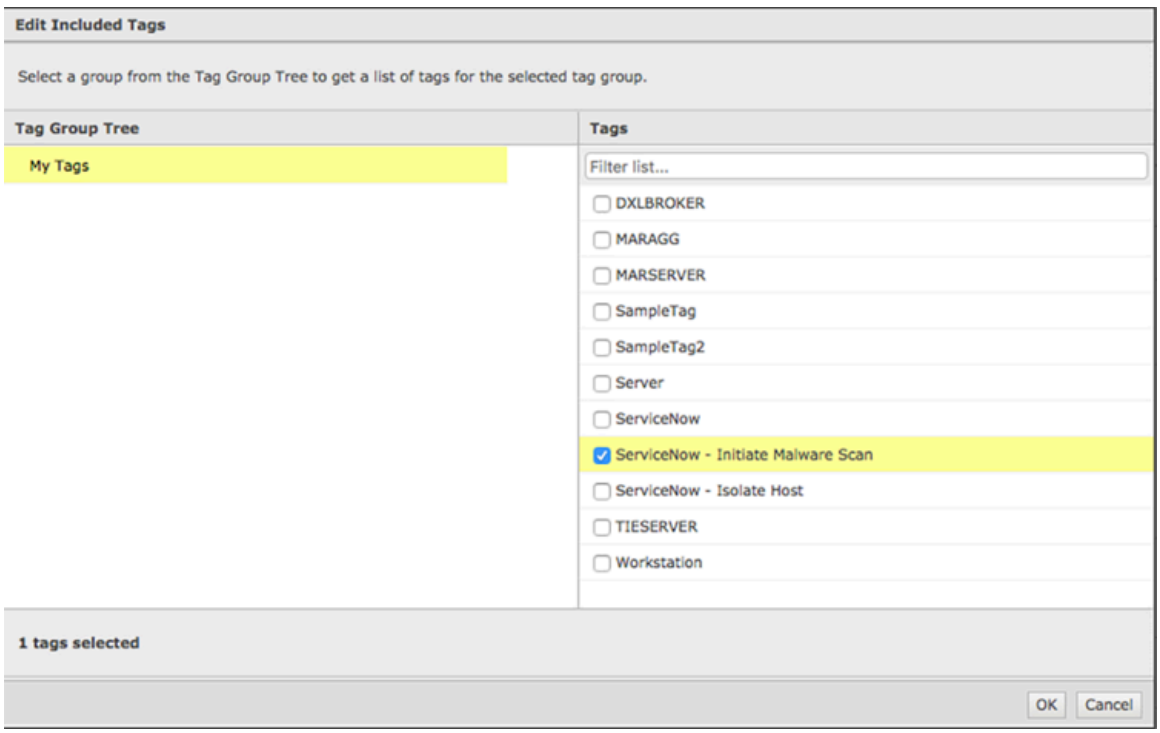

**d.** Klicken Sie im Abschnitt Tags unter dem Optionsfeld und neben Hat eines dieser Tags:auf den **Bearbeitungslink**, um die Kriterien für das Tag zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**e.** Wählen Sie im angezeigten Dialogfeld das Tag Malware-Scan initiieren ServiceNow aus, das Sie in den vorherigen Schritten erstellt haben, und klicken Sie auf **OK**.



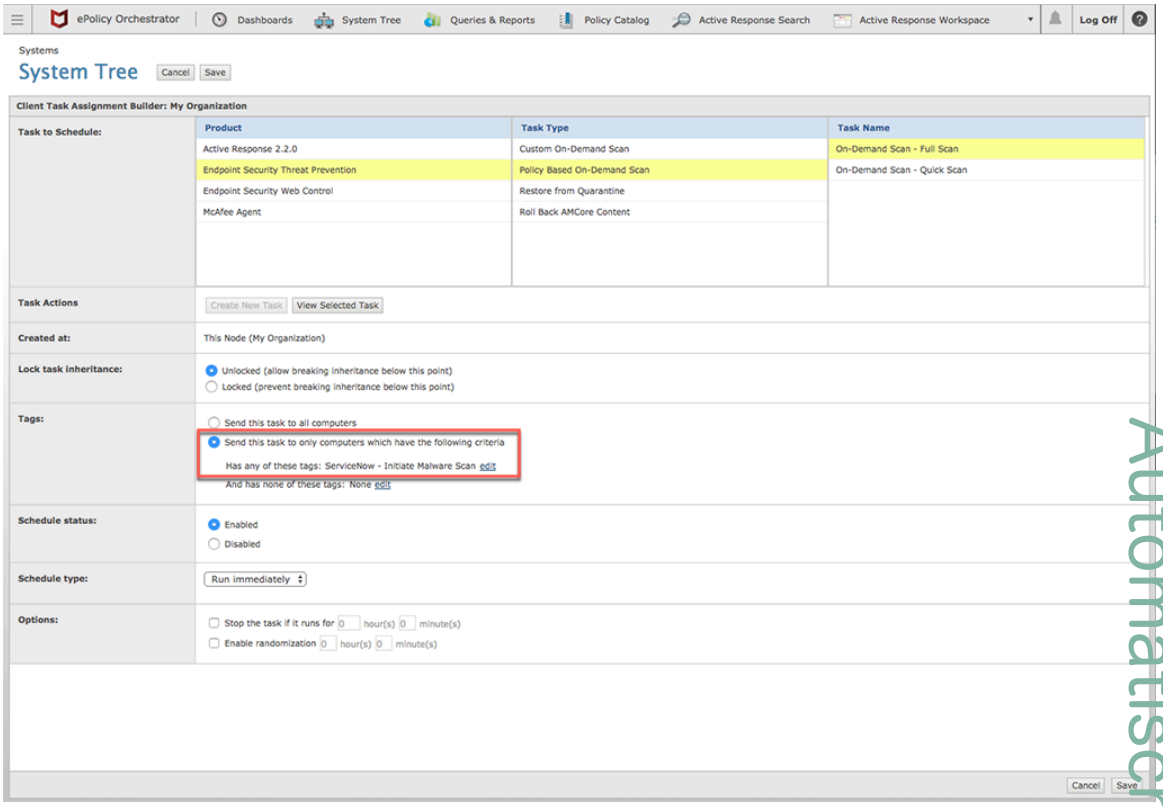

Das von Ihnen erstellte Tag „ServiceNow-Malware-Scan initiieren“ wird der Aktion „Scan bei Bedarf“ zugewiesen.

**f.** Klicken Sie auf **OK**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

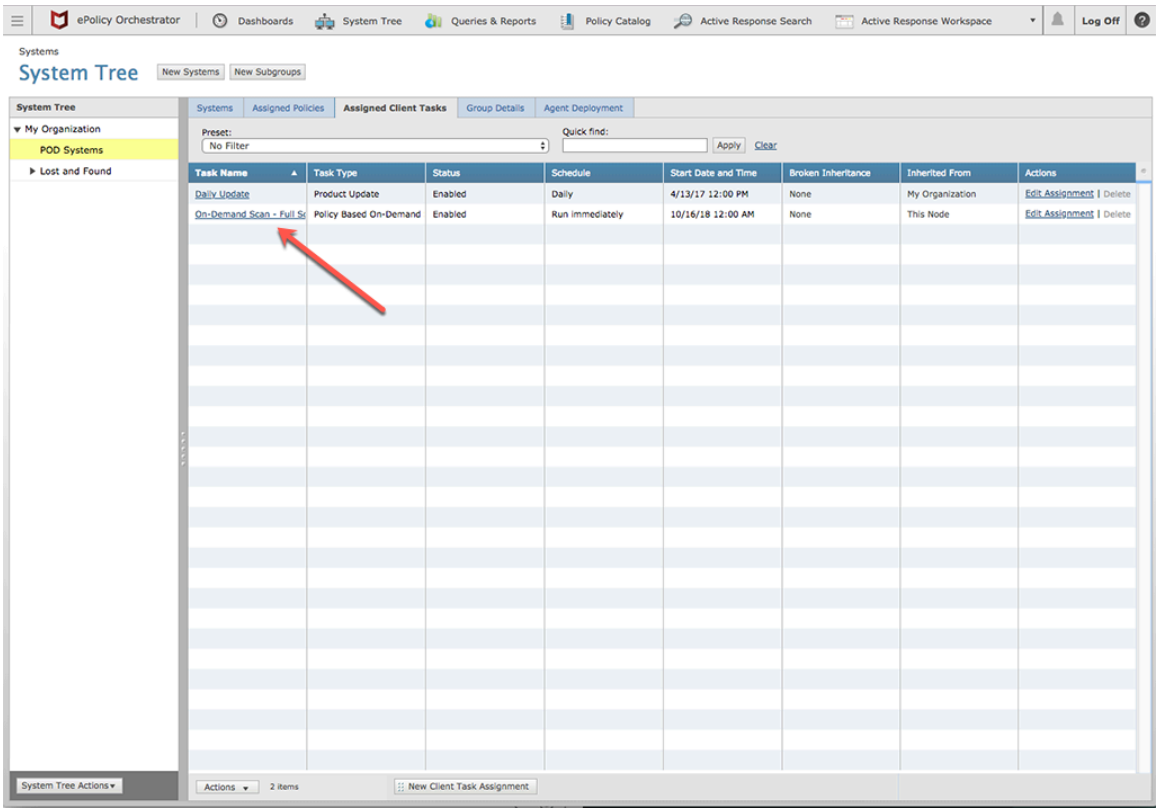
Im Abschnitt Tags wird unter dem Optionsfeld und neben Hat eines dieser Tags:das Tag Malware-Scan initiieren angezeigt.




**g.** Klicken Sie auf **Speichern**.
Auf der Seite „Systemstruktur“ wird die Aufgabe in der Liste „Zugewiesene Client-Aufgaben“ (Registerkarte) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**h.** Wenn Sie der Aktion Host isolieren keine Aktion zugewiesen haben, wiederholen Sie die vorherigen Schritte, um sie zuzuweisen.

Sie haben das Erweiterungs-Plugin erfolgreich installiert, Sicherheits-Tags erstellt und Ihren Tags Aufgaben zugewiesen. Sie haben das Setup für die -Integration in Ihrer McAfee ePO -Konsole abgeschlossen. Der nächste Schritt besteht in der Konfiguration eines Servers in Ihrer Now Platform -Instanz.

## Installieren Sie die Anwendung, und konfigurieren Sie einen Server für die McAfee ePO -Integration

Bevor Sie die Workflows für die Integration aufrufen, installieren und konfigurieren Sie die Anwendung McAfee ePO aus ServiceNow Store in Ihrer Instanz von Now Platform. Die Konfiguration ist erforderlich, um eine Verbindung zur Konsole McAfee ePO herzustellen.

### Vorbereitungen

Erforderliche Rolle: Now Platform Administrator (admin)

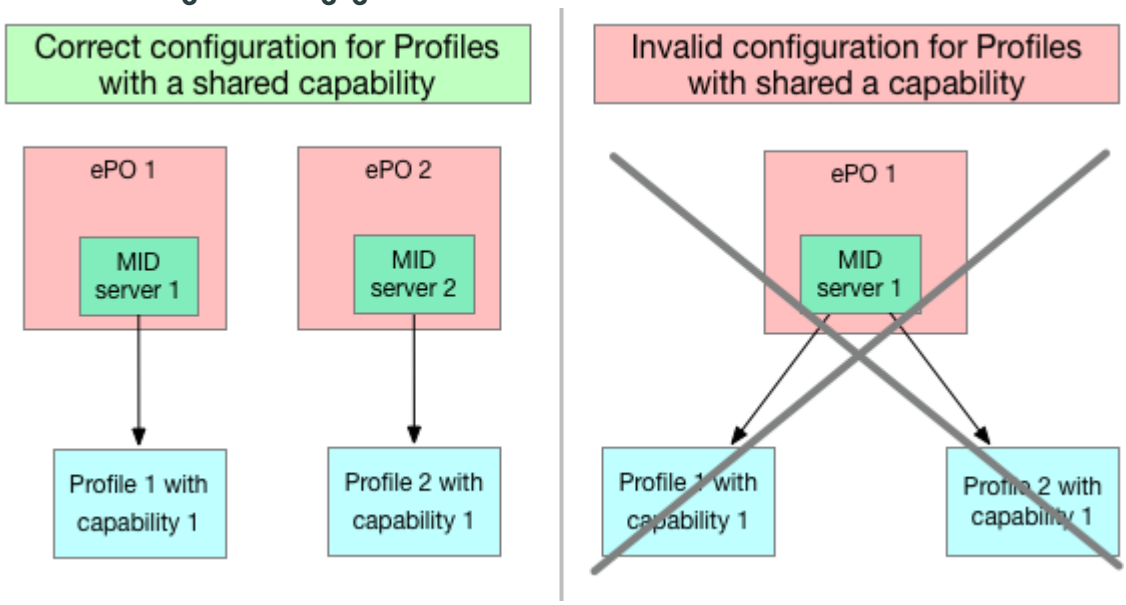
### Warum und wann dieser Vorgang ausgeführt wird

Die Integration unterstützt mehrere Server. Um jedoch Konflikte in Profilen zu vermeiden, die dieselben Auslösebedingungen aufweisen, können Sie eine McAfee ePO -Fähigkeit nicht mit mehreren Profilen teilen, die denselben McAfee ePO -Server verwenden. Wie in der folgenden Abbildung gezeigt, können Sie beispielsweise die Fähigkeit 1 in mehr als einem Profil haben, solange jeder McAfee ePO -Server einem eindeutigen Profil mit der Fähigkeit 1 zugeordnet ist.



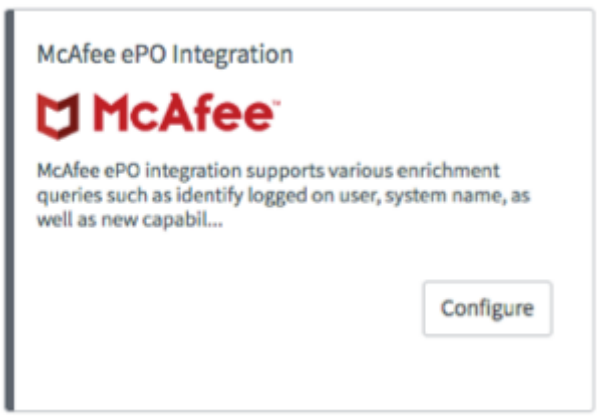
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Einschränkungen für freigegebene McAfee-Profile**




## Prozedur

1. Laden Sie McAfee ePO für Security Operations aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Integrationskachel McAfee ePO für Security Operations, und klicken Sie auf **Konfigurieren**.




4. Füllen Sie die Felder des Formulars aus.

**McAfee ePO-Integrationskonfiguration**

| Feld | Beschreibung |
|---|---|
| Name | Name der Integration, z. B. `demo-1`. |
| ePO-Servername | Name für den McAfee ePO -Server. Wenn Sie nur einen Server verwenden, ist dies beispielsweise `McAfee-Hauptquartier` (McAfee Headquarters). Dieser Name gibt an, wie der Server und die zugehörigen Anmeldeinformationen erkannt werden. |

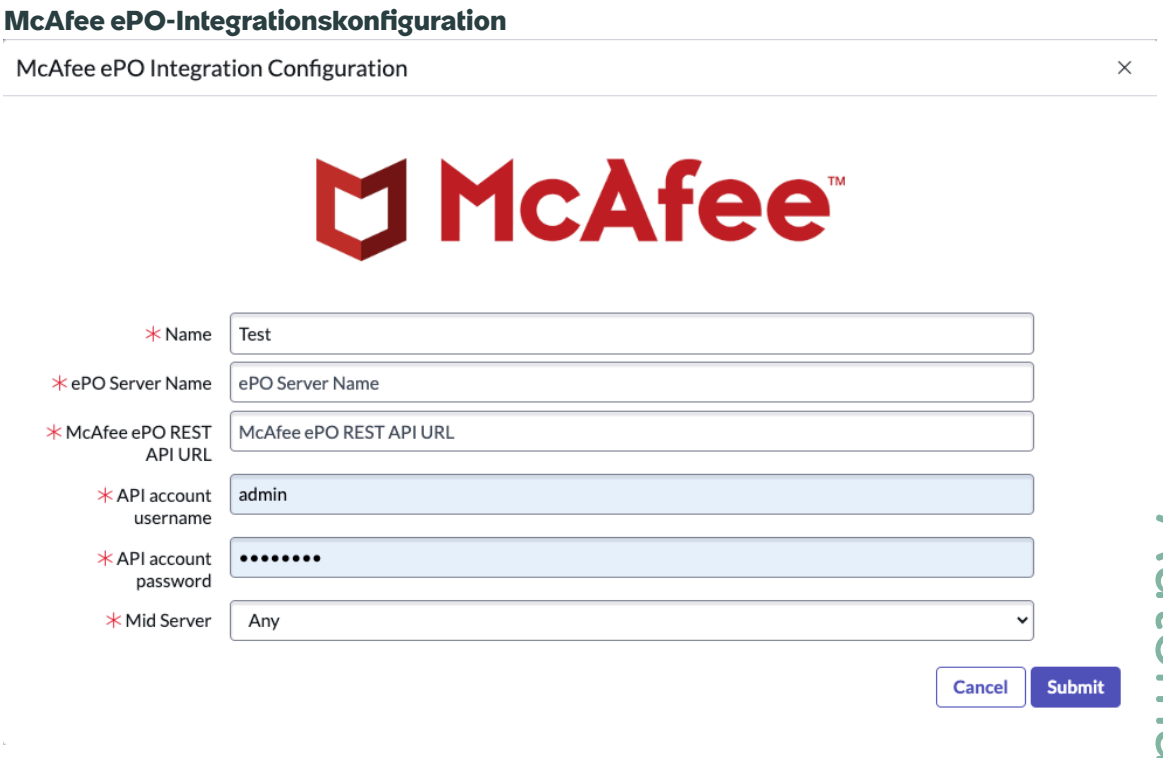
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, geben Sie den Namen für jeden Server ein, und wiederholen Sie den Vorgang. |
| McAfee ePO-REST-API-URL | Basis-URL, die die REST-API McAfee ePO hostet. Geben Sie die URL mit dem Protokoll https:// ein, z. B. https://corp.epo_server:8443. |
| API-Kontobenutzername | Eindeutiger Account-Benutzername, z. B. ServiceNow-API. |
| API-Kontopasswort | Eindeutiges Passwort für das API-Konto. |
| MID-Server | Wählen Sie den Namen des MID Servers aus, den Sie beim Setup Ihrer Now Platform -Instanz konfiguriert haben.<br><br>Sie können einen bestimmten MID Server aus der Liste auswählen oder **Beliebig** auswählen, um die automatische Auswahl eines gültigen MID Servers aus der Liste für diese Integration zu aktivieren.<br><br>**Hinweis:**<br>○ Der während dieser Konfigurationszeit ausgewählte MID Server gilt für die gesamte Integration.<br>○ In dieser Liste werden nur aktive und validierte MID Server angezeigt. Standardmäßig ist der Wert auf **Beliebig**festgelegt.<br><br>Ein Beispielname ist „secops_local_midserver“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **Absenden**.
   Die Liste der McAfee ePO-Konfigurationen wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für einen McAfee ePO -Server erfolgreich abgeschlossen.

**Hinweis:**
Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, wiederholen Sie die Schritte.

### Bearbeiten Sie Sicherheits-Tags in Now Platform für die McAfee ePO -Integration

Bearbeiten Sie im Rahmen des Setups für die Integration die Sicherheits-Tag-Namen, die Sie in Ihrer McAfee ePO -Konsole in Ihrer Now Platform -Instanz erstellt haben. Bearbeiten Sie die Tag-Namen in Ihrer Now Platform -Instanz so, dass sie mit den Namen der Tags in Ihrer McAfee ePO -Konsole übereinstimmen.

#### Vorbereitungen
Erforderliche Rolle: Now Platform Security Incident-Administrator (sn_si.admin)

#### Warum und wann dieser Vorgang ausgeführt wird
Die Sicherheits-Tag-Namen in Ihrer McAfee ePO -Konsole für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ müssen mit den Sicherheits-Tag-Namen in den Datensätzen für diese Funktionen Ihrer Now Platform -Instanz übereinstimmen.

Bevor Sie ein Fähigkeitsprofil zum Ausführen Ihrer -Fähigkeiten erstellen, zeigen Sie die Liste der verfügbaren McAfee ePO -Fähigkeiten an, und bearbeiten Sie die Sicherheits-Tags in Ihrer Now Platform -Instanz, sodass sie mit den Sicherheits-Tag-Namen in Ihrer McAfee ePO -Konsole übereinstimmen.

Weitere Informationen zum Erstellen der Sicherheits-Tag-Namen in der Konsole McAfee ePO finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein..

Automatische Übersetzung

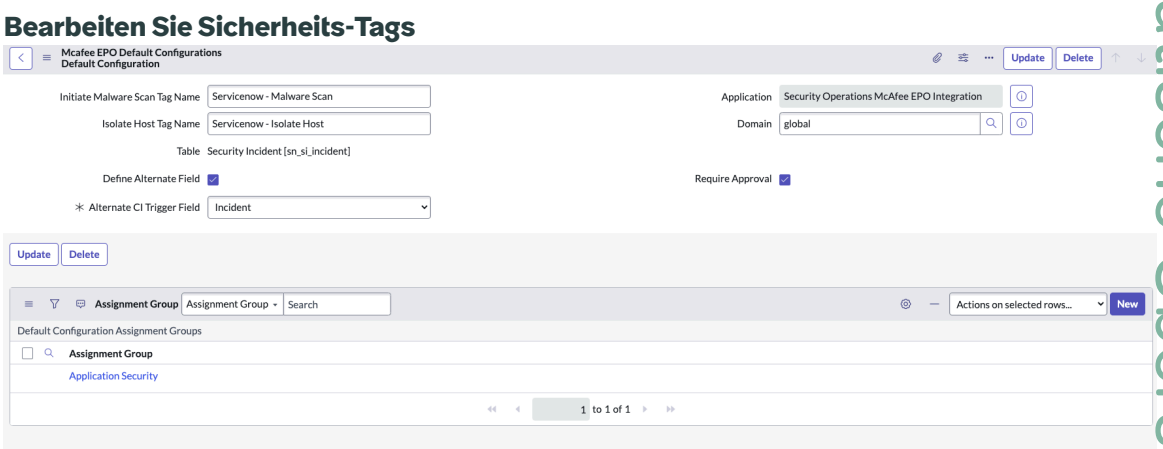
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **McAfee ePO-Integration** > **Standardeinstellungen**.
2. Um den Sicherheits-Tag-Namen der Integration McAfee ePO zu bearbeiten, klicken Sie auf **Standardkonfiguration**.

   **Hinweis:**
   Stellt sicher, dass Sie diese Konfiguration nach der Installation der McAfee ePO -Integration durchführen.

3. Geben Sie im Feld Tag-Namen für „Malware-Scan initiieren“ den Namen des Sicherheits-Tags ein, den Sie in Ihrer McAfee ePO -Konsole für die Aktion „Scan initiieren“ erstellt haben.
   Beispiel: ServiceNow – Malware Scan
4. Geben Sie im Feld Isolate Host Tag Name (Host-Tag-Namen isolieren) den Namen des Sicherheits-Tags ein, den Sie in Ihrer McAfee ePO -Konsole für die Aktion „Host isolieren“ erstellt haben.
   Beispiel: ServiceNow - Isolate Host
5. Wenn Sie das CI-Auslöserfeld bei der Incident-Erstellung nicht verwenden möchten, aktivieren Sie das Kontrollkästchen **Alternatives Feld definieren**.
   Wenn diese Option aktiviert ist, wird die Auswahlliste Alternatives CI-Auslöserfeld angezeigt.




6. Wählen Sie ein alternatives Feld aus der Auswahlliste aus, um nach Ihren CI-Suchkriterien zu suchen.
   In diesem Beispiel gehen Sie als Benutzer mit der Rolle „sn_si.admin“ davon aus, dass das CI-Feld im Security Incident bei der Incident-Erstellung nicht ausgefüllt wird. Alternativ gehen Sie davon aus, dass CI-Informationen für einen FQDN, einen Hostnamen oder eine IP-Adresse im Feld Identifiziertes CI des Security Incident ausgefüllt werden, und wählen das Feld Identifiziertes CI als Alternative aus. Für dieses Beispiel wird das identifizierte CI ausgewählt, Sie können jedoch ein beliebiges Feld im Security Incident für das alternative CI verwenden.
7. Wählen Sie im Feld Domäne mithilfe der Suchoption eine Domäne oder Gruppe für diese Konfiguration aus.
   Beispiel: global.
8. Aktivieren Sie im Feld Genehmigung erforderlich das Kontrollkästchen **Genehmigung** erforderlich, wenn Sie die Isolierungsfunktionen Host isolieren und Entfernen verwenden.

   **Hinweis:**
   Die Funktionen „Malware-Scan initiieren“, „Bedrohungsereignisse auflisten“ und „Systemdetails abrufen“ müssen nicht genehmigt werden.

9. Klicken Sie auf **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der EPO-Tag-Name wird aktualisiert und in der Liste der McAfee ePO-Standardkonfigurationen angezeigt. Der Sicherheits-Tag-Name für die Malware-Scan-Aktion in Ihrer Instanz Now Platform stimmt mit dem Namen für den Scan in Ihrer McAfee ePO -Konsole überein.

Sie haben die EPO-Tag-Namen für den Malware-Scan und die Fähigkeiten zum Isolieren des Hosts in Ihrer Now Platform -Instanz erfolgreich bearbeitet. Der nächste Schritt besteht darin, ein Profil für Ihre Fähigkeiten zu erstellen.

**Zugehörige Informationen**

McAfee-Produktdokumentation

### Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für die Integration von McAfee ePO für Security Operations, die Anforderungen für die Isolierung von Hostcomputern und deren Wiederherstellung im Netzwerk genehmigen kann.

### Vorbereitungen

Sie können die Genehmigungsberechtigung nicht einer Gruppe neu zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

**Hinweis:**
Die Genehmigungsoption in Profile für die McAfee ePO -Integration konfigurieren wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.

Erforderliche Rolle: Now Platform® Security Incident-Administrator (sn_si.admin)

### Warum und wann dieser Vorgang ausgeführt wird

Vom Security Incident-Analysten übermittelte Genehmigungsanforderungen zum Isolieren von Hostcomputern und zum Entfernen der Isolierung werden standardmäßig dem Benutzer mit der Rolle sn_si.admin zugewiesen. Als Benutzer mit dieser Rolle können Sie diese Genehmigungsberechtigung während des Konfigurationsschritts für ein Profil neu zuweisen. Bevor Sie einer Genehmigungsgruppe eine Berechtigung zuweisen können, muss eine Genehmigungsgruppe in der Gruppenliste in Ihrer Now Platform-Instanz verfügbar sein.

### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.
2. Klicken Sie in der Gruppenliste auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsgruppe“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppe, die angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird, z. B. Genehmiger McAfee-Hostisolierung. |
| Gruppen-E-Mail | Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Kontaktpunkts, z. B. Gruppenmanager, McAfeeapproval@servicenow.com |
| Manager | Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Übergeordnet | (Optional) Andere Gruppe, der diese Gruppe angehört, wenn diese Gruppe ein übergeordnetes Element hat. |
| Beschreibung | Zusätzliche Informationen zu dieser Gruppe. |
| Mitglieder einbeziehen | Option zum Einbeziehen von Mitgliedern in diese Gruppe. |
| Standard-Beauftragter | Option zum Auswählen eines Benutzers als Standardbeauftragter für diese Gruppe. Verwenden Sie die Option Suche, um die Liste der Benutzer zu öffnen. |
| Rollen | Option zum Auswählen der Rollen für diese Gruppe. Verwenden Sie die Option Hinzufügen und Entfernen, um Rollen hinzuzufügen und zu entfernen. |
| Typ | Option zum Auswählen einer Kategorie für diese Gruppe. Verwenden Sie die Option Suche, um die Liste der Gruppentypen zu öffnen. |
| Lieferanten | Option zum Auswählen eines Lieferanten für diese Gruppe. Verwenden Sie die Option Suche, um die Liste der Lieferanten zu öffnen. |

4. Klicken Sie auf **Absenden**.
   Die neue Gruppe wird in der Gruppenliste angezeigt.

   Diese Gruppe ist für die Verarbeitung von Anforderungen verfügbar, wenn Sie während der Konfiguration dieses Profils die Option **Genehmigung** erforderlich aktivieren.

   Um von Benutzern mit der Rolle „sn_si.analyst“ übermittelte Anforderungen zu überwachen und zu verarbeiten, navigiert jedes Mitglied der Genehmigungsgruppe zur Registerkarte **Meine Genehmigungen** in Now Platform.

### McAfee ePO Integrationsfähigkeitsprofile

Als Benutzer mit der Rolle „Security Incident-Administrator“ (sn_si.admin) erstellen Sie Profile für die Fähigkeiten McAfee ePO in Ihrer Instanz Now Platform®. Sie gruppieren Abfragen oder Aktionen in Profilen und bestimmen, welche McAfee ePO -Fähigkeiten Sie ausführen möchten, wenn ein neuer Security Incident erstellt wird.

## Fähigkeitsprofile

Sie erstellen Profile™, damit Sie McAfee ePO -Fähigkeiten gruppieren und die Einstellungen für diese Fähigkeiten in Ihrer Now Platform® -Instanz konfigurieren können. Sie haben die Flexibilität, mehrere Profile für diese Fähigkeiten zu erstellen, wodurch Sie bestimmen können, welche Aktionen oder Abfragen aufgerufen werden, wenn ein Security Incident Response (SIR) Incident erstellt wird. Je nach Anforderungen Ihrer Organisation können Sie ein einzelnes Profil erstellen, das beispielsweise Abfragen nach Systemdetails ausführt, Malware-Scans initiiert und Hostcomputer isoliert, oder Sie können mehrere Profile mit jeweils einer eigenen McAfee ePO -Fähigkeit erstellen .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Profiltypen und erforderliche McAfee ePO Fähigkeiten

| Primärer Zweck Ihres Profils | Richten Sie Anforderungen ein | Für diesen Profiltyp erforderliche McAfee ePO-Fähigkeiten |
|---|---|---|
| Erfasst Systemdetails | Keine | **Hostdetails abrufen** |
| Isolieren Sie einen Host | Vergewissern Sie sich bei Ihrem McAfee ePO -Administrator, dass Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in Ihrer McAfee ePO -Konsole erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.. | **Host isolieren** |
| Scannen und suchen Sie nach Bedrohungen auf Ihrem Host | Vergewissern Sie sich bei Ihrem McAfee ePO -Administrator, dass Sie die Sicherheits-Tags für die Aktion „Malware-Scan initiieren“ in Ihrer McAfee ePO -Konsole erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.. | **Initiieren Sie einen Malware-Scan**<br>**Hinweis:** Im Rahmen des Malware-Scans McAfee ePO wird automatisch die Funktion „Bedrohungsereignisse auflisten“ aufgerufen. Sie müssen dem Profil mit der Malware-Scan-Fähigkeit jedoch nicht die Funktion „Bedrohungsereignisse auflisten“ hinzufügen. Die Ergebnisse des Malware-Scans werden auf der Registerkarte Details zum Bedrohungsereignis im Security Incident angezeigt. |
| Entfernen Sie die Isolierung für einen Host | Vergewissern Sie sich bei Ihrem McAfee ePO -Administrator, dass Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in Ihrer McAfee ePO -Konsole erstellt haben. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein.. | **Isolation entfernen** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Profiltypen und erforderliche McAfee ePO Fähigkeiten (Fortsetzung)**

| Primärer Zweck Ihres Profils | Richten Sie Anforderungen ein | Für diesen Profiltyp erforderliche McAfee ePO-Fähigkeiten |
|---|---|---|
| Sammeln von Daten zur Bedrohungsanreicherung | Keine | **Bedrohungsereignisse auflisten** |

## Erstellen Sie ein Fähigkeitsprofil für die McAfee ePO -Integration

Erstellen Sie ein Profil, und wählen Sie die Fähigkeiten McAfee ePO aus, die das Profil ausführen soll.

### Vorbereitungen

Erforderliche Rolle: Now Platform® Security Incident-Administrator (sn_si.admin)

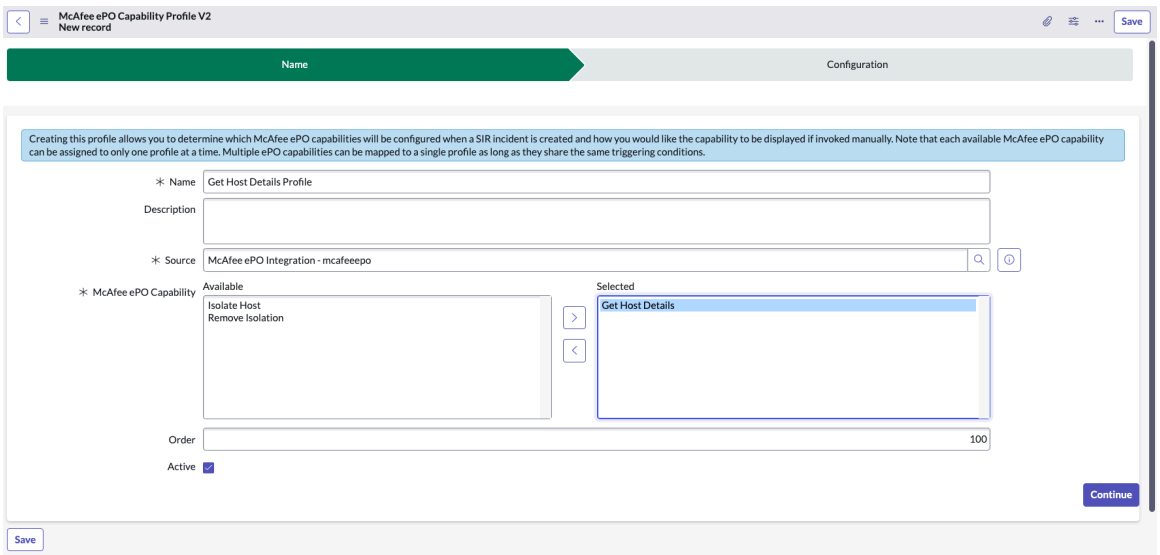
### Warum und wann dieser Vorgang ausgeführt wird

Für diesen Konfigurationsschritt erstellen Sie ein Profil für die Fähigkeiten McAfee ePO. Berücksichtigen Sie beim Erstellen von Profilen die Absicht des Profils, bevor Sie McAfee ePO -Fähigkeiten hinzufügen. Beachten Sie beim Erstellen von Profilen die folgende Tabelle.

In der folgenden Tabelle sind die Fähigkeiten aufgelistet, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll. Erstellen Sie ein einzelnes Profil, das Abfragen nach Hostdetails ausführt, Malware-Scans initiiert, die Isolierung entfernt und Hostcomputer isoliert, oder erstellen Sie mehrere Profile mit jeweils einer eigenen Fähigkeit.

### Prozedur

1. Navigieren zu **McAfee ePO-Integration** > **McAfee ePO-Fähigkeitsprofile**.
   Die Liste McAfee ePO Fähigkeitsprofile wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.




4. Klicken Sie auf **Fortfahren**, um das Profil zu speichern und zu validieren.
   Wenn die Validierung erfolgreich ist, wird die Seite neu geladen, und das **Konfigurationsformular** wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Nächste Maßnahme**
Der nächste Schritt besteht in der Konfiguration Ihres Profils. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie sich die Konzepte zum Konfigurieren von Profilen und Auslösebedingungen ansehen. Weitere Informationen finden Sie unter Richten Sie die McAfee ePO -Konsole für die Integration mit Security Incident Response (SIR) ein. und Definieren von Auslöserbedingungen mit einem Konfigurationselement (CI)-Feld für ein McAfee ePO -Profil.

### Definieren von Auslöserbedingungen mit einem Konfigurationselement (CI)-Feld für ein McAfee ePO -Profil

Nachdem Sie ein Profil erstellt und die McAfee ePO -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen des Profils so, dass es nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind.

Sie haben die Flexibilität, diese Auslösebedingungen festzulegen, sodass das Profil automatisch basierend auf den Standardfeldwerten ausgeführt wird, die mit einem Now Platform® Security Incident Response Security Incident abgeglichen werden. Alternativ können Sie ein Profil so einrichten, dass nach Übereinstimmungen mit Feldwerten gesucht wird, die Sie im Security Incident ausdrücklich identifiziert haben.

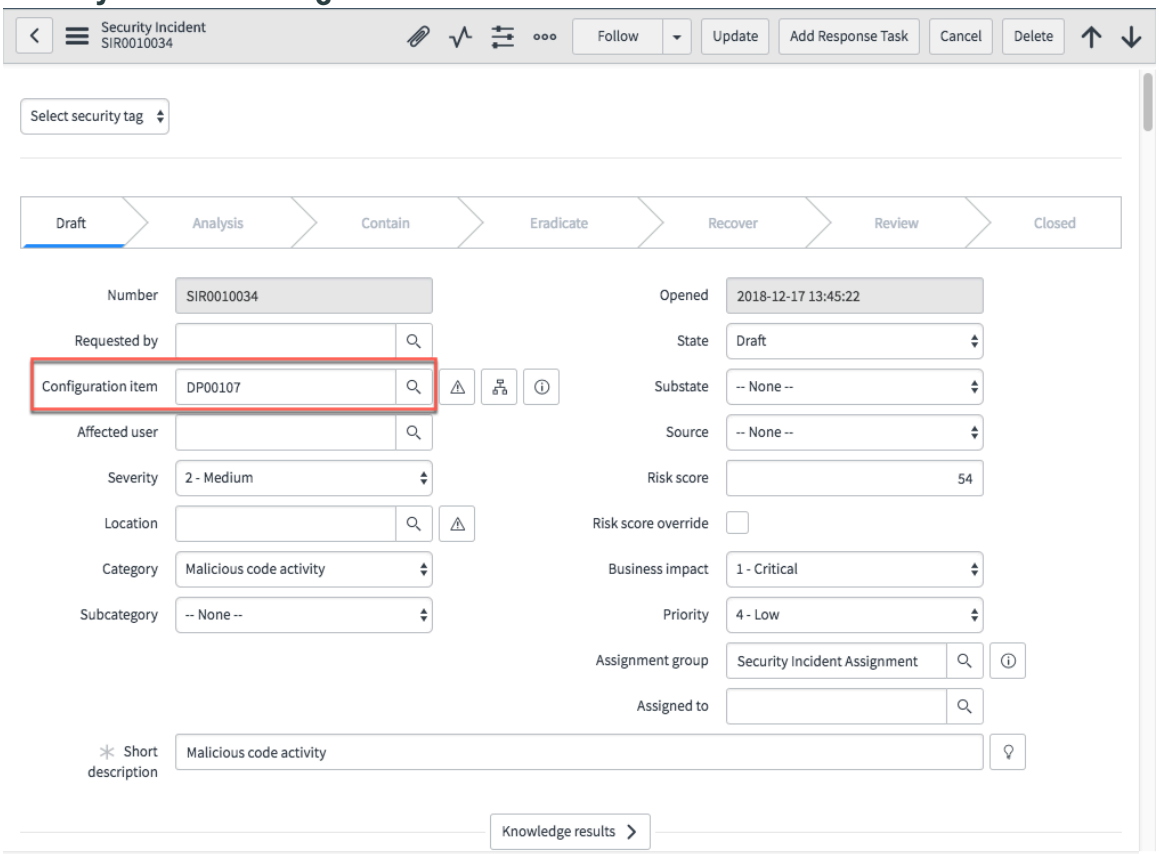
Einer der Schlüssel zur Funktionalität der Integration und zur Funktionsweise eines Profils ist das Feld Configuration Item (CI) im Security Incident Now Platform® Security Incident Response (SIR). Der Wert dieses Felds ist der Prinzipalwert für einen Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in der Datenbank Now Platform® gespeicherten Informationen abzugleichen. Wenn ein SIR Security Incident durch ein Sicherheitsereignis erstellt wird und ein Profil aktiviert ist, werden Ihre Assets auf einen übereinstimmenden Wert für einen vollständig qualifizierten Domänennamen (FQDN), einen Hostnamen oder eine IP-Adresse basierend auf dem Wert von gescannt Feld Konfigurationselement.

Im Idealfall wird ein übereinstimmender Wert in der Datenbank gefunden, und Daten können in der Konsole McAfee ePO für das übereinstimmende Asset gesammelt, in Ihre Instanz Now Platform® abgerufen und in den zugehörigen Listen eines Security Incident angezeigt werden. Die folgende Abbildung zeigt ein Beispiel für das mit einem Hostnamen ausgefüllte Feld Configuration Item in einem SIR Security Incident.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident – Konfigurationselement**




Wenn das Feld Configuration Item (CI) im Security Incident nicht ausgefüllt ist oder keine Übereinstimmung für einen FQDN, einen Hostnamen oder eine IP-Adresse gefunden werden kann, die der Datenbank entspricht, können Sie ein alternatives Feld für die Sicherheitsvorkehrung auswählen Incident, um übereinstimmende CI-Ergänzungsdaten anzuzeigen, die beim Scan Ihrer Assets gefunden wurden.

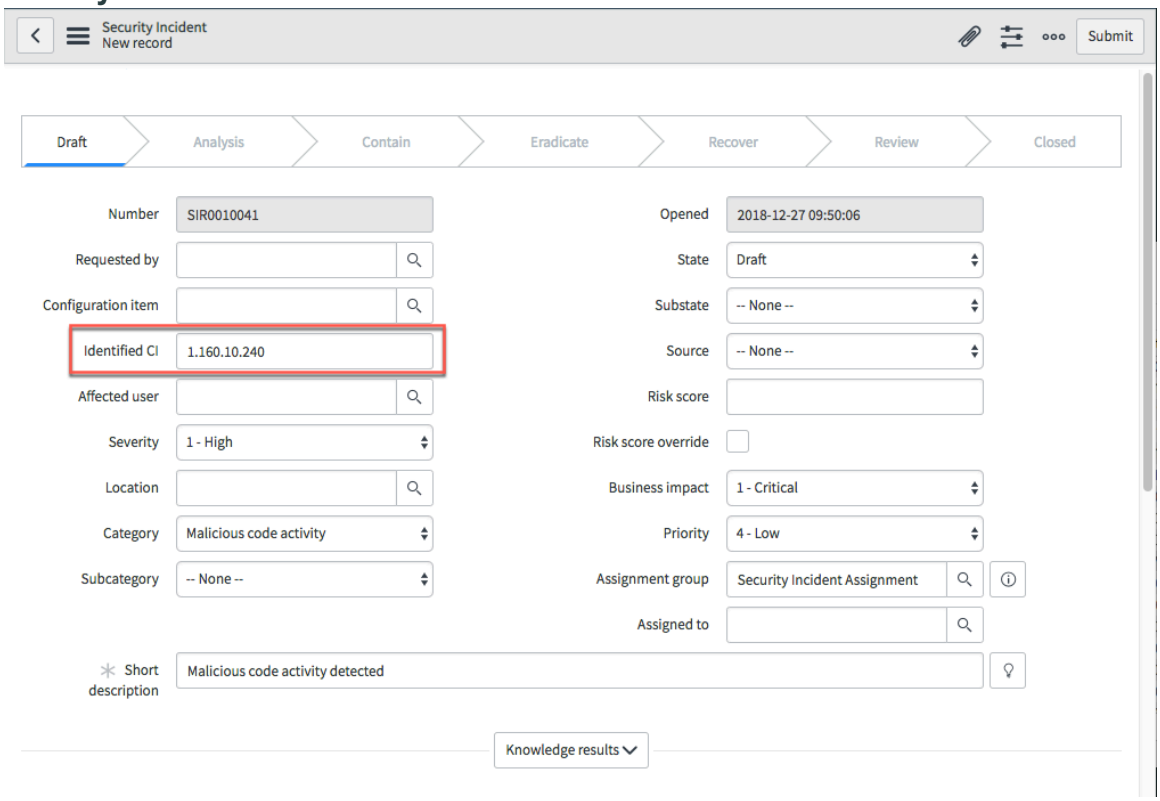
Während des Konfigurationsschritts der Profileinrichtung können Sie ein alternatives CI-Auslöserfeld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass die CI-Ergänzungsdaten aus der Suche McAfee ePO für den zugeordneten Security Incident ausgefüllt werden. Sie können ein beliebiges Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich benutzerdefinierter Felder, die Sie erstellen. Wenn Sie dieses alternative CI-Feld als Sicherung auswählen, stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung nicht für den zugehörigen Security Incident ausgefüllt wird.

Beispiel: Als SOC-Analyst (Security Operations Center) erstellen Sie ein benutzerdefiniertes Feld für einen Security Incident mit der Bezeichnung IP-Adresse für meinen Security Incident. Wenn Sie nicht der Meinung sind, dass der Wert dieses benutzerdefinierten Felds bei der Incident-Erstellung im Feld Configuration Item des Security Incident angezeigt wird, können Sie das Profil so einrichten, dass es nach dieser IP-Adresse sucht. Bei Übereinstimmung wird die IP-Adresse des Security Incident im Feld Ihrer Wahl angezeigt. In der folgenden Abbildung wird das Feld Identifiziertes CI als alternatives Feld für die IP-Adresse für dieses Beispiel ausgewählt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident – Identifiziertes CI**

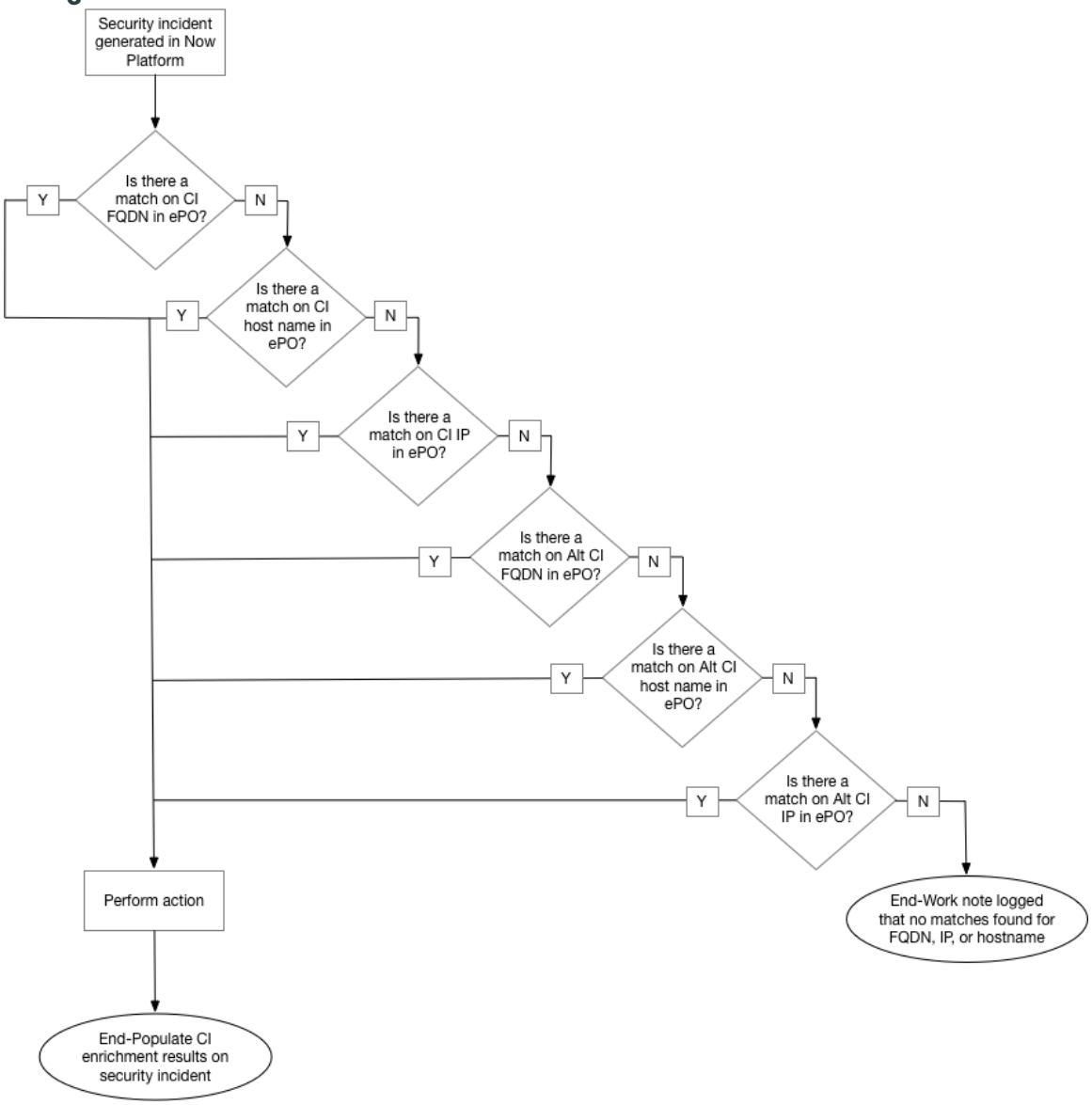



Die folgende Abbildung zeigt, wie bei der ersten Suche des Workflows nach Übereinstimmungen für Konfigurationselemente gescannt wird. Wenn das Feld Alternativer CI-Auslöser aktiviert ist, wird bei der zweiten Suche nach Übereinstimmungen für alternative Werte gescannt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurationselemente-Workflow




Wenn für das CI-Feld oder das alternative CI-Feld keine übereinstimmenden IDs gefunden werden, wird eine Arbeitsnotiz protokolliert und eine Meldung zum Security Incident angezeigt. Wenn keine Übereinstimmungen gefunden werden, werden keine Ergänzungsdaten für die Security Incidents im Zusammenhang mit dem Event ausgefüllt.

Sie aktivieren das alternative CI-Auslöserfeld und wählen das Feld aus, in dem die übereinstimmende ID während des Konfigurationsschritts für ein Profil angezeigt werden soll. Dieser Schritt zum Aktivieren des alternativen CI-Felds wird zusammen mit den anderen Profilkonfigurationsanforderungen in Profile für die McAfee ePO -Integration konfigurierenbeschrieben.

### Profile für die McAfee ePO -Integration konfigurieren

Nachdem Sie ein Profil erstellt und die McAfee ePO -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den von Ihnen definierten Bedingungen aufgerufen wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Profil konfigurieren

In diesem Schritt konfigurieren Sie ein Fähigkeitsprofil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Sie definieren, welche Bedingungen für Security Incidents automatisch die für das Profil ausgewählten McAfee ePO -Fähigkeiten auslösen. Sie haben auch die Möglichkeit, ein alternatives Eingabefeld für das Feld Configuration Item (CI) auszuwählen und Filterbedingungen so festzulegen, dass nur die Security Incidents, die sich auf Ihr auslösendes Event beziehen, das Profil automatisch starten. Der Konfigurationsschritt umfasst die folgenden Einstellungen im Konfigurationsformular für das Profil.

## Alternatives CI-Auslöserfeld (Configuration Item).

In Fällen, in denen das Feld Konfigurationselement (CI) im Security Incident Now Platform® Security Incident Response (SIR) nicht mit einem Wert ausgefüllt ist oder keine Übereinstimmung in der Datenbank gefunden werden kann, können Sie ein alternatives Feld im Security Incident auswählen, um ein beliebiges anzuzeigen übereinstimmende CI-Ergänzungsdaten, die beim Scan Ihrer Assets gefunden wurden. Weitere Informationen zu den Feldern Konfigurationselement und Alternatives Konfigurationselement in einem Security Incident finden Sie unter Definieren von Auslöserbedingungen mit einem Konfigurationselement (CI)-Feld für ein McAfee ePO -Profil.

## Sicherheits-Tags

Damit Sie den Status isolierter Hostcomputer und die Initiierung von Malware-Scans nachverfolgen können, ist eine optionale Tagging-Funktion verfügbar. Standardmäßig ist diese Option im Konfigurationsformular für Profile deaktiviert. Wenn diese Option während des Konfigurationsschritts aktiviert ist, werden Sicherheits-Tag-Namen im Konfigurationsformular angezeigt. Dies sind die Namen der Tags, die für zugehörige Security Incidents angezeigt werden. Diese Tags informieren Sie, wenn eine Hostisolierungsaktion erfolgreich initiiert und genehmigt wird. Nachdem ein Host erfolgreich an das Netzwerk zurückgegeben wurde, wird das Sicherheits-Tag automatisch aus dem Security Incident entfernt. Bei Malware-Scans wird ein Tag für den zugehörigen Security Incident angezeigt, wenn ein Scan geplant ist. Nach Abschluss des Scans wird das geplante Tag automatisch durch ein Tag ersetzt, das angibt, dass der Scan erfolgreich abgeschlossen wurde.

## Automatischer Auslöser basierend auf Incident

Wenn die Option Auto-trigger based on incident (Automatischer Auslöser basierend auf Incident) aktiviert ist, ist der Generator für Filterbedingungen verfügbar, und Sie müssen Filterbedingungen festlegen, die angeben, wann das Profil automatisch ausgeführt wird. Ein gängiger Filter ist „Kategorie ist schädliche Codeaktivität“™ und „Geschäftsauswirkung“ ist 1 – Kritisch™. Mit diesen Filtern wird das Profil nur von Security Incidents gestartet, die sich auf böswilligen Code beziehen und kritische Auswirkungen auf das Geschäft haben. Durch die Verwendung der Option Auto-trigger (Automatischer Auslöser) kann die Anzahl der Security Incidents reduziert werden, die das Profil automatisch aufrufen.

## Genehmigungen

Wenn Ihre Organisation eine zusätzliche Kontrolle über Aktionen wie das Isolieren von Hostcomputern und das Initiieren von Malware-Scans wünscht, können Sie die Option Genehmigung erforderlich während des Konfigurationsschritts für ein Profil aktivieren.

Wenn beispielsweise sowohl die Genehmigungs- als auch die Tagging-Funktion für ein Profil aktiviert sind, wird der zugehörige Security Incident automatisch getaggt,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nachdem eine Anforderung zum Isolieren oder Zurückgeben eines Hostcomputers an das Netzwerk zur Genehmigung übermittelt wurde. Anforderungen werden standardmäßig zur Genehmigung an einen Benutzer mit der Rolle sn_si.admin gesendet. Diese Genehmigung kann jedoch einer anderen Person oder Genehmigungsgruppe zugewiesen werden, um den Anforderungen Ihrer Organisation zu entsprechen. Genehmiger verarbeiten Anforderungen in **Meine Genehmigungen** in ihren Now Platform® -Instanzen. Sicherheits-Tags werden für zugehörige Security Incidents angezeigt. Alle Workflow-Aktivitäten werden auch in Arbeitsnotizen protokolliert, um einen Audit-Pfad zu erstellen.

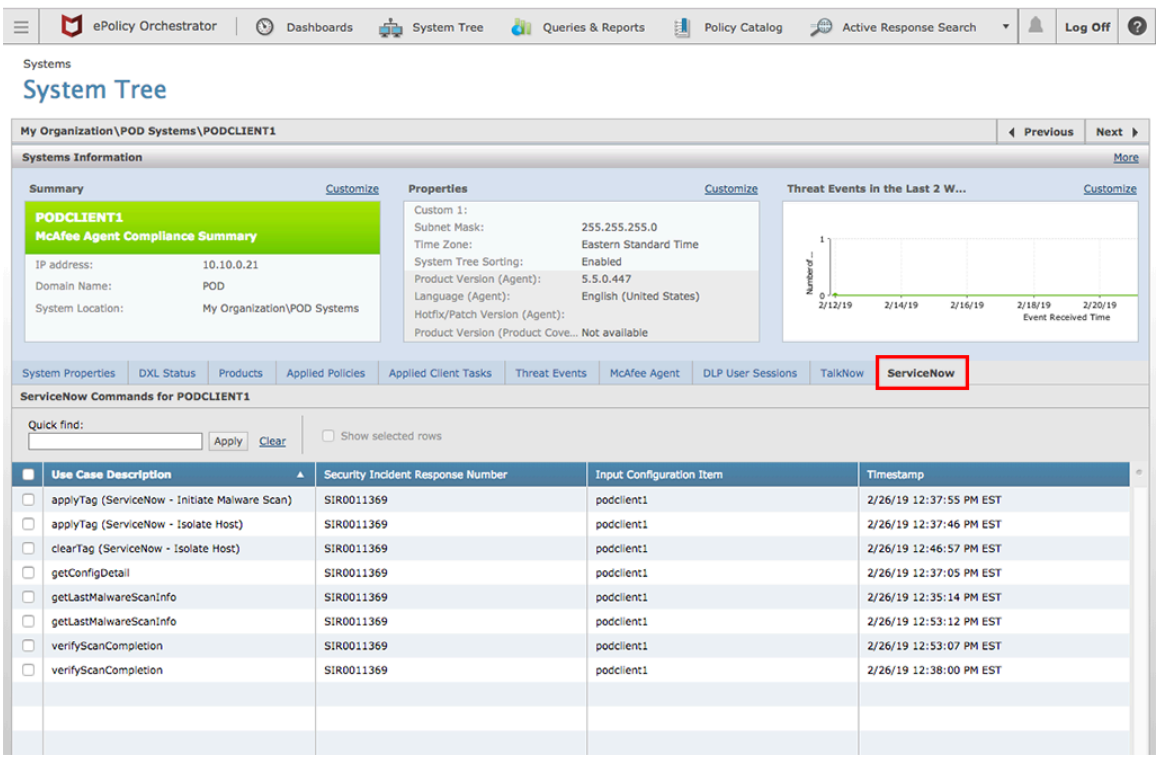
## ServiceNow Audit-Protokoll in der McAfee ePO -Konsole

In Version 5.10.0 von McAfee ePOwird die Registerkarte ServiceNow mit einem Protokoll der Befehle angezeigt, die von Ihrer Instanz Now Platform® initiiert werden. Nachdem eine Aktion oder Abfrage aus einem Profil in Ihrer Instanz Now Platform® auf einem Hostcomputer (Endpunkt) in der Konsole McAfee ePO aufgerufen wurde, wird in der Konsole McAfee ePO ] ein Audit-Protokoll mit Befehlen von ServiceNow erstellt. Dieses Protokoll wird in der Systemstruktur in der Konsole McAfee ePO angezeigt und hilft Ihnen, die Zeiten der Befehle zu überprüfen, die an bestimmte Endpunkte gesendet werden. Führen Sie die folgenden Schritte aus, um protokollierte ServiceNow -Ereignisse auf bestimmten Computern in einer McAfee ePO -Konsole anzuzeigen.

1. Navigieren Sie in der Konsole McAfee ePO zur Systemstruktur, und suchen Sie die Registerkarte ServiceNow.
2. Klicken Sie auf die Registerkarte, um eine Liste der Hostcomputer zu öffnen.
3. Klicken Sie in der Spalte Name auf einen Hostnamen, um das Audit-Protokoll zu öffnen.

In der folgenden Abbildung wird ein Beispiel für ein Protokoll für einen Host (PODCLIENT1) angezeigt.

**PODClient**






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die von den Profilen in Ihrer Instanz Now Platform® initiierten Events werden aufgezeichnet und im Protokoll angezeigt. Überprüfen Sie den Status des Hostcomputers, um sicherzustellen, dass die im Protokoll aufgeführten Events auf dem Host erfolgreich abgeschlossen wurden.

## Beispielprofile

Die folgenden Themen enthalten Beispiele für die Konfiguration von Profilen und das Testen von Security Incidents. Diese Beispiele enthalten Profile für alle McAfee ePO -Fähigkeiten, die für diese Integration verfügbar sind.

### Konfigurieren Sie Profile und Security Incidents für Systemergänzungsabfragen für die McAfee ePO -Integration

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

#### Vorbereitungen

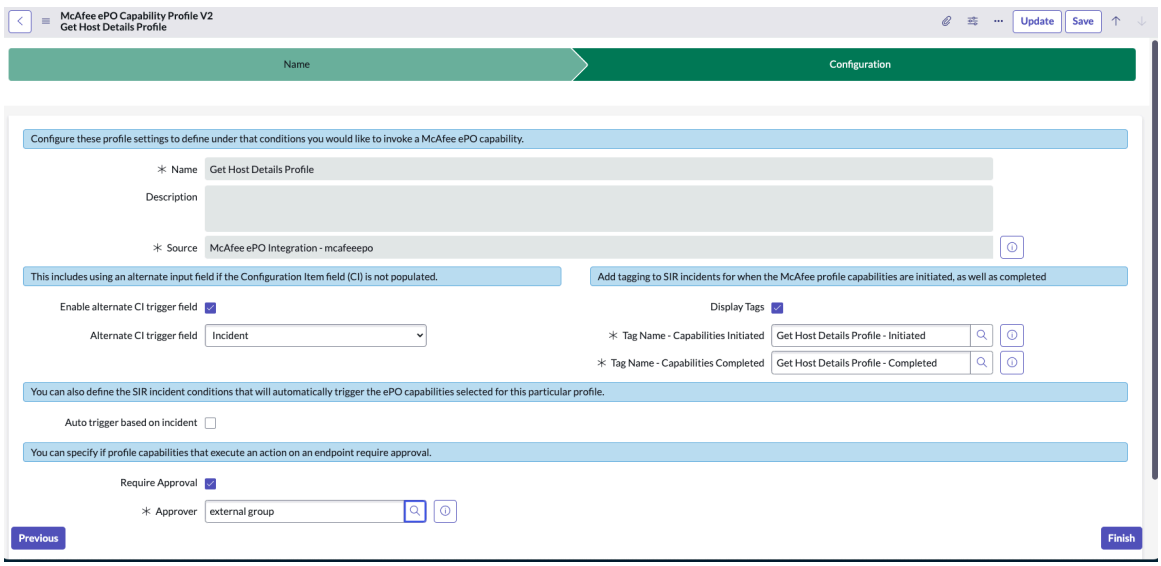
Erforderliche Rolle: Now Platform® Security Incident-Administrator (sn_si.admin)

#### Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die automatisch die Fähigkeiten McAfee ePO auslösen, die Sie für das Profil ausgewählt haben. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld können Sie Filterbedingungen festlegen, sodass nur die Security Incidents, die sich auf Ihr auslösendes Event beziehen, das Profil automatisch auslösen.

#### Prozedur

1. Wenn die Konfigurationsseite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Konfiguration**.
2. Füllen Sie die Felder des Formulars aus




3. Führen Sie die folgenden Schritte aus, um die Option für das alternative CI-Feld zu aktivieren und die Filterbedingungen festzulegen, die dieses Profil automatisch aufrufen.

   a. Aktivieren Sie das Kontrollkästchen **Alternatives CI-Auslöserfeld** aktivieren.
   Das Feld Alternativer CI-Auslöser wird angezeigt. In diesem Beispiel gehen Sie als Benutzer mit der Rolle „sn_si.admin“ davon aus, dass das CI-Feld im Security Incident bei der Incident-Erstellung nicht ausgefüllt wird. Alternativ gehen Sie davon aus, dass CI-Informationen für einen FQDN, einen Hostnamen oder



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine IP-Adresse im Feld Identifiziertes CI des Security Incident ausgefüllt werden, und wählen das Feld Identifiziertes CI als Alternative aus. Für dieses Beispiel wird das identifizierte CI ausgewählt, Sie können jedoch ein beliebiges Feld im Security Incident für das alternative CI verwenden.

**b.** Wählen Sie in der angezeigten Auswahlliste **Alternatives CI-Auslöserfeld** das Feld **Identifiziertes CI** aus.

Alle verfügbaren Felder für den Security Incident werden in der Liste angezeigt, einschließlich aller benutzerdefinierten Felder. Im Feld Alternativer CI-Auslöser wird Identifiziertes CI angezeigt.

Wenn dieses Profil aufgerufen wird und das CI-Feld beim ersten Event-Auslöser nicht für den zugeordneten Security Incident ausgefüllt wird, verwendet das Profil alternativ den Wert aus dem Feld Identifiziertes CI in der Suche.

**c.** Aktivieren Sie das Kontrollkästchen **Automatischer Auslöser basierend auf Incident**.
Der Generator für Filterbedingungen wird angezeigt. Mit dieser Option legen Sie Filterbedingungen fest und geben an, wann das Profil beim Erstellen eines Security Incident automatisch aufgerufen wird.

**d.** Definieren Sie die SIR-Incident-Bedingungen, die automatisch die für dieses bestimmte Profil ausgewählten ePO-Fähigkeiten auslösen.

**e.** Wenn die Profilfähigkeiten, die eine Aktion auf einem Endpunkt ausführen, eine Genehmigung erfordern, aktivieren Sie das Kontrollkästchen **Genehmigung** erforderlich.

**f.** Wählen Sie mithilfe des Suchsymbols eine Genehmigung aus.

4. Klicken Sie auf **Fertigstellen**.
Sie haben das Profil erfolgreich konfiguriert, sodass es bei der Incident-Erstellung automatisch ausgelöst wird und ein alternatives Feld zum Ausfüllen übereinstimmender CI-Ergebnisse verwendet wird.

### Lösen Sie das Profil McAfee ePO manuell aus einem Security Incident aus

Lösen Sie ein Fähigkeitsprofil manuell aus einem Now Platform Security Incident Response (SIR) Security Incident aus.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

**Hinweis:**
Die Genehmigungsoption in Profile für die McAfee ePO -Integration konfigurieren wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Anforderung zum automatischen Abrufen von Hostdetails, zum Isolieren des Hostcomputers oder zum Entfernen der Isolierung eines Computers aufrufen, wenn die im Profil angegebenen Auslöserbedingungen mit den Bedingungen für Security Incidents übereinstimmen. Wenn Sie eine Anforderung alternativ manuell übermitteln möchten, übermitteln Sie die Anforderung direkt aus einem Security Incident.

Sobald Sie das Profil basierend auf den konfigurierten Auslöserbedingungen aktiviert haben, können Sie die Abfrageergebnisse in den Now Platform Security Incidents anzeigen. Mit McAfee ePO -Integrationen können Sie auch einzelne Fähigkeiten für Konfigurationselemente (CIs) ausführen, ohne ein Profil zu verwenden.

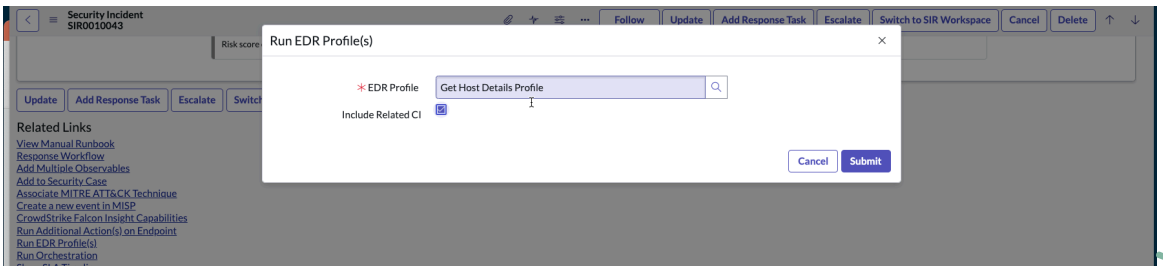


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

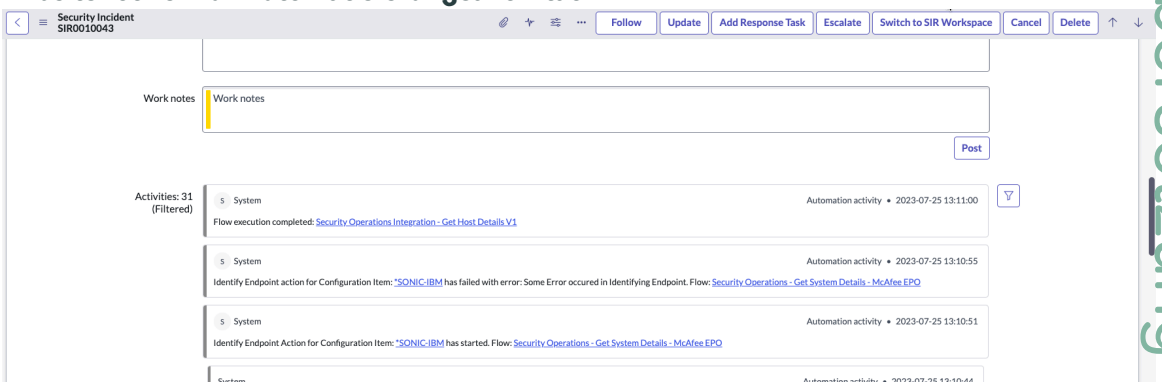
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen McAfee ePO.
3. Wählen Sie im Abschnitt „Zugehörige Listen“ die **Option EDR-Profil(e) ausführen**aus.

**McAfee EDR-Profil ausführen**




4. Suchen Sie ein Profil und wählen Sie es aus der Liste der verfügbaren Profile aus.
   Die Liste der verfügbaren Profile lautet „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Hostdetails abrufen aus.
5. Wählen Sie **Zugehöriges CI einschließen** aus, um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.
   Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ und die Tags „profileinitied“ und „profile-completed“ (Profil abgeschlossen) im Abschnitt „Arbeitsnotizen“ überprüfen.

**Arbeitsnotizen für Automatisierungsaktivität**



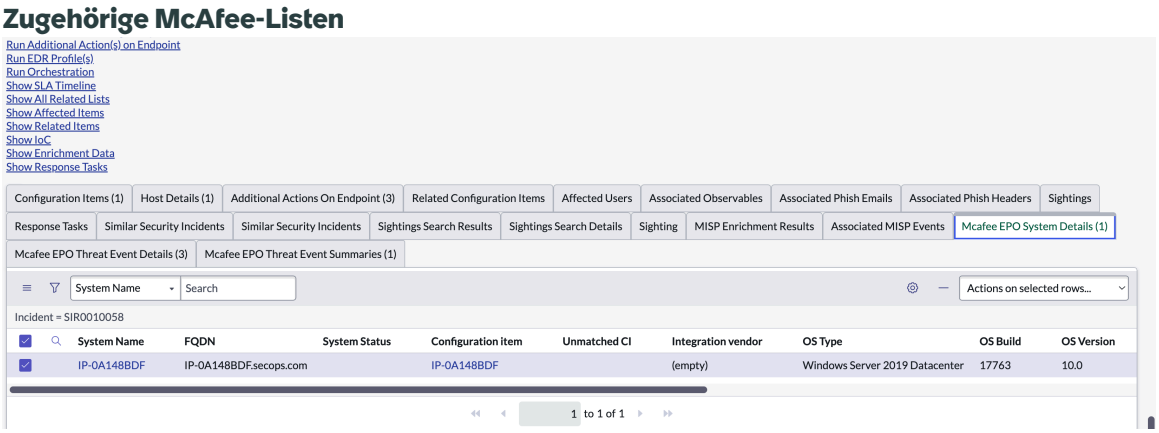

Die Ergebnisse werden in Form von zugehörigen Listen angezeigt, z. B. „Hostdetails abrufen“, „Hostcomputer isolieren“ oder „Isolierung entfernen“.

### Hinweis:

Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel sind die McAfee ePO-Systemdetails eine erweiterte Tabelle der Basistabelle „Hostdetails“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Führen Sie die folgenden Schritte aus, um einzelne Fähigkeiten für ein Konfigurationselement (CI) auszuführen:

   a. Wählen Sie in der zugehörigen Liste Konfigurationselemente das erforderliche CI aus.

   b. Klicken Sie auf die Dropdown-Liste **Aktionen für ausgewählte Zeilen...** und wählen Sie die erforderliche Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Klicken Sie auf **Host isolieren**, um sie für das ausgewählte CI auszuführen.
   Das ausgewählte CI wird vom Netzwerk isoliert.

### Lösen Sie zusätzliche Aktionen in der McAfee ePO -Integration aus

Die Funktionen „Bedrohungsereignisse auflisten“ und „Malware-Scan initiieren“ können über „Zusätzliche Aktionen ausführen“ ausgelöst werden

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können zusätzliche Aktionen in der Integration von McAfee ePO konfigurieren und auslösen, indem **Sie Zusätzliche Aktionen für Endpunkt**ausführen verwenden, einschließlich der Funktionen McAfee ePO Bedrohungsereignisse auflisten und McAfee ePO Malware-Scan initiieren.

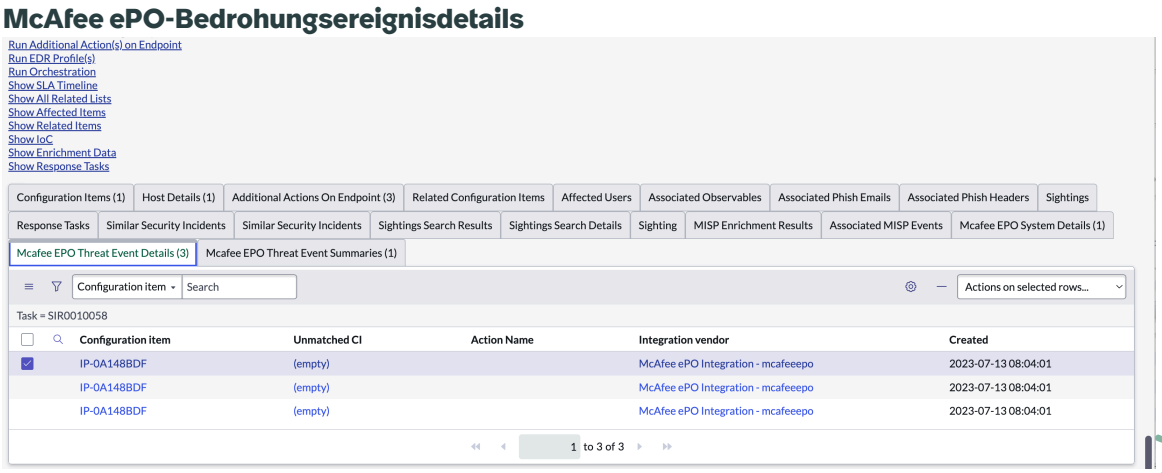
#### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die zusätzlichen Aktionen ausführen möchten.
3. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktion(en) für Endpunkt ausführen**.
4. Suchen Sie die Fähigkeitsimplementierung, die Sie auslösen möchten, und wählen Sie sie aus der Liste der zusätzlichen Aktionen aus.
   Beispiel: McAfee ePO Bedrohungsereignisse auflisten.
5. Wählen Sie **Zugehöriges CI einschließen** aus, um diese zusätzliche Aktion für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken **Sie auf Zusätzliche Aktionen ausführen**.




**Hinweis:**
Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel ist die Tabelle „McAfee ePO-Bedrohungsereignisdetails“ eine erweiterte Tabelle der Basistabelle „Zusätzliche Aktionen für Endpunkt“.

7. Zeigen Sie die McAfee ePO-Bedrohungsereignisdetails in den zugehörigen Listen an, und validieren Sie sie.

### Verwenden der McAfee ePO -Integration in Analyst Workspace

Verwenden Sie die Integration von McAfee ePO, um die Fähigkeiten von McAfee ePO im SIR-Analystenarbeitsbereich zu nutzen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

Bevor Sie die McAfee ePO -Integration im Security Incident Response-Arbeitsbereich verwenden, müssen Sie sie aus dem ServiceNow Store herunterladen und konfigurieren. Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die McAfee ePO -Integration ein.

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können die McAfee ePO -Integration verwenden, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, Profile zum Sammeln von Details zum Host zu verwenden und im Arbeitsbereich Security Incident Response bestimmte Abfragen oder Aktionen für den Endpunkt durchzuführen.

Die McAfee ePO -Integration ermöglicht Analysten die Verwendung der folgenden McAfee ePO -Fähigkeiten im Analyst Workspace Security Incident Response :

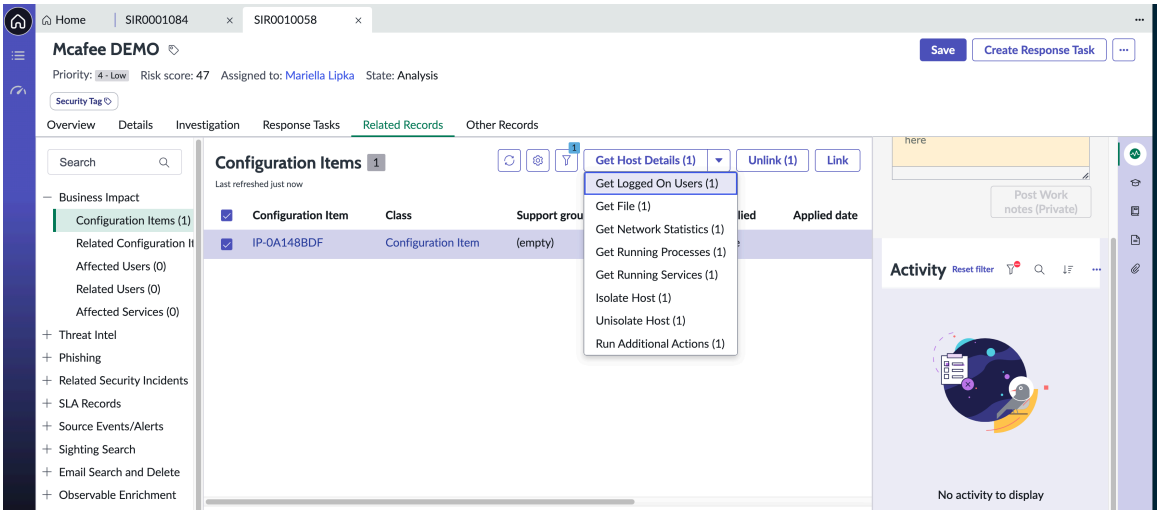
- **Hostdetails abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Zusätzliche Aktion(en) für Endpunkt ausführen**



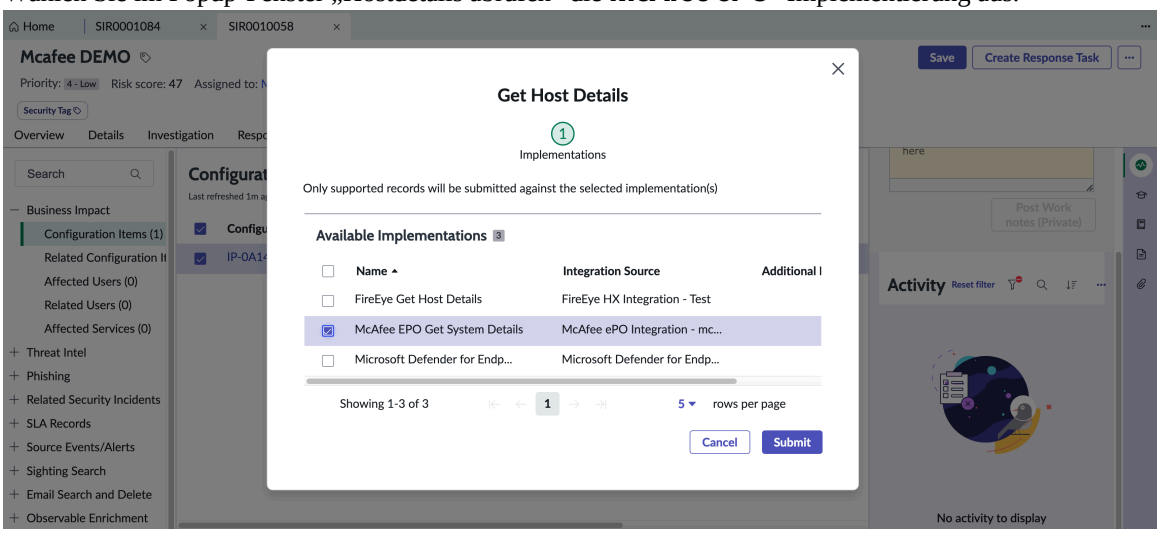
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Um den Security Incident im SIR-Arbeitsbereich zu öffnen, klicken Sie im Security Incident auf Zu SIR-Arbeitsbereich **wechseln**.
2. Wählen Sie im SIR-Arbeitsbereich die Registerkarte **Zugehörige Datensätze** aus.
3. Wählen Sie ein beliebiges **Konfigurationselement**aus, und wählen Sie in der Dropdown-Aktion der zugehörigen Liste eine McAfee ePO-Fähigkeit aus, die ausgelöst werden soll.
   Beispiel: Hostdetails abrufen.




4. Wählen Sie im Popup-Fenster „Hostdetails abrufen“ die **McAfee ePO** -Implementierung aus.

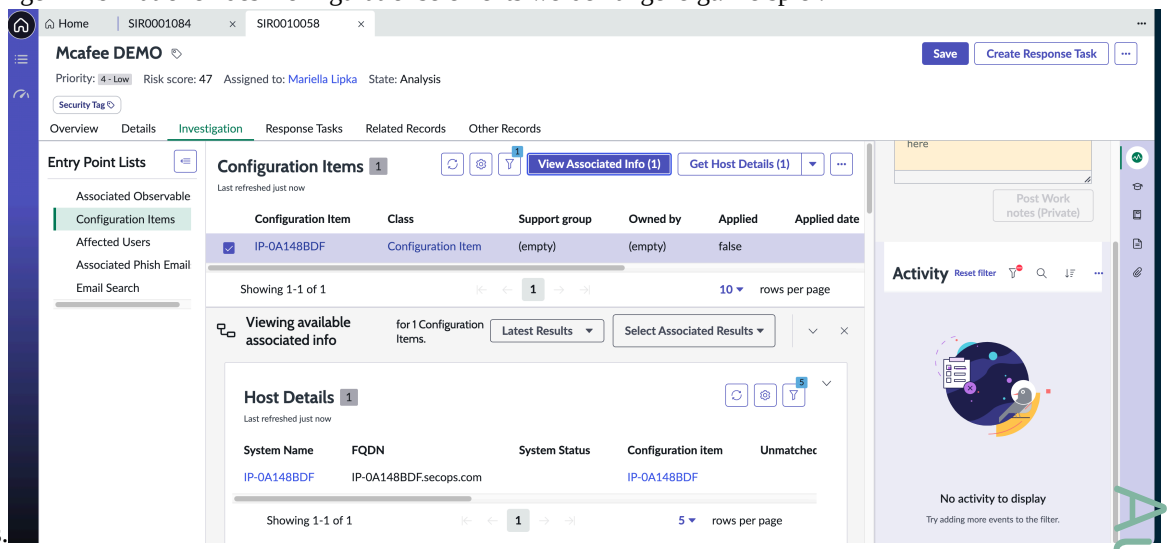



5. Klicken Sie auf **Absenden**.
   Die Fähigkeit „Hostdetails abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.
6. Um die Daten für die ausgelöste Fähigkeit anzuzeigen, wählen Sie die Registerkarte **Untersuchung** aus.
7. Wählen Sie das **Konfigurationselement**aus, und klicken Sie auf die Aktion **Zugehörige Informationen** anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zugehörigen Informationen des Konfigurationselements werden angezeigt. Beispiel:




Hostdetails.

8. Klicken Sie auf das **Konfigurationselement, um die Hostdetails** anzuzeigen.
   Ebenso können Sie versuchen, die anderen McAfee ePO-Fähigkeiten für Ihre Security Incidents im SIR-Analystenarbeitsbereich zu verwenden.
9. Sie können die McAfee ePO-Fähigkeiten in der zugehörigen Liste **Endpoint Detection and Response (EDR)** für Analysen verwenden.
10. Suchen Sie ein Profil und wählen Sie es aus der Liste der verfügbaren Profile aus.
    Die Liste der verfügbaren Profile lautet „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Hostdetails abrufen aus.
11. Wählen Sie die **McAfee ePO-** Implementierung aus, und klicken Sie auf **Absenden**.

## McAfee ESM – E-Mail-Analyse-Integration

Die Integration von ESM - Email Parser wird von einem E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen von ESM verwendet, um Security Incidents zu erstellen.

### Konfigurieren Sie die Integration von McAfee ESM - Email Parser

Bei der Integration von McAfee ESM – Email Parser werden E-Mail-Benachrichtigungen von ESM verwendet, um die Ergänzungs- und Antwort-Workflows voranzutreiben.

#### Vorbereitungen

Erforderliche Rolle: sn_si_admin

#### Warum und wann dieser Vorgang ausgeführt wird

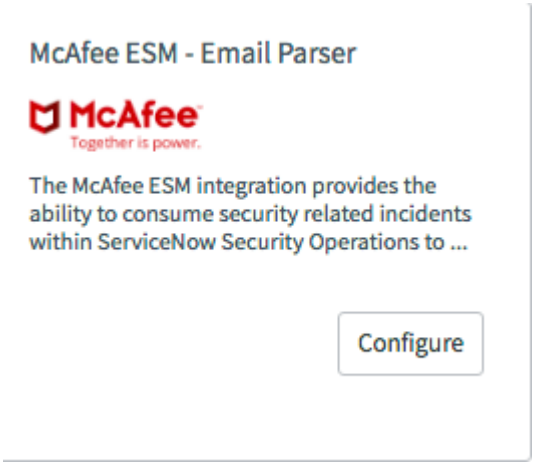
Für die Integration wird eine McAfee ESM-E-Mail-Parser-Vorlage bereitgestellt. Sie muss vor der Integration konfiguriert und aktiviert werden. Durch Aktualisieren des Parsers wird dieser aktiviert.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




2. Klicken Sie auf der Karte „McAfee ESM – E-Mail-Analyse“ auf **Konfigurieren**.
3. Klicken Sie im Dialogfeld „ **McAfee ESM – E - Mail-Analysekonfiguration** “ auf den Link E-Mail-Analyse konfigurieren.
4. Klicken Sie auf den Link **McAfee ESM**, um die Einstellungen im bereitgestellten E-Mail-Parser für Vorlagen zu bearbeiten.
   Füllen Sie mindestens das Feld E- Mail ist von aus. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**.
6. Klicken Sie im Formular **„E-Mail-Analyse** “ auf **Aktualisieren**.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu **Integrationskonfigurationen**zurückkehren.

## McAfee ESM – Integration der Incident-Ergänzung

McAfee ESM -Integration der Incident-Ergänzung durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

### Erkunden

Security Incident Response-Integrationen

### Einrichten

- Beginnen Sie mit der Integration von McAfee ESM – Incident-Ergänzung
- Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

### Verwenden

- Führen Sie eine Sichtungssuche aus
- Security Operations Integration - Sichtungs-such-Workflow
- Workflow „Security Operations – McAfee ESM-Sichtungssuche“.
- Sichtungssuchdetails anzeigen
- Sichtungssuchergebnisse anzeigen

### Entwickeln

- ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Problembehandlung und Hilfe**

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

## Beginnen Sie mit der Integration von McAfee ESM – Incident-Ergänzung

McAfee ESM schützt Endpunkte vor Viren, Spyware, Trojanern und anderen Malware-Bedrohungen und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration McAfee ESM – Incident-Anreicherung verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechende API-Basis-URL und Anmeldeinformationen hinzufügen.

### Vorbereitungen

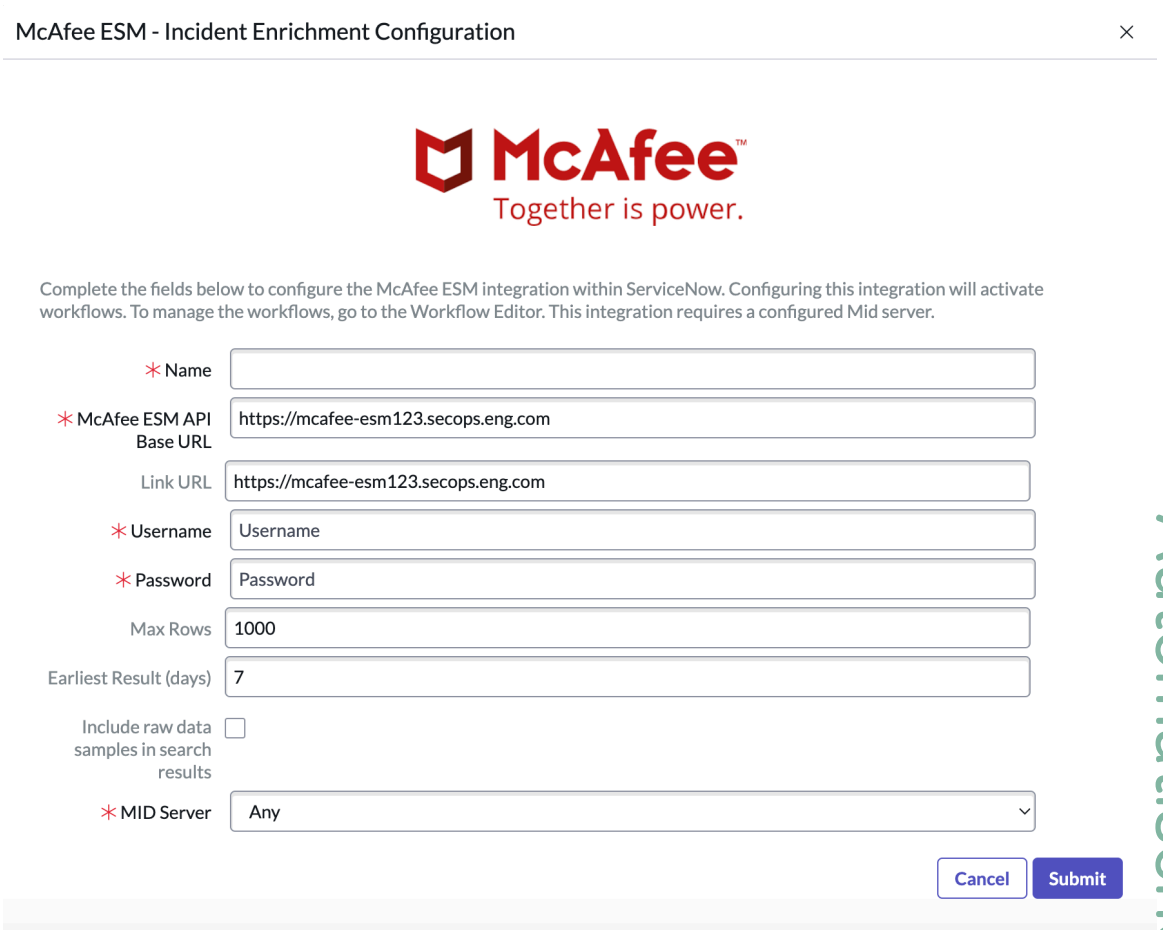
Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie in der Karte McAfee ESM – Incident-Ergänzung auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Basis-URL der McAfee ESM-API | Die Basis-URL, die Sie von der McAfee ESM-Website erhalten haben. |
| Link-URL | [Optional] Die Link-URL, die auf eine McAfee ESM-Instanz verweist, sofern verfügbar.<br>**Hinweis:**<br>Wenn ein Fehler angezeigt wird, verwenden Sie die Basis-URL der McAfee ESM-API. |
| Benutzername | Ihr McAfee ESM-Benutzername. |
| Passwort | Ihr McAfee ESM-Passwort. |
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |
| Rohdatenmuster in | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Suchergebnissen berücksichtigen | von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## Integration „Microsoft Azure Sentinel“

Microsoft Azure Sentinel ist eine cloudbasierte Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Sie können die Integration Microsoft Azure Sentinel verwenden, um Azure Sentinel-Incidents zu erfassen und automatisch Security Incidents in Security Incident Responsezu erstellen.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

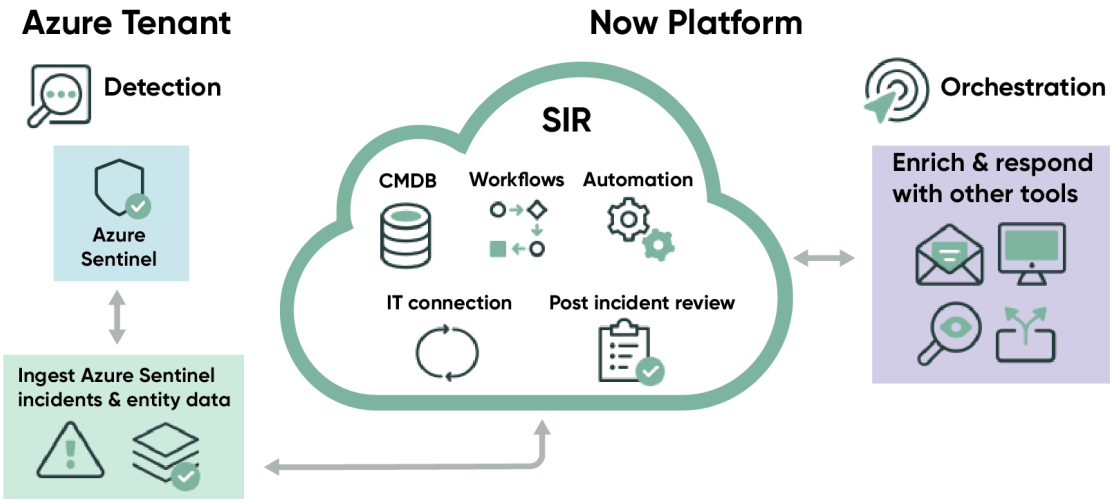
## Übersicht

Im folgenden Diagramm erfahren Sie, wie Microsoft Azure Sentinel in die Anwendungen von Now Platform Security Operations ] integriert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Now Platform - Azure Sentinel integration overview




## Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen Sie Microsoft Azure Sentinel Incidents, die Kandidaten für Security Incidents sind, und automatisieren Sie die Erstellung dieser Security Incidents.
- Ordnen Sie die Incident- und Entitätsfelder Microsoft Azure Sentinel ] den Security Incident-Feldern SIR zu.
- Filtern Sie Microsoft Azure Sentinel Incidents.
- Fassen Sie Incidents mit vorhandenen offenen Security Incidents zusammen, damit Sie keine doppelten Security Incidents erstellen müssen.
- Automatisieren Sie Microsoft Azure Sentinel Incident-Statusaktualisierungen für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

**Hinweis:**
ServiceNow aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss eines Security Incident. Dieses Update enthält auch Kommentare zu zusammengefassten Incidents und neuen Incidents.

- Planen Sie die Incident-Erfassung, um regelmäßig Security Incidents zu erstellen.
- Synchronisieren Sie Microsoft Azure Sentinel Incident-Kommentare mit SIR Arbeitsnotizen.

## Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| Microsoft Produktdokumentations-Website | Microsoft-Website mit Produktdokumentation |
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erste Schritte mit der Integration von Microsoft Azure Sentinel .

Aktivieren und richten Sie das Plugin Microsoft Azure Sentinel – Incident Ingestion „ for Security Operation“ als Schnittstelle mit Ihrer Now Platform -Instanz und Ihrem [ Security Incident Response -Produkt ein.

## Vorbereitungen

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator

Bevor Sie die Microsoft Azure Sentinel -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

## Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie. | Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Die Administratorrolle installiert die Integration aus dem ServiceNow Store und weist die Rolle sn_si.admin zu.<br>• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:<br>◦ Konfiguriert die Integration.<br>◦ Erstellt Incident-Profile.<br>◦ Ordnet die Incident-Datenfelder Microsoft Azure Sentinel den Security Incident-Feldern zu.<br>◦ Plant die laufende Incident-Erfassung.<br>◦ Aktiviert Incident-Aktualisierungen, wenn ein Security Incident Response Incident erstellt oder geschlossen wird.<br>◦ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu. |
| Weisen Sie die erforderlichen Microsoft Azure Rollen zu. | Die folgenden Rollen sind in Microsoft Azure erforderlich, um Ihre Anwendung zu registrieren und zu konfigurieren:<br>• Anwendungsentwickler für die Registrierung der Anwendung.<br>• Mandantenadministrator zum Erteilen von Berechtigungen für die Anwendung durch Aufrufen des Administratoreinwilligungsendpunkts. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| Stellen Sie sicher, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie diese Integration konfigurieren. | Das Plugin ServiceNow IntegrationHub Starter Pack Installer [com.glide.hub.integrations] ist erforderlich.<br><br>Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren, die für die Integration erforderlich sind.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten:<br><br>**1.** Security Incident Response<br>**2.** Security Incident Response-Benutzeroberfläche<br>**3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime)<br>**4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) |
| Registrieren und konfigurieren Sie Ihre Anwendung im Microsoft Azure -Portal. | Registrieren Sie Ihre Anwendung im Portal Microsoft Azure, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung. |



### Registrieren und konfigurieren Sie das Portal Microsoft Azure .

Registrieren Sie Ihre Anwendung im Portal Microsoft Azure, und gewähren Sie Ihren Benutzern Lese- und Schreibzugriff auf die Anwendung.

#### Vorbereitungen

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator

#### Prozedur

**1.** Melden Sie sich beim Microsoft Azure -Portal an.

**2.** Suchen Sie nach **App-Registrierungen**und wählen Sie sie aus.

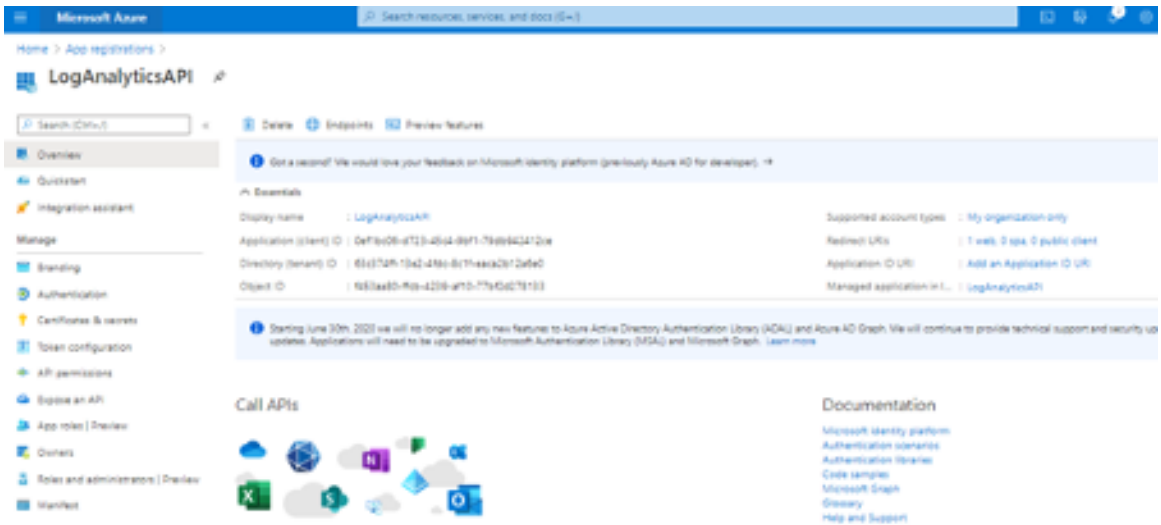
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **New registration (Neue Registrierung)**.
4. Füllen Sie die Felder des Formulars aus.

**Anwendungsformular registrieren**

| Feld | Beschreibung |
|---|---|
| Name | Benutzerorientierter Anzeigename für die Anwendung. Beispiel: LogAnalyticsAPI. |
| Unterstützte Account-Typen | Kontotyp, der diese Anwendung verwenden oder auf die API zugreifen kann. |
| Umleitungs-URI | Umleitungs-URI Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung eines Benutzers an diesen URI weitergeleitet. |

5. Klicken Sie auf **registrieren**.
Nachdem Sie die Anwendung erfolgreich registriert haben, wird die Seite „Übersicht“ angezeigt.




6. Navigieren zu **Verwalten** > **Zertifikate und geheime Schlüssel**.
7. Klicken Sie im Abschnitt Geheime Clientschlüssel auf **Neuer geheimer Clientschlüssel**.
Sie können den geheimen Clientschlüssel später nicht anzeigen. Stellen Sie daher sicher, dass Sie den geheimen Clientschlüssel jetzt in diesem Schritt kopieren und speichern. Wenn Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen erstellen, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.
8. Navigieren zu **Verwalten** > **API-Berechtigungen**.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster API-Berechtigungen anfordern auf die Registerkarte **APIs, die meine Organisation verwendet**.
11. Suchen Sie den Namen der **Log Analytics-API-** App und wählen Sie ihn aus.
12. Wählen Sie in den Log Analytics-API-Berechtigungen **Anwendungsberechtigungen**aus.
Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt wird.
13. Wählen Sie im Abschnitt „Daten“ die **Option Data.Read aus**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Klicken **Sie auf Berechtigungen hinzufügen**.
    Die Berechtigungen werden aktualisiert.
15. Aktivieren Sie die Option **Grant admin consent for Default Directory** (Administratoreinwilligung für Standardverzeichnis gewähren) für die Data.Read-API-Berechtigung, die Sie in Schritt 13 aktiviert haben.
16. Suchen Sie nach **Log Analytics-Arbeitsbereichen**und wählen Sie sie aus.
17. Wählen Sie Ihren Sentinel Log Analytics-Arbeitsbereich aus.
    Sie sehen jetzt die Übersichtsseite des Sentinel Log Analytics-Arbeitsbereichs.
18. Navigieren zu **Zugriffskontrolle (IAM)** > **Rollenzuweisungen**.
19. Klicken Sie auf **Hinzufügen**und wählen **Sie Rollenzuweisung hinzufügen**aus.
20. Füllen Sie die Felder des Formulars aus.

**Formular „Rollenzuweisung hinzufügen“**

| Feld | Beschreibung |
|---|---|
| Rolle | Kontotyp, der diese Anwendung verwenden kann. Wählen Sie **Azure Sentinel-Antwort aus**. |
| Assign access zu (Zugriff zuweisen an) | Berechtigungsumfang, den Sie definieren. Wählen Sie **Benutzer**, **Gruppe**oder **Dienstprinzipal aus**. |
| Auswahlvorgang | Anwendung, die Sie zuvor in Schritt 4 erstellt haben. Beispiel: LogAnalyticsAPI. |

21. Klicken Sie auf **Speichern**.

### Installieren und konfigurieren Sie die Microsoft Azure Sentinel -Integration

Installieren und konfigurieren Sie die Microsoft Azure Sentinel -Integration von ServiceNow Store in Ihrer Instanz von Now Platform, um mit der Erfassung von Azure Sentinel-Incidents zu beginnen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Laden Sie die Microsoft Azure Sentinel -Integration aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Microsoft Azure Sentinel, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

**Microsoft Azure Sentinel Formular „Konfiguration der Incident-Erfassung“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Microsoft Azure Cloud Instanzkonfiguration . |
| Identitäts-URL | Identitäts-URL für den Mandanten Microsoft Azure Cloud Zum Beispiel „login.microsoftonline.com“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation . |
| Azure Resource Manager | Azure Resource Manager-Endpunkt für Mandant Microsoft Azure Cloud Beispiel: management.azure.com. Weitere Informationen finden Sie in der Microsoft Azure-Dokumentation . |
| Mandanten-ID | Microsoft Azure Sentinel Mandanten-ID Dies ist die Instanz, aus der alle Incidents im Portal Microsoft Azure abgerufen werden. |
| Client-ID | Client-ID für die Anwendung, die Sie im Portal Microsoft Azure registriert haben. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel für Ihre registrierte Anwendung. |
| Abonnement-ID | Abonnement-ID für Ihre registrierte Anwendung. |
| Ressourcengruppenname | Ressourcengruppenname für Ihre registrierte Anwendung. |
| Arbeitsbereichsname | Name des Arbeitsbereichs für Ihre registrierte Anwendung. |

5. Klicken Sie auf **Absenden**.

### Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird jede Serverkonfiguration für die Incident-Erfassung auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

## Erstellen Sie ein Profil für Microsoft Azure Sentinel

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform, und bestimmen Sie die Microsoft Azure Sentinel Incidents, die zum Erstellen von Security Incidents geeignet sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Mit der Integration können Sie verschiedene Arten von Incidents erstellen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Incidents werden basierend auf den Profilen erstellt, die Sie in der Instanz Now Platform konfigurieren. Alle Incidents werden anfänglich für einen konfigurierten Incident-Typ in einem Profil erstellt. Erstellte Incidents können dann weiter gefiltert werden, um anzugeben, welche Incidents Security Incidents erstellen.

Alle Incidents, die die Auswahlkriterien in Ihrem Microsoft Azure -Mandanten erfüllen und über die Microsoft Azure Sentinel -API verfügbar sind, werden anfänglich in Ihrer Now Platform -Instanz erfasst.

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Incident-Profil**.
2. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder des Formulars aus.

**Microsoft Azure Sentinel Formular „Konfiguration der Incident-Erfassung“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für das Profil.<br><br>Dieser Name hilft Ihnen, den Profiltyp zu identifizieren, und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist. |
| Aktiv | Indikator, der angibt, dass das Profil aktiv ist.<br><br>Wenn das Profil aktiv ist, bedeutet dies, dass Now Platform Azure Sentinel-Incidents aktiv abfragt und entsprechende Security Incidents in SIR erstellt werden, wenn die Filterbedingungen übereinstimmen. |
| Quelle | Microsoft Azure -Mandanten, den Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Incident-Typen aus, die Sie für das Profil erfassen möchten. |
| Reihenfolge | Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen.<br><br>Der Flow mit der niedrigsten Nummer hat die höchste Priorität.<br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300, 400.<br><br>Der Standardwert ist 100. |
| Beschreibung | Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

4. Um zum Abschnitt „Zuordnung“ zu wechseln, klicken Sie auf **Fortfahren**.

## Nächste Maßnahme

Ordnen Sie einzelne Microsoft Azure Sentinel Incident-Felder den Feldern im Now Platform SIR Security Incident zu.

### Ordnen Sie die Incident-Felder Microsoft Azure Sentinel zu

Ordnen Sie die einzelnen Incident-Felder Microsoft Azure Sentinel den Feldern im Security Incident SIR zu, damit Sie Incidents mit den zugeordneten Daten erstellen können.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wählen Sie auf der Zuordnungsseite im Abschnitt „Azure Sentinel-Feldzuordnung“ eine der Beispiel-Erfassungsmethoden aus.

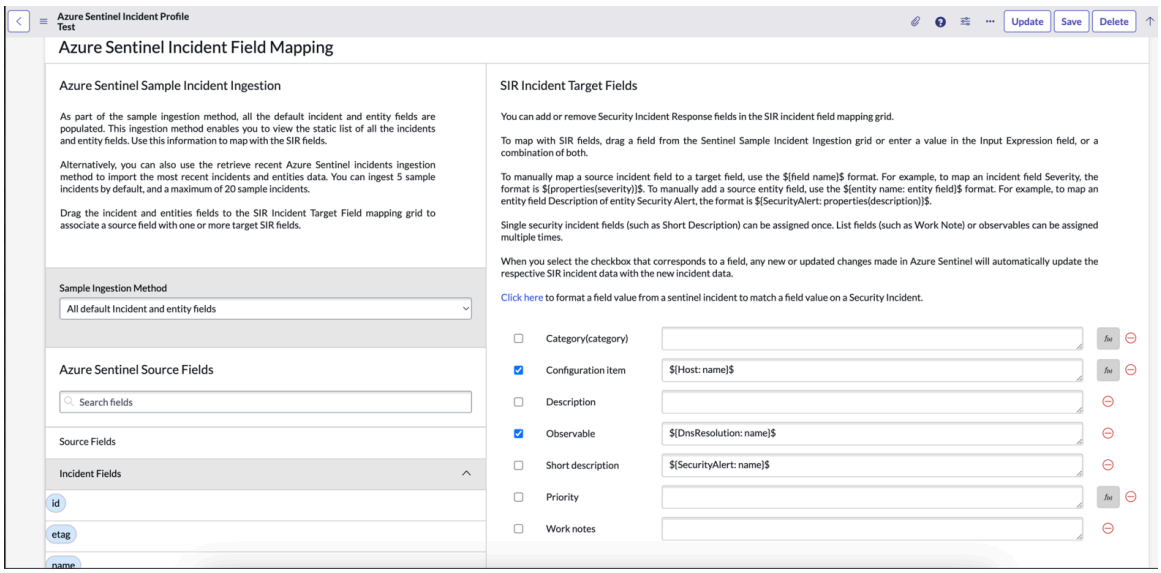
### Beispiel für Erfassungsmethoden

| Feld | Beschreibung |
|---|---|
| Alle standardmäßigen Incident- und Entitätsfelder | Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Incidents und Entitätsfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte.<br><br>Sie können diese Informationen für die Zuordnung zu den Feldern SIR verwenden. |
| Rufen Sie aktuelle Azure Sentinel-Incidents ab | Verwenden Sie diese Erfassungsmethode, um die neuesten Incident- und Entitätsdaten zu importieren.<br><br>Wenn der Azure Sentinel-Incident die Entitätsdaten enthält, werden die Entitätsdaten abgerufen und stehen für die Zuordnung im Abschnitt „Azure Sentinel-Quellfelder“ zur Verfügung. Manchmal enthält der Azure Sentinel-Incident die Entitätsdaten nicht, und daher sind die Entitätsfelder in einem solchen Szenario nicht für die Zuordnung verfügbar.<br><br>Wenn der Azure Sentinel-Incident mehrere Warnungen enthält, wird die früheste Warnung, die Teil des Incident ist, im Zuordnungsabschnitt angezeigt. Während der Erfassung werden auch die frühesten Feldwerte der Sicherheitswarnung verwendet.<br><br>Sie können standardmäßig 5 Beispiel-Incidents und maximal 20 Beispiel-Incidents erfassen.<br><br>Die Beispiel-Incident-Feldwerte werden ausgefüllt, wenn das Profil die Beispiel-Incidents erfasst. Sie können diese Incidents den **SIR-Incident-Zielfeldern zuordnen**. Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt. |
| Importieren Sie Beispieldaten | Klicken Sie auf **Beispieldaten** importieren, um Beispiel-Incidents aus Azure Sentinel zu importieren.<br><br>Diese Schaltfläche wird angezeigt, wenn Sie die Erfassungsmethode Letzte Azure Sentinel-Incidents abrufen auswählen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Das Abrufen von Beispiel-Incidents vom Microsoft Azure Sentinel -Server kann einen Moment dauern.<br><br>Ordnen Sie diese abgerufenen Incidents den **SIR-Incident-Zielfeldern**zu. Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt. |




**2.** Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

**a.** Klicken Sie im Abschnitt „SIR-Incident-Zielfelder“ auf die Map another field Schaltfläche „Weiteres Feld zuordnen“.
Sie zeigt eine Liste von SIR Feldern, aus der Sie ein Feld für ein neues Feld auswählen können, das angezeigt werden soll.

**b.** Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

**Hinweis:**
Mehrere erkennbare Elemente können für denselben Security Incident angezeigt werden. Beispielsweise kann das **Feld** „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder **Konfigurationselement** und **Arbeitsnotizen** mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, die besagt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident eine Liste enthält, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

**c.** Verschieben Sie Ihr Feld per Drag-and-Drop aus dem Abschnitt „Azure Sentinel-Quellfelder“, um es Ihrem neuen Feld zuzuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden durch neue oder aktualisierte Änderungen in Azure Sentinel die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

> **Hinweis:**
> Im Basissystem ist die Systemeigenschaft sn_sec_sentinel.incident_updates standardmäßig auf True festgelegt, um die Microsoft Azure Sentinel Aktualisierungen im Zusammenhang mit neuen Warnungen zu erhalten, die mit SIR verknüpft sind.

- Standardmäßig sind die Felder Betroffene Benutzer, Konfigurationselemente und erkennbare Elemente aktiviert. Dies bedeutet, dass immer dann, wenn dem Incident neue erkennbare Elemente oder zugeordnete Konfigurationselemente oder betroffene Benutzer hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in die entsprechenden zugehörigen Listen in Security Incident Response (SIR) eingetragen werden.
- Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für neue oder aktualisierte Änderungen entspricht, die im Azure Sentinel-Incident-Datensatz in Azure Sentinel vorgenommen werden. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

> **Wichtig:**
> Vor der Auswahl dieser Funktionalität ist eine Due-Diligence-Prüfung erforderlich, da das Überschreiben der vorhandenen Daten zu instabilen Daten für den Analysten führen kann und jede andere Automatisierung, die auch nur durch die Feldwerte des Security Incident festgelegt wird, ebenfalls betroffen sein kann. Daher ist es sehr wichtig, die Due Diligence durchzuführen, bevor Sie eine Überschreibungsfunktion auswählen.

**3.** Um ein Feld zu entfernen, verwenden Sie die „Element entfernen“ neben dem Eingabeausdrucksfeld im Abschnitt „SIR-Incident-Zielfelder“.

**4.** Um einen Feldwert aus dem Abschnitt „Azure Sentinel-Quellfelder“ einem Feld im Abschnitt „SIR-Incident-Zielfelder“ zuzuordnen, verwenden Sie eine der folgenden Aktionen:

**a.** Ziehen Sie den Feldnamen (z. B. id) in die Spalte SIR-Incident-Zielfelder neben einem Feldnamen.

Sie können einen beliebigen Wert aus dem Abschnitt „Azure Sentinel-Quellfelder“ mit einem Feld im Abschnitt „SIR-Incident-Zielfelder“ abgleichen. Felder sind farbcodiert, damit Sie Incident-Felder im Zuordnungsprozess nicht übersehen oder duplizieren. Hellblaue Felder zeigen an, dass noch kein Incident-Feld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes Incident-Feld mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Incident-Informationen nicht zugeordnet wurden.

**b.** Sie können eine Kombination aus Text und Feld hinzufügen.
Beispiel: `Incident-Name ist ${name}$`. Hier kann der `Incident-Name` manuell eingegeben werden, während `${name}$` aus dem Abschnitt „Azure Sentinel-Quellfelder“ zugeordnet wird.

**c.** Sie können ein Quell-Incident- oder -Entitätsfeld direkt manuell eingeben und einem Zielfeld zuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um ein Quell-Incident-Feld manuell zuzuordnen, verwenden Sie das Format ${field name}$. Um beispielsweise ein Incident-Feld Schweregrad zuzuordnen, lautet das Format${properties(severity)}$.
- Um ein Quellentitätsfeld manuell hinzuzufügen, verwenden Sie das Format ${Entitätsname: Entitätsfeld}$. Um beispielsweise ein Entitätsfeld Beschreibung der Entität Sicherheitswarnung zuzuordnen, lautet das Format ${SecurityAlert: properties(description)}$.

Diese Integration klassifiziert bestimmte erkennbare Untertypen. Wenn Sie ein Azure Sentinel-Feld dem erkennbaren SIR-Feld zuordnen, klassifiziert Now Platform das erkennbare Element automatisch. Wenn Sie das eingehende erkennbare Azure Sentinel-Element generisch dem erkennbaren Typ in SIRzuordnen möchten, ziehen Sie das Feld Azure Sentinel per Drag-and-Drop in das Feld Erkennbares Element. Wenn Sie jedoch den erkennbaren Typ für das eingehende erkennbare Azure Sentinel-Element in SIRkennen, ordnen Sie dies speziell dem Feld „Erkennbarer Typ SIR “ zu. Einige Beispiele für bestimmte erkennbare Typen in SIR sind: Erkennbares Element (Domänenname), erkennbares Element (E-Mail-Adresse), erkennbares Element (IP-Adresse (V4)) und erkennbares Element (Hostname).

Wenn Ihre eingehenden Azure Sentinel-Felder Informationen von MITRE-ATT&CK enthalten, ordnen Sie sie dem Feld „Technik“ von MITRE-ATT&CK zu. Stellen Sie sicher, dass das eingehende Azure Sentinel-Feld die Technik-ID oder den Techniknamen MITRE-ATT&CK enthält.

Manchmal werden Incident-Feldwerte in Microsoft Azure Sentinel nicht direkt in die Felder des SIR-Security Incident übertragen. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

5. Um eine Feldübersetzung für ein neues Feld aus einem Azure Sentinel-Incident so zu formatieren, dass er einem Feldwert in einem Security Incident entspricht, klicken Sie auf den Link **Hier** klicken im Header „ **SIR-Incident-Zielfelder** “.

6. Um die Felder zu ändern, die die Feldübersetzung unterstützen, klicken Sie auf die Feldformat Skriptformat Feldübersetzungssymbol.
   Die Felder, die die Feldübersetzung unterstützen, sind **Kategorie**, **Konfigurationselement**und **Priorität**.
   Klicken Sie beispielsweise auf „Feldformat“ neben der Kategorie. Der Skript-Editor für Azure Sentinel-Feldübersetzungen wird geöffnet.

7. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Seite „Zuordnung“ zurückzukehren.
   Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
   ```

   Durch diese Zuordnung wird sichergestellt, dass ein Profil nur konfigurierte Kategorien verwendet.

8. Setzen Sie die Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
   Sie können dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.

9. Klicken Sie auf **Fortfahren**, um zum Abschnitt Filtern und Zusammenfassung zu wechseln.

### Nächste Maßnahme

Definieren und legen Sie Filterbedingungen fest, damit Sie angeben können, welche Incidents Security Incidents erstellen sollen. Sie können dieselben Feldwerte (im Abschnitt „Zuordnung“ definiert) im Generator für



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für die Incident-Generierung (im Abschnitt „Filtern und Zusammenfassung“ ) verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.

### Definieren von Filter- und Zusammenfassungskriterien

Sie können Filterbedingungen definieren und festlegen, um anzugeben, welche eingehenden Microsoft Azure Sentinel Incidents Security Incidents erstellen sollen. Sie können auch zusätzliche Incident-Feldkriterien definieren, die es ermöglichen, einen eingehenden Incident an einen offenen Security Incident anzuhängen, anstatt einen Incident zu erstellen.

### Legen Sie die Filterbedingungen für Security Incidents fest

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen übereinstimmen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren und die Anzahl der von Ihnen erstellten Security Incidents zu begrenzen. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Incidents erfasst, ohne dass die Abfrage oder die Konfiguration der ausgelösten Incidents geändert werden muss.

#### Prozedur

1. Um die Kriterien zu definieren, die ein eingehender Microsoft Azure Sentinel Incident erfüllen muss, damit ein Security Incident erstellt wird, wählen Sie **Filter basierend auf Bedingungen aus**.

   Die Optionen im ersten Feld in den Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt Azure Sentinel-Beispiel-Incident-Erfassung für den von Ihnen erfassten Incident angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Incident, den Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.

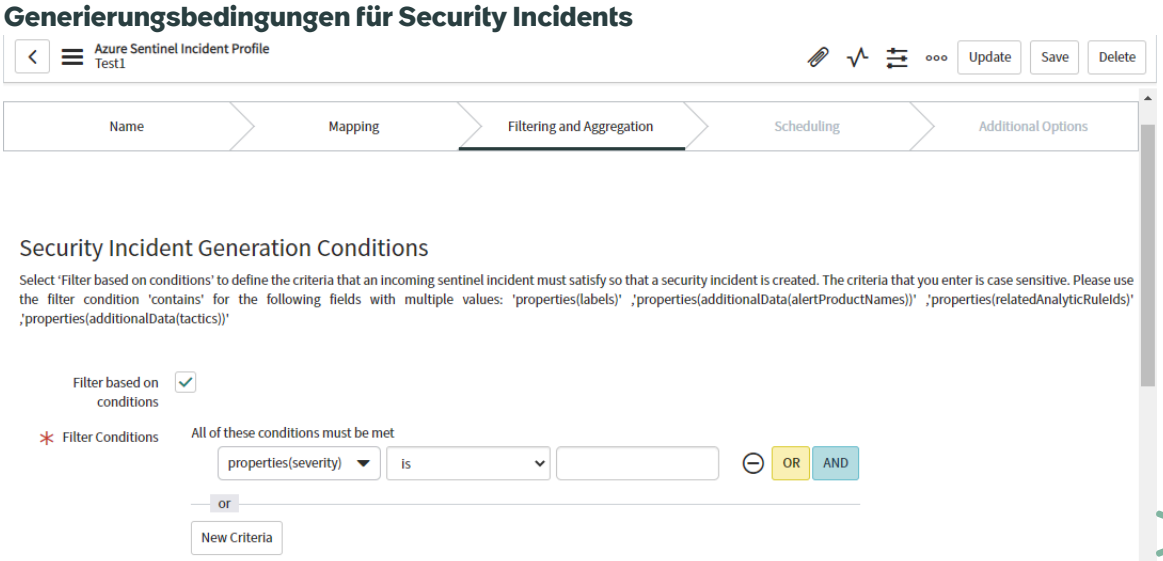
   Verwenden Sie die Filterbedingung `enthält` für die folgenden Felder mit mehreren Werten:

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie die Filterbedingung `Enthält` für die obigen Felder verwenden, um sicherzustellen, dass die Daten richtig gefiltert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.
   - Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.

### Definieren Sie Zusammenfassungsbedingungen

Definieren Sie zusätzliche Incident-Zusammenfassungskriterien, die einen eingehenden Incident mit einem vorhandenen SIR-Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Wenn Sie Wertkriterien für den Feldabgleich für jedes Profil verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Incident-Daten in einem einzigen Security Incident zusammengefasst werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.

Alle zusammengefassten Incidents für einen Security Incident werden in der zugehörigen Liste Zusammengefasste Incidents von Azure Sentinel angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum Incidents zu den vorhandenen Security Incidents hinzugefügt werden.

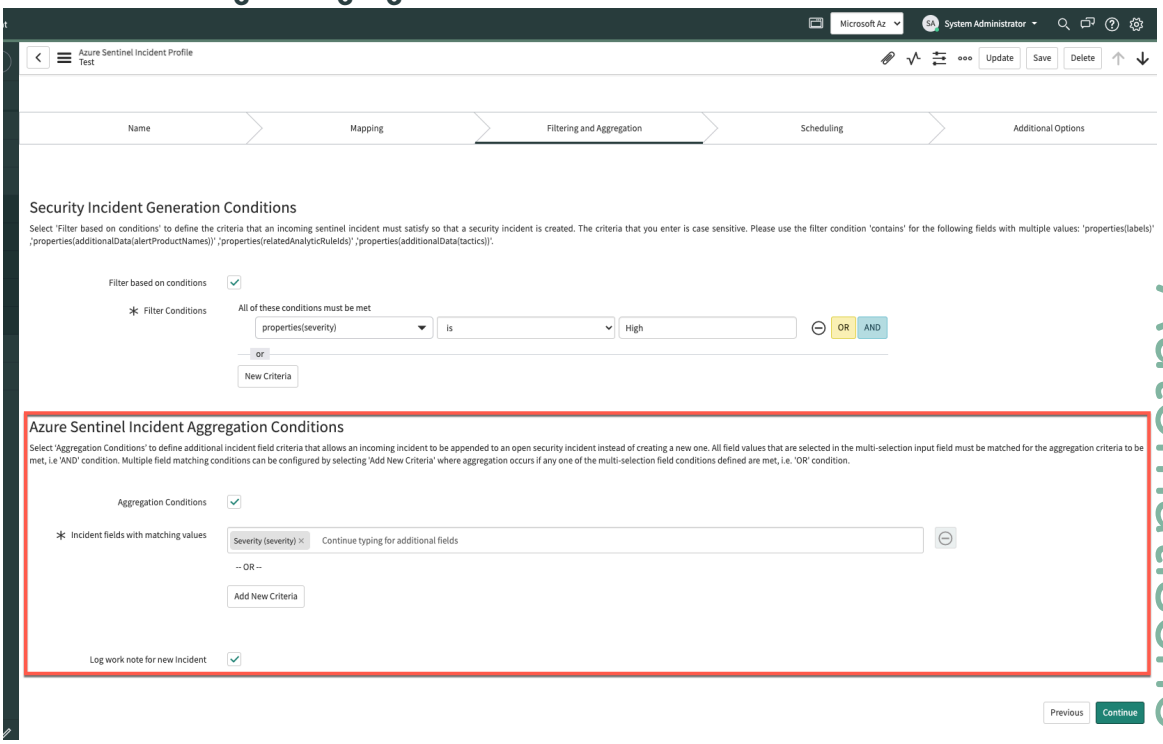


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Um zusätzliche Incident- **Feldkriterien** zu definieren, die es ermöglichen, einen eingehenden Microsoft Azure Sentinel Incident an einen offenen Security Incident anzuhängen, anstatt einen neuen Incident zu erstellen, wählen Sie die Option Zusammenfassungsbedingungen (siehe folgende Abbildung) aus.

**Zusammenfassungsbedingungen**




2. Geben Sie im **Feld Incident-Felder mit übereinstimmenden Werten** die Feldwerte ein, die Sie mit vorhandenen Security Incidents in Ihrer Now Platform -Instanz abgleichen möchten.
Alle Feldwerte, die Sie im Mehrfachauswahl-Eingabefeld ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert, dass es sich um eine *UND* -Bedingung handelt, bei der Felder wie erkennbare Elemente und Konfigurationselemente, die mehrere Feldwerte haben können, ihnen zugeordnet werden. Wenn nur eine Teilmenge der Werte abgeglichen wird, sind die Zusammenfassungsbedingungen für Azure Sentinel-Incidents nicht erfüllt, und es wird ein neuer Security Incident erstellt.
3. Um mehrere Feldabgleichbedingungen hinzuzufügen, klicken Sie auf **Neue Kriterien**hinzufügen
Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Mehrfachauswahl-Feldbedingungen erfüllt ist. Diese Auswahl impliziert die *ODER-* Bedingung.
4. Um die Arbeitsnotiz für einen neuen Incident zu aktualisieren, wenn er einem Security Incident hinzugefügt wird, wählen Sie **Arbeitsnotiz für neuen Incident protokollieren aus**.

   Die Arbeitsnotiz protokolliert, dass ein neuer Incident hinzugefügt wurde, und enthält einen Link zu den Incident-Details. In der Protokollarbeitsnotiz werden auch weitere Details aktualisiert, die Sie dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzufügen.
5. Um den Zeitplan zu konfigurieren, klicken Sie auf **Fortfahren**.

## Nächste Maßnahme

Legen Sie einen Zeitplan fest, um die Incident-Daten und erfassten Incidents abzurufen, die den Kriterien im Profil entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Planen Sie den Incident-Abruf Microsoft Azure Sentinel .

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und die Microsoft Azure Sentinel Incidents zu erfassen, die den Kriterien im Profil entsprechen.

## Vorbereitungen

Erforderliche Rolle: sn_sni.admin

## Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft zukünftige Microsoft Azure Sentinel Incidents abgefragt werden sollen, die der Incident-Profilkonfiguration entsprechen.

Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Zeitplanung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung festzulegen, aktivieren **Sie Incident-Erfassungszeit festlegen**. Die nachfolgende Erfassung basiert auf dem Abfrageintervall.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Incident-Integration von Microsoft Azure Sentinel auswirken. Planen Sie bei der Zeitplanung, dass die Systemlast auf die Dringlichkeit eines Incident abgestimmt wird. Für alle Profile wird ein Standardwert von einer Minute festgelegt. Sie können diese Einstellung basierend auf der Dringlichkeit des Incident und der erwarteten Auslastung Ihres Systems ändern.

Für alle Warnungen, die dem Incident in einem bestimmten Abfrageintervall hinzugefügt werden, wird ein Prozess ausgeführt und dann an die zugehörigen Listen der Azure Sentinel-Warnungen angehängt, und die Arbeitsnotiz wird ebenfalls veröffentlicht.

## Prozedur

1. Füllen Sie die Felder des Planungsformulars aus.

   Konfigurieren Sie den -Zeitplan, um zu definieren, wie und wann Sie Incidents aus dem Microsoft Azure -Mandanten abrufen.

   **Formular „Zeitplanung“**

| Feld | Beschreibung |
|---|---|
| Fortlaufende Incident-Erfassung | Laufende Incident-Erfassung, die die Instanz Now Platform ] für neue Incidents vom Mandanten Microsoft Azure abruft. Security Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung übereinstimmen. |
| Abfrageschritt (Minuten) | Abfragehäufigkeit, die in Minuten definiert ist. |
| Incident-Erfassungszeit festlegen | Incident-Erfassung, die auf dem konfigurierten Datum und der Uhrzeit basiert.<br><br>Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall. |
| Eingabe Incident-Erfassungszeit | Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Einmaliger Abruf | Aktivieren Sie dieses Kontrollkästchen, um das einmalige Abrufen historischer Azure Sentinel-Incidents zuzulassen und dann den Datenabgleich durchzuführen. Wenn Sie dieses Kontrollkästchen aktivieren, ruft die Anwendung alle offenen und geschlossenen Azure Sentinel-Incidents für den Zeitraum bis zu ungefähr 6 Monaten ab.<br><br>Bei der Verarbeitung der Daten werden sowohl laufende Incidents als auch Verlaufsdaten abgerufen, aber die Verarbeitung der laufenden Incidents hat Vorrang vor dem Abrufen historischer Daten. Andernfalls kann das Abrufen historischer Daten je nach Dauer und Anzahl der erfassten Incidents einige Zeit in Anspruch nehmen .<br><br>**Hinweis:**<br>Die abgerufenen historischen Azure Sentinel-Incidents werden Deduplizierungsprüfungen unterzogen, um Duplikate in der Security Incident Response-Anwendung zu verhindern. |
| Seit Datum | Das Datum, seit dem die historischen Incidents aus Azure Sentinel erfasst wurden.<br><br>**Hinweis:**<br>Die Incident-Daten werden ungefähr aus den letzten 6 Monaten abgerufen. |

Auf der Planungsseite können Sie definieren, wie und wann Incidents aus dem -Mandanten Microsoft Azure abgerufen werden.

2. Um zur Seite „Zusätzliche Optionen“ zu navigieren, klicken Sie auf **Fortfahren**.

### Automatisieren Sie die Aktualisierungen und Abschlüsse von Incidents anhand des Incident-Status SIR .

Automatisieren Sie die Aktualisierungen und Abschlüsse von Incidents anhand des Incident-Status SIR. Die Microsoft Azure Sentinel -Integration verfügt über eine bidirektionale Schnittstelle, die es beiden Incidents ermöglicht, Security Incidents zu erstellen und die Incidents zu aktualisieren, nachdem der Security Incident erstellt oder geschlossen wurde.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Füllen Sie die Details im Formular aus.
   Befolgen Sie die Anweisungen, um die Konfiguration für die Aktualisierung von Incidents abzuschließen, wenn Sie einen Security Incident in SIRerstellen oder schließen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Automatisieren von Incident-Aktualisierungen“.**

| Kategorie | Feld | Beschreibung |
|---|---|---|
| Aktualisierungen der Incident-Erstellung | Aktualisiert den Status von Azure Sentinel-Incidents bei SIR-Incident-Erstellung | Option, mit der Sie die automatisierte Funktion zur Aktualisierung von Incidents verwenden können. Der Incident-Status Microsoft Azure Sentinel wird in Microsoft Azure Incident mit den Kommentaren aktualisiert, nachdem der Incident SIR in Now Platformerstellt wurde. |
| | Anfangsstatusaktualisierung für Incident | Anfänglicher Incident-Status, der in der Umgebung Microsoft Azure Sentinel aktualisiert wird. Sie können **Neu** oder **Aktiv** als Status auswählen. |
| | Anfangskommentare, die an den Incident zurückgesendet werden | Anfangskommentare, die zum Incident in der Umgebung Microsoft Azure Sentinel veröffentlicht werden.<br><br>Bearbeiten Sie den Standardtext, der im Kommentarbereich angezeigt wird, indem Sie die Ersetzungsvariablen im Format ${field name}$ für ein beliebiges Feld im Incident-Formular SIR hinzufügen oder ändern. |
| Updates zum Incident-Abschluss | Schließen von Azure Sentinel-Incidents nach SIR-Incident-Abschluss | Option, mit der Sie die automatisierte Funktion zur Aktualisierung des Incident-Status verwenden können. Microsoft Azure Sentinel Incidents werden im Incident Microsoft Azure mit den Kommentaren geschlossen, nachdem der Incident SIR im Incident Now Platform] geschlossen wurde. |
| | Statusaktualisierung für Abschluss-Incident | Statusaktualisierung im Incident Microsoft Azure Sentinel, wenn der Incident in SIRgeschlossen wird. |
| | Abschlusskommentare werden an den Incident zurückgesendet | Kommentare, die an den Incident im Incident Microsoft Azure Sentinel gesendet werden, wenn der Incident in SIRgeschlossen wird.<br><br>Bearbeiten Sie den Standardtext, der im Kommentarbereich angezeigt wird, indem Sie die Ersetzungsvariablen im Format ${field name}$ für ein beliebiges Feld im Incident-Formular SIR hinzufügen oder ändern. |
| | Incident-Klassifizierung und Abschlussgrund | Methode für die Incident-Klassifizierung und den Abschlussgrund, die zum |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

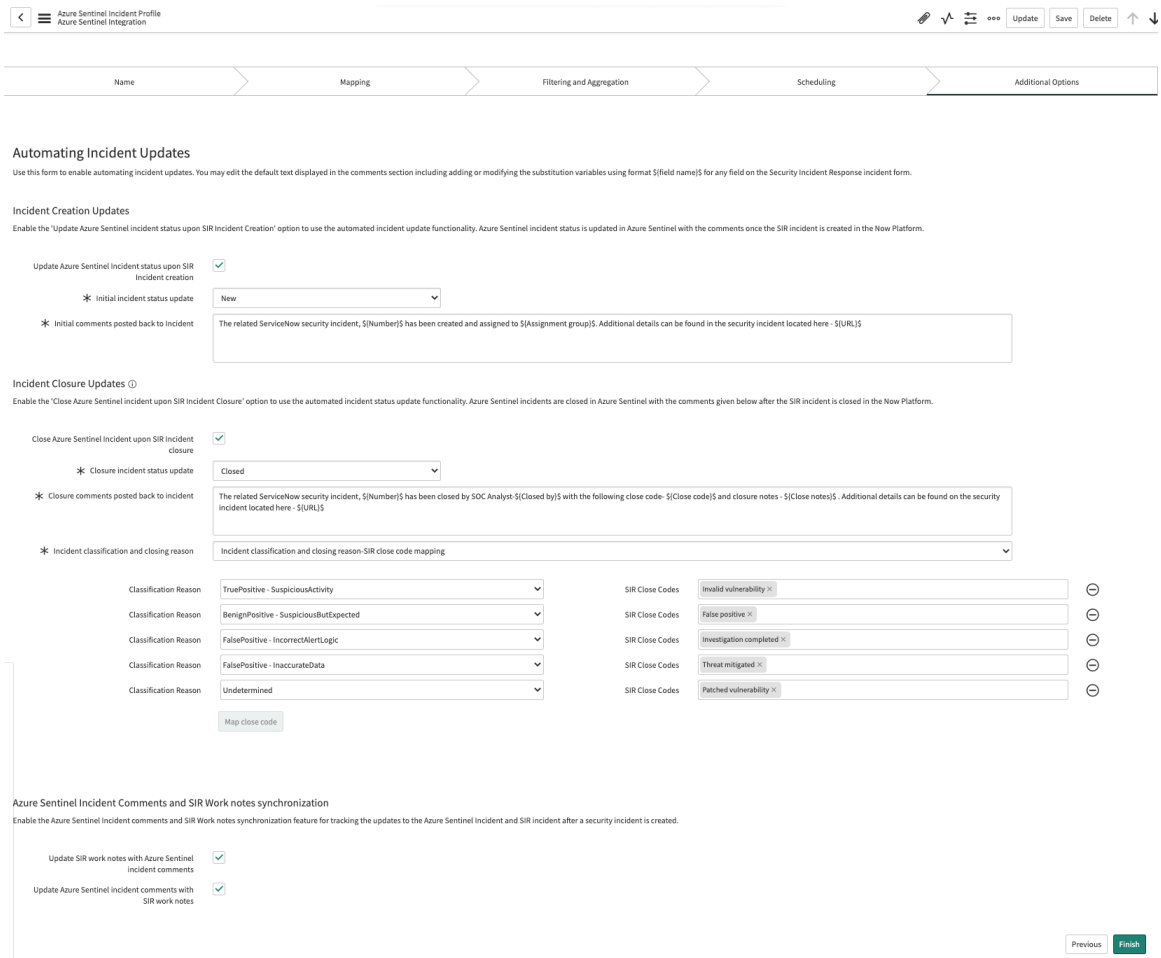
| Kategorie | Feld | Beschreibung |
|---|---|---|
| | | Schließen des Incident in der Microsoft Azure Sentinel -Umgebung verwendet wird.<br><br>Wählen Sie die Methode **Standardmäßige Incident-Klassifizierung und Abschlussgrund** aus, um den Incident in der Umgebung Microsoft Azure Sentinel zu schließen. Wenn Sie diese Methode auswählen, müssen Sie die **standardmäßige Incident-Klassifizierung und den Abschlussgrund**definieren. Wenn Sie einen Incident in SIR schließen, wird der Incident-Status in Azure Sentinel ebenfalls mit der angegebenen **Standard-Incident-Klassifizierung und dem angegebenen Abschlussgrund**geschlossen.<br><br>Wählen Sie die **Zuordnungsmethode Incident-Klassifizierung und Abschlussgrund – SIR-Abschlusscode**, um die Incidents zu schließen und die Klassifizierungsgründe den Abschlusscodes SIR zuzuordnen. Sie können mehrere SIR Abschlusscodes einem einzelnen Klassifizierungsgrund zuordnen. Nachdem Sie einen Incident in SIR mit dem Abschlusscode geschlossen haben, wird der Incident-Status in Azure Sentinel ebenfalls mit der zugeordneten Incident-Klassifizierung und dem Abschlussgrund geschlossen.<br><br>Wenn der Klassifizierungsgrund und die Abschlusscodes SIR nicht zugeordnet sind oder keine Übereinstimmung gefunden wird, wird der Incident mit dem Standardklassifizierungsgrund „Nicht bestimmt“ in der Umgebung Microsoft Azure Sentinel geschlossen. |
| Synchronisierung von Azure Sentinel-Incident-Kommentaren und SIR-Arbeitsnotizen | SIR-Arbeitsnotizen mit Azure Sentinel-Incident-Kommentaren aktualisieren | Option, die Sie auswählen können, um Ihre Microsoft Azure Sentinel -Kommentare in den SIR -Arbeitsnotizen zu aktualisieren. Der Kommentar in den |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Kategorie | Feld | Beschreibung |
|---|---|---|
| | | Arbeitsnotizen SIR wird mit dem Präfix `Comment from Sentinel`angezeigt. Der Kommentar enthält auch die Sentinel-ID, Analystendetails und den Zeitstempel. |
| | Azure Sentinel-Incident-Kommentare mit SIR-Arbeitsnotizen aktualisieren | Option, die Sie auswählen können, um Ihre SIR Arbeitsnotizen in den Microsoft Azure Sentinel Incident-Kommentaren zu aktualisieren. Der Kommentar in Microsoft Azure Sentinel wird mit dem Präfix `Comment from ServiceNow`angezeigt. |

Das folgende Beispiel zeigt die Konfigurationsoptionen, die für die Automatisierung von Incident-Updates verfügbar sind.




**2.** Klicken Sie auf **Fertigstellen**.

## Nächste Maßnahme

Das Profil wird in den Status „Warten“ verschoben. Wenn die Bestätigungsmeldung anzeigt, dass das Setup und die Konfiguration abgeschlossen sind, können Sie das Profil aktivieren.

### Kopieren Sie ein Microsoft Azure Sentinel -Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein Profil zu erstellen. Wenn Sie mehrere Profile erstellen, können Sie die Einstellungen eines vorhandenen Profils wiederverwenden, indem Sie diese Profile kopieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

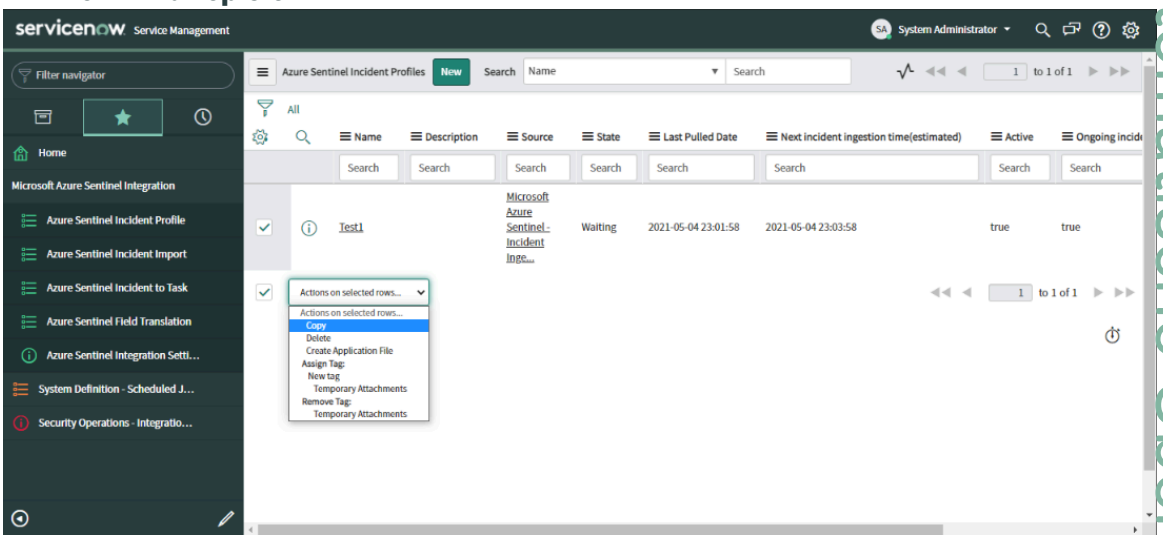
### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um die Erstellung doppelter Profile zu vermeiden. Das kopierte Profil ist ebenfalls deaktiviert (auf „falsch“ festgelegt), um sicherzustellen, dass Sie es nicht versehentlich aktivieren, bevor Sie die Konfiguration abgeschlossen haben. Sie können die Profile kopieren und vorhandene Zuordnungen für Security Incidents verwenden, die Sie bereits in der Vorschau angezeigt und überprüft haben.

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Profil**.
2. Wählen Sie in der Liste Azure Sentinel-Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie dann in der Liste Aktionen für ausgewählte Zeilen auf **Kopieren**, wie im folgenden Beispiel gezeigt.

**Ein Profil wird kopiert**

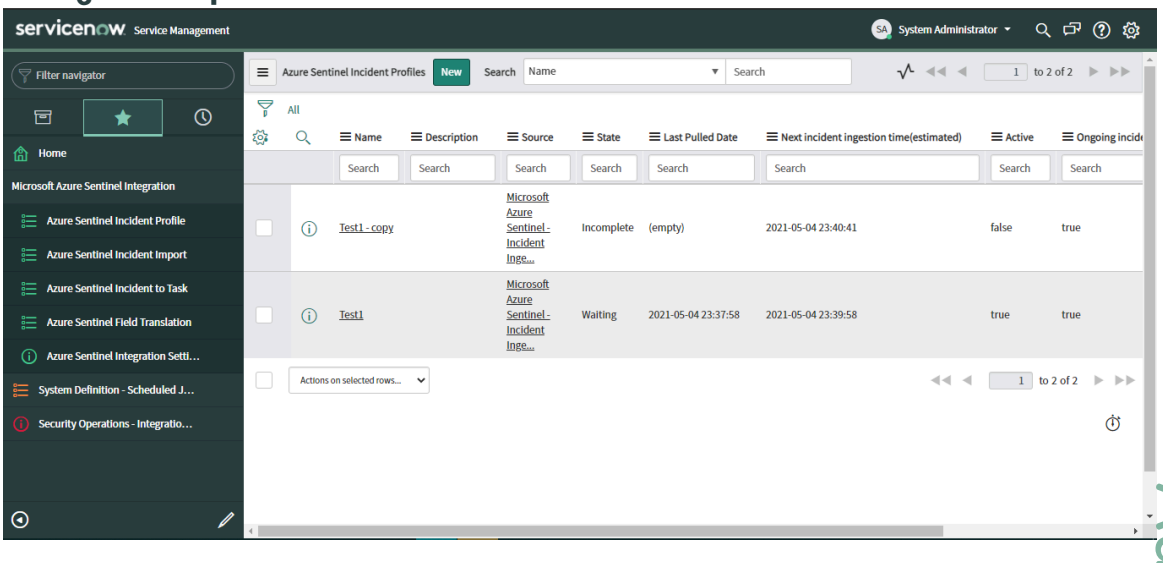



Das Profil wird kopiert und in der Liste angezeigt (siehe folgendes Beispiel). Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält das Wort „Kopie“. Obwohl das ursprüngliche Profil aktiviert ist (true), wird die Kopie an dieser Stelle deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen wie erforderlich für das neue Profil gelten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Anzeigen der kopierten Incident-Profile




Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Der Spaltenstatus Aktiv ist auf „false“ festgelegt, was bedeutet, dass das Profil aktiviert werden muss.

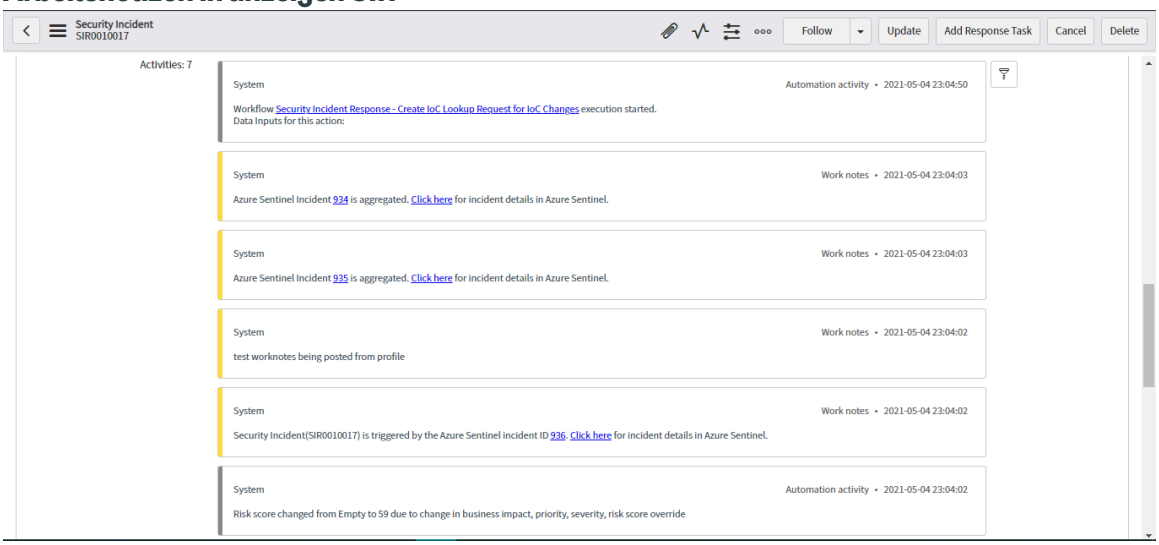
### SIR -Formular nach einer Incident-Erfassung

Nachdem Now Platform den Incident Microsoft Azure Sentinel ] erfasst hat, wird ein Security Incident erstellt und die Aktualisierungen werden an diesem Security Incident-Datensatz vorgenommen.

## Arbeitsnotizen

Eine Arbeitsnotiz wird veröffentlicht, wenn ein Incident zusammengefasst wird und Sie die Option **Arbeitsnotiz für neuen Incident** protokollieren in den Zusammenfassungskriterien für Incidentskonfiguriert haben. Das folgende Beispiel zeigt die Arbeitsnotizen in SIR.

### Arbeitsnotizen in anzeigen SIR




Wenn Sie auf die Incident-Nummer klicken, können Sie den internen Incident-Importdatensatz anzeigen, der die Incident-Rohdaten enthält. Das folgende Beispiel zeigt die Rohdaten zu Incidents in SIR.

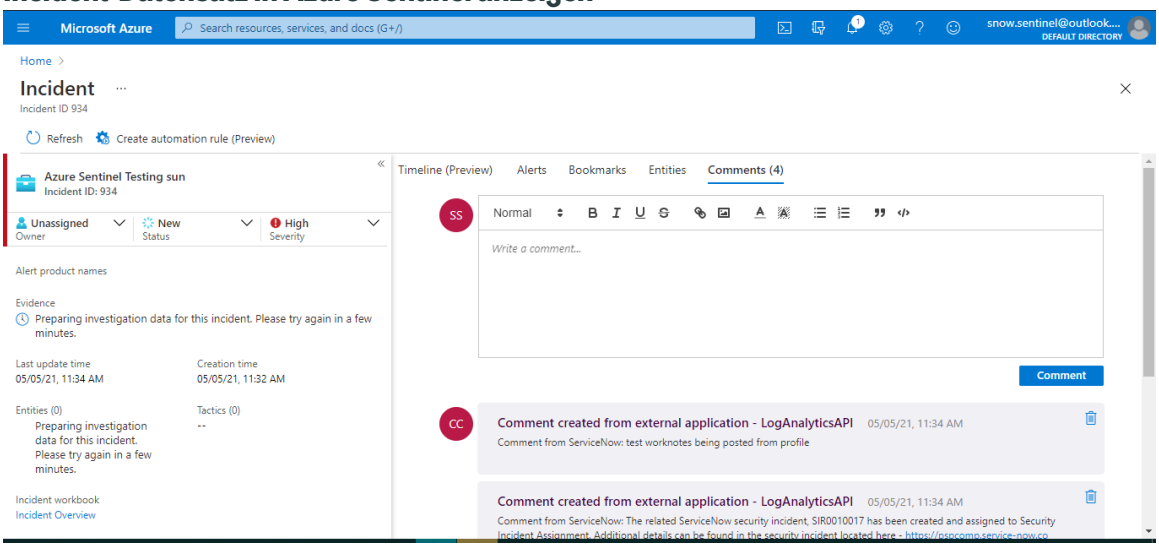


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Anzeigen der Incident-Rohdaten in SIR

Wenn Sie auf den Link Hier klicken **klicken**, können Sie den Datensatz in der Umgebung Microsoft Azure Sentinel anzeigen. Das folgende Beispiel zeigt den Datensatz in der Umgebung Microsoft Azure Sentinel.

### Incident-Datensatz in Azure Sentinel anzeigen

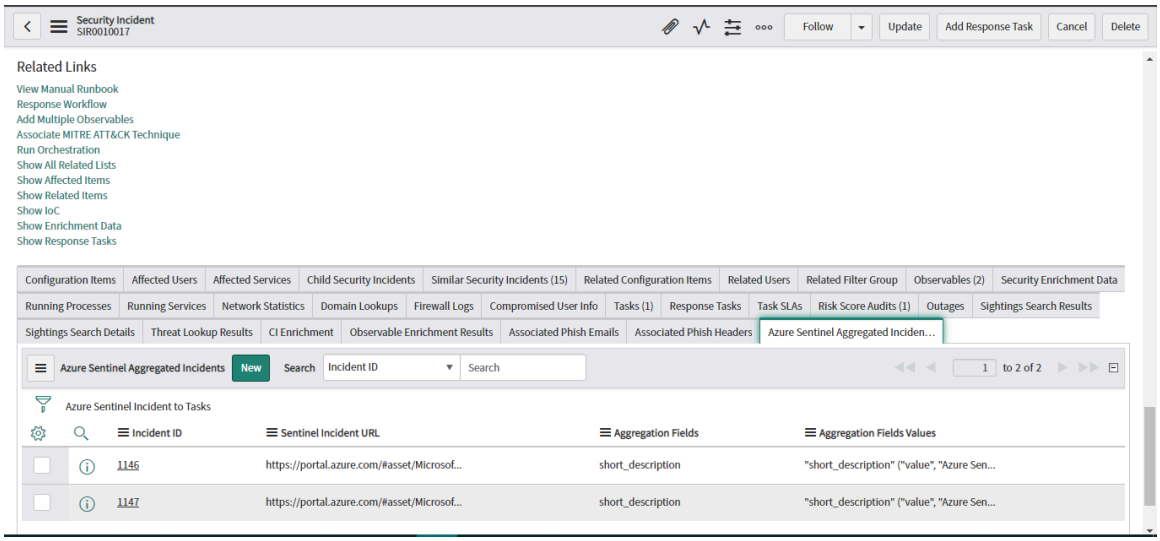



## Aggregierte Sentinel-Incidents

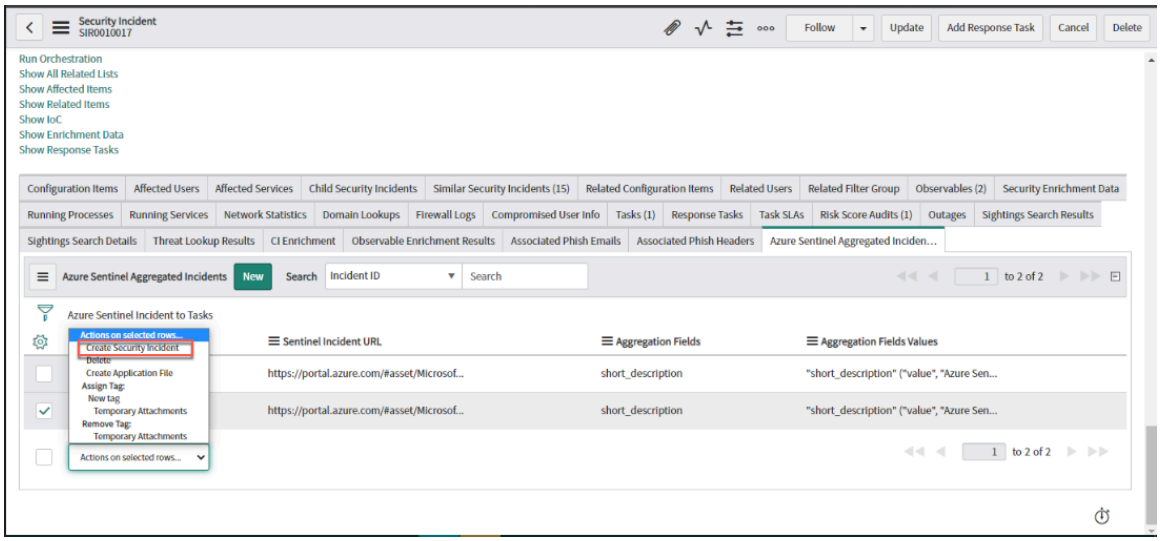
Aggregierte Sentinel-Incidents anzeigen: Zeigen Sie die Incidents an, die zum Security Incident zusammengefasst werden. Navigieren zu **Alle zugehörigen Listen anzeigen** > **Zusammengefasste Microsoft Azure Sentinel-Incidents**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Security Incident erstellen: Wählen Sie einen Incident aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie dann auf **Security Incident erstellen**. Mit dieser Option wird ein neuer Security Incident für den Incident erstellt. Dieser Incident wird aus dem übergeordneten Security Incident deaggregiert.



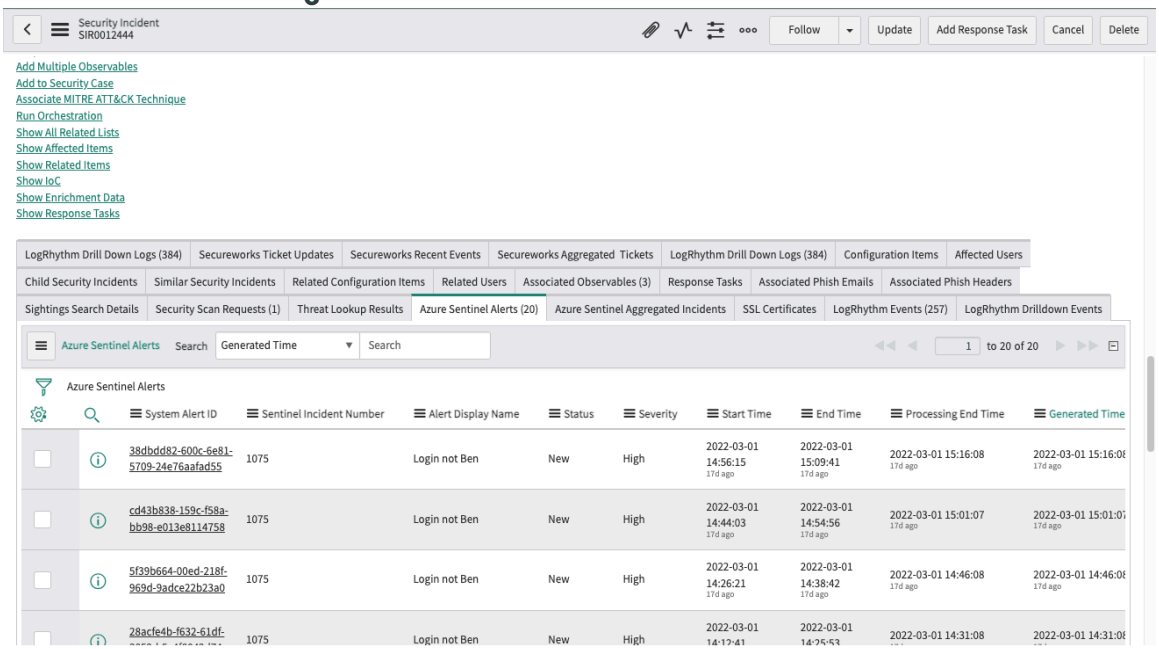

## Azure Sentinel-Warnungen

Um die Warnungen anzuzeigen, die dem Sentinel-Incident zugeordnet sind, der den Security Incident ausgelöst hat, navigieren Sie zu **Alle zugehörigen Listen anzeigen** > **Azure Sentinel-Warnungen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Azure Sentinel-Warnungen




### Überprüfen Sie die Integrationseinstellungen von Microsoft Azure Sentinel .

Überprüfen Sie die Integrationseinstellungen von Microsoft Azure Sentinel, damit Sie die Systemeigenschaften an Ihre Umgebung anpassen können.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Integration: Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

#### Microsoft Azure Sentinel Integrationseinstellungen

| Eigenschaftsname | Beschreibung |
|---|---|
| Erzwingen Sie ein Limit für die Anzahl der Tage, für die Beispieldaten abgerufen werden können.<br><br>sn_sec_sentinel.max_num_of_days_for_sample_data | Maximale Anzahl von Tagen, für die Sie Beispieldaten aus der Umgebung Microsoft Azure Sentinel abrufen können.<br>Typ: Ganzzahl<br><br>Standardwert: 7 |
| Erhalten Sie Aktualisierungen im Zusammenhang mit neuen Warnungen, die mit SIR verknüpft sind.<br><br>sn_sec_sentinel.incident_updates | Aktivieren Sie die Option, um Incident-Updates zu erhalten.<br><br>Typ: Boolesch<br>Standardwert: True |
| Das Trennzeichen zum Aufteilen der Werte in Microsoft Azure Sentinel Feldzuordnungen. | Das Trennzeichen zum Aufteilen der Werte in Microsoft Azure Sentinel Feldzuordnungen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaftsname | Beschreibung |
| --- | --- |
| sn_sec_sentinel.delimiter | Typ: Zeichenfolge<br><br>Standardwert: ', ' (Komma mit Leerzeichen) |
| Erzwingen Sie eine Begrenzung der Anzahl der Beispiel-Incidents, die abgerufen werden können.<br><br>sn_sec_sentinel.max_num_of_sample_incidents_per_call | Maximale Anzahl von Beispiel-Incidents, die Sie aus der Umgebung Microsoft Azure Sentinel für die Erfassung abrufen.<br><br>Typ: Ganzzahl<br><br>Standardwert: 5<br><br>Maximaler Beispielwert: 20 |
| Erzwingen Sie eine Begrenzung der Anzahl von Sentinel-Incidents, die zu einem einzelnen Incident zusammengefasst werden können.<br><br>sn_sec_sentinel.max_aggregations_per_si | Grenzwert für Incident-Zusammenfassung für einen Security Incident. Wenn beispielsweise 102 Incidents vorhanden sind, werden die ersten 100 zu Security Incident_1 und die verbleibenden 2 zu Security Incident_2 zusammengefasst.<br><br>Typ: Ganzzahl<br><br>Standardwert: 100 |
| Erzwingen Sie eine Begrenzung der Anzahl von Security Incidents, die innerhalb von 24 Stunden erstellt werden können.<br><br>sn_sec_sentinel.max_si_per_day | Maximale Anzahl von Security Incidents, die innerhalb von 24 Stunden im Now Platformerstellt werden können.<br><br>Typ: Ganzzahl<br><br>Standardwert: 1000 |
| Maximaler Paginierungsgrenzwert für das Abrufen der Incident-Daten in einem REST-Aufruf.<br><br>sn_sec_sentinel.max_page_size | Paginierungsgrenze für das Abrufen der Incident-Daten in einem REST-Aufruf aus der Microsoft Azure Sentinel -Umgebung.<br><br>Typ: Ganzzahl<br><br>Standardwert: 100 |
| API-Versionswert für Incidents.<br><br>sn_sec_sentinel.sentinel_security_incident_api_version | Die Microsoft-API-Version zum Abrufen von Sentinel-Incidents.<br>Standardwert: 2021-10-01 |
| API-Versionswert für Warnungen.<br><br>sn_sec_sentinel.sentinel_security_alert_api_version | Die Microsoft-API-Version zum Abrufen von Sentinel-Warnungen.<br>Standardwert: 2021-10-01 |
| API-Versionswert für Entitäten.<br><br>sn_sec_sentinel.sentinel_security_entities_api_version | Die Microsoft-API-Version zum Abrufen von Sentinel-Entitäten.<br>Standardwert: 2021-10-01 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaftsname | Beschreibung |
| --- | --- |
| sn_sec_sentinel.logging.verbosity | Die Ausführlichkeitsstufe des Protokolls der Anwendung, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren:<br>○ **Fehler**<br>○ **warnen**<br>○ **Info**<br>○ **debuggen**<br>Standardwert: **info**. |

3. Klicken Sie auf **Speichern**.
   Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

### Domänentrennung und Microsoft Azure Sentinel -Integration

Domänentrennung wird für diese Anwendung unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

## Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

## Funktionsweise der Domänentrennung in der Microsoft Azure Sentinel -Integration

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie einen Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne.

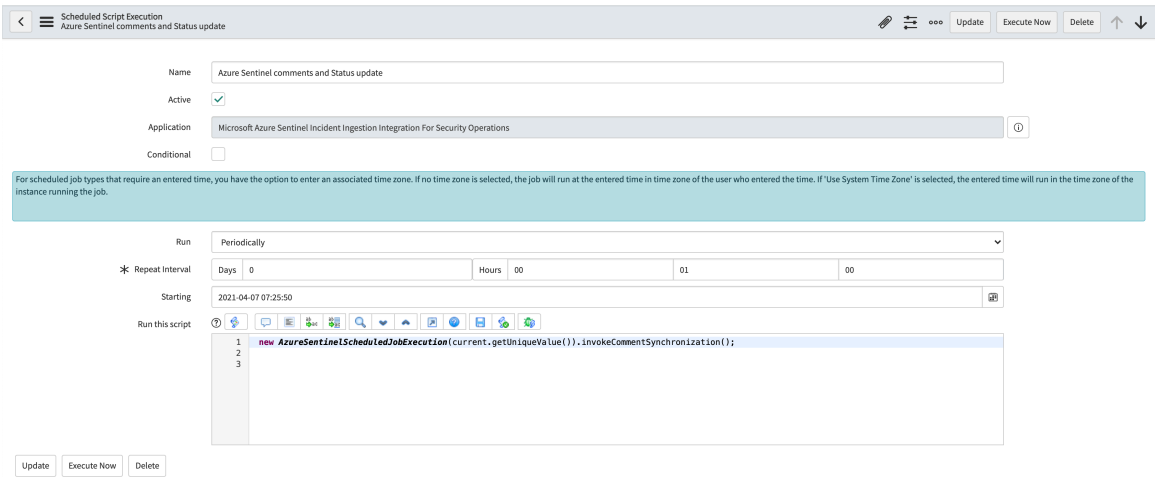
  **Hinweis:**
  Verwenden Sie beim Erstellen des Profils die Domänenauswahl, um eine Domäne auszuwählen. Erstellen Sie den Benutzer nicht in der übergeordneten Domäne und ändern Sie später die Domäne des Profils. Sie sollten einen Benutzer für jede Domäne für Ihr Profil mit der Rolle sn_si.admin haben. Verwenden Sie diesen Benutzer, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie die folgenden geplanten Aufgaben für jede Domäne:
  - Azure Sentinel ruft Warnungen und Entitäten ab
  - Azure Sentinel-Kommentarsynchronisierung
  - Azure Sentinel-Statusaktualisierung
  - Azure Sentinel – Profilprozess
  - Azure Sentinel – Prozessrohdaten
  - Azure Sentinel-Datenbereinigung
  - Historischer Azure Sentinel-Kommentarabruf

  **Hinweis:**
  Nachdem Sie die geplanten Aufgaben repliziert haben, suchen Sie im Navigator nach dem Modul „Module access policy“ (Modulzugriffsrichtlinien), und zeigen Sie die kürzlich erstellten Datensätze an, deren **Zielskript** die neu erstellten geplanten Aufgaben anzeigt. Ändern Sie den Feldwert **Ergebnis** in **Nachverfolgen**.

- Ändern **Sie Ausführen als** vom Systembenutzer in den Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne, und führen Sie dann die geplante Aufgabe aus.

Das folgende Beispiel zeigt, wie der Azure Sentinel-Kommentar- und Statusaktualisierungsauftrag repliziert und als Systembenutzer ausgeführt wird.




**Zugehörige Informationen**

Domänentrennung für Service Provider



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vergleich der Integrationen Microsoft Azure Sentinel und Microsoft Graph-Sicherheits-API mit SIR

Sie können die Unterschiede zwischen Microsoft Azure Sentinel - und Microsoft Graph-Sicherheits-API -Integrationen anzeigen und die richtige Integration mit Ihrer Now Platform -Instanz auswählen.

## Microsoft Azure Sentinel – Incident Ingestion – Übersicht

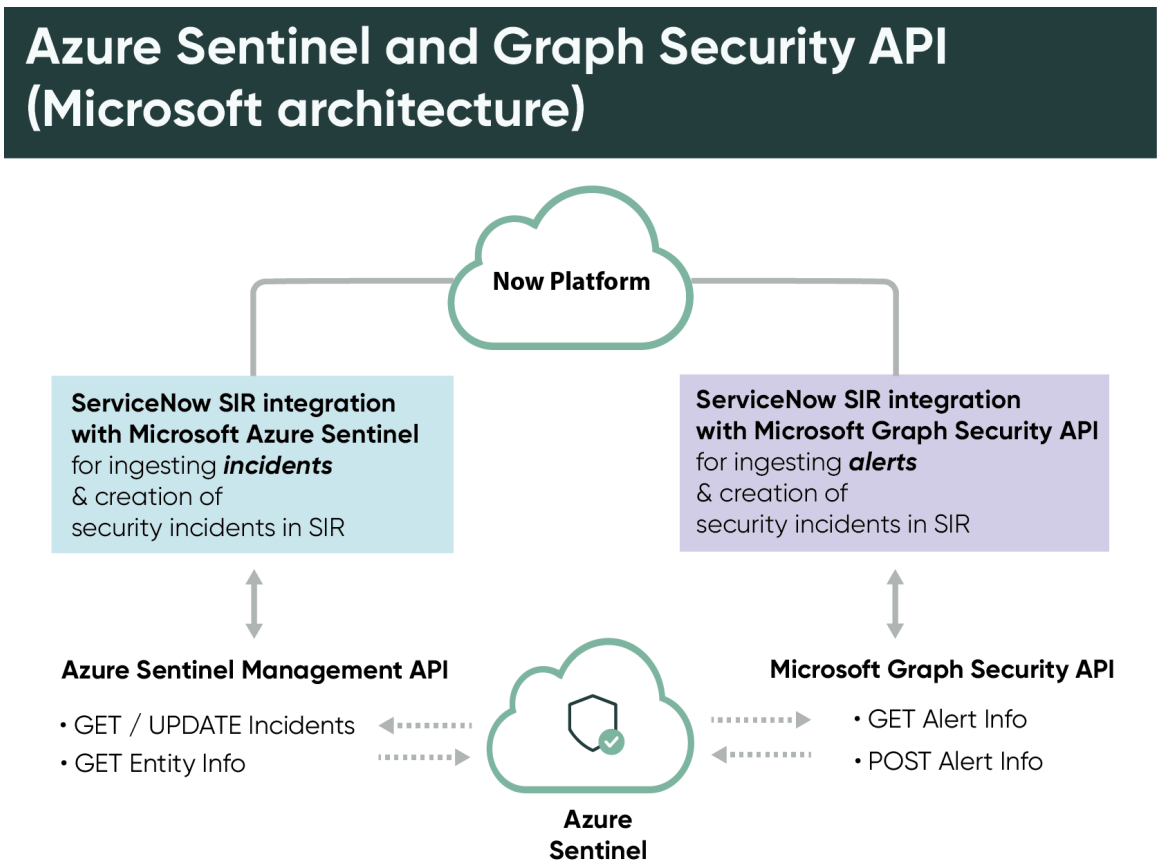
Microsoft Azure Sentinel ist eine cloudbasierte SIEM- (Security Information Event Management) und SOAR-Lösung (Security Orchestration Automated Response). Microsoft Azure Sentinel bietet intelligente Sicherheitsanalysen und Bedrohungsdaten im gesamten Unternehmen. Es bietet eine einzige Lösung für Warnungserkennung, Bedrohungstransparenz, proaktive Suche und Reaktion auf Bedrohungen.

## Microsoft Graph-Sicherheits-API – Übersicht

Microsoft Graph-Sicherheits-API ist ein intermediärer Service (oder Broker), der eine einzelne programmgesteuerte Schnittstelle für die Verbindung mehrerer Sicherheitsanbieter (nativ von Microsoft sowie ServiceNow Partner) bereitstellt.

Die Microsoft Graph-Sicherheits-API -Integration behebt diese Probleme, indem Microsoft Graph-Sicherheits-API verwendet wird, um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. Warnungen von Microsoft-Sicherheitsanbietern werden erfasst, und Security Incidents werden automatisch in Security Incident Responseerstellt.

### Zusammenfassung der Funktionsunterschiede




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Microsoft Azure Sentinel vs Microsoft Graph-Sicherheits-API

| Microsoft Azure Sentinel | Microsoft Graph-Sicherheits-API |
|---|---|
| Erfasst Microsoft Azure Sentinel Incidents zusammen mit Entitätsinformationen (sofern verfügbar) und automatisiert die Erstellung von Security Incidents in SIR. | Erfasst Warnungen von mehreren Sicherheitsanbietern (einschließlich Azure Sentinel) in einem Standardschema und automatisiert die Erstellung von Security Incidents in SIR. |
| Automatisiert Microsoft Azure Sentinel Incident-Statusaktualisierungen für Security Incident Response, sodass Sie Security Incidents erstellen und schließen können.<br>**Hinweis:**<br>ServiceNow aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss eines Security Incident. | Unterstützt Warnungsaktualisierungen (Änderung des Warnungsstatus und Schließung von Warnungen) für ausgewählte Sicherheitsanbieter.<br>**Hinweis:**<br>Weitere Informationen zu den von Microsoft Graph-Sicherheits-API unterstützten Sicherheitsanbietern finden Sie in der Microsoft-Dokumentation . |
| Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält:<br>• Die vorläufige Incident-Untersuchung befindet sich in Microsoft Azure Sentinel, die nachfolgende Untersuchung befindet sich in SIR.<br>• Microsoft Azure Sentinel Incidents in SIRerfassen | Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält:<br>• Führen Sie eine Incident-Untersuchung in SIRdurch.<br>• Erfassen Sie Microsoft Azure Sentinel Warnungen in SIR.<br>• Incidents werden nicht in Microsoft Azure Sentinelerstellt. |
| Warnung ist eine Entität in Microsoft Azure Sentinel. Sie können keine eigenständigen oder spezifischen Warnungen mit der Microsoft Azure Sentinel Management API abrufen. Sie können nur die Warnungsdaten abrufen, die einem Incident zugeordnet sind. Die mit dieser Integration verfügbaren Warnungsdaten sind umfangreicher als die mit Microsoft Graph-Sicherheits-APIverfügbaren Warnungsdaten. | Die normalisierten Warnungsdaten Microsoft Azure Sentinel sind verfügbar. Die Warnungsfelder Microsoft Azure Sentinel, die intern in Microsoft Graph-Sicherheits-APIzugeordnet sind und in Microsoft Graph-Sicherheits-APIverfügbar sind, können in dieser Integration verwendet werden. |
| | Sie können mit dieser Integration keine Warnungen in Microsoft Azure Sentinel aktualisieren. |

## Integration „Microsoft Defender for Endpoint“

Mit Microsoft Defender for Endpoint können Sie bekannte und unbekannte Bedrohungen auf jedem Endpunkt proaktiv untersuchen, analysieren und eindämmen.

Die Microsoft Defender for Endpoint -Integration hilft Sicherheitsanalysten, Security Incidents effizient zu untersuchen und zu beheben, ohne zwischen Tools navigieren zu müssen.

Sie können diese Integration verwenden, um Konfigurationen zu erstellen, um die Hostdetails, Details der angemeldeten Benutzer, Details zu zugehörigen Computern und andere Ergänzungsfunktionen abzurufen. Sie können die Isolierung eines Computers vom Zugriff auf die Netzwerke anfordern oder die Isolierung der Computer aufheben. Anforderungen können von den Genehmigern akzeptiert oder abgelehnt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Schlüsselfunktionen

Microsoft Defender for Endpoint bietet die folgenden Hauptfunktionen:

- Führen Sie eine Unternehmenssicherheitssuche durch, um potenzielle schädliche erkennbare Elemente über Endpunkte hinweg zu erkennen und Korrekturmaßnahmen zu ergreifen.
- Führen Sie Antwortaktionen durch, z. B. Host isolieren, Isolierung entfernen, App-Ausführung einschränken, Antivirenscan ausführen, App-Beschränkung entfernen sowie Datei anhalten und unter Quarantäne stellen.
- Erstellen oder aktualisieren Sie Indikatoren.
- Führen Sie eine Ergänzung erkennbarer Elemente durch, und rufen Sie Daten im Zusammenhang mit Indikatoren ab.

**Microsoft Defender for Endpoint**

| Erkunden | Installieren | Konfigurieren |
|---|---|---|
| Erste Schritte mit Microsoft Defender für Endpunkt | Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration | Konfigurieren Sie Profile und Security Incidents für Microsoft Defender for Endpoint |
| **Fähigkeitsprofil** | **Zusätzliche Konfigurationen** | **Verschiedenes** |
| Erstellen Sie ein Fähigkeitsprofil für die Microsoft Defender for Endpoint-Integration. | Zusätzliche Konfigurationen, die Sie in Microsoft Defender for Endpoint ausführen können | Erstellen und konfigurieren Sie ein Profil für Sichtungssuche und Indikatoren mit Microsoft Defender für Endpunkt. |

### Registrieren und konfigurieren Sie Microsoft Defender for Endpoint im Portal Microsoft Azure.

Registrieren Sie die Anwendung Microsoft Defender for Endpoint im Microsoft Azure-Portal, und gewähren Sie Lese- und Schreibzugriff auf die Anwendung.

**Vorbereitungen**
Erforderliche Rolle: Anwendungsentwickler, Mandantenadministrator.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Melden Sie sich beim Microsoft Azure-Portal an.
2. Geben Sie App-Registrierungen in das Suchfeld ein, und klicken Sie auf **Neue Registrierung**klicken.
3. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, und klicken Sie auf **Registrieren**.
   Ein Beispielname ist Microsoft Defender for Endpoint. Der Umleitungs-URI wird verwendet, während die Administratoreinwilligung für die Anwendung erteilt wird.
4. Wählen Sie auf der Seite „ **App registrations** “ die Anwendung aus, die Sie in Schritt 3 registriert haben.
5. Wählen Sie unter Verwalten die Option **Zertifikate und geheime Schlüssel**aus.
6. Um einen geheimen Clientschlüssel zu erstellen, wählen Sie **Neuer geheimer Clientschlüssel**aus.
7. Kopieren Sie den geheimen Clientschlüssel, und speichern Sie ihn.

   Falls Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen geheimen Clientschlüssel generieren.
8. Navigieren zu **Verwalten** > **API-Berechtigungen**.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster API-Berechtigungen anfordern auf die Registerkarte **APIs, die meine Organisation verwendet**.
11. Suchen Sie nach **WindowsDefenderATP**und wählen Sie es aus.
12. Wählen Sie in den WindowsDefenderATP-Berechtigungen **Anwendungsberechtigungen**aus.
    Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt wird.
13. Fügen Sie die folgenden Berechtigungen auf Anwendungsebene hinzu, und erteilen Sie die Administratoreinwilligung für die neu hinzugefügten API-Berechtigungen.

| Berechtigung | Anzeigename der Berechtigung |
|---|---|
| Computer.Lesen.Alle | Lesen Sie alle Computerprofile |
| Benutzer.Lesen.Alle | Benutzerprofile lesen |
| Rechner.Isolieren | Computer isolieren |
| Computer.Ausführung einschränken | Beschränken Sie die Codeausführung |
| Computer.Scan | Scannen Sie den Computer |
| Computer.StoppUndQuarantäne | Stoppen und unter Quarantäne stellen |
| URL.Lesen.Alle | URLs lesen |
| Datei.Lesen.Alle | Dateiprofile lesen |
| Ip.Lesen.Alle | Lesen Sie IP-Adressprofile |
| Ti.LesenSchreiben.Alle | Indikatoren lesen und schreiben |

### Beginnen Sie mit der Integration von Microsoft Defender for Endpoint .

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung Microsoft Defender for Endpoint aus dem ServiceNow Store installieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vorbereitungen**
Erforderliche Rolle: admin

Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen für Now Platform und Security Incident Response (SIR) zugewiesen haben. | Die folgenden Rollen sind erforderlich:<br>**1.** Sie müssen über die Rolle „Systemadministrator“ (admin) verfügen, um die Anwendung für die Integration zu installieren.<br>**2.** Sie benötigen die Rolle „Security Incident-Administrator“ (sn_si.admin), um die Integration zu konfigurieren sowie Profile zu erstellen, zu aktivieren und zu entfernen.<br>**3.** Um mit Security Incidents arbeiten zu können, benötigen Sie die Rolle „Security Incident-Analyst“ (sn_si.analyst). Benutzer mit dieser Rolle können alle in der Integration verfügbaren Fähigkeiten initiieren. |
| Vergewissern Sie sich, dass die zur Unterstützung der Integration erforderlichen ServiceNow-Kernanwendungen installiert und aktiviert sind, bevor Sie die Anwendung installieren. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation zu gewährleisten:<br>**1.** Security Incident Response<br>**2.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime)<br>**3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) |
| Vergewissern Sie sich, dass Sie eine Genehmigungsgruppe erstellt haben, bevor Sie die Genehmigungsoption für Profile aktivieren. | Ein optionaler Genehmigungsworkflow ist verfügbar, um Hostcomputer zu isolieren, sie im Netzwerk wiederherzustellen und zusätzliche Aktionen für den Endpunkt auszuführen.<br>Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünscht, aktivieren Sie während der Konfiguration der Profile die Option Genehmigung erforderlich. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | In einem Szenario, in dem das Profil verfügbar ist, hat die Profilkonfiguration für die Genehmigung Vorrang. In einem Szenario, in dem das Profil nicht verfügbar ist, werden die Genehmigungen basierend auf den Standardeinstellungen behandelt.<br><br>Als Sicherheitsadministrator können Sie die Genehmigung einrichten, während Sie die Profile und die Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in der Gruppenliste in Ihrer Instanz verfügbar sein.<br><br>Um Anforderungen zu überwachen und zu verarbeiten, die von Benutzern mit der Rolle „sn_si.analyst“ übermittelt werden, muss jedes Mitglied der Genehmigungsgruppe zu Meine Genehmigungen in Now Platform®navigieren. Alternativ finden die Genehmiger die Anforderungen, die ausschließlich für die Integration von Microsoft Defender for Endpoint übermittelt wurden, im Modul „Genehmigungen“. Weitere Informationen zum Erstellen einer Benutzergruppe finden Sie unter Benutzergruppen erstellen . |

## Nächste Maßnahme

Sie haben Ihre Now Platform® -Instanz erfolgreich für die Microsoft Defender for Endpoint -Integration eingerichtet. Der nächste Schritt besteht darin, die Anwendung Microsoft Defender for Endpoint aus dem ServiceNow Store für die -Integration zu installieren.

### Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration

Installieren und konfigurieren Sie die Microsoft Defender for Endpoint -Integration aus dem ServiceNow Store in Ihrer Now Platform -Instanz. Beginnen Sie mit der Erstellung von Fähigkeitsprofilen mithilfe der -Konfigurationen.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Prozedur

1. Laden Sie die Microsoft Defender for Endpoint-Integration aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel „Microsoft Defender für Endpunkt“, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die folgenden Felder des Formulars aus.



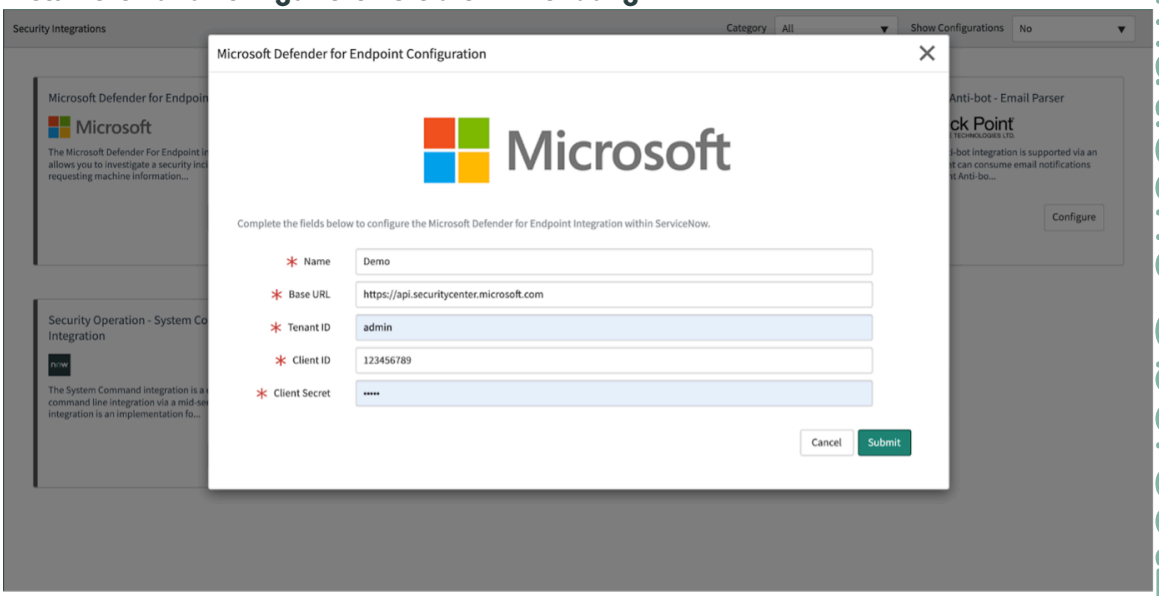
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie Microsoft Defender für Endpunkt

| | |
|---|---|
| Name | Name für die Microsoft Defender for Endpoint Instanzkonfiguration . |
| Basis-URL | Die Servicebasis-URL für Microsoft Defender for Endpoint |
| Mandanten-ID | Die Mandanten-ID Microsoft Defender for Endpoint. Alle Aktionen werden in dieser Instanz ausgeführt. |
| Client-ID | Client-ID für die Anwendung, die Sie im Microsoft Azure-Portal registriert haben |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel für Ihre registrierte Anwendung. |

5. Klicken Sie auf **Absenden**.

### Installieren und konfigurieren Sie die Anwendung




## Ergebnisse

Die Konfigurationsliste Microsoft Defender for Endpoint wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für Microsoft Defender for Endpointabgeschlossen.

### Microsoft Defender for Endpoint Standardeinstellungen

Es gibt zusätzliche Konfigurationseinstellungen, die Sie nach Abschluss der Installation vornehmen müssen.

Nach Abschluss der Installation finden Sie das Modul „Standardeinstellungen“ unter der Anwendung Microsoft Defender for Endpoint im linken Navigationsbereich. Sie enthält die Standardeinstellungen für verschiedene Microsoft Defender for Endpoint -Funktionalitäten.

Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt).

## Zusätzliche Konfigurationen

Im Folgenden finden Sie zusätzliche Konfigurationseinstellungen:

Automatische Übersetzung

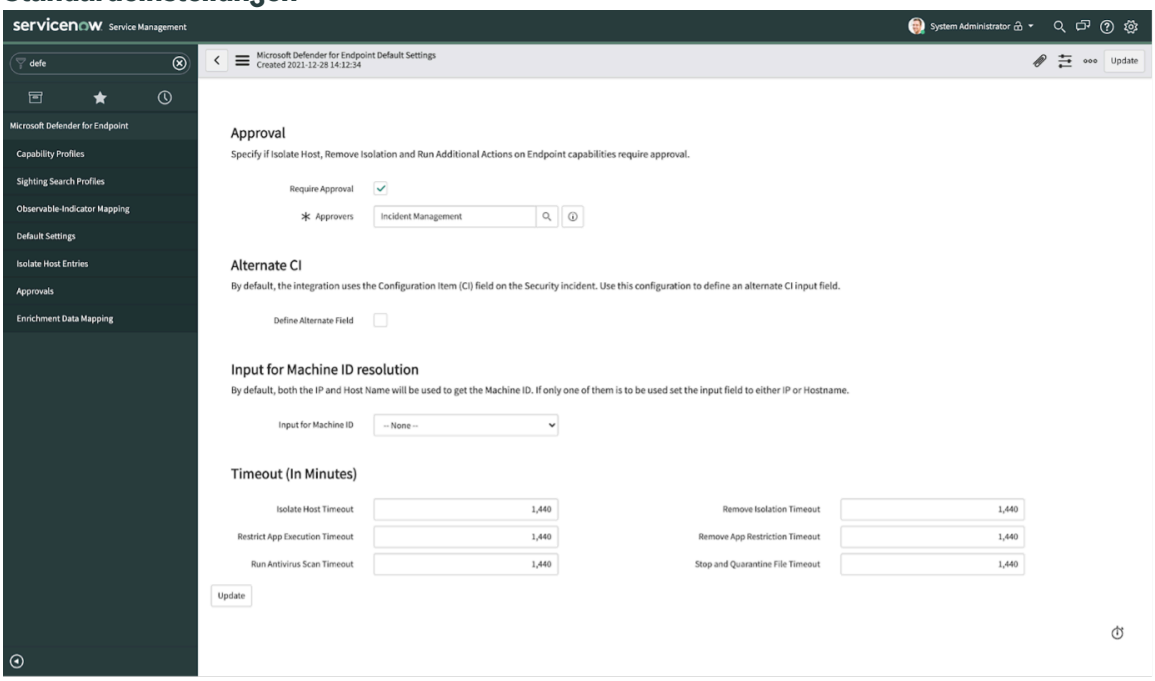
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Genehmigung**: Diese Genehmigung gilt speziell für die Aktionen „Host isolieren“, „Hostisolierung entfernen“ und zusätzliche Aktionen wie „App-Ausführung einschränken“, „App-Beschränkung entfernen“ und „Virenscan ausführen“. Sie können diese Genehmigung nur verwenden, wenn Aktionen direkt über die zugehörige Liste ausgelöst werden und keine Profile vorhanden sind. Wenn für diese Fähigkeiten Profile vorhanden sind, hat die Genehmigungskonfiguration im Profil Vorrang.
  - **Genehmigung**erforderlich: Wenn Sie „Genehmigung erforderlich“ aktivieren, ist das Feld **Genehmiger**im Formular verfügbar.
  - **Genehmiger**: Liste der Genehmigergruppen. Nachdem Sie eine Anforderung gesendet haben, ist eine Genehmigung durch die Gruppe erforderlich, um die Anforderung abzuschließen.
- **Alternatives CI**: Wenn Sie dieses Kontrollkästchen aktivieren, wird die Liste der Felder angezeigt, in denen ein alternatives CI an die Fähigkeit übergeben werden kann. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“. Verwenden Sie diese Konfiguration, um ein alternatives CI-Eingabefeld nur für die Fähigkeit „Zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Verwenden Sie für die anderen Fähigkeiten die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, übernehmen die Fähigkeiten das CI-Feld aus dem Security Incident-Formular.
- **Eingabe für Auflösung der Agent-ID**: Standardmäßig werden IP und Hostname verwendet, um die Agent-ID abzurufen. Wenn Sie nur eine davon verwenden möchten, legen Sie das Eingabefeld entweder auf IP oder Hostname fest.
- **Zeitüberschreitung**:
  - Zeitüberschreitung für**Hostisolierung (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeiten „Host isolieren“ an.
  - Zeitüberschreitung für**Isolierung entfernen (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „Zeitüberschreitung für Isolierung entfernen“ an.
  - Zeitüberschreitung für**App-Ausführung einschränken (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „App-Ausführung einschränken“ an.
  - Zeitüberschreitung für App-Beschränkung**entfernen (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „App-Beschränkung entfernen“ an.
  - Zeitüberschreitung für**Antivirus-Scan ausführen (in Minuten):** Gibt den Ausführungsschwellenwert für die Funktion „Antivirus-Scan ausführen“ an.
  - Zeitüberschreitung für**Stoppen und Quarantäne von Dateien (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „Datei stoppen und unter Quarantäne stellen“ an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Standardeinstellungen




## Ordnen Sie die Indikatortypen Microsoft Defender for Endpoint zu

Ordnen Sie den erkennbaren Typ ServiceNow dem Indikatortyp Microsoft Defender for Endpoint zu. Diese Zuordnung wird in den Aktionen „Anreicherung erkennbarer Elemente“ und „Indikator erstellen“ in Microsoft Defender verwendet.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst (schreibgeschützt)

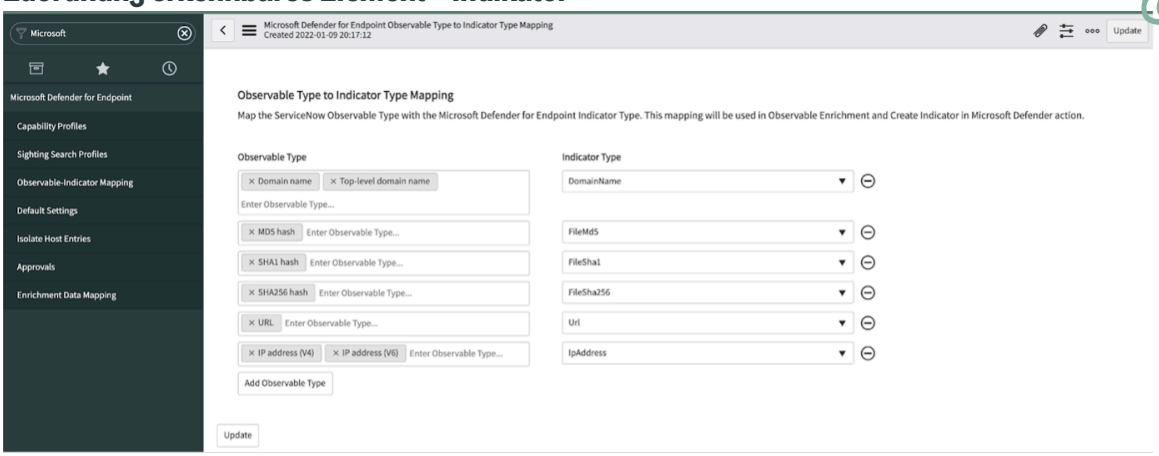
### Warum und wann dieser Vorgang ausgeführt wird

In einem Szenario, in dem der erkennbare Typ keinem Indikatortyp zugeordnet ist, sind solche erkennbaren Elemente nicht für die Ergänzung erkennbarer Elemente und die Indikatorerstellung in Microsoft Defender für Endpunkt geeignet.

### Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Zuordnung erkennbares Element – Indikator**.

### Zuordnung erkennbares Element – Indikator




2. Fügen Sie einen erkennbaren Typ auf eine der folgenden Arten hinzu, oder aktualisieren Sie ihn:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Erkennbaren Typ**hinzufügen.
- Um das erkennbare Element für die Zuordnung des Indikatortyps zu aktualisieren, klicken Sie auf eine vorhandene Zeile.

3. Um die Zuordnung zu speichern, klicken Sie auf **Aktualisieren**.

### Erstellen Sie ein Fähigkeitsprofil für die Microsoft Defender for Endpoint -Integration

Erstellen Sie ein Profil, und wählen Sie die Fähigkeiten Microsoft Defender for Endpoint aus, die das Profil ausführen soll.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Profile werden erstellt, um die Fähigkeiten zu vereinen oder zu gruppieren, was Analysten bei der Durchführung der Untersuchung oder Korrektur helfen würde. Sie können dem Profil die folgenden Fähigkeiten hinzufügen:

- Hostdetails abrufen
- Angemeldete Anwender abrufen
- Host isolieren
- Isolation entfernen

Sie können die Fähigkeiten „Host isolieren“ und „Hostisolierung entfernen“ nicht mit anderen Fähigkeiten verbinden, während Sie ein Profil erstellen. Profile für diese Fähigkeiten müssen einzeln erstellt werden. Während hingegen die Fähigkeiten „Hostdetails abrufen“ und „Angemeldete Benutzer abrufen“ zusammengefasst werden können. Sie können Profile einzeln erstellen oder sie je nach Anforderung vollständig oder in Teilen zusammenfassen.

**Hinweis:**
Nachdem eine Fähigkeit in ein Profil aufgenommen wurde, kann sie nicht in ein anderes Profil aus derselben Quelle aufgenommen werden.

#### Prozedur

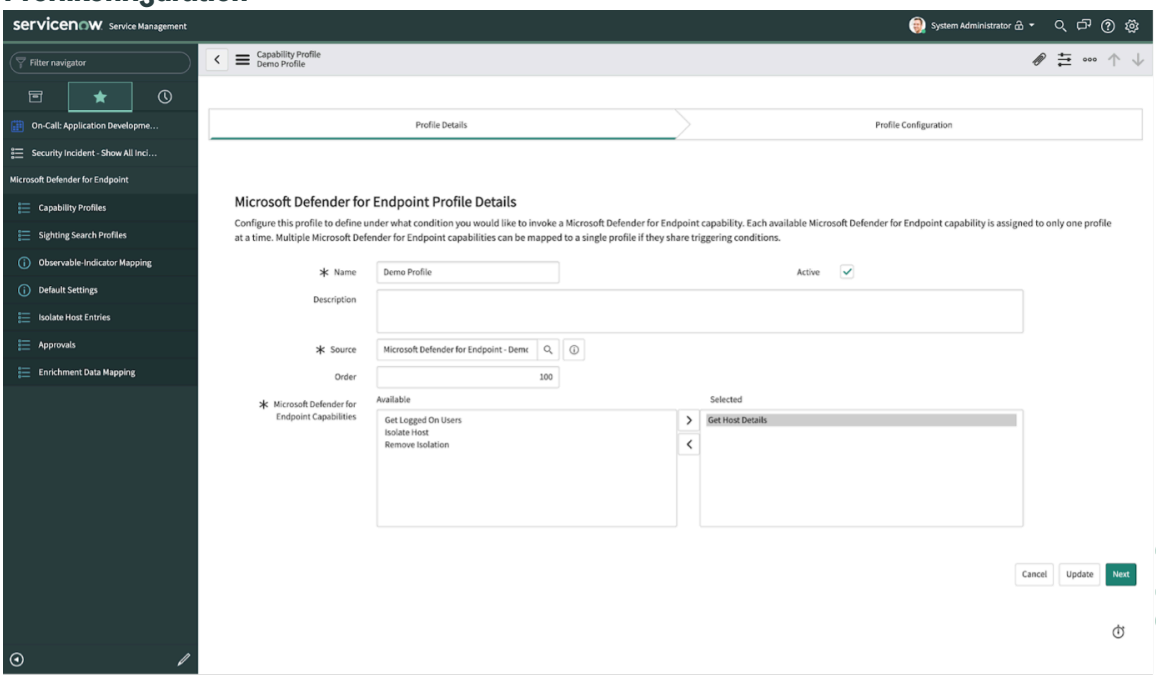
1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**.

   Die Liste der Microsoft Defender for Endpoint-Fähigkeitsprofile wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Profilkonfiguration




2. Klicken **Neu**.
3. Füllen Sie die Felder des Formulars aus.

#### Formular „Fähigkeitsprofil“

| Feld | Beschreibung |
|---|---|
| Name | Name für das Fähigkeitsprofil Microsoft Defender for Endpoint. Anhand dieses Namens können Sie den Profiltyp identifizieren und beschreiben. |
| Beschreibung | Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben. |
| Quelle | Name der Quelle Microsoft Defender for Endpoint. Nur konfigurierte Quellen sind in der Liste verfügbar. |
| Microsoft Defender for Endpoint-Fähigkeiten | Fähigkeiten des Profils Microsoft Defender for Endpoint. Wählen Sie die gewünschten Fähigkeiten für dieses Profil aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt. |
| Reihenfolge | Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen.<br><br>Der Flow mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300, 400. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Aktiv | Option, um anzugeben, dass das Profil aktiv ist. Nachdem das Profil aktiv ist, wird das Profil automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben. |

4. Klicken Sie auf, um mit der Profilkonfiguration fortzufahren **Weiter**.

### Nächste Maßnahme

Der nächste Schritt besteht in der Konfiguration Ihres Profils. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie die Wie-Profile sowie die konfigurierten und auslösenden Bedingungen überprüfen. Weitere Informationen finden Sie unter Auslösebedingungen in einem Konfigurationselement.

#### Auslösebedingungen in einem Konfigurationselement

Nachdem Sie ein Profil erstellt und die Microsoft Defender for Endpoint -Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass das Profil nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind.

## So lösen Sie Bedingungen in einem Konfigurationselement aus

Sie können Auslöserbedingungen festlegen, sodass das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der der Auslöserbedingung entspricht. Wenn die Auslöserbedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie für den Security Incident auf das Formular EDR-Profil ausführen klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in Now Platform Configuration Management Database (CMDB)gespeicherten Informationen abzugleichen. Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird CMDB durchsucht, um den Hostnamen oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname oder die IP-Adresse wird verwendet, um die Agent-ID auf Microsoft Defender for Endpoint aufzulösen und den Endpunkt zu identifizieren.

In einem idealen Szenario wird ein übereinstimmender Wert in der Datenbank gefunden, und Daten werden in der Konsole Microsoft Defender for Endpoint für das übereinstimmende Asset gesammelt. Die Daten für verschiedene Fähigkeiten werden in Ihre Instanz Now Platform Configuration Management Database (CMDB) abgerufen und in den zugehörigen Listen eines Security Incident angezeigt. Wenn das Feld Konfigurationselement (CI) im Security Incident nicht mit einem Hostnamen mit oder einer IP-Adresse ausgefüllt wird, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, das entweder den Hostnamen oder die auszuführende IP enthält die Agent-ID-Auflösung.

Während des Konfigurationsschritts der Profileinrichtung können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt auf Microsoft Defender for Endpointidentifizieren können. Sie können ein beliebiges Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich benutzerdefinierter Felder, die Sie erstellen. Durch die Auswahl dieses alternativen CI-Felds als Sicherung stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung für den zugeordneten Security Incident nicht ausgefüllt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Zu diesen Fähigkeiten gehören „Hostdetails abrufen“, „Angemeldete Benutzer abrufen“, „Host isolieren“ und „Isolierung entfernen“. Für alle zusätzlichen Aktionen muss das alternative CI im Modul „Standardeinstellungen“ konfiguriert werden.

### Konfigurieren Sie Profile und Security Incidents für die Microsoft Defender for Endpoint -Integration

Erstellen Sie ein Profil, und wählen Sie die Fähigkeiten Microsoft Defender for Endpoint aus, die das Profil ausführen soll. Sie müssen die Einstellungen so konfigurieren, dass das Profil nur unter den definierten Bedingungen ausgelöst werden kann.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt)

#### Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Bei Bedarf können Sie ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen und Filterbedingungen festlegen, damit das Profil automatisch ausgelöst werden kann, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

**Hinweis:**
Sie können erst zur Seite „Profilkonfiguration“ navigieren, nachdem Sie die Seite „Profildetails“ aufgerufen haben.

#### Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**.
2. Klicken Sie nach Abschluss des Abschnitts „Profildetails“ auf **Weiter**.
   Überprüfen und konfigurieren Sie die Abschnitte.
3. Wählen Sie im Abschnitt „Incident-Kriterien definieren (Automatisierung)“ die Option **Incident-Kriterien definieren** aus, um Microsoft Defender for Endpoint -Fähigkeiten im Profil automatisch auszulösen.
   Incident-Kriterien definieren (Automatisierung): Definieren Sie die Bedingungen für Security Incidents, die automatisch die Microsoft Defender for Endpoint-Fähigkeiten für das Profil auslösen. Wenn Sie die Option **Incident-Kriterien definieren** nicht auswählen, können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.

   **Hinweis:**
   Die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ können nicht automatisch ausgelöst werden.

   a. Wählen Sie in den **Filterbedingungen**das erforderliche Feld aus.
   b. Fügen Sie **neue Kriterien hinzu**, und definieren Sie auch die **ODER-** oder **UND-** Bedingung.
4. Aktivieren Sie im Abschnitt „Genehmigungen“ das Kontrollkästchen **Genehmigung** erforderlich, um eine zusätzliche Steuerungsebene bereitzustellen.

   Wenn Sie diese Option auswählen, haben Sie mehr Kontrolle bei der Verwendung der Microsoft Defender for Endpoint-Fähigkeiten zum Isolieren von Hostcomputern, Wiederherstellen im Netzwerk und Abrufen von Dateien.

   Die Option Genehmigungen in der Profilkonfiguration wird nur für die Funktionen „Host isolieren“ und „Hostisolierung entfernen“ angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Abschnitt „Zusätzliche Konfiguration“ die Option **Alternatives Feld** definieren aus, um ein alternatives Eingabefeld zu definieren.
   Zusätzliche Konfiguration: Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um die Microsoft Defender for Endpoint-APIs abzufragen .

   **Hinweis:**
   Weitere Informationen finden Sie unter Auslösebedingungen in einem Konfigurationselement.

   a. Wählen Sie die Option **Alternatives Feld definieren** aus.

   b. Wählen Sie das Eingabefeld aus **Alternatives CI-Auslöserfeld**.

6. Aktivieren Sie im Abschnitt Tags die **Checkbox Tag anzeigen**, um die Kennzeichnung von Security Incidents zu aktivieren. Der Profilname wird bei Aktivierung des Tags vorangestellt.

   Sie können Security Incidents optional mit Tags für Profil initiiert, Profil abgeschlossen und Profil fehlgeschlagen versehen. Standardmäßig ist diese Option für alle Profile deaktiviert.

7. Klicken **Fertig**.

### Überprüfen Sie die Auslöserbedingungsfilter

Validieren Sie das Profil, und stellen Sie sicher, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.analyst

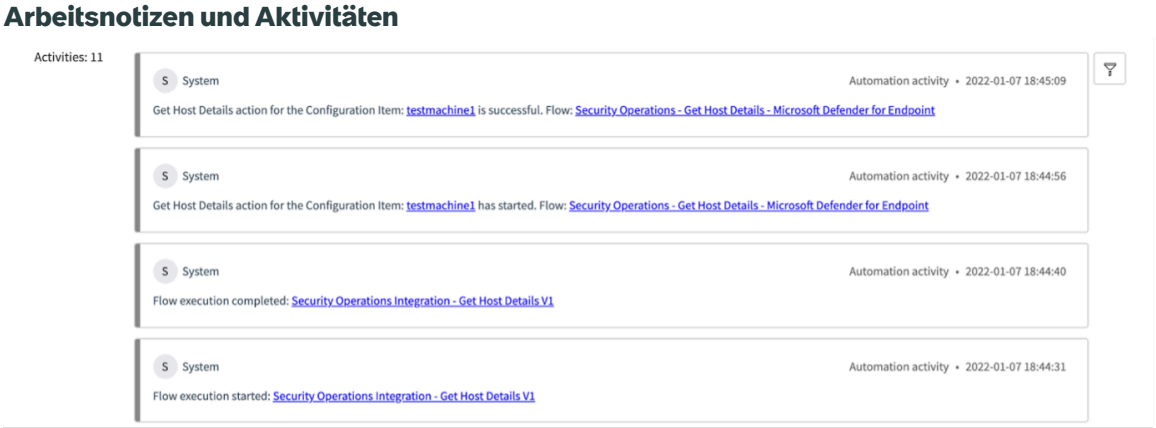
#### Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in den Now Platform® Security Incidents anzeigen.

#### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Um einen neuen Security Incident zu erstellen, wählen Sie **Neu**.
3. Um das entsprechende Profil auszulösen, geben Sie die Filterbedingungen an, die im Fähigkeitsprofil angegeben sind.
4. Klicken **Speichern**.
5. Um den Abschnitt „Arbeitsnotizen und Aktivitäten“ zu validieren, zeigen Sie die Datensätze an, die mit den Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ gekennzeichnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Um alle Daten in den zugehörigen Listen zu validieren, klicken Sie auf **Alle**zugehörigen Listen anzeigen.
7. Klicken Sie auf eine beliebige Registerkarte **Zugehörige Liste**, um die Details zu validieren. Beispiel: Hostdetails.

## Lösen Sie die Fähigkeiten Microsoft Defender for Endpoint über Zugehörige Links aus

Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Sie können nicht nur das Profil für das CI oder das alternative CI des Security Incident ausführen, sondern auch das Profil für CI-Werte in der zugehörigen Liste Configuration Item ausführen, indem Sie **Zugehöriges CI einbeziehen** im Dialogfeld auswählen. Dadurch werden auch die Daten für die CI-Werte abgerufen, die in der zugehörigen Liste vorhanden sind. Alternativ können Sie das Profil nur für die in der zugehörigen Liste enthaltenen CI-Werte ausführen.

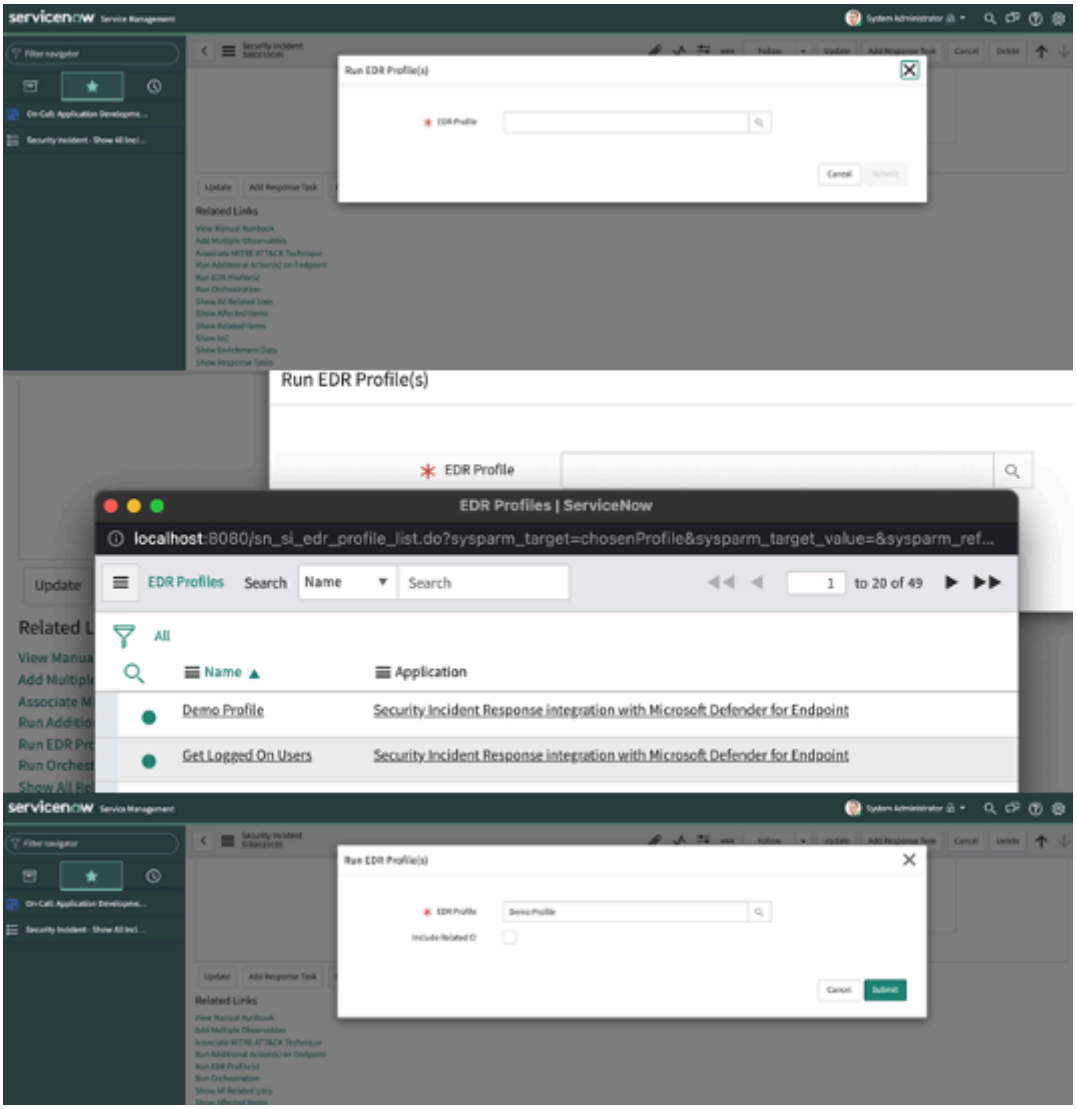
### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen Microsoft Defender for Endpoint.
3. Klicken Sie im Abschnitt Zugehörige Links auf **EDR-Profil(e) ausführen**.
4. Suchen Sie ein Profil, wählen Sie es aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wählen Sie ein Profil aus




Das ausgewählte Profil wird manuell ausgelöst.

5. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
6. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

## Lösen Sie Microsoft Defender for Endpoint aus der zugehörigen Liste „Configuration Item“ aus

Lösen Sie ein Fähigkeitsprofil manuell aus der zugehörigen Liste des Konfigurationselements aus.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident, den Sie überprüfen möchten, mit den Informationen Microsoft Defender for Endpoint.
3. Klicken **Alle zugehörigen Listen anzeigen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die zugehörige Liste Configuration Item.
5. Wählen Sie die hinzugefügten Konfigurationselemente aus.
6. Wählen Sie unter **Aktionen** für ausgewählte Zeilen eine Fähigkeit aus.
   Die ausgewählte Fähigkeit wird manuell ausgelöst.
7. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

### Zusätzliche Konfigurationen in Microsoft Defender for Endpoint

Die Microsoft Defender for Endpoint -Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Standardaktionen hinausgehen.

Microsoft Defender for Endpoint unterstützt die folgenden zusätzlichen Konfigurationen:

### Konfigurieren Sie die Fähigkeit „Host isolieren“ in Microsoft Defender for Endpoint

Isolieren Sie den Host basierend auf der Schwere des Angriffs vom Zugriff auf das Netzwerk in Microsoft Defender for Endpoint. Durch die Isolierung des Hosts vom Netzwerk können Sie weitere böswillige Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

#### Anforderungen für die Fähigkeit „Host isolieren“.

| Fähigkeit | Erforderlich | Beschreibung |
|---|---|---|
| Host isolieren | Isolierungstyp | (Erforderlich) Typ der Isolierung (Vollständig oder Selektiv). |
| | Anmerkung | (Erforderlich) Kommentar, der der Aktion zugeordnet werden soll. |

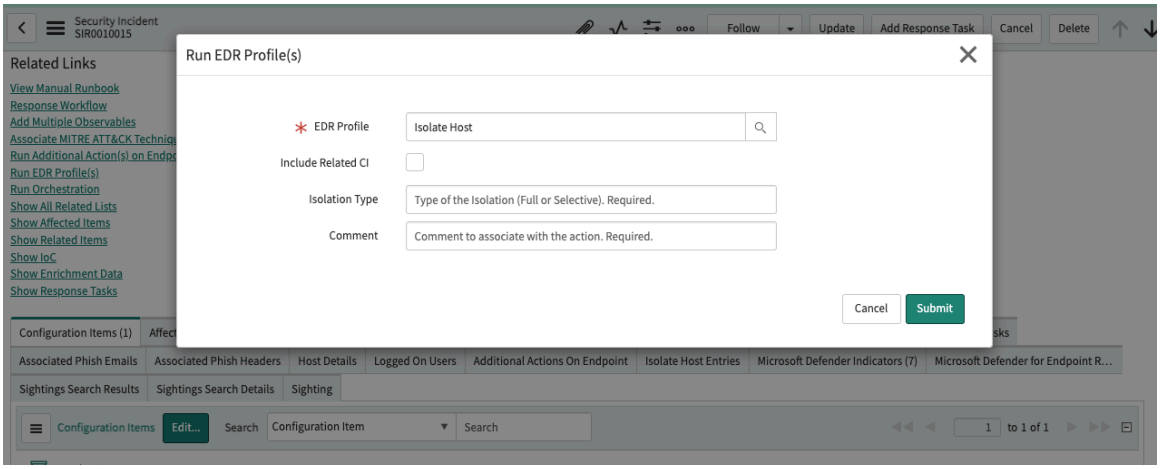
#### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt Zugehörige Links auf **EDR-Profil(e) ausführen**.
4. Wählen Sie ein Profil mit der **Fähigkeit Host isolieren** aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Host isolieren




Alternativ können Sie die folgenden Schritte ausführen:

**a.** Klicken Sie im Abschnitt „ **Zugehörige Listen“ auf Alle**zugehörigen Listen anzeigen.

**b.** Klicken Sie auf die zugehörige Liste **Configuration Item**.

**c.** Wählen Sie **Host isolieren** aus, und wählen Sie die entsprechenden Fähigkeiten aus.

5. Validieren Sie die Automatisierungsaktivität und den Aktivitätenbereich, und stellen Sie sicher, dass die Daten den Erwartungen entsprechen.
6. Zeigen Sie die Daten an, und validieren Sie die Details des isolierten Hosts in den zugehörigen Listen.

## Konfigurieren Sie die Funktion „Hostisolierung entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Isolierung eines Hosts, der zuvor in Microsoft Defender for Endpointvom Netzwerk isoliert war. Sie können andere böswillige Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

### Vorbereitungen

#### Anforderungen für die Fähigkeit „Isolierung entfernen“.

| Fähigkeit | Erforderliche Eingabe | Beschreibung |
|---|---|---|
| Isolation entfernen | Anmerkung | (Erforderlich) Kommentar, der der Aktion zugeordnet werden soll. |

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

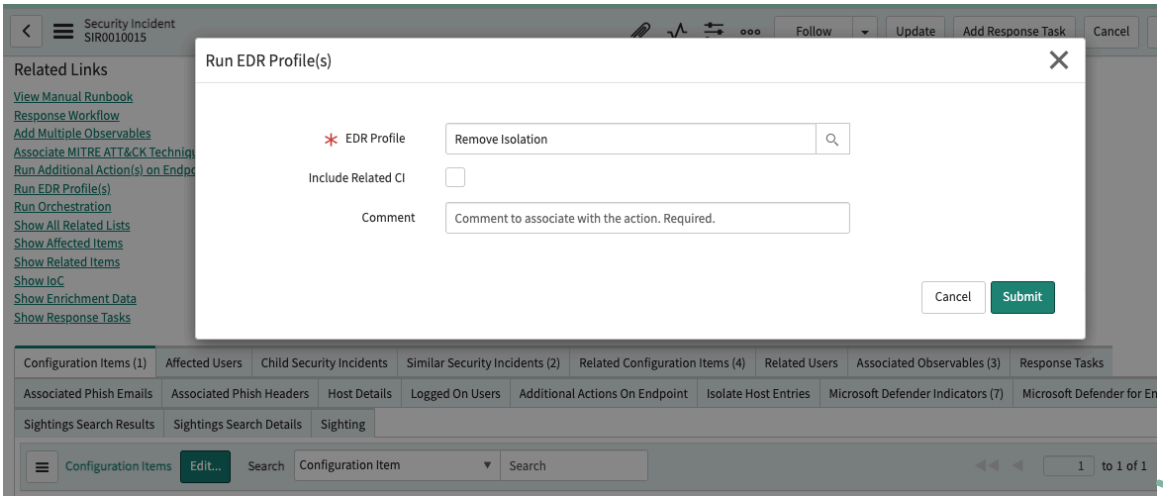
### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt Zugehörige Links auf **EDR-Profil(e) ausführen**.
4. Wählen Sie ein Profil mit der **Fähigkeit „Isolierung entfernen“** aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Isolation entfernen




Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „ **Zugehörige Listen“ auf Alle** zugehörigen Listen anzeigen.

b. Klicken Sie auf die zugehörige Liste **Configuration Item**.

c. Wählen **Sie Isolierung entfernen** aus, und wählen Sie die entsprechenden Fähigkeiten aus.

5. Validieren Sie die Automatisierungsaktivität und den Aktivitätenbereich.
6. Zeigen Sie die Daten an, und validieren Sie die Details des isolierten Hosts in den zugehörigen Listen.
7. Validieren Sie die Automatisierungsaktivitäten der Ausführung.

## Konfigurieren Sie die Funktion Antivirus-Scan ausführen in Microsoft Defender for Endpoint

Initiieren Sie per Remotezugriff einen Antivirenscan, um Malware zu identifizieren und zu beheben, die möglicherweise auf einem gefährdeten Gerät vorhanden ist. Führen Sie den Scan als Teil des Untersuchungs- oder Reaktionsprozesses aus.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

### Anforderungen für die Funktion „Antivirus-Scan ausführen“.

| Eingabe | Beschreibung |
|---|---|
| Scantyp | (Erforderlich) Typ des Scans (Vollständig oder Schnell). |
| Anmerkung | (Erforderlich) Kommentar, der der Aktion zugeordnet werden soll. |

### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.

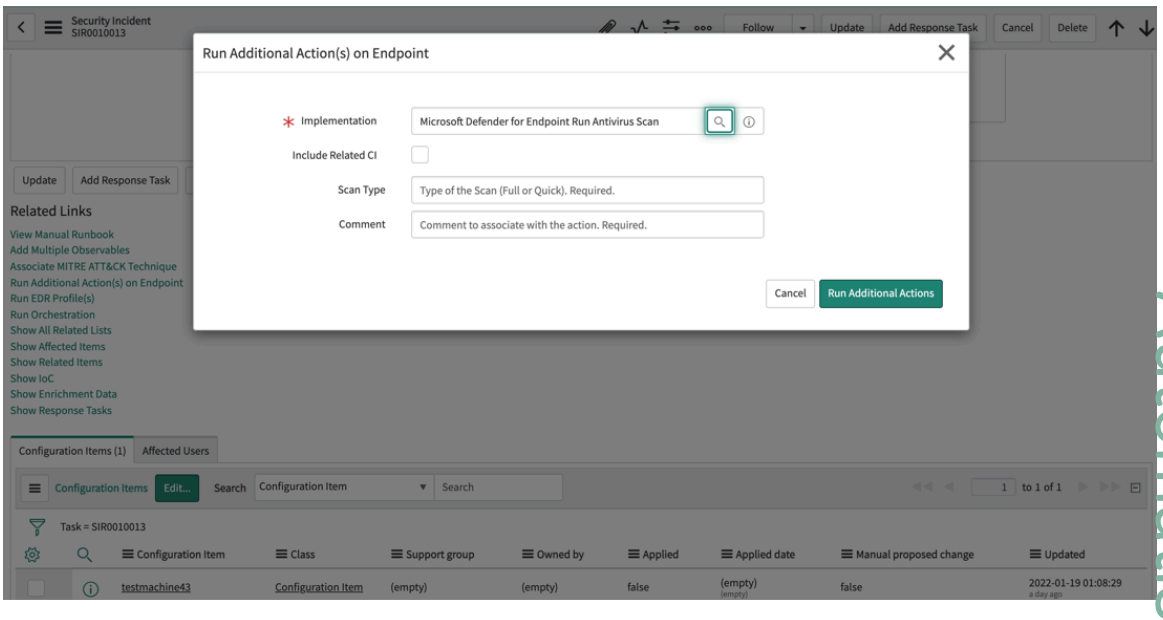


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.

**b.** Durchsuchen Sie die erforderliche Fähigkeit, und wählen Sie sie aus.
Klicken Sie beispielsweise auf die Fähigkeit **Antivirus-Scan** ausführen.

**Führen Sie einen Virenscan aus**




Alternativ können Sie die folgenden Schritte ausführen:

**a.** Klicken Sie im Abschnitt „ **Zugehörige Listen“ auf Alle**zugehörigen Listen anzeigen.

**b.** Klicken Sie auf die zugehörige Liste **Configuration Item**.

**c.** Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen die **Option Zusätzliche Aktionen für Endpunkt ausführen aus**.

Nachdem Sie die Implementierung der Fähigkeit **Antivirus-Scan** ausführen ausgewählt haben, werden die Eingabefelder **Zusätzlicher Scan-Typ** und **Kommentar** angezeigt.

**3.** Wählen Sie den **Scan-Typ** aus, den Sie ausführen möchten (Schnell oder Vollständig), und fügen Sie einen Kommentar hinzu, bevor Sie den Scan ausführen.

**4.** Um die Antivirenprüfung zu initiieren, klicken Sie auf **Zusätzliche Aktion ausführen**.

**5.** Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.

**6.** Validieren Sie den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

## Konfigurieren Sie die Funktion „App-Ausführung einschränken“ in Microsoft Defender for Endpoint

Um einen Angriff einzudämmen, beschränken oder sperren Sie ein Gerät und verhindern, dass nachfolgende Versuche potenziell schädlicher Programme ausgeführt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

### Anforderungen für die Fähigkeit „App-Ausführung einschränken“.

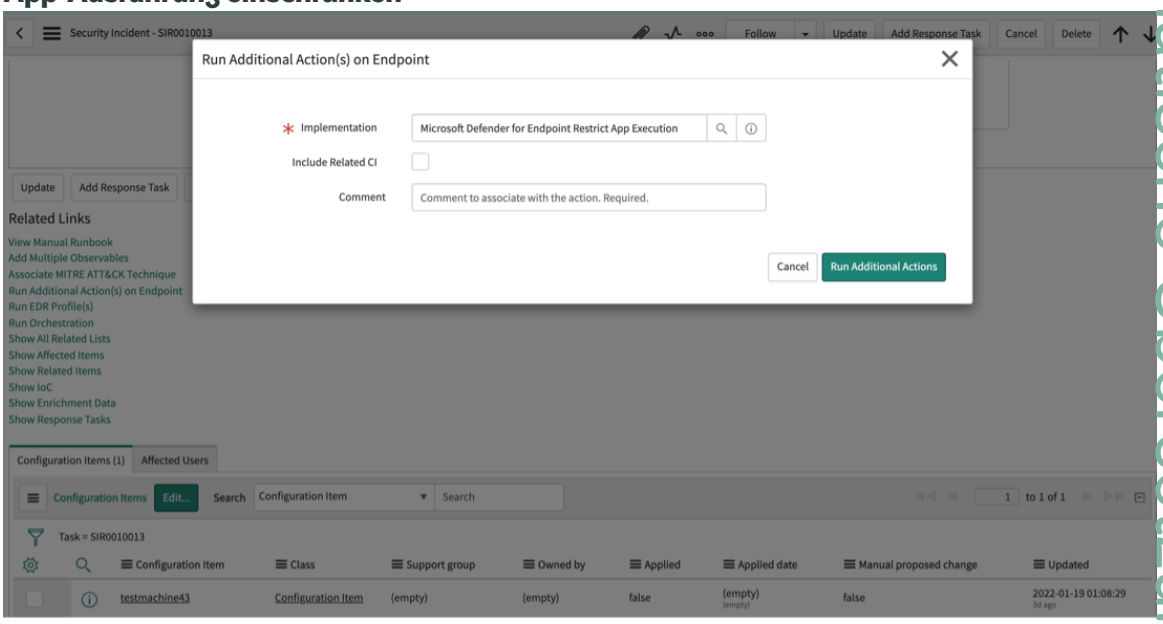
| Eingabe | Beschreibung |
|---|---|
| Anmerkung | (Erforderlicher) Kommentar, der der Aktion zugeordnet werden soll) |

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

## Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.
   b. Durchsuchen und wählen Sie die Fähigkeit **App-Ausführung beschränken**.

**App-Ausführung einschränken**




Alternativ können Sie die folgenden Schritte ausführen:

   a. Klicken Sie im Abschnitt „ **Zugehörige Listen“ auf Alle**zugehörigen Listen anzeigen.
   b. Klicken Sie auf die zugehörige Liste **Configuration Item**.
   c. Wählen Sie die hinzugefügten Konfigurationselemente aus.
   d. Wählen Sie unter Aktionen für ausgewählte Zeilen die **Option Zusätzliche Aktionen für Endpunkt ausführen aus**.
3. Um App-Ausführung einschränken auf dem Computer zu aktivieren, klicken Sie auf **Zusätzliche Aktion ausführen**.
4. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
5. Validieren Sie den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie die Funktion „App-Beschränkung entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Einschränkungen einer Anwendung auf dem Gerät.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

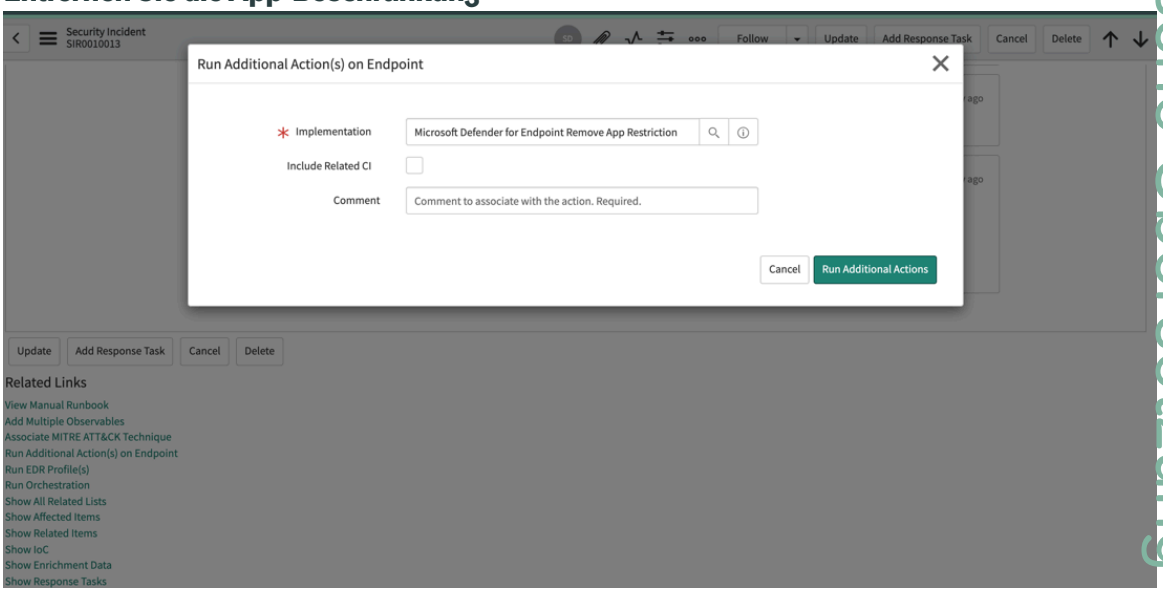
### Anforderungen für die Fähigkeit „App-Beschränkung entfernen“.

| Eingabe | Beschreibung |
|---|---|
| Anmerkung | (Erforderlicher) Kommentar, der der Aktion zugeordnet werden soll) |

## Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
   a. Klicken Sie im Abschnitt „Zugehörige Links“ auf **Zusätzliche Aktionen für Endpunkt ausführen**.
   b. Durchsuchen und wählen Sie die Fähigkeit **App-Beschränkung entfernen**.

**Entfernen Sie die App-Beschränkung**




Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt „ **Zugehörige Listen“ auf Alle**zugehörigen Listen anzeigen.
b. Klicken Sie auf die zugehörige Liste **Configuration Item**.
c. Wählen Sie die hinzugefügten Konfigurationselemente aus.
d. Wählen **Sie Zusätzliche Aktionen für Endpunkt ausführen aus**.
Das Eingabefeld Zusätzlicher Kommentar wird angezeigt.

3. Um die App-Einschränkung zu entfernen, klicken Sie auf **Zusätzliche Aktion ausführen**.
4. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
5. Validieren Sie den Status der Aktion in den zugehörigen Listen „Zusätzliche Aktionen für Endpunkt“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie die Fähigkeit Zugehörige Computer aus Defender-Fähigkeit abrufen in Microsoft Defender for Endpoint

Ruft die Liste der zugehörigen Computer bestimmter erkennbarer Elemente ab.

## Vorbereitungen

Unterstützte erkennbare Typen: Domänenname, SHA1-Hash und Benutzername

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

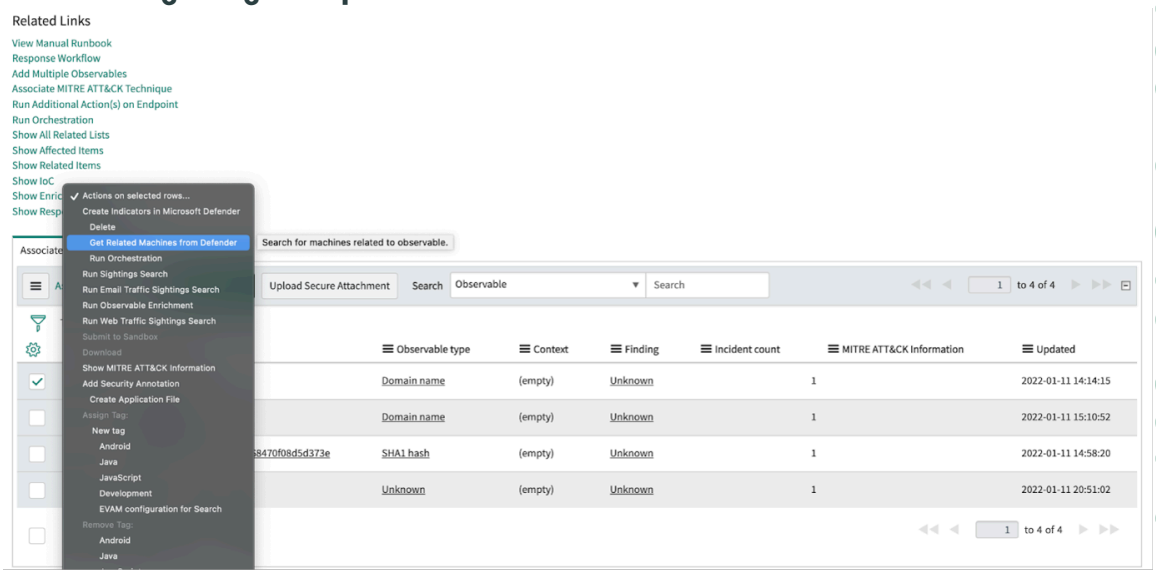
## Warum und wann dieser Vorgang ausgeführt wird

Sie können die Liste der Computer abrufen, die auf die bestimmten erkennbaren Elemente zugegriffen haben. Sie können die Liste in der Microsoft Defender for Endpoint-Tabelle „Details zugehöriger Computer“ speichern. Sie können die Fähigkeit „Zugehörige Computer aus Defender abrufen“ über die zugehörige Liste „Zugeordnete erkennbare Elemente“ auslösen.

## Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.

**Rufen Sie zugehörige Computer von Defender ab**




3. Klicken Sie im Abschnitt „Zugehörige Links“ auf **IoC anzeigen**.
4. Klicken Sie auf die zugehörige Liste Zugeordnete erkennbare Elemente.
5. Wählen Sie die zugeordneten erkennbaren Elemente aus.
6. Wählen Sie in der Liste „Aktionen“ die Fähigkeit **Zugehörige Computer aus Defender** abrufen aus.
7. Validieren Sie die Automatisierungsaktivität und den Aktivitätenbereich.
8. Zeigen Sie die Daten an, und validieren Sie die Microsoft Defender for Endpoint-bezogenen Computerdetails in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie die Funktion zum Stoppen und Quarantänen von Dateien in Microsoft Defender for Endpoint

Dateien über die Microsoft Defender-Plattform anhalten und unter Quarantäne stellen

#### Vorbereitungen

Unterstützte erkennbare Typen: SHA1-Hash

#### Anforderungen für die Fähigkeit zum Stoppen und Quarantänen von Dateien

| Eingabe | Beschreibung |
|---|---|
| Anmerkung | (Erforderlicher) Kommentar, der der Aktion zugeordnet werden soll) |

Erforderliche Rolle: sn_si.admin oder sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Aktion „Datei anhalten und unter Quarantäne stellen“ nur für bestimmte erkennbare Elemente vom Typ SHA1 ausführen. Speichern Sie die Details in der Tabelle „Zusätzliche Aktionen für Endpunkt“. Sie können die Funktion „Datei anhalten und unter Quarantäne stellen“ über die zugehörige Liste „Microsoft Defender for Endpoint – Zugehörige Computer“ auslösen.

#### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
3. Klicken Sie im Abschnitt „ **Zugehörige Links“ auf Alle zugehörigen Listen anzeigen**.
4. Klicken Sie auf die zugehörige Liste Microsoft Defender for Endpoint Related Machines (Details zu zugehörigen Computern).
5. Wählen Sie einen oder mehrere Datensätze aus.
6. Wählen Sie unter **Aktionen** für ausgewählte Zeilen die Funktion **Stoppen und Datei unter Quarantäne** stellen aus.
7. Validieren Sie die Automatisierungsaktivität und den Aktivitätenbereich.
8. Zeigen Sie die Daten an, und validieren Sie die Daten in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.

### Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche mit der Microsoft Defender for Endpoint -Integration

Erstellen und konfigurieren Sie das Sichtungssuchprofil automatisch mit Microsoft Defender for Endpoint.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können den Sichtungssuch-Workflow verwenden, um Sichtungssuchen durchzuführen. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen, die auf den



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtungssuchkonfigurationen basieren, und führt die Suchvorgänge aus, die auf dem konfigurierten Workflow basieren.

Microsoft Defender for Endpoint stellt ein Basissystem-Sichtungssuchprofil bereit, mit dem Sie die automatischen Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen für erkennbare Elemente einer Organisation zugreifen und auch die Sichtungen anderer Organisationen anzeigen.

### Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche: Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder des Formulars aus.

**Formular „Sichtungssuchkonfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name für das Sichtungssuchprofil. |
| Ist gespeicherte Suche | Option zum Speichern der Suchkonfiguration. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und nach Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen. |
| Sichtungssuchquelle | Die für die Sichtungssuche in der Microsoft Defender for Endpoint -Integration konfigurierte Quelle. |
| Suchen | Native Suchzeichenfolge, die eine Abfrage bildet. |
| Aktiv | Option zum Aktivieren der gespeicherten Suchkonfiguration. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen. |
| Erkennbarer Typ | Typ der erkennbaren Kategorie. Zum Beispiel IP-Adresse, Hash-Wert, URL und Domänenname. |
| Maximales erkennbares Element pro Suche | Maximale Anzahl von erkennbaren Elementen, die Sie in einer Suchabfrage anzeigen können. Legen Sie diesen Wert für diese Integration auf 1 fest. |
| Sichtungssuchparameter | Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden. |

4. Klicken Sie auf **Absenden**.

## Führen Sie eine manuelle Sichtungssuche in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in Microsoft Defender for Endpoint durch, um die Verbreitung einer Bedrohung im Laufe der Zeit zu bestimmen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Folgende erkennbare Typen werden unterstützt:

- Domänenname
- IP-Adresse (V4)
- IP-Adresse (V6)
- MD5-Hash
- SHA1-Hash
- SHA256-Hash

### Prozedur

1. Navigieren Sie zu **Security Incidents**.
2. Öffnen Sie eine vorhandene SIR, oder erstellen Sie eine neue SIR.
3. Klicken Sie in den zugehörigen Links auf **IoC anzeigen**.
4. Klicken Sie auf die zugehörigen Listen Zugeordnete erkennbare Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste „Aktionen“ auf **Anreicherung erkennbarer Elemente ausführen**.
7. Wählen Sie die erkennbaren Elemente unter **Aktion** für ausgewählte Zeilen aus, und klicken Sie auf **Sichtungssuche ausführen**.

   **Hinweis:**
   Die Sichtungssuche wird für die erkennbaren Elemente Domänenname, IP-Adresse (V4), IP-Adresse (V6), MD5-Hash, SHA1-Hash und SHA256-Hash unterstützt.

8. Geben Sie den Zeitrahmen für die Suche an, und klicken Sie auf **Suche**.

   **Hinweis:**
   Microsoft Defender für Endpunkt unterstützt die Sichtungssuche nur für die letzten 30 Tage. Wenn Ihre Bereichsabfrage früher als die letzten 30 Tage ist, werden bei der Sichtungssuche keine Daten abgerufen. Wenn sich Ihre Bereichsabfrage mit den letzten 30 Tagen überschneidet, werden nur die Sichtungen der letzten 30 Tage abgerufen. Wenn Ihre Bereichsabfrage innerhalb der letzten 30 Tage liegt, werden die Sichtungen von der definierten Startzeit bis zur aktuellen Uhrzeit abgerufen.

9. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie **auf Details** der Sichtungssuche, um die Details der Sichtungssuche anzuzeigen.
11. Klicken Sie auf die Registerkarte **Sichtung**, um Details anzuzeigen, und auf die Registerkarte **Sichtungssuchergebnisse**, um Suchergebnisse zu erhalten.

    Sie können zusätzliche Informationen zu der jeweiligen Sichtung im Feld **Zusammenfassung** anzeigen.

### Führen Sie eine automatische Ergänzung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Führen Sie eine automatische Ergänzung erkennbarer Elemente in Microsoft Defender for Endpoint durch, um erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen anzureichern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Vergewissern Sie sich, dass Sie die Systemeigenschaft **Security Incident Response** aktiviert haben. Diese Option löst die Fähigkeit zur Ergänzung erkennbarer Elemente in SIR aus, wenn ein erkennbares Element einem Security Incident zugeordnet wird.

Erforderliche Rolle: sn_si.admin, sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Sie können diese Funktion während Untersuchungen der Reaktion auf Incidents verwenden, um eine identifizierte Bedrohung einzudämmen. Wenn dem Security Incident neue erkennbare Elemente zugeordnet werden, können Sie die Ergänzung erkennbarer Elemente in der Microsoft Defender for Endpoint-Fähigkeit zur automatischen Ausführung aktivieren.

### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
3. Validieren Sie die Automatisierungsaktivität, sobald die neuen erkennbaren Elemente dem Security Incident zugeordnet wurden.
4. Zeigen Sie die Ergebnisse der Anreicherung in der zugehörigen Liste Indikatoren des Security Incident an. In der folgenden Tabelle finden Sie weitere Informationen zur Ergänzung erkennbarer Elemente.

**Microsoft Defender-Indikator**

| Feld | Beschreibung |
|---|---|
| Indikator-ID | Identität der Indikatorentität. Klicken Sie auf **Öffnen**, um den Datensatz in der Instanz Now Platform detailliert anzuzeigen |
| Erkennbares Element | Das dem Ergebnis zugeordnete erkennbare Element. |
| Titel | Titel für den Indikator. |
| Indikatortyp | Typ des Indikators. |
| Aktion | Vom Indikator ausgeführte Aktion. |
| Empfohlene Aktion | Empfohlene Aktionen für den Indikator. |
| Integrationslieferant | Integration der Defender-Quelle, aus der die Daten abgerufen werden. |
| Ablaufdatum | Ablaufzeit für den Indikator. |
| Abrufdatum | Datum, an dem der Ergänzungsdatensatz erstellt wurde. |

## Führen Sie eine manuelle Ergänzung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Ergänzung erkennbarer Elemente durch, um erkennbare Elemente mit zusätzlichen Informationen aus Microsoft Defender for Endpointanzureichern.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint -Integration ermöglicht die Ergänzung erkennbarer Elemente für alle erkennbaren Typen, die im Modul „Erkennbares Indikator-Zuordnung“ zugeordnet sind.

### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den Microsoft Defender for Endpoint-Informationen überprüfen möchten.
3. Klicken Sie **auf Alle anzeigen zugehörige Listen**.
4. Klicken Sie auf die Registerkarte **Zugeordnete erkennbare** Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste „Aktionen“ auf **Anreicherung erkennbarer Elemente ausführen**.
7. Wählen Sie eine Microsoft Defender for Endpoint **-Quelle** aus, und verschieben Sie sie in die Spalte **Ausgewählt**, um anzugeben, welche Implementierung Sie zum Anreichern der ausgewählten erkennbaren Elemente verwenden möchten.
8. Klicken Sie auf **Absenden**.
9. Um den Status der Ausführung zu validieren, zeigen Sie die Arbeitsnotizen an.
10. Um die Ergebnisse anzuzeigen, klicken Sie auf die Registerkarte **Microsoft Defender-Indikator**. In der folgenden Tabelle finden Sie weitere Informationen zur Ergänzung erkennbarer Elemente.

#### Microsoft Defender-Indikator

| Feld | Beschreibung |
|---|---|
| Indikator-ID | Identität der Indikatorentität. Klicken Sie auf **Öffnen**, um den Datensatz in der Instanz Now Platform detailliert anzuzeigen |
| Erkennbares Element | Das dem Ergebnis zugeordnete erkennbare Element. |
| Titel | Titel für den Indikator. |
| Indikatortyp | Typ des Indikators. |
| Aktion | Vom Indikator ausgeführte Aktion. |
| Empfohlene Aktion | Empfohlene Aktionen für den Indikator. |
| Integrationslieferant | Integration der Defender-Quelle, aus der die Daten abgerufen werden. |
| Ablaufdatum | Ablaufzeit für den Indikator. |
| Abrufdatum | Datum, an dem der Ergänzungsdatensatz erstellt wurde. |

## Indikatoren in Microsoft Defender for Endpoint erstellen

Erstellen Sie mithilfe von Microsoft Defender for EndpointIndikatoren aus zugeordneten erkennbaren Elementen des Security Incident.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

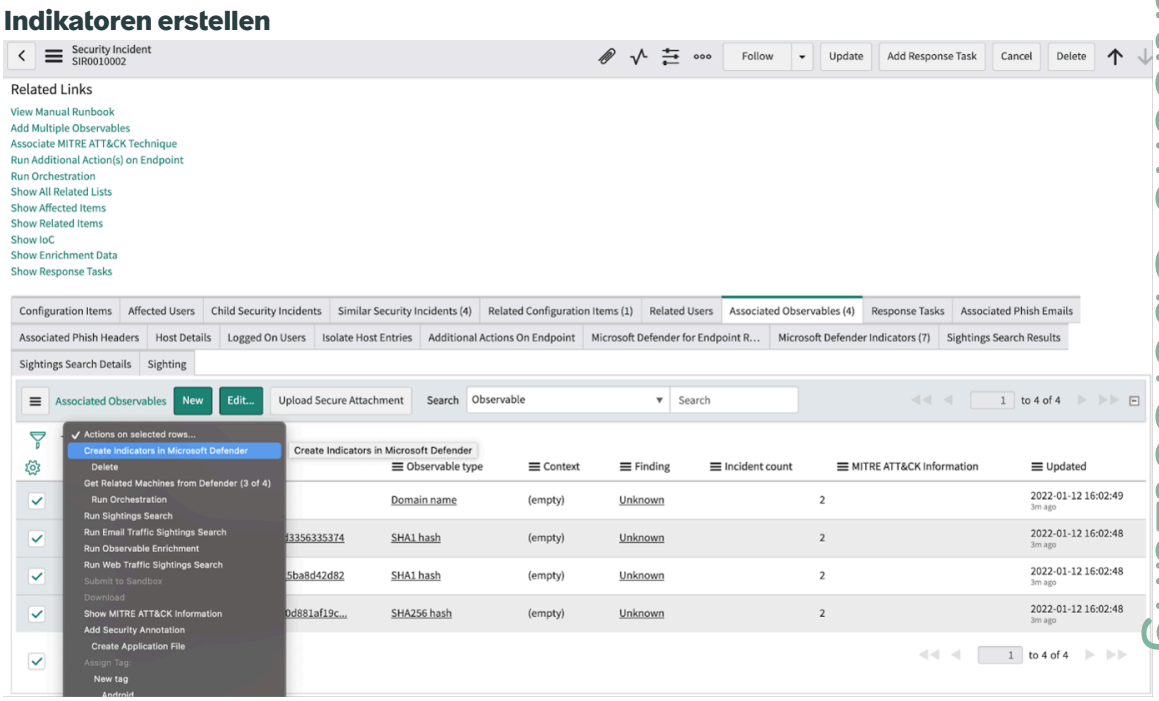
### Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint -Integration ermöglicht die Ergänzung erkennbarer Elemente für alle erkennbaren Typen, die im Zuordnungsmodul „Erkennbares Indikator“ zugeordnet sind.

Indikatoren erstellen bietet Ihnen die Möglichkeit, eine Liste von Indikatoren für die Erkennung sowie für die Verhinderung und Reaktion von Blockierungen festzulegen. Sie können die Indikatoren aus dem zugeordneten erkennbaren Element des Security Incident erstellen.

### Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie Indikatoren in Microsoft Defender für Endpunkt erstellen möchten.
3. Klicken Sie auf die zugehörigen Listen Zugeordnete erkennbare Elemente.
4. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie neue erkennbare Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in den **Aktionen** für ausgewählte Zeilen auf **Indikator in Microsoft Defender erstellen**.




7. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Ausgewählte erkennbare Elemente | Betroffene erkennbare Elemente. Diese Aktion kann verwendet werden, um Indikatoren für mehrere erkennbare Elemente zu erstellen. Wenn Sie die Auswahl eines erkennbaren Elements aufheben möchten, können Sie dies tun, indem Sie die Auswahl der erkennbaren Elemente in der Liste aufheben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Wenn die unterstützten erkennbaren Typen nicht zugeordnet sind, werden die Indikatoren in Microsoft Defender für solche erkennbaren Elemente nicht erstellt. |
| Titel | Titel für den Indikator. |
| Beschreibung | Beschreibung für den Indikator. |
| Ablaufzeit | Ablaufzeit für den Indikator. |
| Empfohlene Aktionen | Empfohlene Aktionen, die für den Indikator ausgeführt werden müssen. |
| Quelle | Integrationskonfiguration zum Erstellen des Indikators. |
| Aktion | Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Mögliche Werte:<br>○ **Warnen**<br>○ **Blockieren**<br>○ **Audit**<br>○ **'BlockierenUndKorrektur**<br>○ **Zulässig** |
| Anwendung | Die Microsoft Defender for Endpoint-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden. |
| Schweregrad | Schweregrad des Indikators. Mögliche Werte:<br>○ **Niedrig**<br>○ **Zuverlässige Anzeige**<br>○ **Hoch** |
| RBAC-Gruppennamen | RBAC-Gruppennamen, auf die der Indikator angewendet würde. Die Namen befinden sich in einer durch Kommas getrennten Liste. |

8. Klicken **Sie auf Indikator erstellen**
9. Validieren Sie die Aktivitäts- und UI-Nachrichten.
10. Klicken Sie auf die Registerkarte **Microsoft Defender-Indikator**, um die Ergebnisse anzuzeigen.

### Aktualisieren Sie Indikatoren in Microsoft Defender for Endpoint

Aktualisieren Sie die vorhandenen Indikatoren in Microsoft Defender for Endpoint über das Kontextmenü der Liste oder über die Formularansicht des Microsoft Defender-Indikators.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin, sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

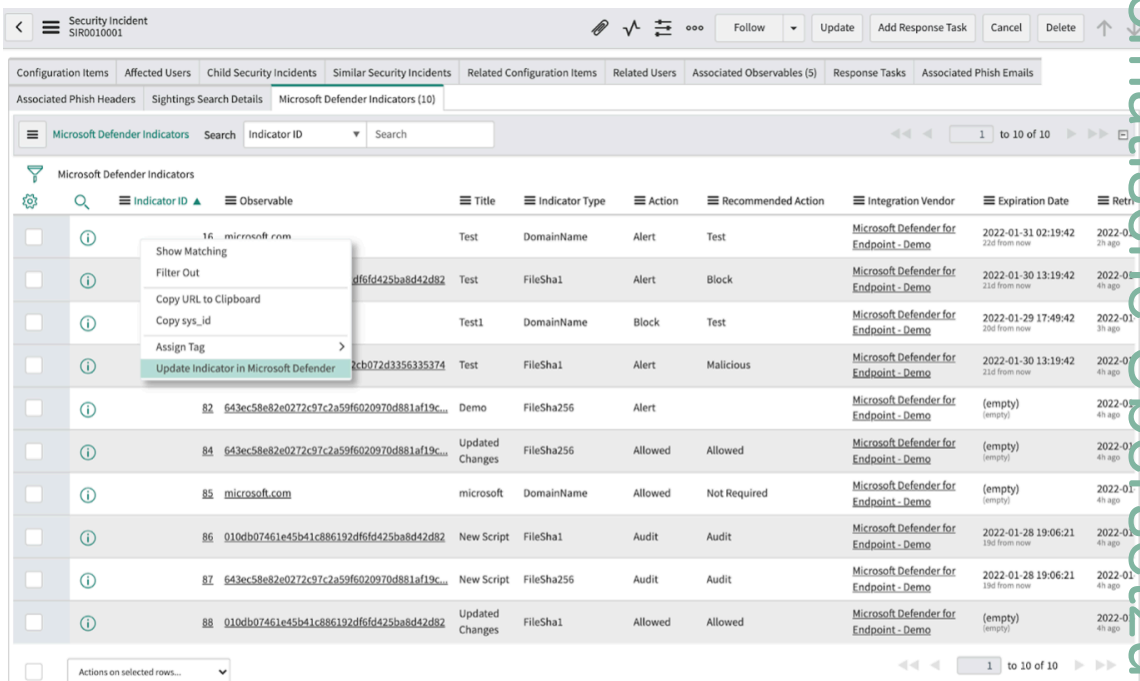
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**.
2. Klicken Sie auf **Alle zugehörigen Listen anzeigen**, und klicken Sie dann auf die Registerkarte **Microsoft Defender-Indikatoren**.

### Hinweis:

Sie müssen die zugehörige Liste für die Microsoft Defender-Indikatoren konfigurieren, die in den zugehörigen Listen für Security Incidents angezeigt werden. Weitere Informationen finden Sie unter Formular-UI-Aktionen.

3. Aktualisieren Sie die Microsoft Defender für Endpunkt-Indikatoren auf eine der folgenden Arten:
   - Um die Indikatoren aus dem Kontextmenü der Liste zu aktualisieren, wählen Sie die Zeile des Indikators aus, den Sie aktualisieren möchten, und klicken Sie **in der Microsoft Defender-Option auf Indikator** aktualisieren.

**Aktualisieren Sie Indikatoren mit dem Kontextmenü der Liste**

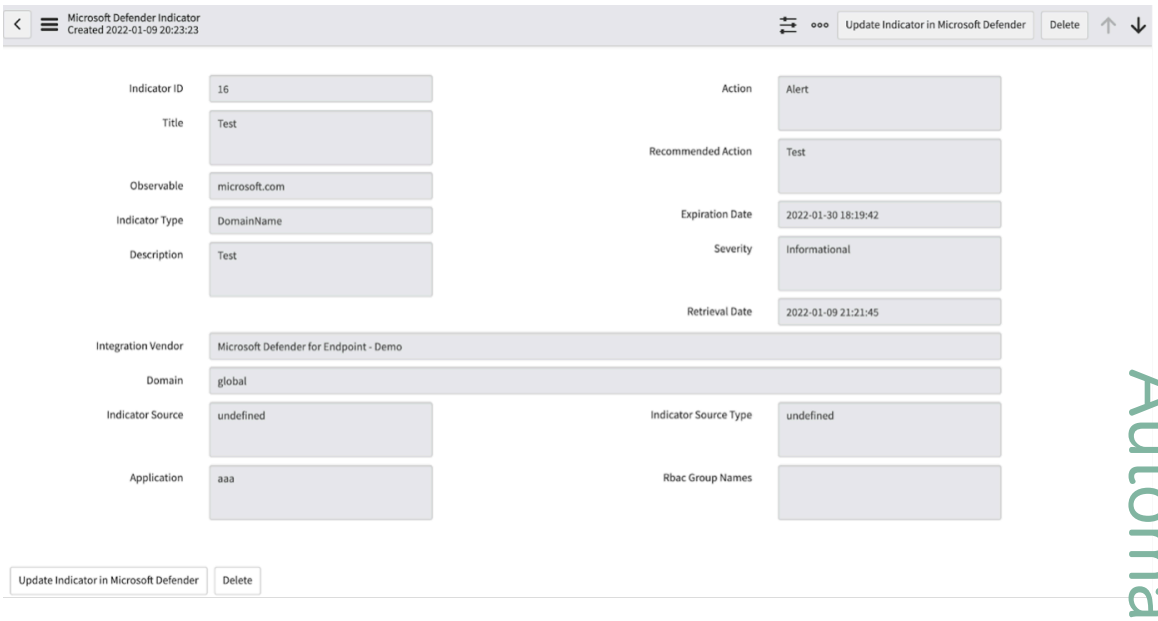



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Indikatoren in der Formularansicht zu aktualisieren, klicken Sie in der Formularansicht auf **Indikator in Microsoft Defender** aktualisieren.

**Aktualisieren Sie Indikatoren in der Formularansicht**




**4.** Füllen Sie die Felder des Formulars aus.

**Formular „Microsoft Defender-Indikator“**

| Feld | Beschreibung |
|---|---|
| Titel | Titel für den Indikator. |
| Beschreibung | Beschreibung für den Indikator. |
| Ablaufzeit | Ablaufzeit für den Indikator. |
| Empfohlene Aktionen | Empfohlene Aktionen, die für den Indikator ausgeführt werden sollen. |
| Quelle | Integrationskonfiguration zum Erstellen des Indikators. |
| Aktion | Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Mögliche Werte:<br>○ **Warnen**<br>○ **Blockieren**<br>○ **Audit**<br>○ **BlockierenUndKorrektur**<br>○ **Zulässig** |
| Anwendung | Die Microsoft Defender for Endpoint-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden. |
| Schweregrad | Schweregrad des Indikators. Mögliche Werte: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ **Niedrig**<br>○ **Zuverlässige Anzeige**<br>○ **Hoch** |
| RBAC-Gruppennamen | RBAC-Gruppennamen, auf die der Indikator angewendet wird. Die Namen befinden sich in einer durch Kommas getrennten Liste. |

5. Klicken Sie **auf Indikator aktualisieren**.
6. Validieren Sie die Aktivitäts- und UI-Nachrichten.

### Domänentrennung in der Microsoft Defender for Endpoint -Integration

Domänentrennung wird in der Microsoft Defender for Endpoint -Integration unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

## Support-Stufe
Support: Standard

Führen Sie die folgenden Schritte für die Domänentrennung aus:

1. Erstellen Sie einen Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne.
2. Führen Sie die Integrationsverfahren Microsoft Defender for Endpoint in der entsprechenden Domäne aus.

### Quotengrenzkonfiguration in der Microsoft Defender for Endpoint -Integration

Konfigurieren Sie die Quotengrenze der API und die Zeitüberschreitung für die Quotengrenze für die Microsoft Defender for Endpoint -Integration.

## Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.analyst (schreibgeschützt)

## Prozedur

1. Geben Sie im Navigationsfilter sys.properties.listein.
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Suchen und ändern Sie die folgenden Eigenschaften gemäß Ihren Anforderungen.

| Eigenschaftsname | Beschreibung |
|---|---|
| sn_sec_defender_ep.rate_limit_timeout_in_minutes | Wenn eine Anforderung nicht innerhalb des angegebenen Zeitrahmens ausgeführt wird, wird die Ausführung angehalten und eine entsprechende Fehlermeldung angezeigt.<br><br>Standardwert: 75. |
| sn_sec_defender_ep.request_per_hour_limit | Wenn der konfigurierte API-Aufruf innerhalb einer Stunde auf demselben Endpunkt erfolgt, wird |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaftsname | Beschreibung |
| --- | --- |
| | die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist.<br><br>Standardwert: 1500. |
| sn_sec_defender_ep.request_per_minute_limit | Wenn der konfigurierte API-Aufruf innerhalb einer Minute auf demselben Endpunkt erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist.<br><br>Standardwert: 100. |
| sn_sec_defender_ep.import_indicator_request_per_minute_limit | Wenn der konfigurierte API-Aufruf am Endpunkt innerhalb einer Minute erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist.<br><br>Standardwert: 30. |

## Integration „Microsoft Exchange Online“

Für die Microsoft Exchange Online -Integrationsanwendung von ServiceNowwird das Produkt Now Platform® Security Incident Response (SIR) mit dem Service Microsoft Exchange Online integriert, einem der cloudbasierten Services in der Office 365-Produktsuite von Microsoft. Ihr SOC-Analyst (Security Operation Center) kann die E-Mail-Umgebung Ihres Unternehmens nach sicherheitsbezogenen Bedrohungen durchsuchen und Phishing-E-Mails mit E-Mail-Such- und Löschfunktionen entfernen und korrigieren.

## Übersicht

Als Security Incident-Analyst führen Sie die Integration über die Security Analyst-Schnittstelle aus, und der Workflow gibt E-Mail-Nachrichtendetails zurück, die den Suchkriterien entsprechen. E-Mail-Suchen basieren auf Kriterien, die Betreffzeilen sowie Absender- und Empfänger-E-Mail-Adressen umfassen. Nach Abschluss der E-Mail-Suche können Sie verdächtige E-Mails aus dem Microsoft Exchange Online -Service löschen. Ein optionaler Genehmigungsprozess kann so konfiguriert werden, dass vor dem Löschen von E-Mails eine Genehmigung angefordert wird.

Diese Integration zum Suchen und Löschen von E-Mails kann mit einem umfassenderen Workflow oder Runbook für Phishing-Antwort-Incidents verwendet werden. Nachdem ein Unternehmensbenutzer oder -mitarbeiter eine verdächtige E-Mail erhalten und sie dem Phishing-Antwortteam oder Posteingang des Unternehmens gemeldet hat, wird die gemeldete E-Mail an Now Platform weitergeleitet und als Security Incident kategorisiert. Nachdem Sie sich vergewissert haben, dass es sich bei einer E-Mail um einen Phishing-Angriff handelt, können Sie als Analyst, der für die Untersuchung von Phishing-Incidents verantwortlich ist, eine E-Mail-Suche starten, um festzustellen, ob andere Unternehmensbenutzer diese Phishing-E-Mail erhalten haben. Mit der Suche können Sie zugehörige E-Mails aus derselben Phishing-Kampagne finden und andere potenzielle Opfer identifizieren, die die E-Mail möglicherweise erhalten und gelesen und möglicherweise auch auf eine schädliche URL geklickt oder einen Anhang geöffnet haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Schlüsselfunktionen

Die Integration umfasst die folgenden wichtigen Funktionen:

- Konfigurieren Sie Suchkriterien für Phishing-Bedrohungen in Security Incident Response basierend auf Kombinationen der Felder „Absender“, „Empfänger“ und „Betreff“ in E-Mail-Nachrichten.
- Bei umfangreichen und langwierigen E-Mail-Suchen wird der Security Incident-Analyst per E-Mail über den erfolgreichen Abschluss der Suche und die Anzahl der übereinstimmenden Nachrichten informiert.
- Der Status für einzelne Nachrichten informiert Sie, wenn Empfänger verdächtige E-Mails gelesen oder gelöscht haben.
- Wenn konfiguriert, stellen optionale Genehmigungsprozesse sicher, dass verdächtige E-Mails nicht ohne vorherige Genehmigung gelöscht werden.
- Ein vollständiger Auditpfad für Löschanforderungen, der die Anzahl der gelöschten E-Mails enthält, wird in den Arbeitsnotizen von Security Incidents protokolliert.
- Wenn Tagging konfiguriert ist, zeichnen Sicherheits-Tags auf, wenn E-Mail-Such- und Lösch-Workflows initiiert und für Security Incidents erfolgreich abgeschlossen werden.

## Unterstützte Versionen Microsoft Exchange Online .

Diese Integration unterstützt Services von Microsoft Exchange Online, die Teil der Office 365-Suite von Microsoft sind. Die Integration unterstützt keine gehosteten Microsoft Exchange-Umgebungen. Microsoft führt Microsoft Exchange Online -Services in der Exchange 2016-Version aus.

## Voraussetzungen

Das Plugin „com.snc.si_dep“ ist für jede Version von Now Platform erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations Anwendungen müssen über den ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

## Integrationsarchitektur und Systemverbindung

Weitere Informationen zur Architektur der Integration, einschließlich wichtiger Begriffe und Details zur Verbindung externer Systeme, finden Sie unter Integrationsarchitektur und externe Systemverbindung für die Microsoft Exchange Online -Integration.

## Prüfliste

Die folgenden Themen sind nummeriert. Befolgen Sie die unten aufgeführten Themen in der Reihenfolge, in der sie angezeigt werden, um eine reibungslose Installation und Konfiguration der Anwendung zu gewährleisten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Prüfliste dieser Schritte zum Ausdrucken finden Sie unter Prüfliste für die Microsoft Exchange Online -Integration. Sie können diese Liste verwenden, um Ihren Fortschritt zu überwachen, während Sie die End-to-End-Aufgaben der Einrichtung, Konfiguration und Überprüfung der Ergebnisse der Integration durcharbeiten.

## Einschränkungen

1. Die Verfügbarkeit von Daten über die Microsoft Threat-Hunting-API unterliegt Verzögerungen, die durch die Latenz zwischen Exchange Server, Graph API und Search-API verursacht werden. Die Synchronisierung zwischen der Search-API und dem Exchange-Server kann einige Minuten dauern. Die Latenzzeit ist variabel und kann von Instanz zu Instanz unterschiedlich sein.
2. Hier werden die Einschränkungen der Such-API, der Kontingente und der Ressourcenzuteilung erläutert: https://learn.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0#advanced-hunting

### Richten Sie Ihr Microsoft Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein

Führen Sie die folgenden Setup-Aufgaben in Ihrem Microsoft Azure-Portal aus, bevor Sie die Anwendung ServiceNow für diese Integration installieren. Dieses Konto ermöglicht den Zugriff auf den Mandanten Microsoft Exchange Online für E-Mail-Nachrichtendetails.

#### Vorbereitungen

Erforderliche Rolle: Microsoft Azure-Portaladministrator

Dieses Konto ist für den Zugriff auf den Mandanten Microsoft Exchange Online erforderlich, um zusätzliche E-Mail-Nachrichtendetails zu erfassen und E-Mail-Nachrichten zu löschen. Dieses Konto wird im Azure-Portal von Microsoft eingerichtet.

Die Images in den folgenden Aufgaben sind privilegiert und proprietär und werden mit Erlaubnis von Microsoftverwendet. Dieser Inhalt kann von Microsoftaktualisiert werden. Informationen zum Überprüfen, ob Sie Zugriff auf die aktuellen Inhalte haben, finden Sie auf der Microsoft -Dokument-Website.

In den folgenden Abbildungen wird ServiceNow Inc. für den Kontonamen in den Beispielen für das Azure-Portal angezeigt. In Ihrem Azure-Portalkonto wird der Unternehmensname für Ihren Account im Azure-Portal angezeigt.

#### Prozedur

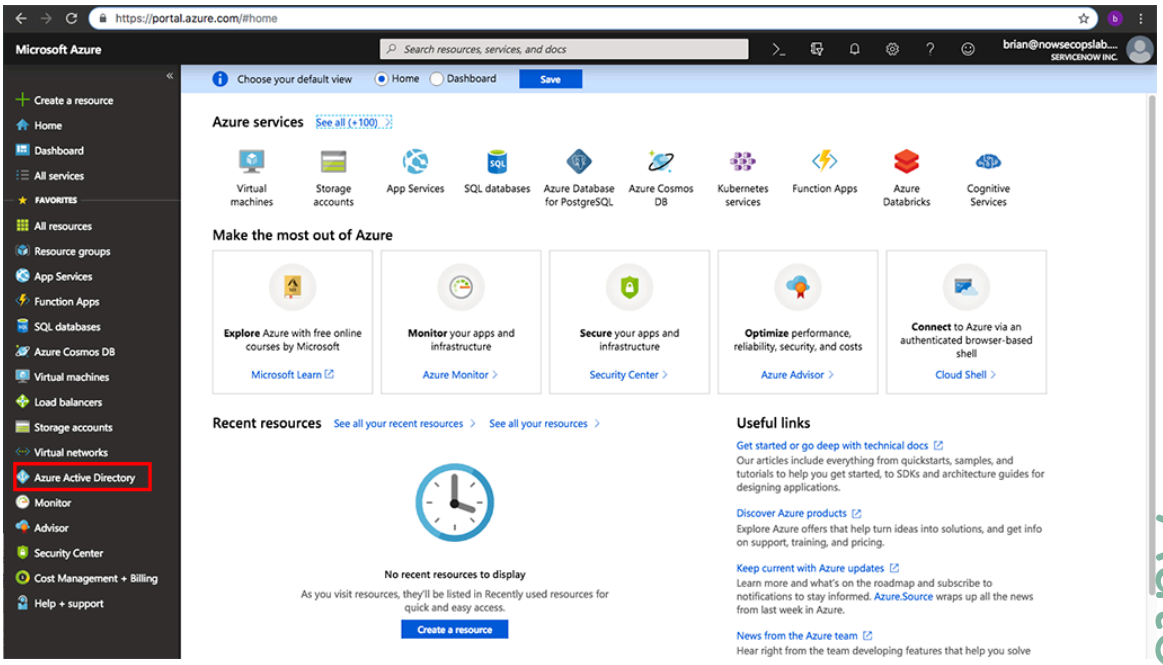
Wenn Sie im Azure-Portal Microsoft keine Anwendungs-ID für die OAuth-Authentifizierung erstellt haben, führen Sie die folgenden Schritte aus.

a. Melden Sie sich beim Microsoft Azure-Portal mit den Anmeldeinformationen Ihres Azure-Portaladministrators an.

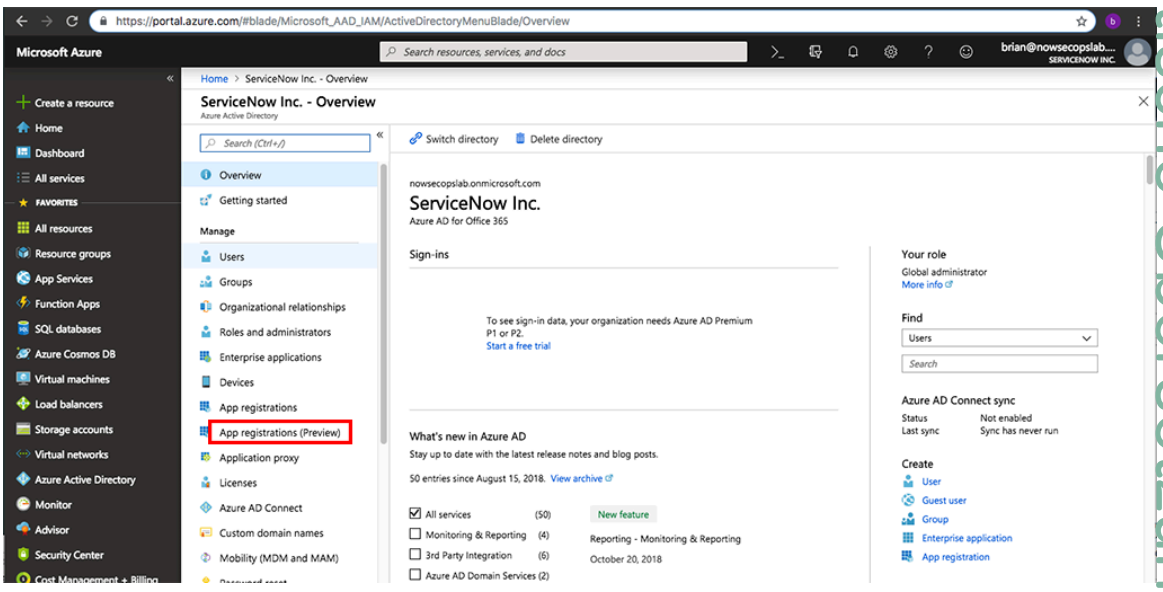
b. Klicken Sie im linken Navigationsbereich der Startseite auf **Azure Active Directory**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



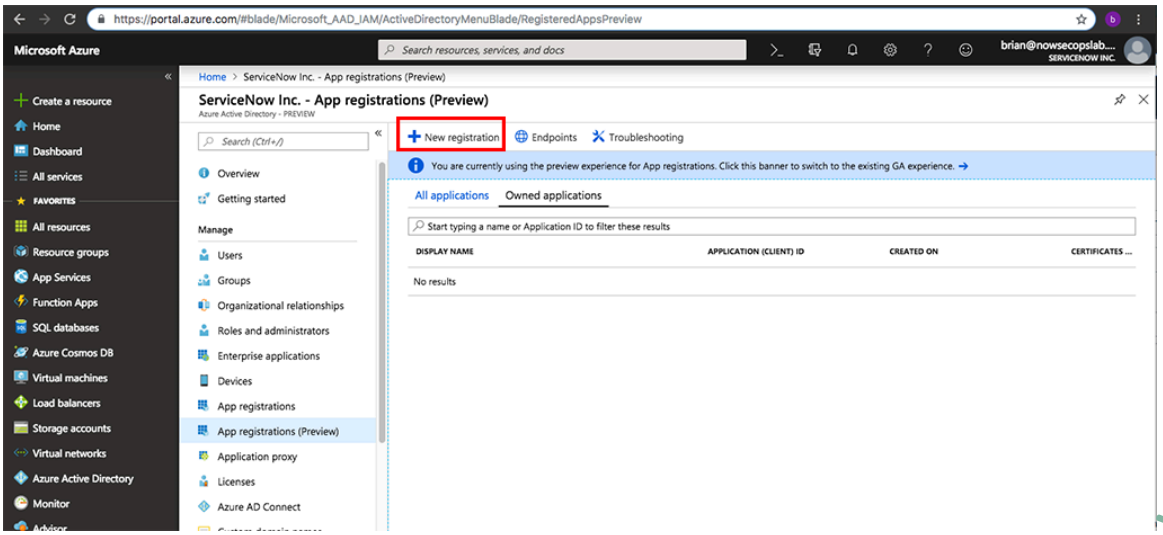

**c.** Klicken Sie im angezeigten Übersichtsbereich auf **App-Registrierungen (Vorschau)**.




**d.** Klicken Sie im angezeigten Bereich App-Registrierungen (Vorschau) auf **Neue Registrierung**.

Automatische Übersetzung

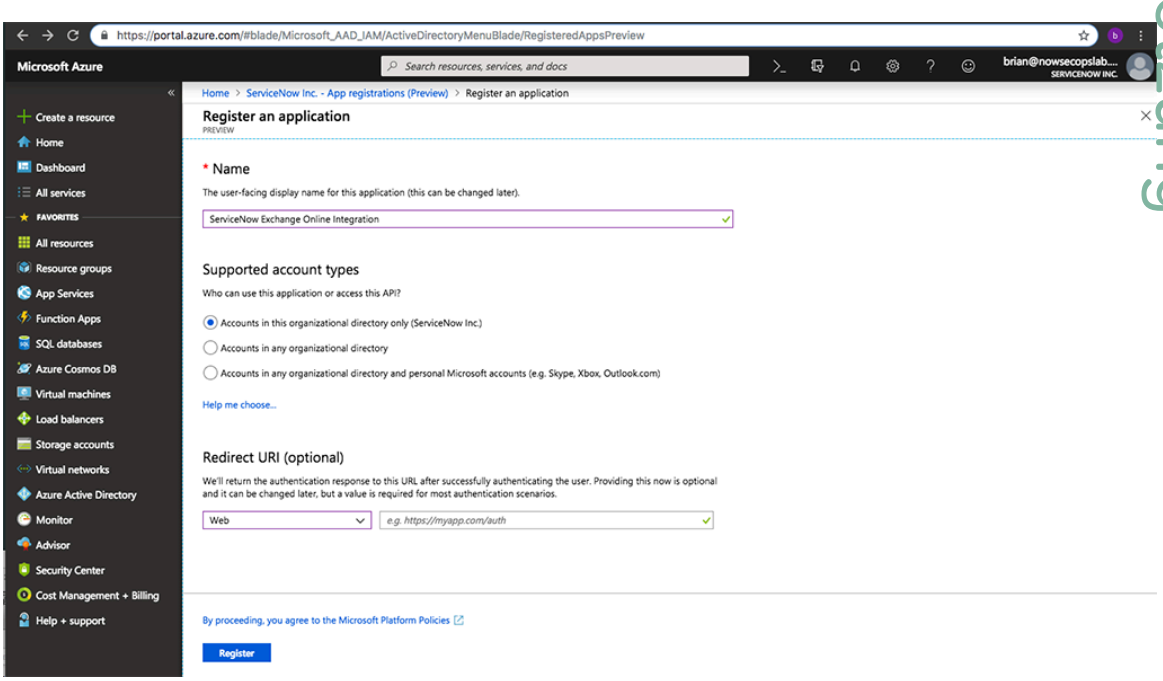
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**e.** Füllen Sie das angezeigte Formular Anwendung registrieren aus.

Ein Beispiel für ein ausgefülltes Formular wird nach der Tabelle angezeigt.

| Feld | Beschreibung |
|---|---|
| **Name** | Name für die Anwendung. In diesem Beispiel wird `ServiceNow Exchange Online-Integration` eingegeben. |
| **Unterstützte Account-Typen** | Klicken Sie für diesen Account unter Unterstützte Account-Typen auf **Accounts in diesem Organisationsverzeichnis (nur ServiceNow Inc.)**. Diese Domäne wird für die E-Mail-Suche verwendet. |
| **Umleitungs-URL (optional)** | Wenn Sie einen Wert für dieses Feld eingeben, wird er von der Integration nicht verwendet. |

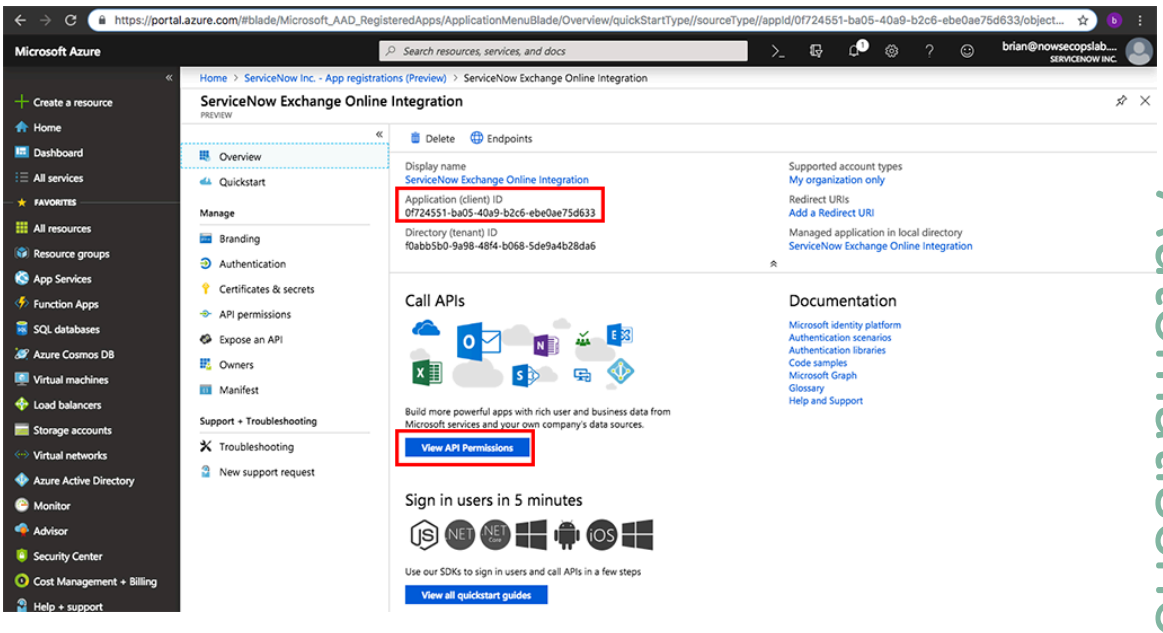



Automatische Übersetzung

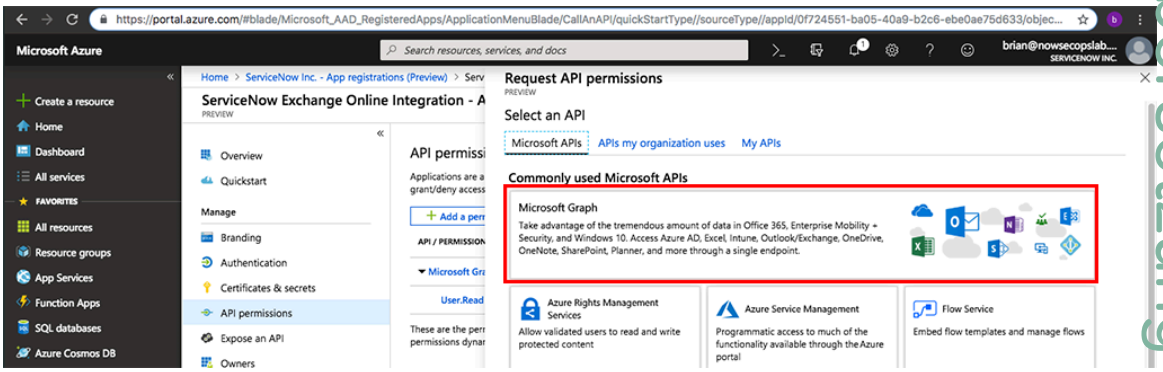
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**f.** Klicken Sie auf **registrieren**.
Eine Anwendungs-ID wird erstellt. Diese ID ähnelt einem Benutzernamen. Sie geben diesen Wert auf der Konfigurationsseite im Feld **OAuth-Anwendungs-ID** während des Konfigurationsschritts in Ihrer Now Platform -Instanz ein, der in Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanzbeschrieben wird.

**g.** Wenn die Anwendungs-ID (Client) im Bereich „ServiceNow Exchange Online-Integration“ angezeigt wird, klicken Sie auf **API**-Berechtigungen anzeigen.



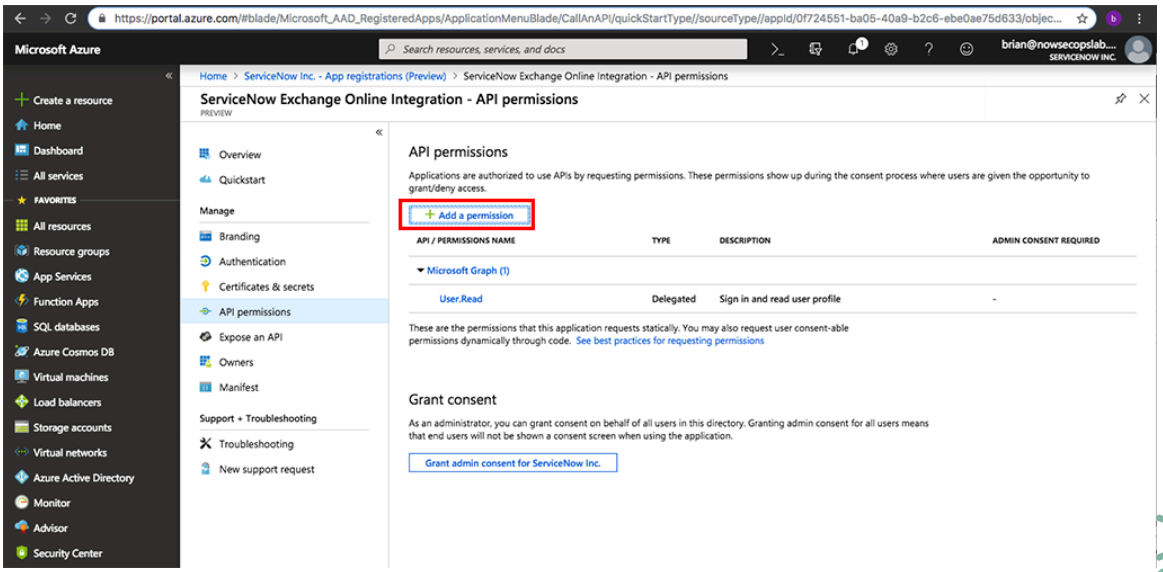

**h.** Klicken Sie im angezeigten Bereich API-Berechtigungen anfordern auf **Microsoft Graph**.



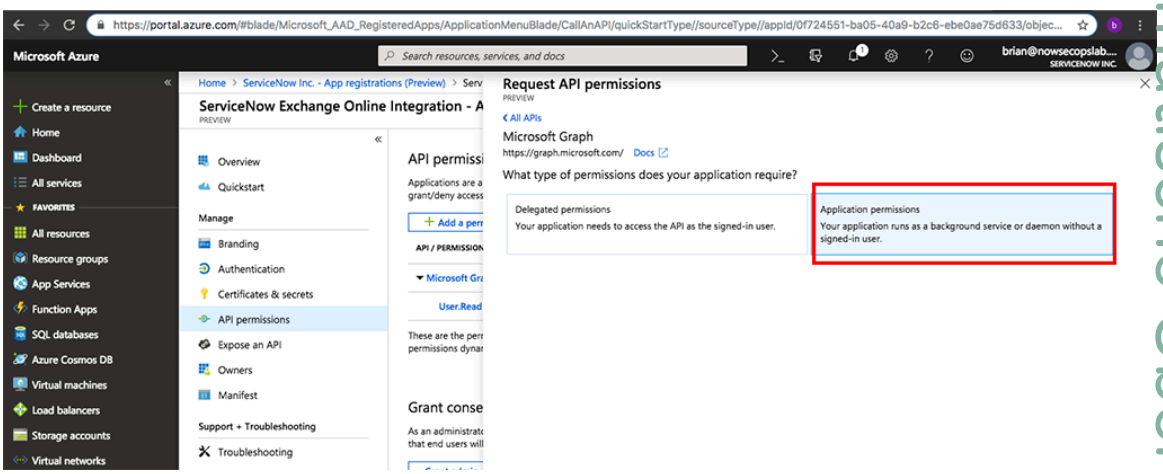

**i.** Klicken Sie im angezeigten Bereich „ServiceNow Exchange Online-Integration – API-Berechtigungen“ auf **Eine Berechtigung hinzufügen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



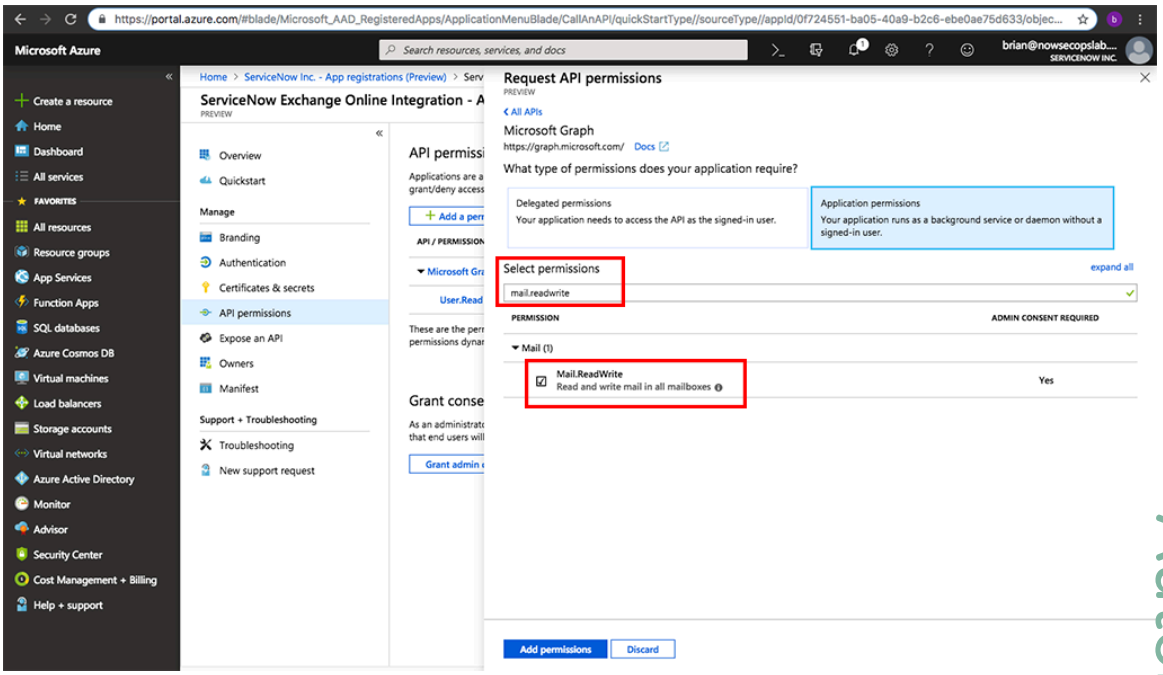

**j.** Klicken Sie im angezeigten Bereich API-Berechtigungen anfordern auf **Anwendungsberechtigungen**.




**k.** Geben Sie im angezeigten Feld Berechtigungen auswählen **Mail.ReadWrite** ein, und aktivieren Sie das Kontrollkästchen **Mail.ReadWrite**.

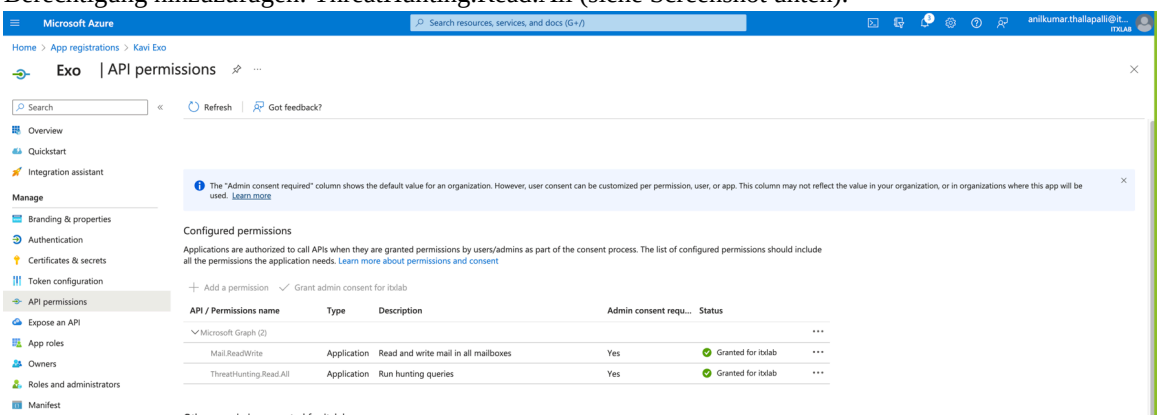
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**l.** Klicken **Sie auf Berechtigungen hinzufügen**.

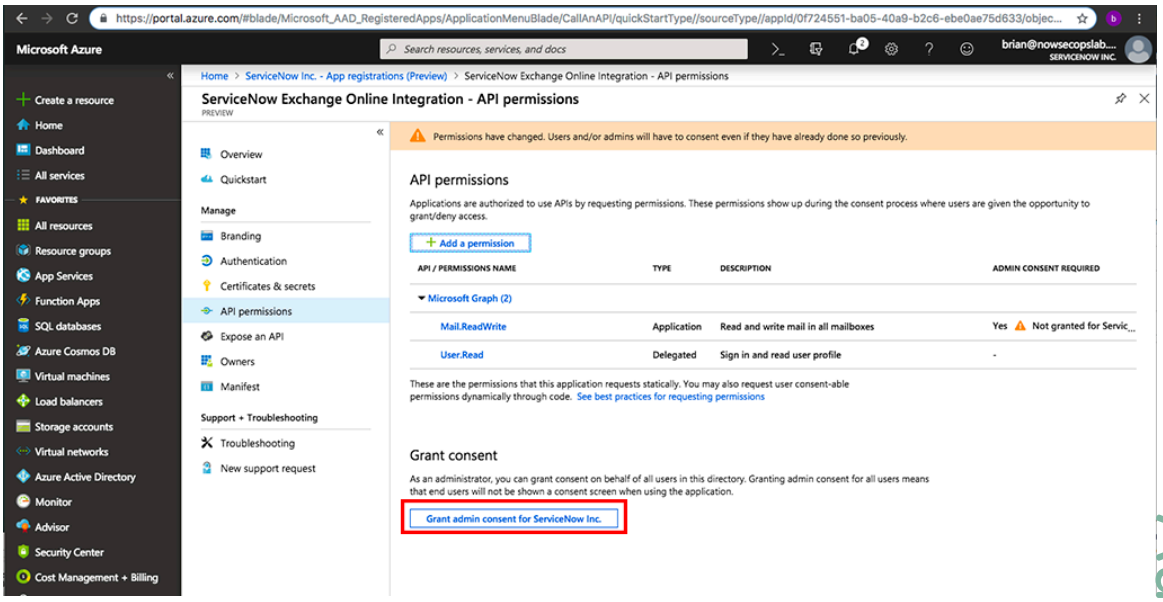
**m.** Wiederholen Sie die Schritte von Schritt i bis Schritt l, um der API-Berechtigungsliste eine weitere Berechtigung hinzuzufügen: ThreatHunting.Read.All (siehe Screenshot unten).




**n.** Klicken Sie im angezeigten Bereich ServiceNow Exchange Online-Integration – API-Berechtigungen auf **Grant Admin Consent for**(Administratoreinwilligung für gewähren).<your organization name> .

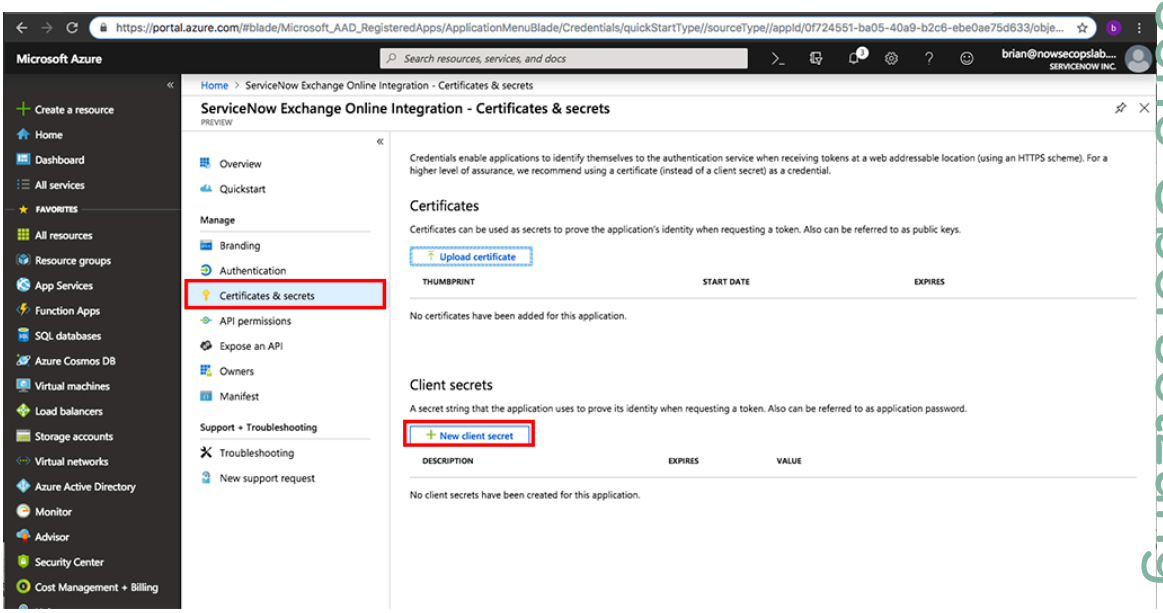
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**o.** Um die zuvor eingegebene API-Auswahl (Microsoft Graph API) zu bestätigen, klicken Sie auf **Bestätigen**.

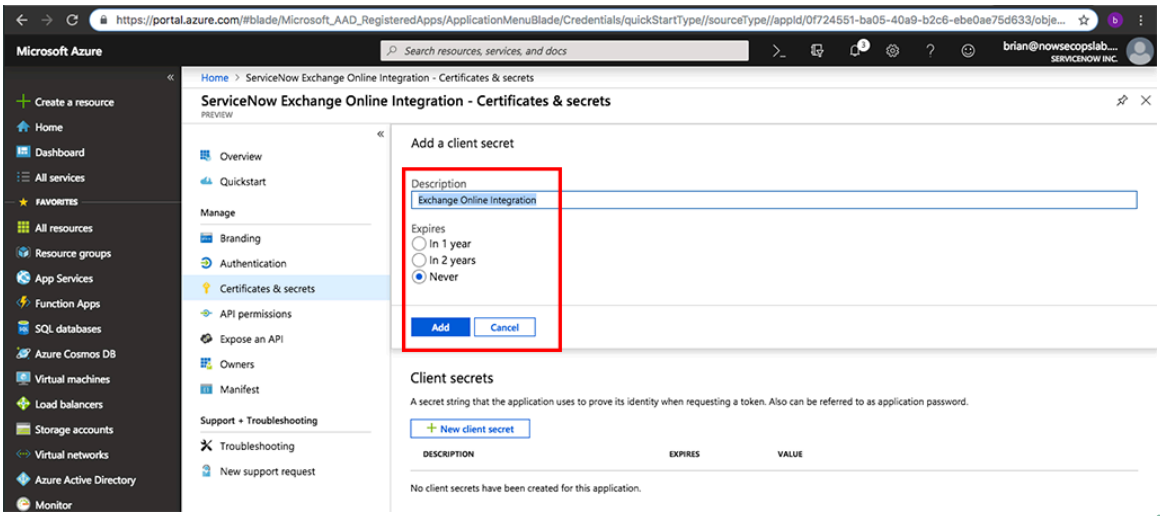
**p.** Klicken Sie im Bereich „ServiceNow Exchange Online-Integration – Zertifikate und geheime Schlüssel“ auf **Zertifikate und** geheime Schlüssel, gefolgt von **Neuer geheimer Clientschlüssel** (Passwort).



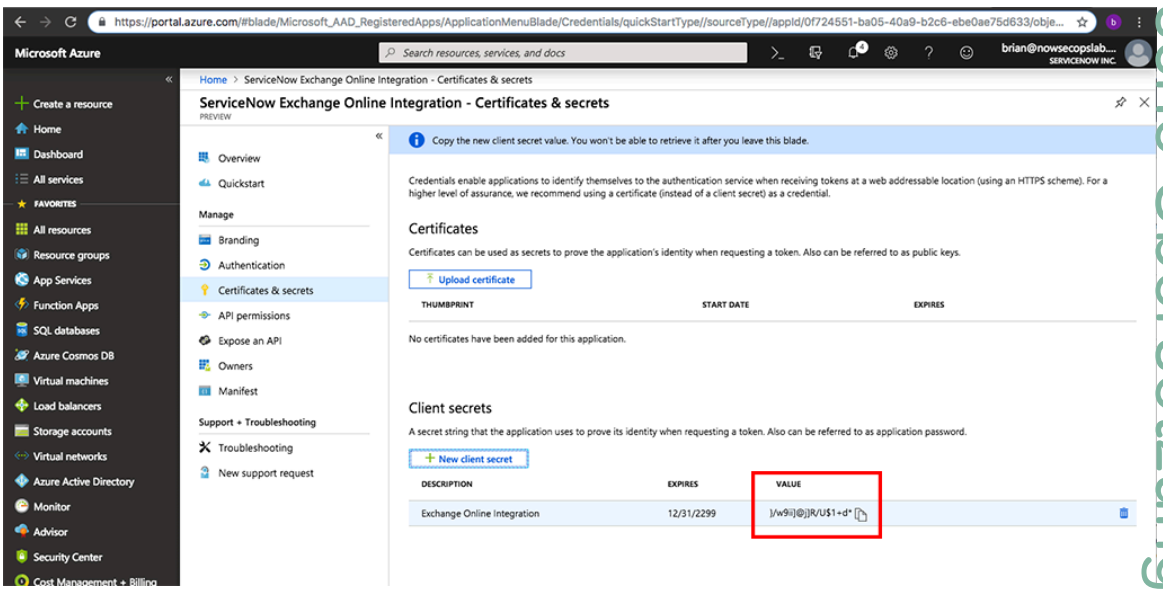

**q.** Geben Sie im Formular, das im Bereich „ServiceNow Exchange Online-Integration – Zertifikate und Geheimnisse“ angezeigt wird, den Namen für die Anwendung in das Feld Beschreibung ein, klicken Sie auf eine Option für den Ablauf, und klicken Sie auf **Hinzufügen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Im angezeigten Bereich „Zertifikate und geheime Schlüssel“ im Abschnitt „Geheime **Clientschlüssel** “ wird unter Wertdie Zeile mit dem neuen geheimen Clientschlüssel (Passwort) ausgefüllt. Bewahren Sie dieses Passwort an einem sicheren Ort auf. Nachdem Sie diese Seite verlassen haben, ist dieser Passwortwert nicht mehr sichtbar. Sie geben dieses Passwort auf der -Konfigurationsseite während des Konfigurationsschritts für die Integration in Ihre Now Platform**-Instanz in das Feld OAuth-Client-Secret** ein. Die Konfigurationsschritte für die Integration werden in Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanzbeschrieben.




Sie haben erfolgreich eine Anwendungs-ID für die OAuth-Authentifizierung im Azure-Portal Microsoft erstellt.

## Nächste Maßnahme

Sie sind bereit, Ihre Now Platform® -Instanz für die Integration einzurichten.

### Richten Sie die Exchange Online-Integration mit Security Incident Response ein

Für die Authentifizierung mit Anwendungsobjekten ist ein anfängliches Onboarding erforderlich. Anwendung und Dienstprinzipal werden austauschbar verwendet, aber eine Anwendung ist wie ein Klassenobjekt, während ein Dienstprinzipal wie eine Instanz der Klasse ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Anwendungs- und Dienstprinzipalobjekten in Azure Active Directory finden Sie unter Anwendungs- und Dienstprinzipalobjekte in Azure Active Directory . Einen detaillierten visuellen Flow zum Erstellen von Anwendungen in Azure AD finden Sie unter Azure Active Directory-Anwendungen und -Dienstprinzipale erstellen, die auf -Ressourcen zugreifen können .

Führen Sie die folgenden Schritte aus, um Folgendes einzurichten:[store-future: BEGIN review]

1. Registrieren Sie die Anwendung in Azure AD.
2. Weisen Sie der Anwendung API-Berechtigungen zu.

   Damit das Anwendungsobjekt auf Ressourcen zugreifen kann, muss es über die Anwendungsberechtigung `ThreatHunting.Read.All` und `Mail.ReadWrite` verfügen.
3. [store-future: BEGIN review]Generieren Sie ein selbstsigniertes Zertifikat, und gewähren Sie Zugriff auf den privaten Schlüssel.

   Erstellen und konfigurieren Sie ein selbstsigniertes X.509-Zertifikat, das zur Authentifizierung Ihrer Anwendung bei Azure AD verwendet wird, während Sie das Nur-App-Zugriffstoken anfordern. Zertifikate der nächsten Generation (CNG) werden für die reine App-Authentifizierung mit Exchange nicht unterstützt. CNG-Zertifikate werden in modernen Windows-Versionen standardmäßig erstellt. Sie müssen ein Zertifikat von einem CSP-Schlüsselanbieter verwenden. `(-Provider = 'Microsoft starkes kryptografisches Provider')`.

   [End]
4. [store-future: BEGIN review]Hängen Sie das Zertifikat an die Azure AD-Anwendung an.[End]
5. [store-future: BEGIN review]Weisen Sie der Anwendung Azure AD-Rollen zu.

   Der Anwendung muss die Azure AD-Rolle „ `Compliance-Administrator` “ zugewiesen sein.

   [End]
6. [store-future: BEGIN review]Erstellen Sie einen neuen Dienstprinzipal.[End]

[End]

## Schritt 1: Anwendung in Azure AD registrieren

1. Öffnen Sie das Azure AD-Portal .
2. **Geben** Sie im Suchfeld oben auf der Seite **App-Registrierungen**ein.
3. Wählen Sie **App-Registrierungen** aus den Ergebnissen im Abschnitt „Services“ und dann App-Registrierungen aus den Ergebnissen im Abschnitt „ **Services** “ aus.

   Alternativ können Sie mithilfe von https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade zur Seite „ **App-Registrierungen**“ navigieren.
4. Wählen Sie auf der Seite „ **App-Registrierungen** “ die Option **Neue Registrierung**aus.
5. Konfigurieren Sie auf der Seite **„Anwendung registrieren“** die folgenden Einstellungen:

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie eine Beschreibung ein. Beispiel: ExO PowerShell-CBA. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Unterstützte Account-Typen | Vergewissern Sie sich, dass **nur Accounts in diesem Organisationsverzeichnis (** <YourOrganizationName> (nur Einzelmandant) ist ausgewählt.<br><br>Um die Anwendung als Multi-Mandanten-Anwendung für delegierte Exchange Online-Szenarien festzulegen, wählen Sie den Wert Accounts in einem beliebigen Organisationsverzeichnis (Beliebiges Azure AD-Verzeichnis – Multi-Mandanten-Verzeichnis) aus. |

6. Wählen Sie nach Abschluss der App-Registrierung **Registrieren** aus, und schließen Sie die App-Seite.

### Schritt 2: Weisen Sie der Anwendung API-Berechtigungen zu

Die Verfahren in diesem Abschnitt ersetzen alle Standardberechtigungen, die automatisch für die neue App konfiguriert wurden. Die App benötigt die ersetzten Standardberechtigungen nicht.

1. Wählen Sie auf der App-Seite **Manifest** unter Verwaltung aus.
2. Suchen Sie auf der Manifestseite den Eintrag „ `requiredResourceAccess` “ (in oder um Zeile 52).
3. Ändern Sie die Werte `resourceAppId`, `resourceAccess id`und `resourceAccess type` wie im folgenden Code-Fragment gezeigt:

```
"requiredResourceAccess": [
    {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
            {
                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                "type": "Role"
            },
            {
                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                "type": "Role"
            }
        ]
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        }

],
```

4. Wählen Sie **Speichern**.
5. Wählen Sie auf der **Manifestseite** unter Management die Option **API-Berechtigungen** aus.
6. Füllen Sie die Felder auf der Seite „ **API-Berechtigungen** “ aus.

| Feld | Beschreibung |
|---|---|
| API-/Berechtigungsname | Vergewissern Sie sich, dass der Wert ThreatHunting.Read.All und Mail.ReadWrite angezeigt wird. |
| Status | Der derzeit falsche Wert ist **Nicht gewährt für**<Organization> , und dieser Wert muss geändert werden.<br><br>Wählen Sie **Grant admin consent for (Administratoreinwilligung gewähren für) aus**<Organization> , lesen Sie den Bestätigungsdialog, der sich öffnet, und wählen Sie dann **Ja**.<br><br>Der Statuswert sollte jetzt **Gewährt für**lauten<Organization> . |

7. Schließen Sie die aktuelle API-Berechtigungsseite (nicht die Browserregisterkarte), um zur Seite „App-Registrierungen“ zurückzukehren.

[store-future: BEGIN review]

## Schritt 3: Selbstsigniertes Zertifikat generieren und Zugriff auf den privaten Schlüssel gewähren

Erstellen Sie ein selbstsigniertes x.509-Zertifikat, indem Sie wie folgt vorgehen:

- Verwenden Sie die Cmdlets New-SelfSignedCertificate , Export-Certificate und Export-PfxCertificate in einer Windows PowerShell-Sitzung mit erhöhten Rechten (als Administrator ausführen), um ein selbstsigniertes Zertifikat anzufordern und es in .cer und .pfx (standardmäßig SHA1) zu exportieren. Beispiel:

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName "snowsecops.onmicrosoft.com"
 -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"

# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- Gewähren Sie dem MID-Servicebenutzer mit dem privaten Schlüssel Zugriff, indem Sie die folgenden Schritte ausführen:

  1. Öffnen **Sie die MMC (Microsoft Management Console)**.
  2. Navigieren Sie in der Microsoft Management Console (MMC) zu **Zertifikate (lokaler Computer)** > **Persönlich** > **Zertifikate**.

     (Wenn MMC kein Menüelement hat, fügen Sie es hinzu, indem Sie zu navigieren **Datei** > **Snap-in Hinzufügen/Entfernen**.
  3. Klicken Sie mit der rechten Maustaste auf das von Ihnen generierte Zertifikat.
  4. Erweitern **Alle Aufgaben** > **Private Schlüssel verwalten**
  5. Fügen Sie den **MID-Service-Benutzer** der Liste der Zugriffsberechtigten hinzu.

[End]

[store-future: BEGIN review]

## Schritt 4: Hängen Sie das Zertifikat an die Azure AD-Anwendung an

Nachdem Sie das Zertifikat bei Ihrer Anwendung registriert haben, können Sie den Fingerabdruck zur Authentifizierung verwenden.

1. Wählen Sie auf der Seite „ **Apps-Registrierung** “ am Ende von Schritt 2 auf der Registerkarte „ **Eigene Anwendungen** “ Ihre Anwendung aus.

   Wenn Sie zur **Registrierungsseite für Apps** zurückkehren müssen, verwenden Sie https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps , vergewissern Sie sich, dass die Registerkarte **Eigene Anwendungen** ausgewählt ist, und wählen Sie dann Ihre Anwendung aus.
2. Wählen Sie **Zertifikate und geheime** Schlüssel unter Verwalten aus.
3. **Wählen Sie auf der Seite „Zertifikate und geheime** Schlüssel“, die sich öffnet, **Zertifikat hochladen aus**.
4. Navigieren Sie zu dem selbstsignierten Zertifikat (.cer -Datei), das Sie in Schritt 3erstellt haben.
5. Wählen Sie nach Abschluss **Hinzufügen**aus.

   Das Zertifikat wird jetzt im Abschnitt „Zertifikate“ angezeigt.
6. Notieren Sie sich CertificateThumbPrint, und schließen Sie die aktuelle Seite „Zertifikate und **geheime** Schlüssel“.

[End]

[store-future: BEGIN review]

## Schritt 5: Weisen Sie der Anwendung Azure AD-Rollen zu

1. Öffnen Sie das Azure AD-Portal .
2. **Suchen** Sie im Feld Suche oben auf der Seite nach **Rollen und Administratoren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Azure AD-Rollen und -Administratoren** aus den Ergebnissen im Abschnitt „Services“ aus.

   Alternativ können Sie mithilfe von https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade zur Seite „ **Azure AD-Rollen und -Administratoren**“ navigieren.

4. Suchen und wählen Sie auf der Seite „ **Azure AD-Rollen und** -Administratoren“ eine der unterstützten Rollen aus, indem Sie in den Ergebnissen auf den Namen der Rolle (nicht auf das Kontrollkästchen) klicken.

   Suchen und wählen Sie die Rolle „ **Compliance-Administrator** “.

5. Wählen Sie auf der Seite „ **Zuweisungen** “ die **Option Zuweisungen hinzufügen**aus.
6. Suchen Sie im Popup- **Fenster Zuweisungen** hinzufügen nach der App, die Sie in Schritt 1erstellt haben, und wählen Sie sie aus.
7. Wählen Sie nach Abschluss **Hinzufügen**aus.
8. Kehren Sie zur Seite „ **Zuweisungen** “ zurück, und vergewissern Sie sich, dass die Rolle der App zugewiesen wurde.

[End]

[store-future: BEGIN review]

## Schritt 6: Erstellen Sie einen neuen Dienstprinzipal

**Wichtig:**
Stellen Sie sicher, dass Sie eine Verbindung mit **Security & Compliance PowerShell hergestellt** haben, bevor Sie die Schritte zum Erstellen eines neuen -Dienstprinzipals ausführen. Das Erstellen eines neuen Dienstprinzipals ohne Verbindung mit PowerShell funktioniert nicht (Ihre Azure-App-ID und Objekt-ID werden benötigt, um den neuen Dienstprinzipal zu erstellen).

1. Führen Sie den folgenden Befehl aus, um die Details der Azure-Anwendung zu speichern, die Sie in Schritt 1 registriert haben:<AppName> ) in einer Variablen:

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   Ausführliche Informationen zu Syntax und Parametern finden Sie unter Get-AzureADServicePrincipal .

2. Stellen Sie im selben PowerShell-Fenster eine Verbindung zu Security & Compliance PowerShell her :

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint "<Your_Certificate_ThumbPrint>" -AppID
 $AADApp.AppId -Organization "<Your_organization>
```

   Führen Sie die folgenden Befehle aus, um ein Dienstprinzipalobjekt für die Azure-Anwendung zu erstellen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId -DisplayName
"<Descriptive Name>"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter New-ServicePrincipal .

[End]

### Richten Sie Ihre Now Platform® -Instanz für die Microsoft Exchange Online -Integration ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz von [ Now Platform® ausführen müssen, bevor Sie die Anwendung Microsoft Exchange Online installieren. Überprüfen Sie die Prüfliste, und vergewissern Sie sich, dass Sie diese Aufgaben abgeschlossen haben, bevor Sie die Anwendung Microsoft Exchange Online für die Integration herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

#### Vorbereitungen

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben. | Die folgenden ServiceNow Rollen sind erforderlich:<br>• Der Systemadministrator (admin) installiert Anwendungen und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) konfiguriert die Anwendung für die Integration. Bei Bedarf weist die Security Incident-Administratorrolle dem Security Incident-Analysten (sn_si.analyst) auch die E-Mail-Lese- und Schreibrollen (sn_sec_cmn.cap_email_write und sn_sec_cmn.cap_email_read) zu. Die Rollen (sn_sec_cmn.cap_email_read) und (com.snc.security_incident) werden mit dem Produkt Security Incident Response installiert. Sie werden standardmäßig dem Security Incident-Administrator zugewiesen und können bei Bedarf neu zugewiesen werden.<br>• Der Security Incident-Analyst (sn_si.analyst) führt E-Mail-Suchen durch und löscht E-Mails. Diese Rolle überprüft auch, ob E-Mails gelöscht wurden, und arbeitet mit Security Incidents.<br>  ○ Die Schreibrolle ermöglicht es sn_si.analyst, E-Mail-Suchen zu bearbeiten, zu erstellen, durchzuführen und Nachrichten zu löschen. Es gibt keine separate Rolle, die zum Löschen von Nachrichten erforderlich ist. |

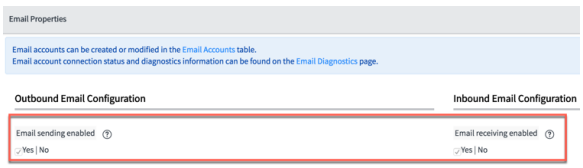


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | ○ Mit der Leserolle kann sn_si.analyst Ergebnisse in zugehörigen Listen zu Security Incidents anzeigen.<br><br>**Hinweis:**<br>Der sn_si.analyst muss über die Rollen (sn_sec_cmn.cap_email_read) und (sn_sec_cmn.cap_email_write) verfügen, um E-Mail-Suchergebnisse anzuzeigen und E-Mail-Suchabfragen zu erstellen und auszuführen.<br><br>Wenn nicht zugewiesen, wird in den folgenden Schritten beschrieben, wie die Rollen (sn_sec_cmn.cap_email_read) und (sn_sec_cmn.cap_email_write) dem Security Incident-Analysten zugewiesen werden.<br><br>Weitere Informationen zum Zuweisen von Rollen in Security Incident Responsefinden Sie unter Mit SIR installierte Rollen. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Das Plugin „ Security Incident Response Dependency“ (com.snc.si_dep) ist erforderlich. Es installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |
| Wenn Ihre Organisation E-Mail-Benachrichtigungen von Now Platform verwenden möchte, stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist. | Befolgen Sie diese Schritte, um sicherzustellen, dass die Funktion zum Senden und Empfangen von E-Mails in Ihrer Now Platform® -Instanz aktiviert ist. Diese Funktion benachrichtigt Benutzer per E-Mail, wenn Such- und Löschanforderungen initiiert und erfolgreich abgeschlossen wurden.<br>1. Navigieren zu **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**.<br>2. Vergewissern Sie sich in der Konfiguration für ausgehende E-Mails, dass E-Mail-Versand aktiviert und E-Mail-Empfang aktiviert ist.<br><br>Diese Funktion zum Senden/Empfangen von E-Mails ist erforderlich, damit Ihr Security Incident-Analyst E-Mail-Benachrichtigungen von Now Platform®erhält. Wenn die Löschgenehmigungsfunktion aktiviert ist, werden Anforderungen zum Löschen von E-Mails auch per E-Mail an Genehmiger gesendet. Abgesehen von der Aktivierung dieser E-Mail-Eigenschaft ist kein weiteres Setup erforderlich, um E-Mails in Now Platform®zu senden und zu empfangen. |
| |  |

Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird

Als Now Platform Security Incident-Administrator (sn_si.admin) werden Ihnen die Rollen „E-Mail-Leser und -Schreiber“ (sn_sec_cmn.cap_email_read) und „“ (sn_sec_cmn.cap_email_write) automatisch zugewiesen, wenn Sie das Produkt Security Incident Response (SIR) herunterladen. Als Security Incident-Administrator weisen Sie diese Rollen dem Security Incident-Analysten (sn_si.analyst) oder einer anderen Rolle zu. Wenn Sie diese Rollen nicht dem Security Incident-Analysten oder einer anderen Rolle zugewiesen haben, führen Sie die folgenden Schritte aus, um sie zuzuweisen.

### Prozedur

1. Navigieren zu **Organisation** > **Benutzer**.
2. Klicken Sie auf das Modul **Benutzer**.



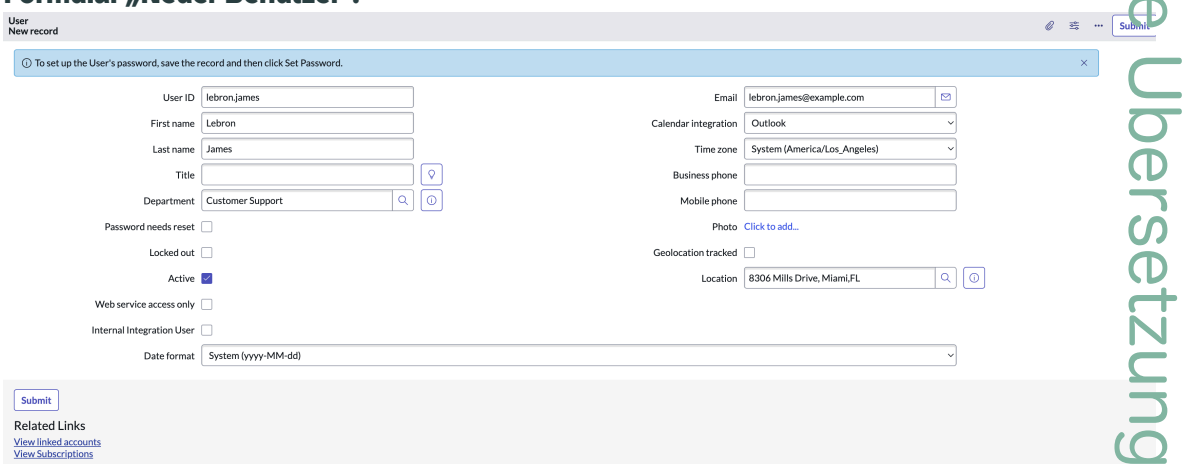
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie in der angezeigten Benutzerliste auf **Neu**.

**b.** Füllen Sie das angezeigte Formular „Neuer Benutzer“ aus.

| Feld | Beschreibung |
|---|---|
| Benutzer-ID | Benutzer-ID für die Rolle Now Platform „ Security Incident-Analyst“, z. B. `jferguson`. |
| E-Mail | E-Mail-Adresse des Unternehmens. Die Benachrichtigungen für E-Mail-Suchergebnisse und E-Mail-Löschbestätigungen werden an diese E-Mail-Adresse gesendet. In diesem Beispiel wird `jferguson@servicenow.com` verwendet, aber jede Unternehmens-E-Mail-Adresse kann verwendet werden, um diese E-Mail-Benachrichtigungen zu erhalten, wie von Ihrer Organisation benötigt. |
| Vorname | Vorname |
| Nachname | Nachname |
| Titel | Beispiel:`Security Incident-Analyst`, `Sicherheitsanalyst`oder `Security Operations Center (SOC) Analyst`. |

**Formular „Neuer Benutzer“.**




**c.** Klicken Sie auf **Absenden**.
Der neue Benutzer wird in der Benutzerliste angezeigt.

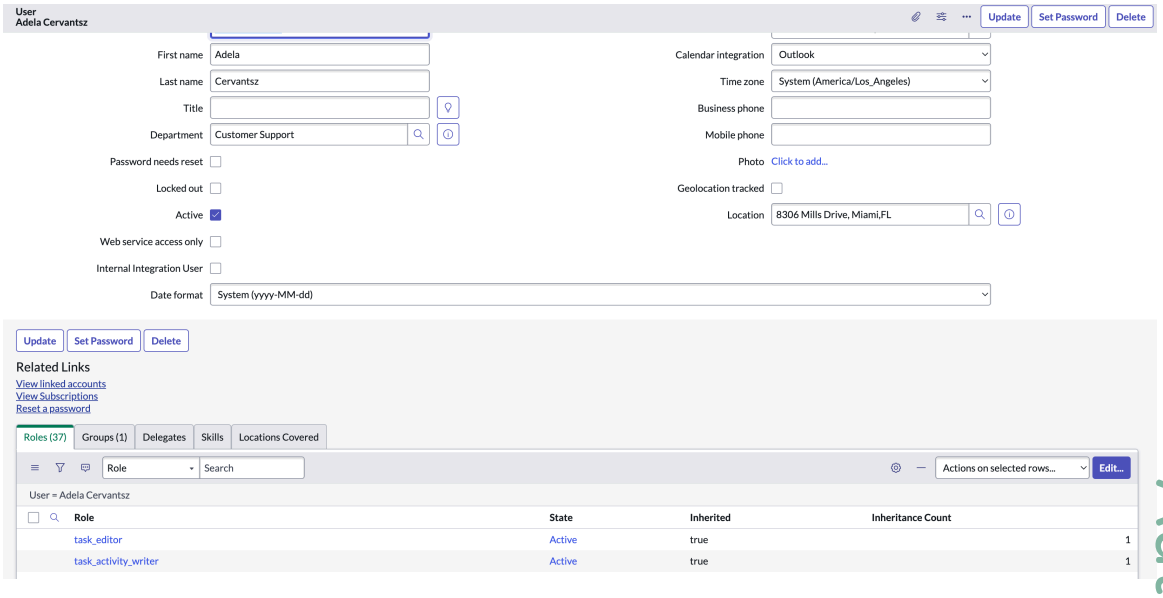
**3.** Klicken Sie in der Benutzerliste in der Spalte Benutzer-ID auf den Namen des Benutzers, dem Sie die Rollen `sn_sec_cmn.cap_email_read` und `sn_sec_cmn.cap_email_read` zuweisen möchten.

**4.** Klicken Sie im geöffneten Datensatz im Abschnitt „Zugehörige Links“ auf **Bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Benutzer bearbeiten“.**



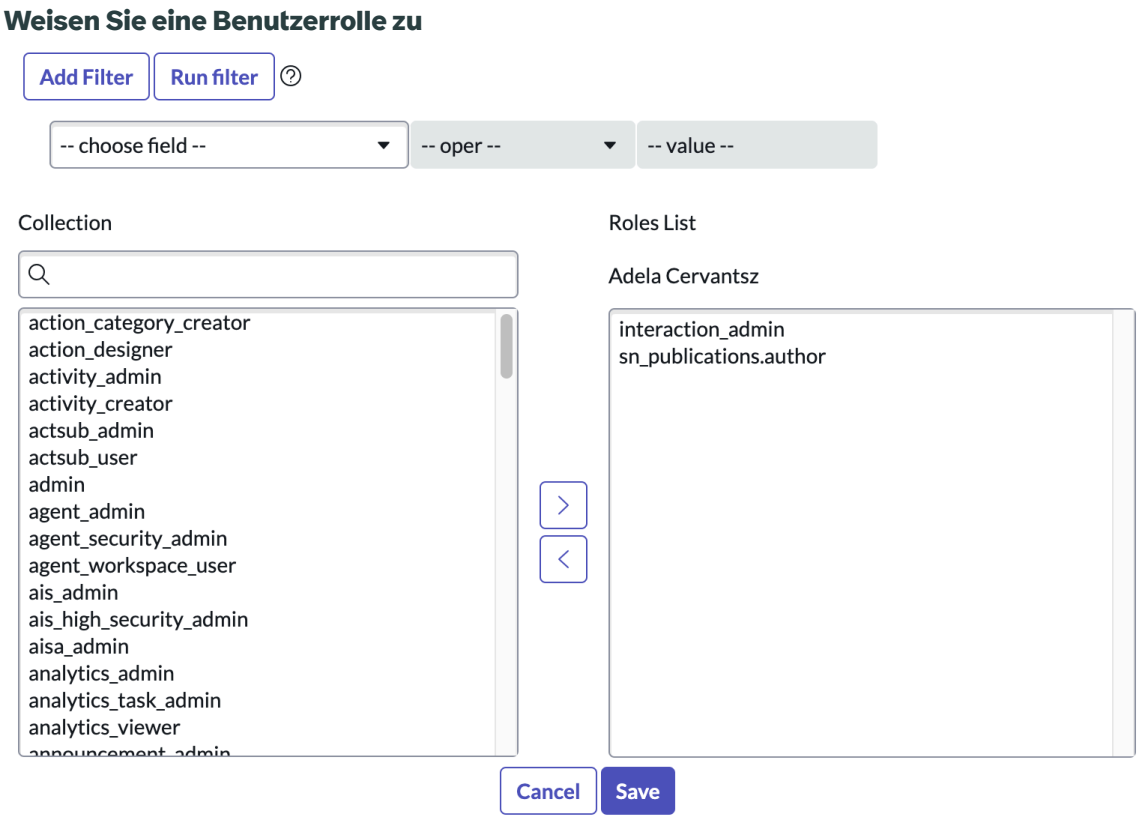

5. Geben Sie im angezeigten Formular „ Mitglieder bearbeiten“ sn_sec_cmn.cap_email_read in das Feld Sammlung ein.

> **Hinweis:**
> Die Spalte unter dem Feld wird automatisch ausgefüllt. Wenn dem Benutzer die Rolle sn_si.analyst nicht zugewiesen wurde, geben Sie sn_si.analyst auch in das Feld Sammlung ein. In der folgenden Abbildung wurde die Rolle sn_si.analyst bereits Joe Ferguson zugewiesen.

6. Wählen Sie in der Spalte Sammlung aus, und verschieben Sie sn_sec_cmn.cap_email_read und sn_sec_cmn.cap_email_read und sn_si.analyst (falls nicht bereits zugewiesen) in die Rollenliste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

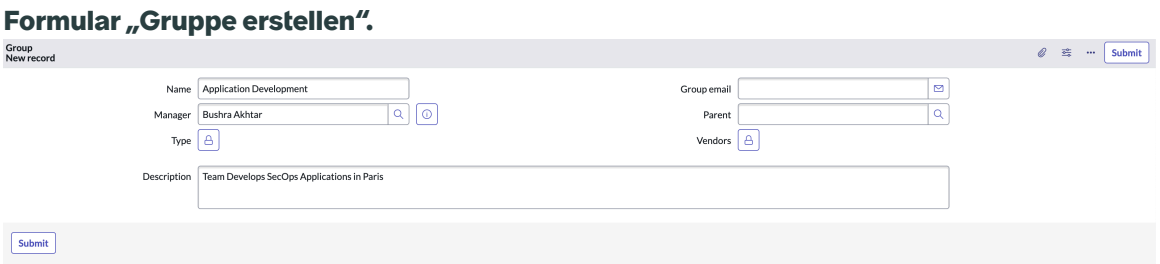



7. Klicken Sie auf **Speichern**.
   Die Rollen sn_sec_cmn.cap_email_read und sn_sec_cmn.cap_email_read werden dem Sicherheitsanalysten (jferguson) zugewiesen.
8. Fügen Sie Benutzer hinzu, und weisen Sie Rollen nach Bedarf für Ihre Organisation zu.
9. **Wahlweise:** Wenn Sie die Genehmigungsfunktion für E-Mail-Löschanforderungen aktivieren möchten, führen Sie die folgenden Schritte aus, um eine Genehmigungsgruppe zu erstellen.

   a. Navigieren zu **Benutzeradministration** > **Gruppen**.

   b. Klicken Sie in der angezeigten Gruppenliste auf **Neu**.

   c. Füllen Sie die Felder im Formular aus.




   Weitere Informationen zum Erstellen von Gruppen und Zuweisen von Rollen finden Sie unter Benutzergruppen erstellen .

   d. Klicken Sie auf **Absenden**.
   In der Spalte Name wird die neue Gruppe in der Gruppenliste angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können dieser Gruppe weitere Benutzer hinzufügen. Ein Benutzer erbt Rollen von allen Gruppen, denen er angehört. Sie können Rollen auch direkt einem Benutzer zuweisen. Weitere Informationen finden Sie unter Managing roles. Jeder Benutzer kann vom Sicherheitsanalysten übermittelte E-Mail-Löschanforderungen genehmigen. Es ist nur ein Benutzer erforderlich, um die Anforderung zu genehmigen oder abzulehnen.

Wenn Ihr Unternehmen mit dieser Integration eine zusätzliche Kontrolle über das Löschen von E-Mails haben möchte, aktivieren Sie die optionale Genehmigungsfunktion. Aktivieren Sie während des **Konfigurationsschritts** auf der Registerkarte Zusätzliche Einstellungen das Kontrollkästchen Aktivieren, um Genehmigungen zu aktivieren. Im vorherigen Beispiel ist jeder Benutzer der Exchange Online-Genehmigergruppe verfügbar, um Löschanforderungen per E-Mail-Benachrichtigung zu verarbeiten.

### Installieren Sie die Anwendung Microsoft Exchange Online für die Integration von ServiceNow Microsoft Exchange Online .

Bevor Sie die Integration in Ihrer Instanz ausführen, installieren Sie die Microsoft Exchange Online- Anwendung für die Integration aus dem ServiceNow Store.

#### Vorbereitungen

Führen Sie alle in den erforderlichen Prüflisten aufgeführten Aufgaben aus, bevor Sie die Anwendung aus ServiceNow Store in Ihrer Instanz von Now Platform ] installieren.

Erforderliche Rolle: admin

**Wichtig:**
Wenn Sie Demodaten installieren, wird automatisch eine Demokonfiguration ohne Anmeldeinformationen erstellt. Dies kann zu Fehlern führen. Weitere Informationen finden Sie unter KB0755880.

#### Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Nachdem Sie die Anwendung von ServiceNow Storeinstalliert haben, konfigurieren Sie sie so, dass eine Verbindung zu Ihrer Instanz von Now Platform hergestellt wird.

#### Zugehörige Informationen

Richten Sie Ihr Microsoft Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein

Richten Sie die Exchange Online-Integration mit Security Incident Response ein

Richten Sie Ihre Now Platform -Instanz für die Microsoft Exchange Online -Integration ein

### Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanz

Nachdem Sie die Anwendung von ServiceNow Storeinstalliert haben, konfigurieren Sie sie so, dass eine Verbindung zu Ihrer Instanz von Now Platform hergestellt wird. Durch diese Aktivierung werden die Such- und Lösch-Workflows aktiviert.

#### Vorbereitungen

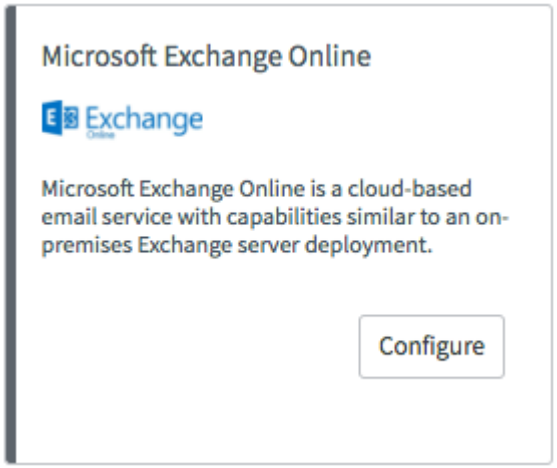
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

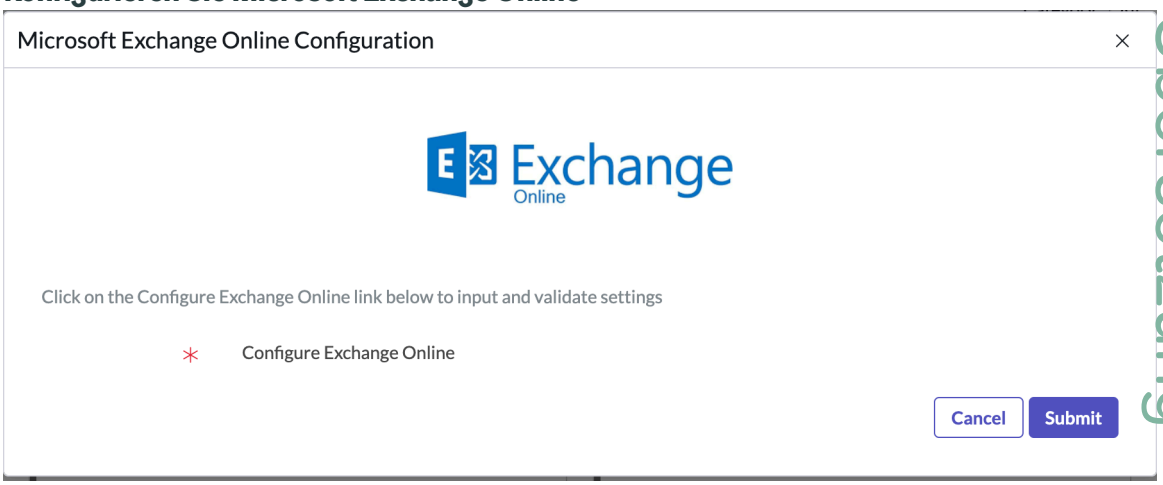
1. Navigieren Sie in Ihrer Instanz Now Platform zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Kachel Microsoft Exchange Online.
3. Klicken Sie auf **Konfigurieren**.




4. Klicken Sie im angezeigten Dialogfeld Microsoft Exchange Online Konfiguration auf **Exchange Online konfigurieren**.

Ein Beispiel für ein ausgefülltes und validiertes Formular folgt der Tabelle.

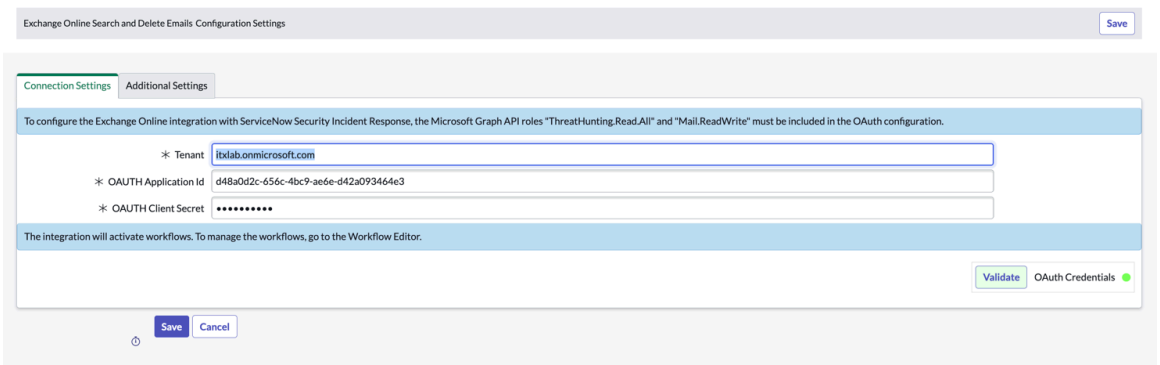
**Konfigurieren Sie Microsoft Exchange Online**



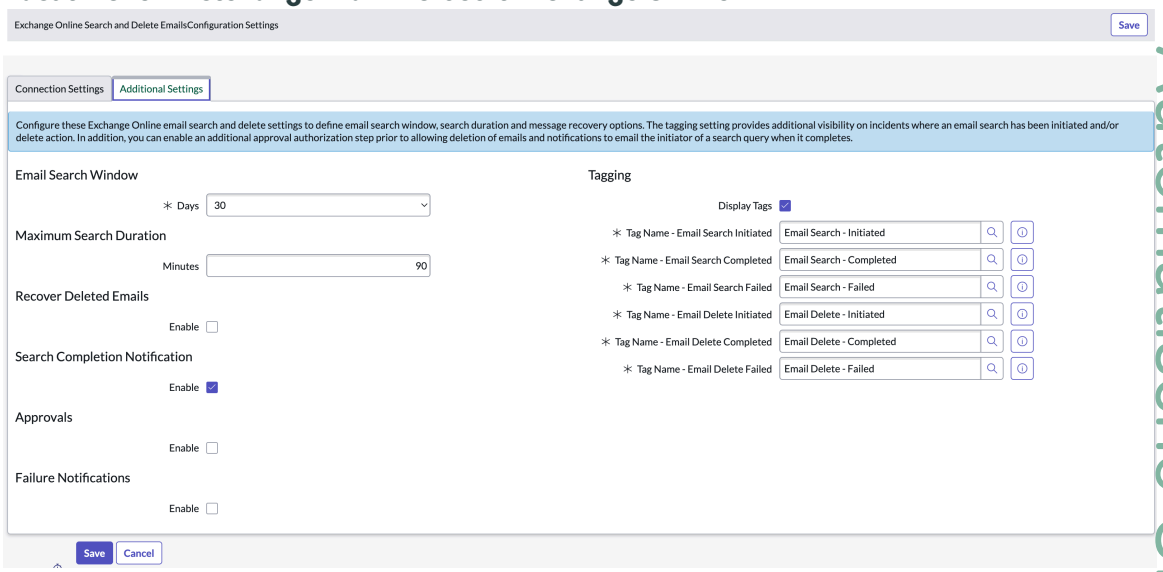

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Microsoft Exchange Online-Verbindungseinstellungen




### Zusätzliche Einstellungen für Microsoft Exchange Online




**5.** Wählen Sie eine, um fortzufahren.

**Trouble?**
Wenn eine Fehlermeldung angezeigt wird oder eine oder mehrere der Indikatoren rechts neben der Schaltfläche Validieren rot sind, stellen Sie sicher, dass die von Ihnen eingegebenen Anmeldeinformationen für das Benutzerkonto gültig sind. Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie erneut auf **Speichern**.

### Validierung nicht erfolgreich

In der folgenden Tabelle finden Sie weitere Informationen zur Schaltfläche **Validieren** und zu den farbigen Symbolen.

| Status der Schaltfläche „Validieren“ und der Indikatoren | Beschreibung |
|---|---|
| Validieren-Schaltfläche ist grün. | Gibt an, dass OAuth gültig ist. |
| Validieren-Schaltfläche ist hellrot. | Schaltfläche „Exchange Online OAuth-Anmeldeinformationen“ ist rot: Gibt an, dass die Exchange Online OAuth-Anmeldeinformationen ungültig sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Status der Schaltfläche „Validieren“ und der Indikatoren | Beschreibung |
|---|---|
| | **Hinweis:** Wenn eines der Verbindungsfelder wie Mandanten-ID, Client-ID oder Client-Secret ungültig ist, werden die entsprechenden Fehlermeldungen angezeigt. Stellen Sie sicher, dass Sie die gültigen Verbindungsdetails angeben. |

### Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an

Definieren Sie als Benutzer mit der Rolle sn_si.analyst Suchkriterien und senden Sie eine E-Mail-Suchanforderung basierend auf Incident-Details in einem Security Incident-Datensatz.

#### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Die Abbildungen in diesem Verfahren werden mit **Formularen** mit Registerkarten angezeigt, die in den Systemeinstellungen ausgewählt sind. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt „Formulare mit Registerkarten anzeigen“ in Formularlayout konfigurieren auf der ServiceNow-Website mit Produktdokumentation .

Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird

Der Status einzelner Nachrichten, die der Suchabfrage entsprechen, und die Ergebnisse der Suche werden im Security Incident-Datensatz gemeldet. Wenn E-Mail-Benachrichtigungen aktiviert sind, können Sie die Suchergebnisse aus einer E-Mail-Nachricht anzeigen.

Suchkriterien können Absenderadressen, Empfängeradressen oder Betreffnamen von Nachrichten sein. Die folgenden Kombinationen der Suchparameter Betreff, Absender und Empfänger werden häufig verwendet, um Phishing-bezogene E-Mail-Nachrichten zu finden, die Teil einer einzelnen Phishing-Kampagne sein können:

- Suchen Sie alle ursprünglichen E-Mails, die von einem Phishing-Account gesendet wurden: Suchen Sie nach Absender.
- Alle ursprünglichen E-Mails für eine einzelne Phishing-Kampagne suchen: Suchen Sie nach Betreff und Absender.
- Suchen Sie alle E-Mails, die für eine einzelne Phishing-Kampagne empfangen wurden (ursprünglich und weitergeleitet, beliebiger Absender): Suchen Sie nach Betreff.
- Suchen Sie alle weitergeleiteten E-Mails für eine einzelne Phishing-E-Mail von einem einzelnen Benutzer: Suche nach Empfänger + Betreff.
- Suchen Sie alle Phishing-bezogenen E-Mails, die an einen einzelnen Benutzer gesendet wurden: Suchen Sie nach Absender und Empfänger.

**Hinweis:**
Suchvorgänge werden für E-Mails durchgeführt, die innerhalb der letzten 30 Kalendertage gesendet oder empfangen wurden, es sei denn, während der Ersteinrichtung wird ein kürzeres Suchfenster konfiguriert. Eine erfolgreiche E-Mail-Suche ist erforderlich, bevor Sie E-Mails löschen können.

Das folgende Beispiel zeigt, wie Sie eine Suche aus einem Now Platform Security Incident initiieren. Ein Security Incident wird basierend auf der ursprünglichen E-Mail eines

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mutmaßlichen Phishing-Angriffs auf dem Microsoft Exchange Online -Server Ihrer Organisation erstellt. In diesem Beispiel lautet das Suchkriterium Absender (Von) plus Betreff, wobei „Von“ phisher@cbazyx.comund der Betrefflog in to your account(Anmeldedaten) ist.

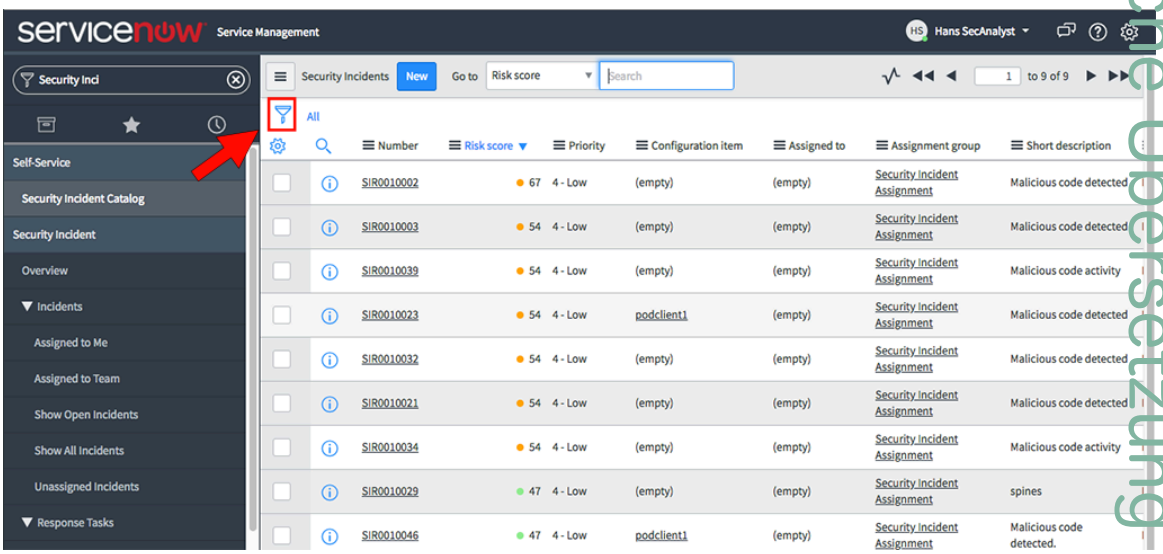
Ergebnisse für Suchvorgänge nach Themen werden zurückgegeben, wenn die Suche Textzeichenfolgen findet, die Schlüsselwörter enthalten, die den eingegebenen Suchkriterien entsprechen. In diesem Beispiel lautet der Betreff log in to your account(Beim Konto anmelden). Verwenden Sie den **AND-** Operator, um die Suchbedingungen „Von“ und „Betreff“ zu trennen und Ergebnisse für alle E-Mail-Nachrichten zurückzugeben, die diese Suchkriterien enthalten. Die folgenden Schritte beschreiben, wie Sie eine Suche einrichten, die nur E-Mails findet, die Betreffzeilentext enthalten, der von einem bestimmten Phishing-Account gesendet wurde.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, an dem Sie arbeiten.
2. Führen Sie alternativ die folgenden Schritte aus, um einen Filter so festzulegen und auszuführen, dass nur Security Incidents angezeigt werden, die durch Phishing-Ereignisse erstellt wurden.

   a. Navigieren zu **Security Incident** > **Alle Incidents anzeigen** , um die Liste der Security Incidents zu öffnen.

   b. Klicken Sie in der oberen linken Ecke der angezeigten Liste auf das Filtersymbol.

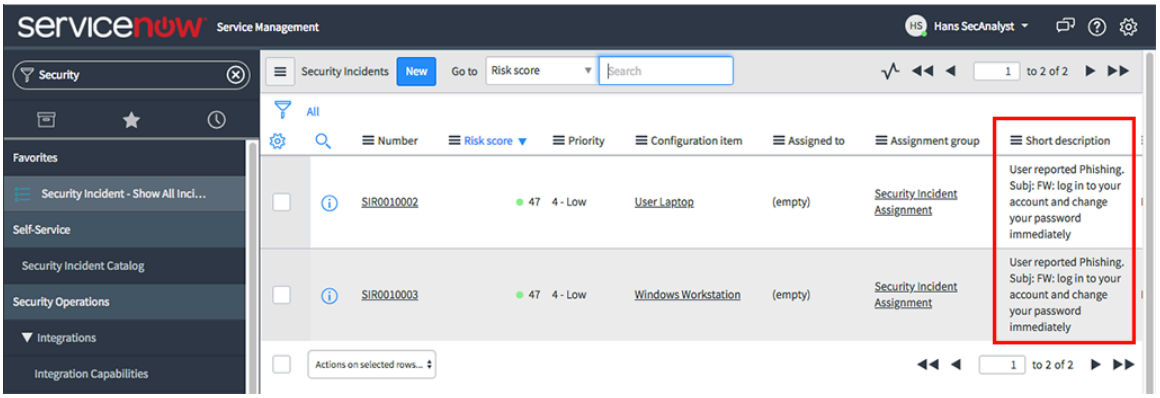



   c. Wählen Sie in den angezeigten Feldern aus **Kurzbeschreibung** > **enthält** Geben Sie in den **Auswahllisten Benutzer gemeldetes Phishing** ein, und klicken Sie auf **Ausführen**.

   Die Phishing-bezogenen Security Incidents werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

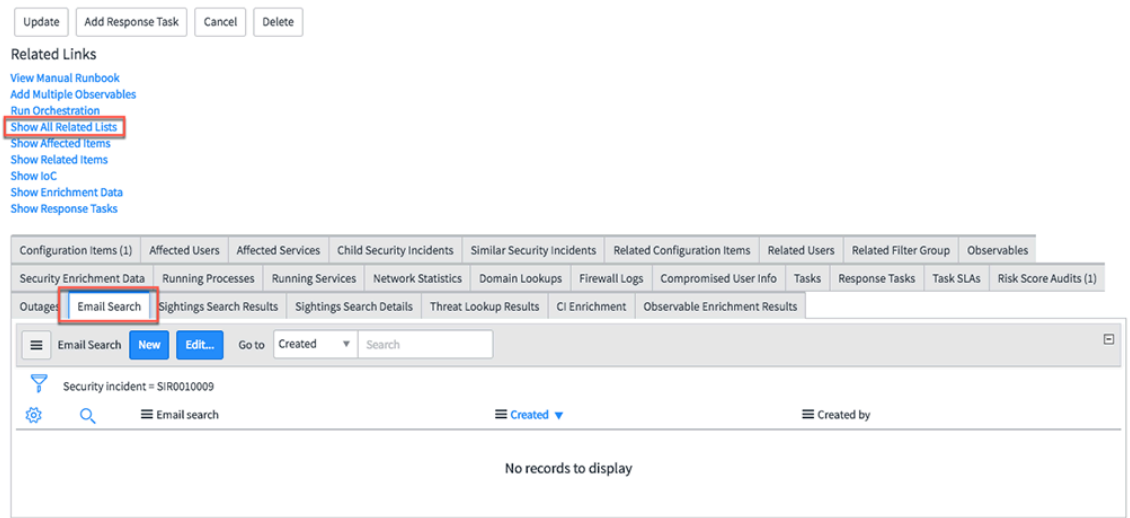



**d.** Verwenden Sie den Text in der Spalte Kurzbeschreibung, um den Security Incident zu finden, an dem Sie arbeiten.

**e.** Klicken Sie in der Spalte Nummer auf einen Security Incident, um einen Datensatz zu öffnen.

**3.** Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen, um diese zugehörige Liste anzuzeigen.



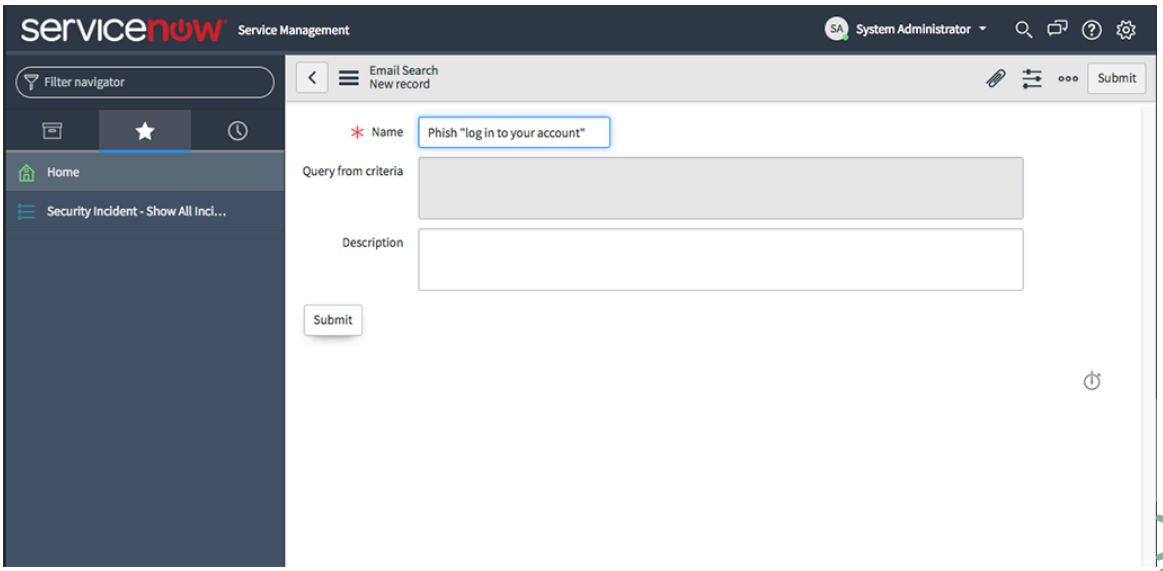

**4.** Klicken Sie in der zugehörigen Liste E-Mail-Suche auf **Neu**, um einen neuen E-Mail-Suchdatensatz zu erstellen.
Das Formular „E-Mail-Suche“ wird angezeigt. Wenn Sie der Meinung sind, dass Sie diese Suchabfrage für denselben Phishing-bezogenen Incident mit geringfügigen Änderungen erneut ausführen möchten, können Sie diesen Suchabfragedatensatz erneut verwenden. Es ist jedoch unwahrscheinlich, dass Sie diese Suche nach einem anderen Phishing-bezogenen Incident verwenden, da Phishing-Kampagnen dynamisch sind und sich die Absender- und Nachrichtenfelder häufig ändern.

**5. Wahlweise:** Um einen vorhandenen Suchabfragedatensatz zu bearbeiten, klicken Sie auf **Bearbeiten**.

**6.** Füllen Sie die Felder im Formular „E-Mail-Suche“ aus.

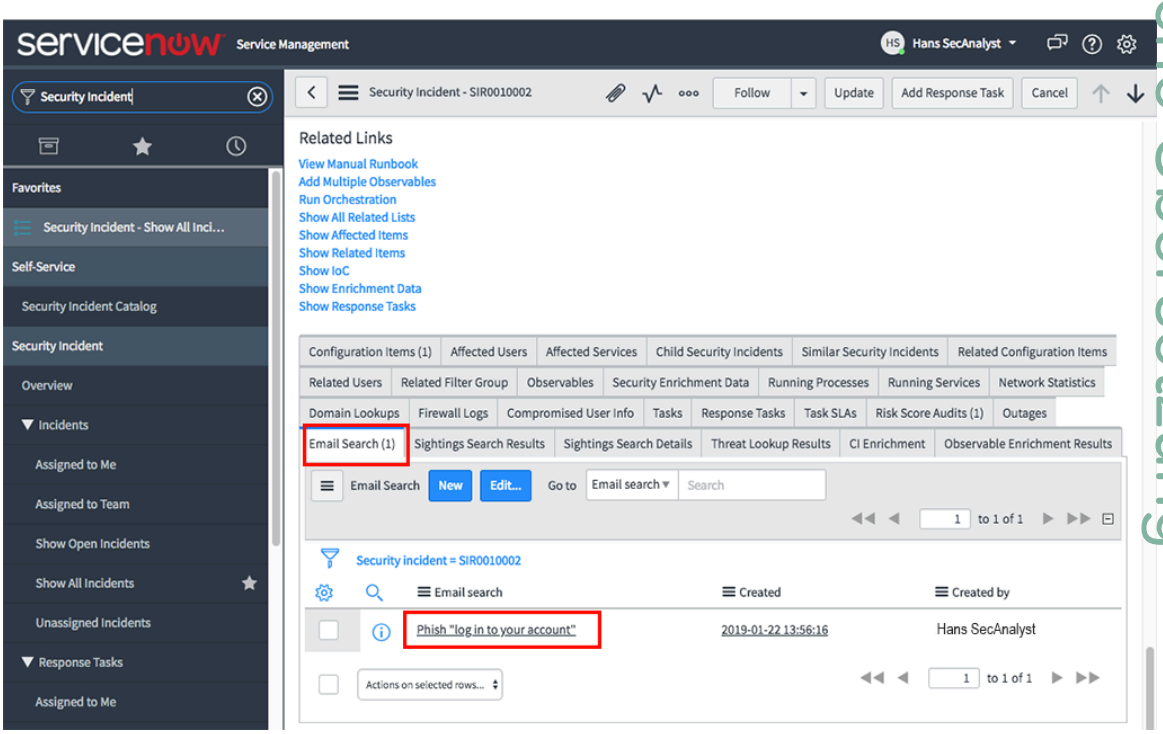
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Klicken Sie auf **Absenden**.
   Der Security Incident wird angezeigt, und der Name der E-Mail-Suche wird in der Spalte E-Mail-Suche in der zugehörigen Liste „E-Mail-Suche“ angezeigt. Bevor Sie diese neue Suchabfrage verwenden können, müssen Suchkriterien für den Suchdatensatz definiert werden.

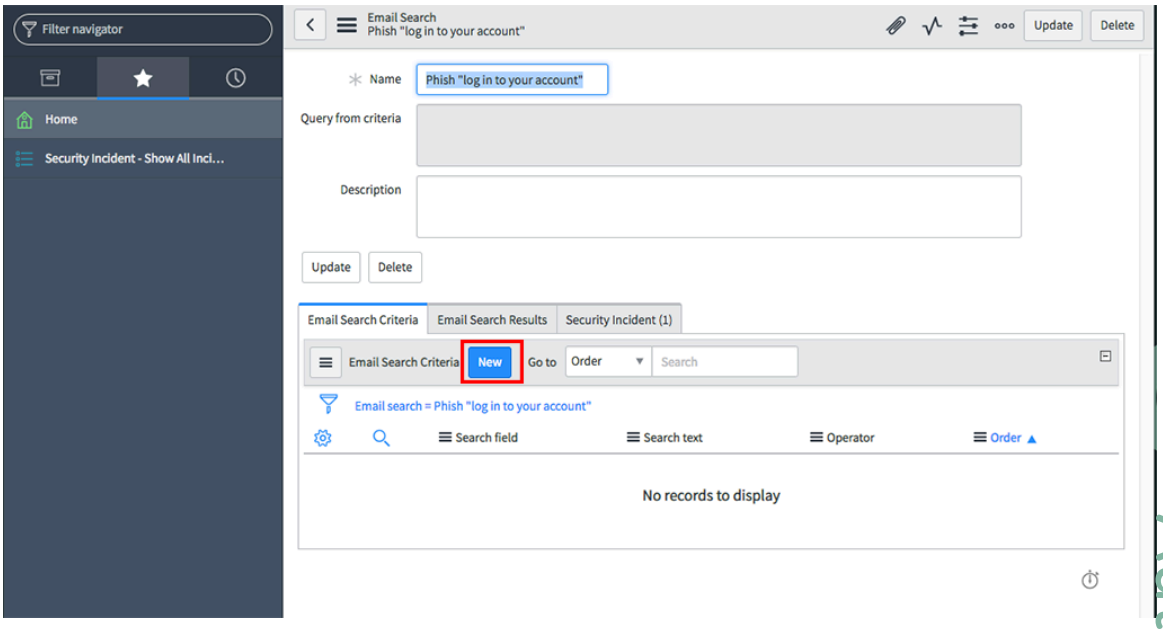
8. Um Suchkriterien zu definieren, klicken Sie bei ausgewählter zugehöriger Liste „E-Mail-Suche“ in der Spalte „E-Mail-Suche“ auf **Phishing „melden Sie sich bei Ihrem Konto an“**.




9. Klicken Sie im angezeigten E-Mail-Suchdatensatz auf die zugehörige Liste E-Mail-Suchkriterien und dann auf **Neu**.

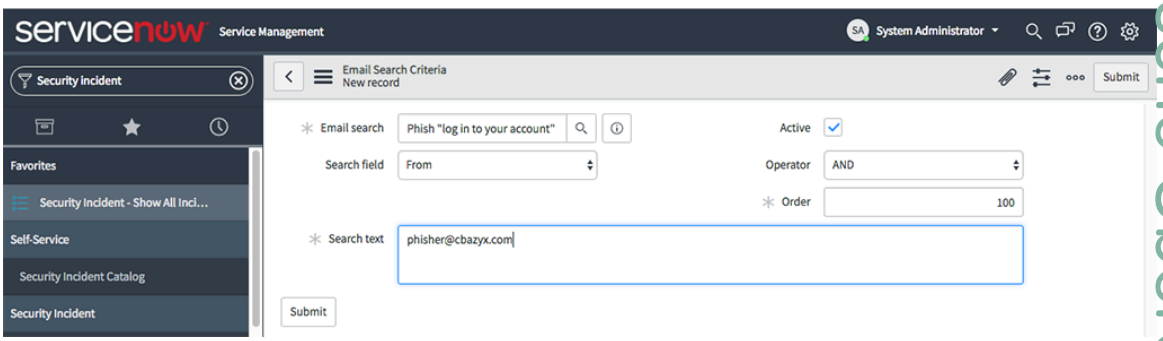
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

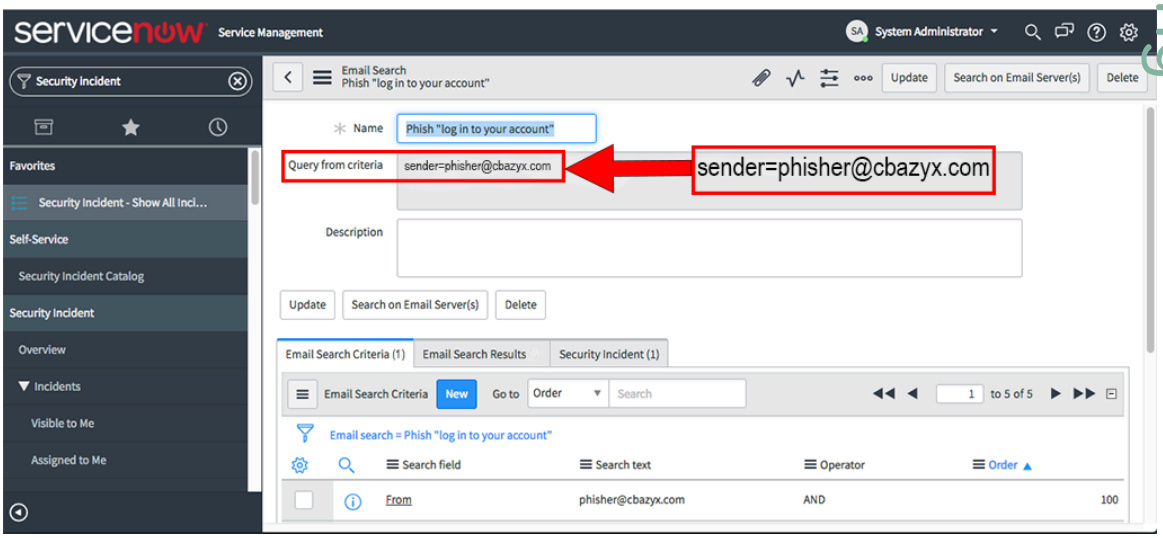



**10.** Füllen Sie die Felder im Formular „E-Mail-Suchkriterien“ aus.

Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.




**11.** Klicken Sie auf **Absenden**.
Der E-Mail-Suchdatensatz wird angezeigt. Im Feld **Abfrage anhand von Kriterien** werden die Suchkriterien angezeigt, die Sie für den Absender (Von) hinzugefügt haben.

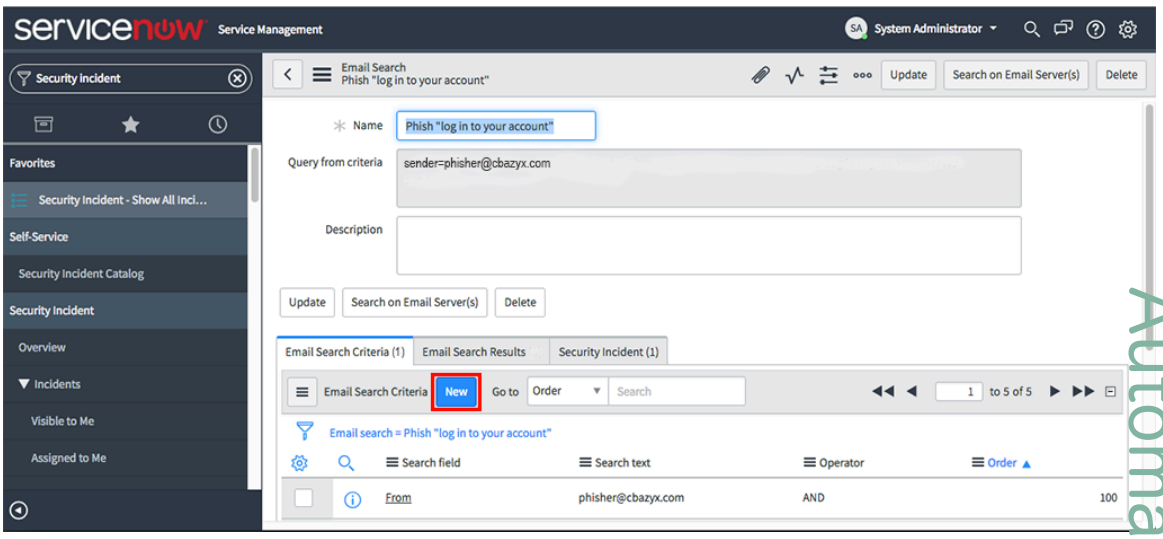



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**12.** Um diese E-Mail-Suchkriterien mit weiteren Informationen zu aktualisieren, sodass die Abfrage die gewünschte Bedingung für Betreff und Absender enthält, führen Sie die Schritte zum Hinzufügen einer weiteren Suchbedingung aus.

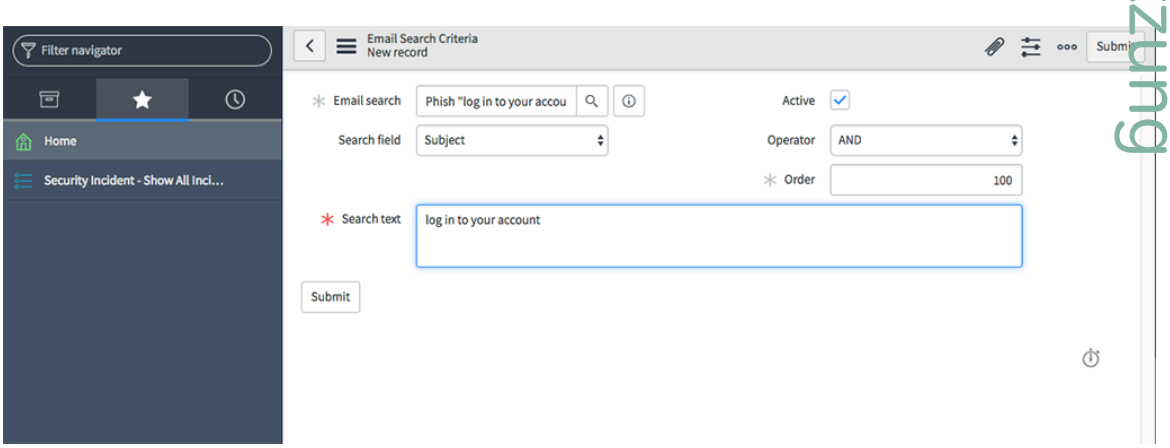
**a.** Klicken Sie in der zugehörigen Liste E-Mail-Suchkriterien auf **Neu**.




**b.** Wählen Sie in der Liste Suchfeld im Datensatz „E-Mail- **Suchkriterien**“, der angezeigt wird, **Betreff**aus.

**c.** Wählen Sie in der Liste Operator die Option**UND** oder **ODER**aus.
Wenn Sie **OR**auswählen, gibt die Suche Ergebnisse zurück, wenn entweder Schlüsselwörter in der Betreffzeilen-Textzeichenfolge übereinstimmen oder die E-Mail-Adressbedingung erfüllt ist. **UND** ist für dieses Beispiel ausgewählt, damit die Suche nur Ergebnisse für E-Mails zurückgibt, die die Schlüsselwörter der Betreffzeichenfolge enthalten und mit der E-Mail-Adresse des Absenders übereinstimmen.

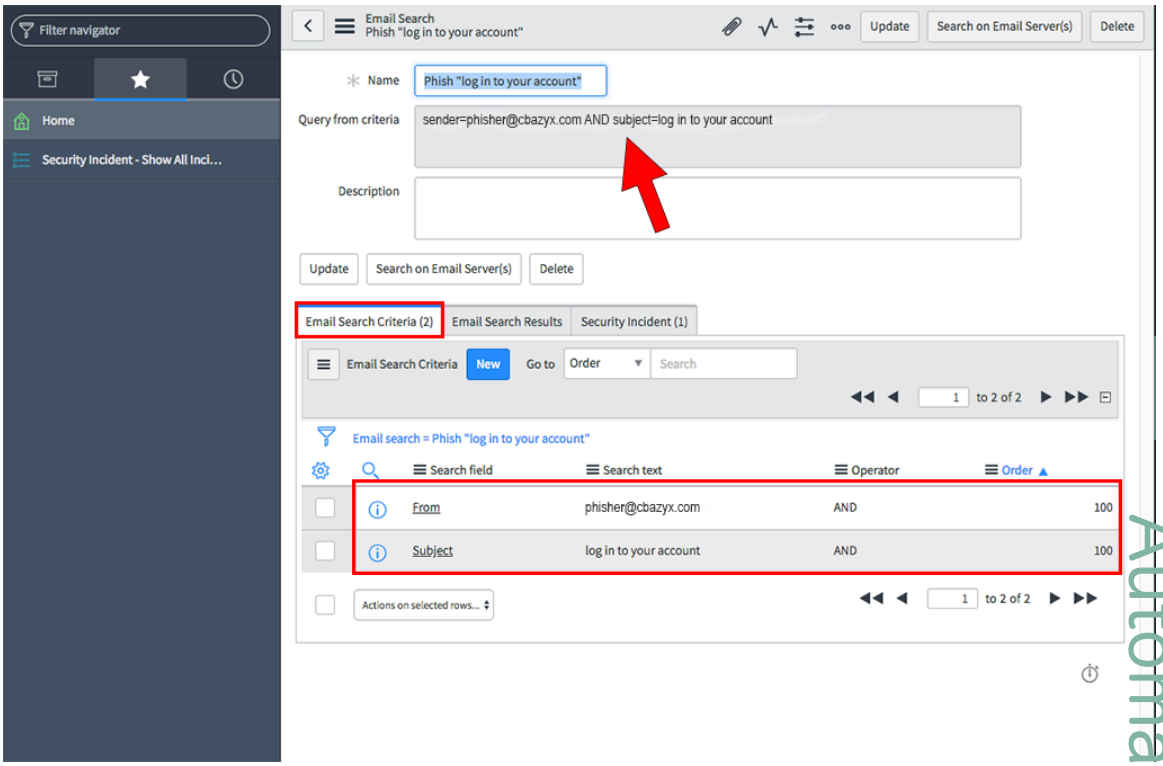
**d.** Geben Sie im Feld **Suchtext** den Wert für Betreffzeilentext ein, und melden Sie sich bei Ihrem -Konto an.




**e.** Klicken Sie auf **Absenden**.
Die neue Bedingung wird in der zugehörigen Liste E-Mail-Suchkriterien angezeigt, und beide Bedingungen werden im Feld **Abfrage aus Kriterien** angezeigt, getrennt durch den Operator **UND**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



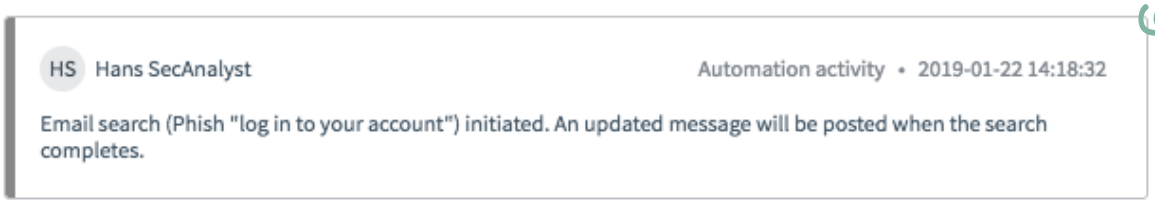

**f. Wahlweise:** Wenn Sie mehr als zwei Suchbedingungen haben und Sie **AND** auswählen, um die einzelnen Bedingungen zu trennen, legen Sie den Wert für die Reihenfolge fest, um sie zu priorisieren.

**g.** Fügen Sie nach Bedarf Suchkriterien hinzu, ändern oder entfernen Sie sie, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen am Datensatz zu speichern.

**13.** Wählen Sie eine Option aus, um fortzufahren.

**14.** Um eine E-Mail-Suche zu initiieren, klicken Sie im E-Mail- **Suchdatensatz auf E-Mail-Server**durchsuchen.
Eine Nachricht wird angezeigt, die angibt, dass die Suchanforderung übermittelt wurde.

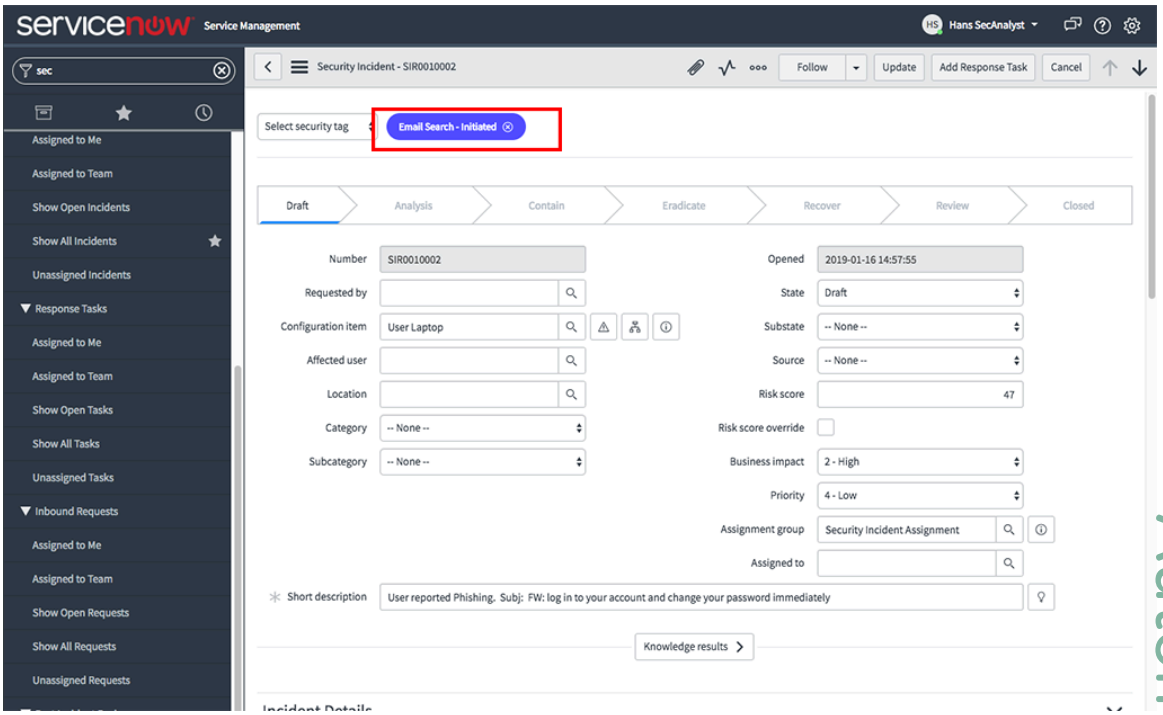
Im Security Incident-Datensatz wird eine Arbeitsnotiz angezeigt, die angibt, dass eine Suche initiiert wurde.




Wenn Tagging aktiviert ist, wird oben im Security Incident-Datensatz das Sicherheits-Tag E- Mail-Suche – Initiiert angezeigt.

Automatische Übersetzung

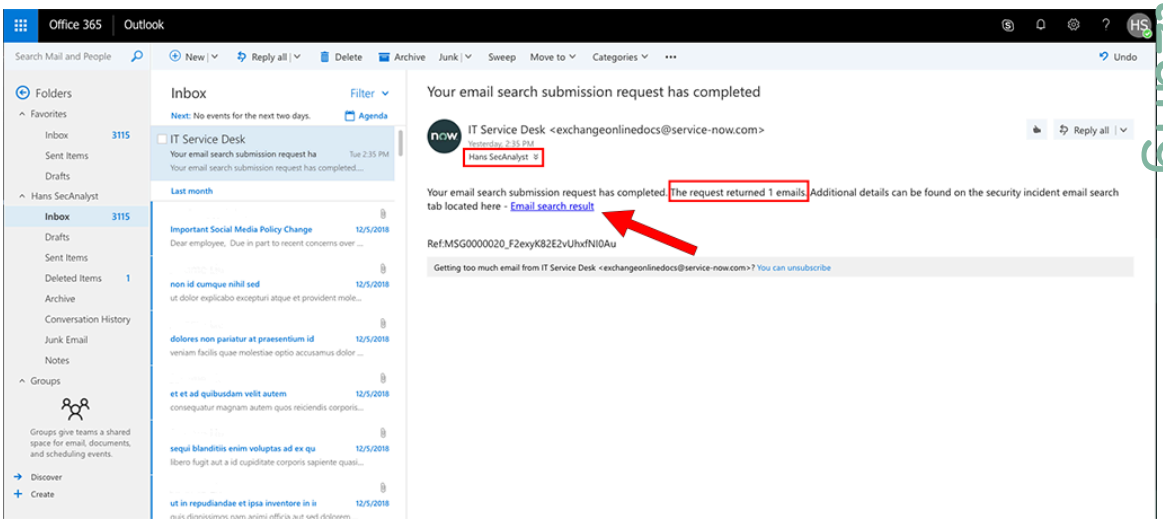
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn die Suche erfolgreich abgeschlossen wurde und E-Mail-Benachrichtigungen aktiviert sind, wird eine E-Mail an die E-Mail-Adresse der Person gesendet, die die Suche initiiert hat.

In diesem Beispiel hat der Benutzer mit der Rolle „sn_si.analyst“, „Hans SecAnalyst“, diese Suche übermittelt. Die folgende Abbildung zeigt, dass diese Benachrichtigung an ein Konto in Microsoft Exchange Onlinegesendet wird. Diese Benachrichtigungen können jedoch bei Bedarf an einen anderen E-Mail-Service gesendet werden.

Mit dieser Benachrichtigung können Sie alle übereinstimmenden Ergebnisse anzeigen, die nachverfolgt und gelöscht werden müssen. Das folgende Beispiel zeigt, dass eine E-Mail den Suchkriterien entspricht. Ein E-Mail-Suchergebnis-Link zum E-Mail-Suchergebnisdatensatz in Ihrer Now Platform -Instanz wird ebenfalls bereitgestellt. Wenn Sie den Suchdatensatz anzeigen möchten, klicken Sie auf diesen Link.



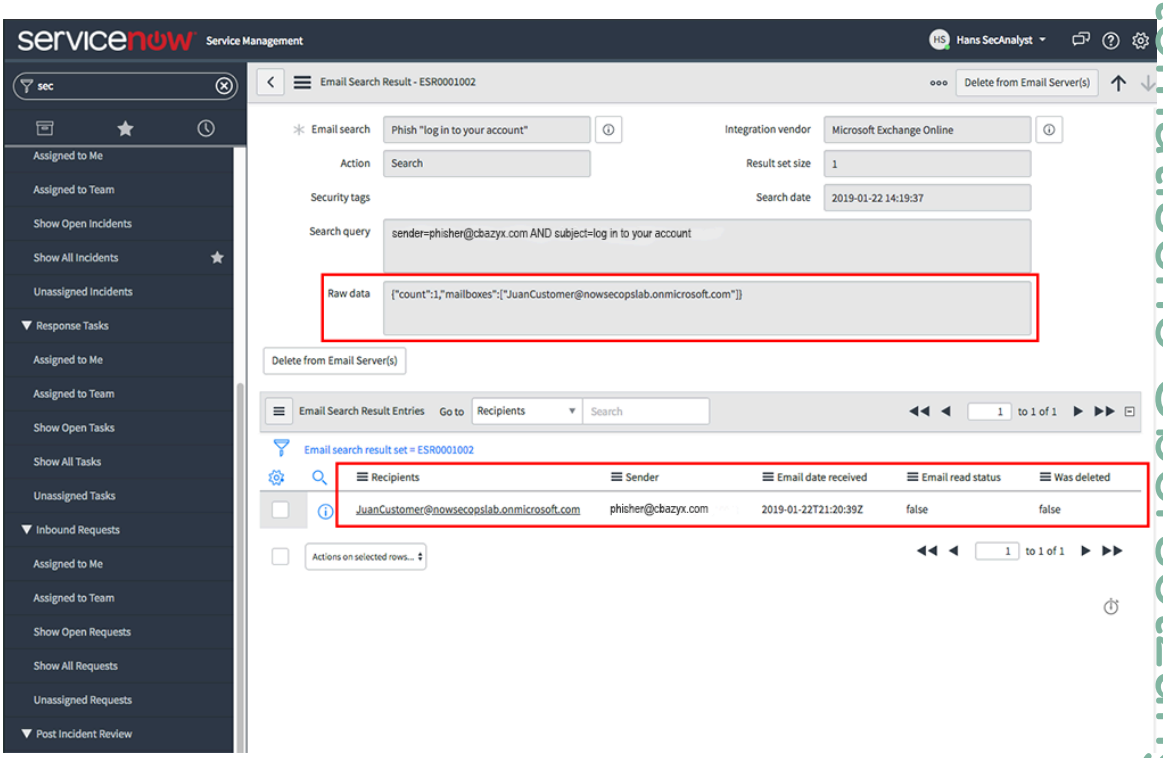

**15.** Klicken Sie in dieser E-Mail auf den Link **E-Mail-Suchergebnis**, um die Suchergebnisse anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der E-Mail-Suchergebnisdatensatz wird angezeigt. In diesem Datensatz können Sie die folgenden Daten überprüfen.

- Im Feld **Rohdaten werden** die E-Mail-Anzahl für die Anzahl der E-Mails angezeigt, die den Suchkriterien {"count":1}entsprechen, und die Postfachadressen, unter denen die E-Mails gefunden wurden ["JuanCustomer@nowsecopslab.onmicrosoft.com"].
- In der Spalte Empfänger lautet der Empfänger (JuanCustomer@nowsecopslab.onmicrosoft.com).
- In der Spalte Absender wird die Quelle der E-Mail angezeigt.
- In der Spalte Empfangene E-Mail werden das Datum und die Uhrzeit des E-Mail-Empfangs angezeigt, damit Sie die Zeitachsen der Phishing-Kampagne nachverfolgen können.
- In der Spalte E- Mail-Lesestatus wurde die E-Mail in diesem Beispiel nicht gelesen (false). Wenn eine E-Mail gelesen wurde, wird „ true “ angezeigt.
- In der Spalte Wurde gelöscht wurde die E-Mail in diesem Beispiel nicht gelöscht. Wenn eine E-Mail gelöscht wurde, wird true angezeigt.

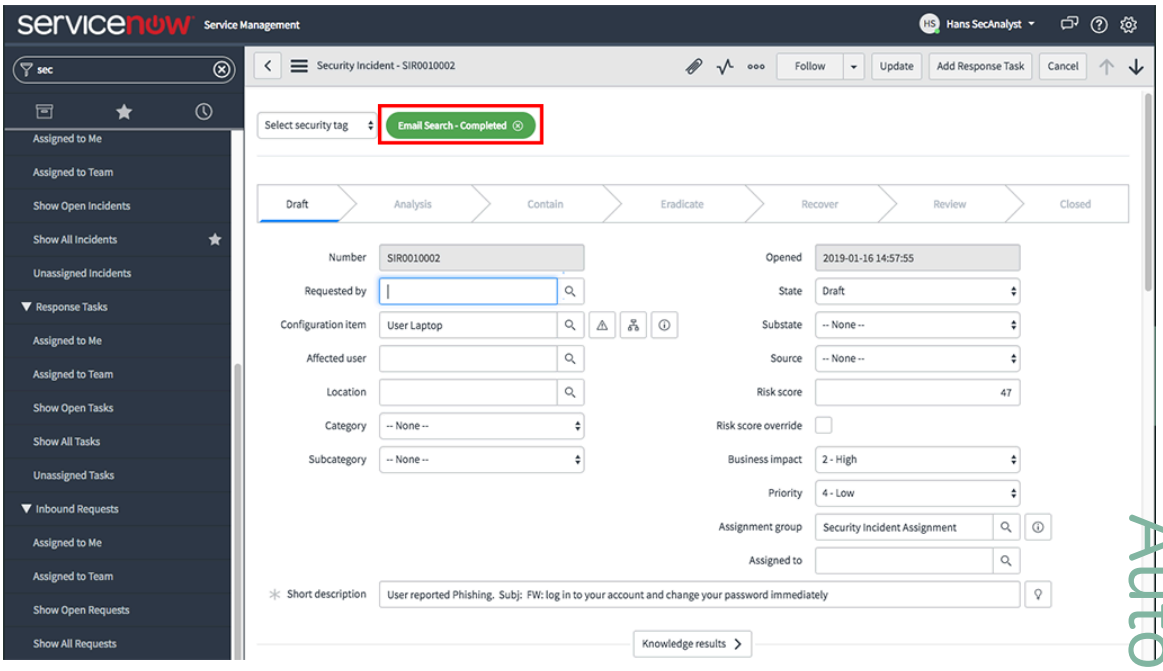



**16.** Führen Sie alternativ die folgenden Schritte aus, um die Suchergebnisse aus dem Security Incident anzuzeigen.

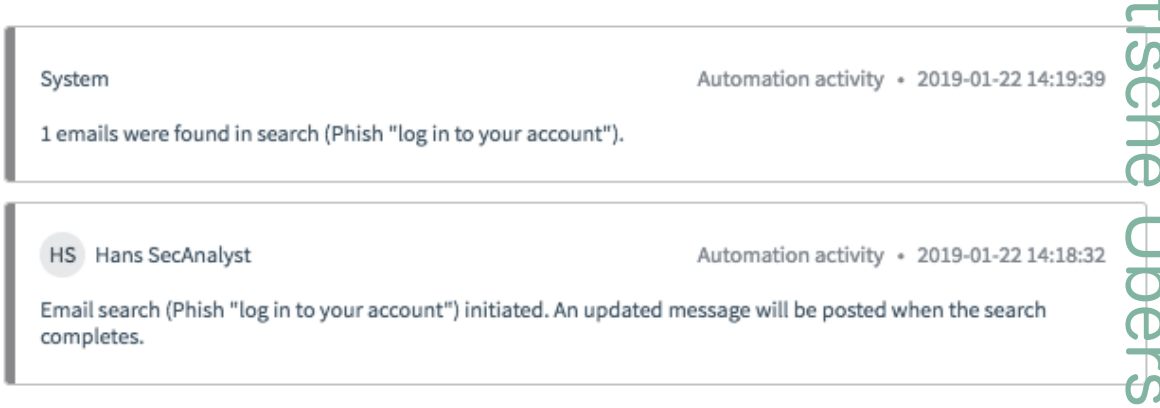
**a.** Navigieren zu **Security Incident** > **Incidents** und öffnen Sie den Security Incident, mit dem Sie arbeiten.
Wenn die Suche oben im Datensatz erfolgreich abgeschlossen wurde, ersetzt das Sicherheits-Tag „E-Mail-Suche – Abgeschlossen “ das Sicherheits-Tag „E- Mail-Suche – Initiiert “.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Arbeitsnotizen werden angezeigt, dass die Suche erfolgreich abgeschlossen wurde und eine übereinstimmende E-Mail gefunden wurde.

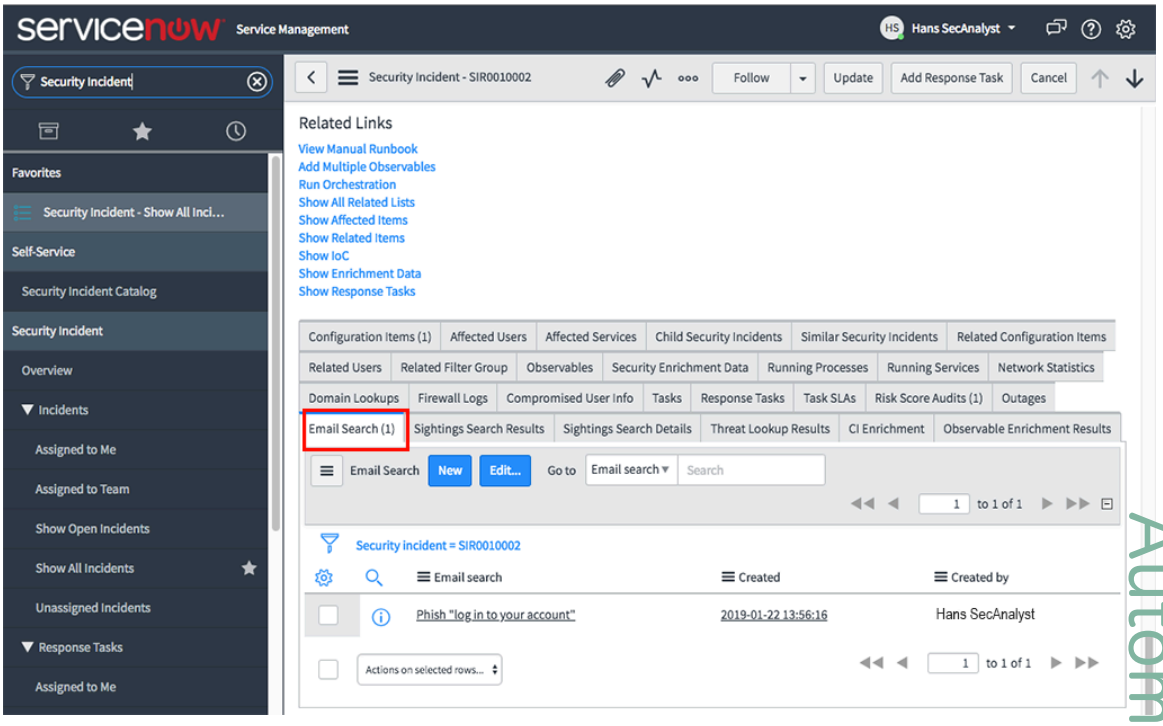



**b.** Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

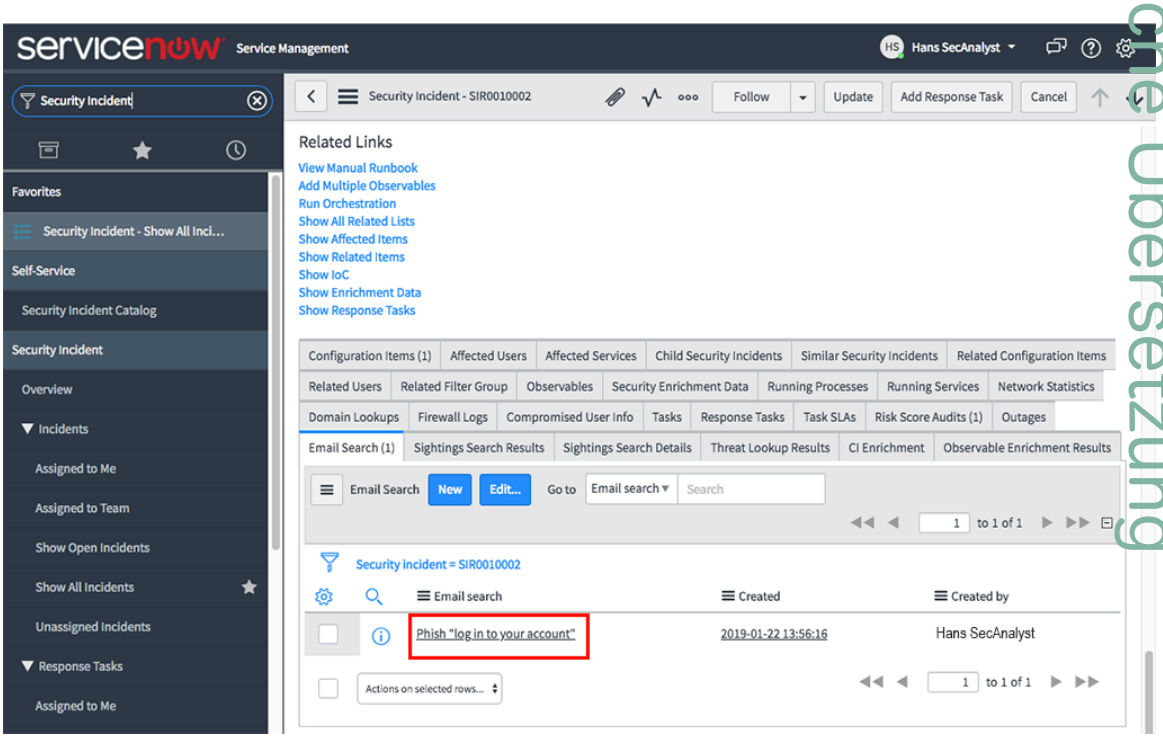
Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf den zugehörigen Link**Alle zugehörigen Listen** anzeigen, um diese zugehörige Liste anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**c.** Wählen Sie die zugehörige Liste „E-Mail-Suche“ aus und klicken Sie in der Spalte „E-Mail-Suche“ auf den Namen Ihrer Suche.



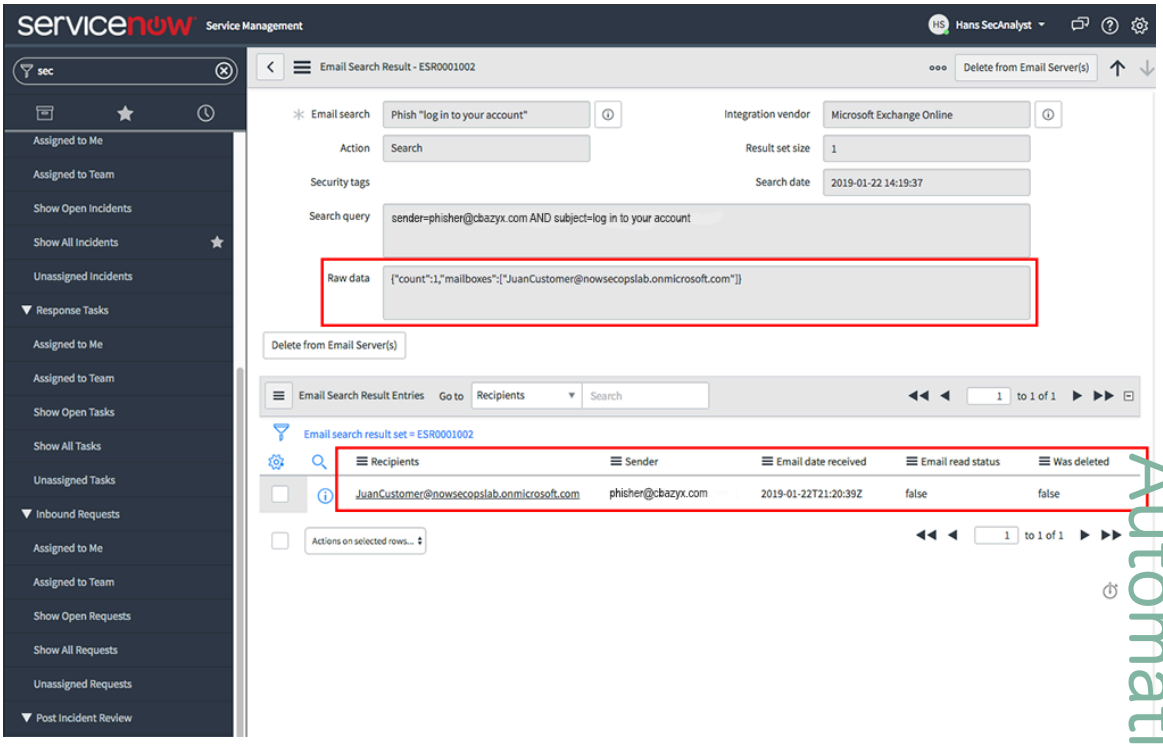

**d.** Klicken Sie im Datensatz „E-Mail-Suche“ auf die zugehörige Liste „E-Mail-Suchergebnisse“.

**e.** Klicken Sie in der Spalte Suchdatum auf das Datum der Suche, um die Daten anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der E-Mail-Suchergebnisdatensatz wird angezeigt.




Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde, werten Sie die Ergebnisse aus. Wenn Sie der Meinung sind, dass E-Mails korrigiert werden müssen, können Sie E-Mails jetzt löschen oder die Genehmigung zum Löschen anfordern.

### Fordern Sie die Löschgenehmigung für E-Mails im Microsoft Exchange-Onlinedienst an

Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde und übereinstimmende Nachrichten identifiziert wurden, können Sie alle verdächtigen E-Mails im Zusammenhang mit dem Security Incident und der Phishing-Kampagne dauerhaft aus dem Microsoft Exchange-Onlinedienst löschen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Das System löscht Ihre letzten erfolgreichen Suchergebnisse.

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn die Genehmigungen und E-Mail-Benachrichtigungen aktiviert sind, senden Sie vor der E-Mail-Entfernung eine Anforderung zum Löschen von E-Mails an eine Genehmigungsgruppe.

E-Mail-Suchergebnisse werden mit allen empfangenen Nachrichten angezeigt. Um sicherzustellen, dass Phishing-E-Mails erfolgreich gelöscht werden, werden die Löschergebnisse in den Arbeitsnotizen des zugehörigen Security Incidents veröffentlicht. Wenn Tagging aktiviert ist, wird auch ein Sicherheits-Tag für den zugehörigen Security Incident angezeigt. Wenn die E-Mail nicht erfolgreich gelöscht wird, werden Sie auch in den Arbeitsnotizen benachrichtigt.

Abhängig von Ihren Organisationsrichtlinien müssen Sie möglicherweise eine Genehmigung anfordern, bevor Sie Phishing-E-Mails löschen. Der Löschungsgenehmigungsprozess erfordert Informationen über die Anzahl der zu löschenden E-Mails und möglicherweise Zugriff auf andere Nachrichtendetails. Für die Verarbeitung der Löschanforderung wird einem Genehmiger in einer E-Mail-Benachrichtigung die entsprechende Anzahl der E-Mail-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

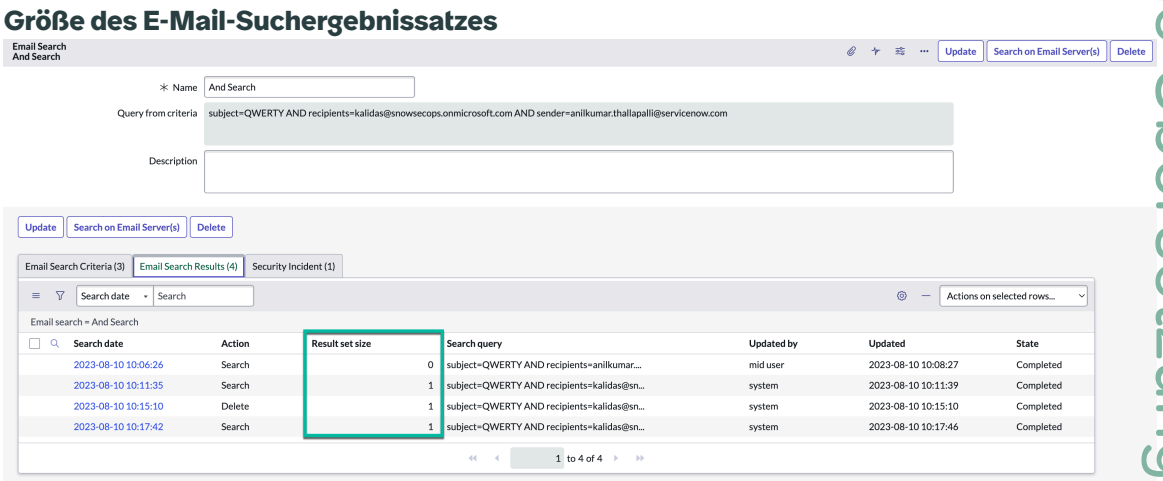
Nachrichten, der Security Incident-Link für den Zugriff auf vollständige Nachrichtendetails und Links zum Genehmigen oder Ablehnen bereitgestellt. Die Links in dieser E-Mail ermöglichen es einem Genehmiger, die Löschanforderung aus der E-Mail-Benachrichtigung zu akzeptieren oder abzulehnen. Ein vollständiger Auditpfad mit Zeitstempel ist ebenfalls verfügbar, der nachverfolgt, wann sich der Genehmigungsstatus in Arbeitsnotizen geändert hat. Wenn eine Genehmigungsgruppe zugewiesen ist, kann ein Benutzer in der Gruppe die Anforderung für die gesamte Gruppe bearbeiten. Jedes Mitglied der Genehmigungsgruppe erhält eine E-Mail-Benachrichtigung für die Anforderung.

Wenn Sie als Benutzer mit der Rolle „sn_si.analyst“ feststellen, dass E-Mails korrigiert werden müssen, führen Sie die erforderlichen Schritte zum Löschen von E-Mails aus. Wenn Genehmigungen aktiviert sind, fordern Sie die Genehmigung zum Löschen von E-Mails aus dem Service Microsoft Exchange Online an.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident > Alle Incidents anzeigen**.
2. Klicken Sie auf die zugehörige Liste E- **Mail-Suche**.
3. Wählen Sie die zugehörige Liste „E-Mail-Suche“ aus und klicken Sie in der Spalte „E-Mail-Suche“ auf den Namen Ihrer Suche.
   Die Suchergebnisse werden in der zugehörigen Liste „E-Mail-Suchergebnisse“ angezeigt.

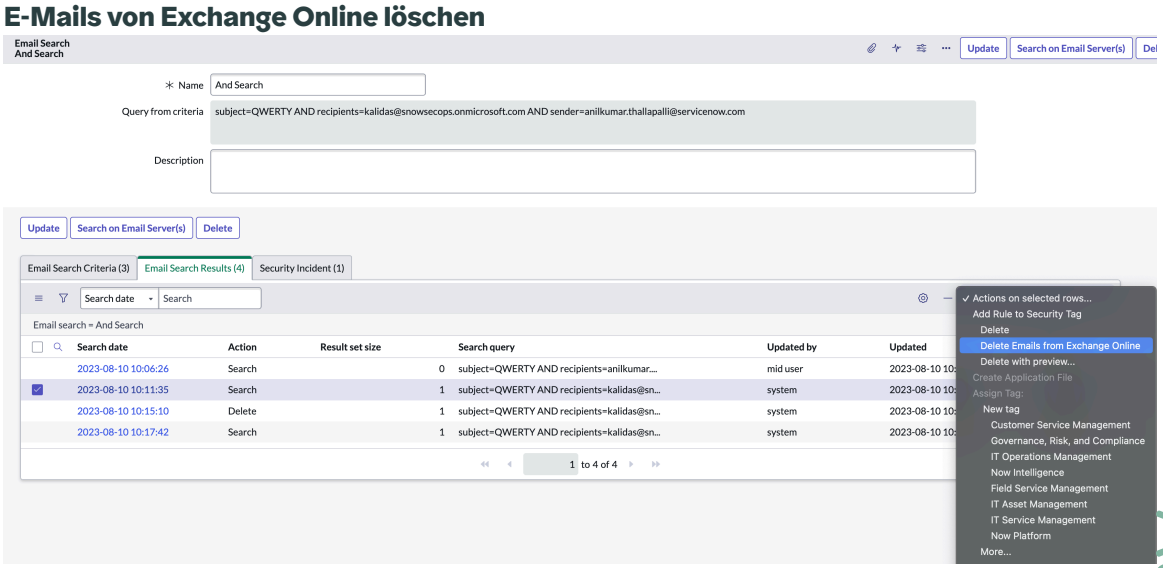
   In diesem Beispiel hat diese Suche E-Mails gefunden, die Ihren Suchkriterien entsprechen. Im Datensatz sind zwei Suchaktionen aufgeführt. Eine Suche hat keine Übereinstimmungen (0), und die andere Suche hat eine übereinstimmende E-Mail-Adresse (1).




4. Um E-Mail-Elemente zu löschen, die einer Suche zugeordnet sind, aktivieren Sie links neben der Spalte Suchdatum das Kontrollkästchen eines Suchergebnissatzes.
   Sie können einen einzelnen Ergebnissatz oder mehrere Ergebnissätze aus der Liste auswählen.
5. Wählen Sie die Ergebnissätze aus, die Sie löschen möchten.

Automatische Übersetzung

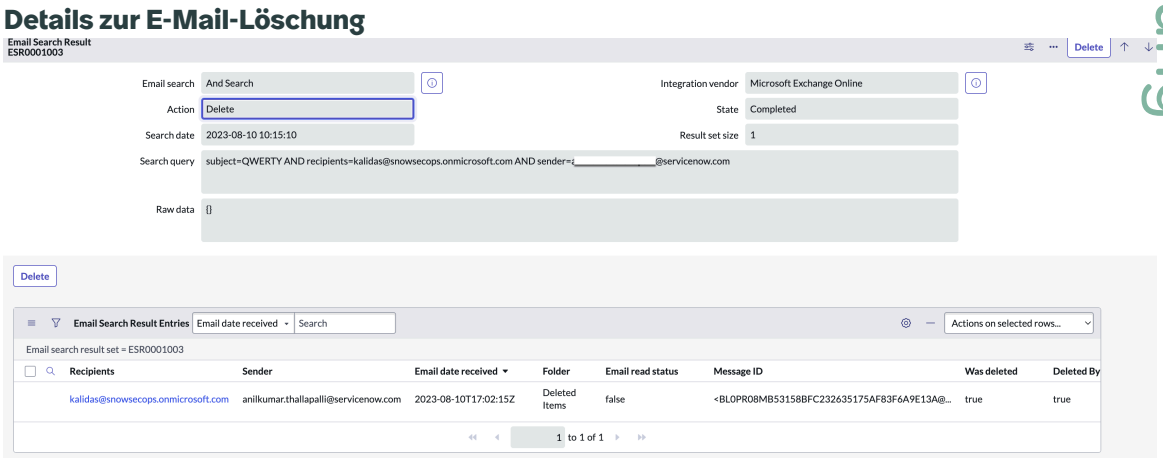
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**6.** Wählen Sie unten in der zugehörigen Liste „E-Mail-Suchergebnisse“ aus der Liste Aktionen für ausgewählte Zeilen die Option E- **Mails aus Exchange Online** löschen aus, um alle E-Mail-Elemente zu löschen, die einer oder mehreren Ergebnismengen vom Exchange Online-Server zugeordnet sind.
Wenn ein Ergebnissatz mehr als eine E-Mail enthält, müssen Sie den Datensatz „E-Mail-Suchergebnis“ nicht öffnen und einzelne E-Mails auswählen, um sie zu löschen. Alle E-Mail-Elemente mit dem Status „ falsch “ in der Spalte Wurde gelöscht im Datensatz „E-Mail-Suchergebnis“ werden gelöscht, nachdem Sie E- **Mails aus Exchange Online**löschen ausgewählt haben.

Wenn ein E-Mail-Element in einem Ergebnissatz bereits gelöscht wurde, lautet der Status in der Spalte Wurde gelöscht im Datensatz „E-Mail-Suchergebnis“ true. Diese Elemente werden nicht erneut gelöscht.

Wenn die Genehmigungsoption während des Konfigurationsschritts deaktiviert ist, werden die mit dem Ergebnissatz verknüpften E-Mails gelöscht, nachdem Sie E- **Mails aus Exchange Online**löschen ausgewählt haben. Die Ergebnismenge selbst wird nicht gelöscht. Der Status aller gelöschten E-Mail-Elemente des Ergebnissatzes wird jedoch in der Spalte Wurde gelöscht des Datensatzes „E-Mail-Suchergebnis“ auf „ true “ aktualisiert. Weitere Informationen zur Genehmigungsfunktion finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanz.




Diese E-Mails werden aus dem Mandanten Microsoft Exchange Online gelöscht, für den Sie die Suchvorgänge ausgeführt haben. Wenn die E-Mails erfolgreich gelöscht wurden, wird eine Arbeitsnotiz angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

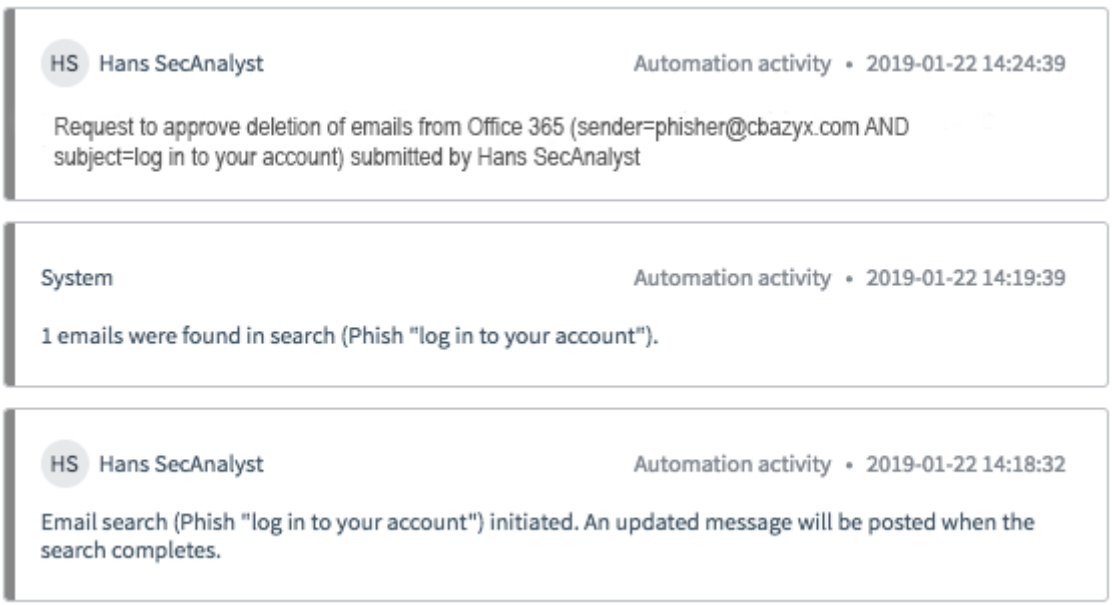
Im Security Incident-Datensatz wird das Sicherheits-Tag „E- Mail-Löschung abgeschlossen “ angezeigt.

Wenn Genehmigungen für Löschanforderungen deaktiviert sind, haben Sie E-Mails erfolgreich aus dem Mandanten Microsoft Exchange Online gelöscht.

Wenn während des Konfigurationsschritts Genehmigungen für Löschanforderungen aktiviert sind, wird nach Auswahl von E- **Mails aus Exchange Online**löschen eine E-Mail-Benachrichtigung an jedes Mitglied der Genehmigungsgruppe gesendet, die Sie während des Konfigurationsschritts ausgewählt haben.

Wenn Tagging während des Konfigurationsschritts aktiviert ist, wird das Sicherheits-Tag E- Mail-Löschung initiiert im zugehörigen Security Incident-Datensatz angezeigt. Weitere Informationen zum Tagging finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanz.

Arbeitsnotizen werden angezeigt, wenn eine Anforderung zum Löschen von E-Mails vom Benutzer mit der Rolle sn_si.analyst (Hans SecAnalyst) gesendet wird.



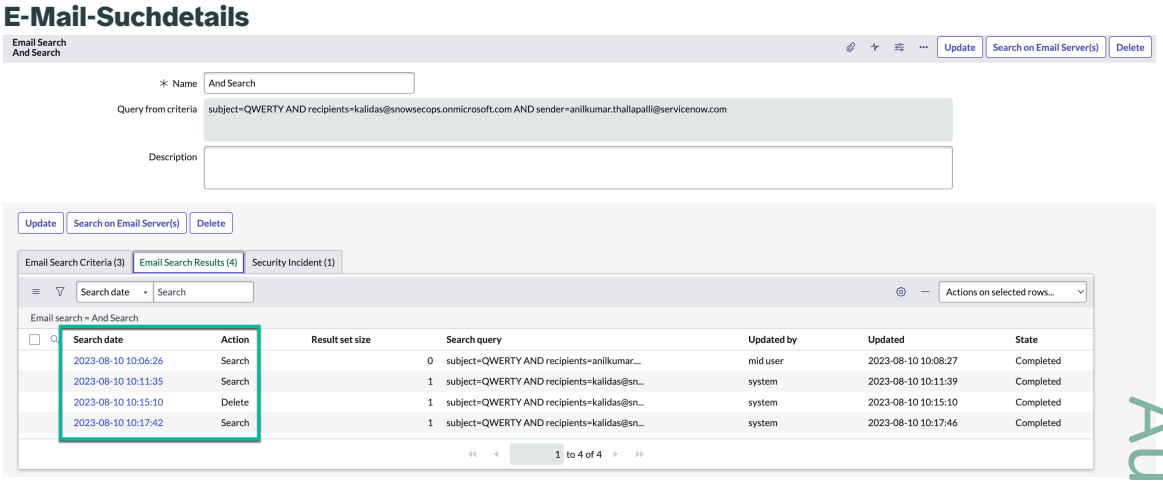

Wenn Genehmigungen aktiviert sind, besteht der nächste Schritt darin, die Löschanforderung zu verarbeiten.

7. Wenn Sie alternativ die Details und einzelnen E-Mail-Elemente eines Suchdatensatzes anzeigen möchten, bevor Sie ihn löschen oder eine Löschanforderung senden, führen Sie die folgenden Schritte aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wählen Sie die zugehörige Liste „E-Mail-Suchergebnisse“ aus und klicken Sie in der Spalte „Suchdatum“ auf das Datum einer Suche, die Sie überprüfen möchten.




Die folgenden Informationen zu den E-Mails werden angezeigt:

- Empfänger
- Absender
- Empfangsdatum der E-Mail
- E-Mail-Lesestatus (wahr oder falsch)
- Wurde gelöscht („true “ oder „ false“)
- Nach Integration gelöscht (wahr oder falsch)

**Hinweis:**

Der Wert wird auf „true“ festgelegt, wenn die E-Mail gelöscht wird, wenn der Analyst „Von E-Mail-Server löschen“ initiiert.

Die Arbeitsnotizen werden mit der Gesamtzahl der gelöschten Datensätze aktualisiert, einschließlich der nach Integration und Benutzer gelöschten Datensätze.

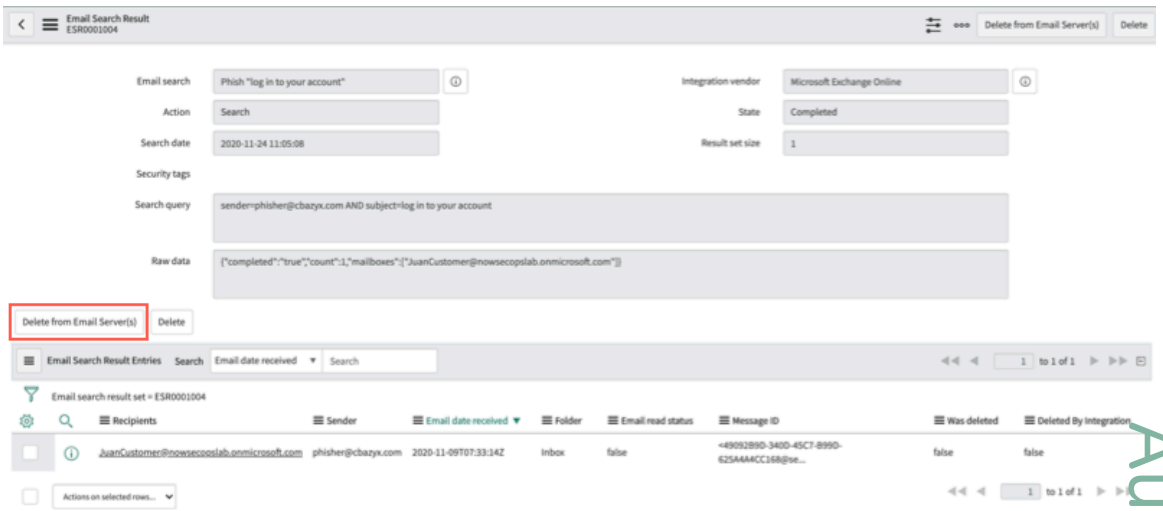
**b.** Nachdem Sie die Daten überprüft haben, klicken Sie **auf Von E-Mail-Server(n)**löschen, um alle E-Mails zu löschen oder eine Anforderung zum Löschen aller E-Mails zu senden.

Wie im vorherigen Beispiel beschrieben, müssen Sie, wenn im Suchergebnisdatensatz mehrere E-Mail-Adressen aufgeführt sind, die einzelnen E-Mail-Adressen nicht auswählen, um sie zu entfernen. Die Löschanforderung entfernt alle mit der Suche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verknüpften E-Mails, wenn in den letzten Suchergebnissen in der Spalte Wurde gelöscht false angezeigt wird.




Wenn Genehmigungen aktiviert sind, haben Sie erfolgreich eine Anforderung zum Löschen von E-Mails übermittelt. Die Sicherheits-Tags und Arbeitsnotizen werden im zugehörigen Security Incident-Datensatz angezeigt, wie im vorherigen Beispiel beschrieben. Als Genehmiger besteht der nächste Schritt darin, die Löschanforderung zu verarbeiten.

### Genehmigen Sie E-Mail-Löschanforderungen für die Microsoft Exchange Online -Integration

Wenn die Genehmigungsoption in Ihrer Instanz Now Platform aktiviert ist, werden Anforderungen zum Löschen von E-Mails per E-Mail an jedes Mitglied der Genehmigungsgruppe gesendet. Sie wählen die Genehmigungsgruppe während des Konfigurationsschritts aus. Genehmigungen bieten Ihrer Organisation eine zusätzliche Kontrolle über die Löschung von E-Mails.

#### Vorbereitungen

Vergewissern Sie sich, dass die Option **Genehmigungen** auf der Registerkarte Zusätzliche Einstellungen des Exchange Online-Formulars „Konfigurationseinstellungen für E-Mails durchsuchen und löschen“ ausgewählt ist.

Vergewissern Sie sich, dass Sie die Optionen E-Mail E- **Mail-Versand aktiviert**und E- **Mail-Empfang aktiviert** in Ihrer Now Platform -Instanz für Genehmigungsanforderungen aktiviert haben. Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die Microsoft Exchange Online -Integration ein.

Wenn der Benutzer mit der Rolle sn_si.analyst E-Mail-Löschanforderungen sendet, werden diese Anforderungen standardmäßig per E-Mail an sn_si.admin gesendet. Wenn Sie eine Genehmigungsgruppe erstellt haben, erhält jedes Mitglied der Gruppe eine Benachrichtigung. Genehmiger können E-Mail-Löschanforderungen direkt über die E-Mail-Benachrichtigung verarbeiten. Alternativ können Anforderungen aus den E-Mail-Suchergebnisdatensätzen in Now Platform Instanzen verarbeitet werden. In diesem Thema werden beide Genehmigungsmethoden beschrieben.

Die folgenden Informationen beschreiben die Anforderung in der E-Mail-Benachrichtigung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Datensatznummer des E-Mail-Suchergebnisses**

Eindeutige Nummer, die dem Suchdatensatz von Now Platform als Teil des Auditpfads zugewiesen wird.

**Name des Analysten, der die Anforderung übermittelt hat**

Name der Person, die die Anforderung als Teil des Auditpfads übermittelt hat.

**Link zum Security Incident**

Ein Link zu dem Security Incident im Zusammenhang mit dem Phishing-Ereignis. Zeigen Sie den Security Incident mit den Arbeitsnotizen, E-Mail-Suchen und E-Mail-Suchergebnissen direkt aus der E-Mail an.

**Links zum Genehmigen oder Ablehnen**

Links zum Genehmigen oder Ablehnen der Anforderung aus der E-Mail-Benachrichtigung. Nachdem Sie auf einen der beiden Links geklickt haben, initiiert das System automatisch den zugehörigen Workflow, und eine Arbeitsnotiz wird im Security Incident-Datensatz veröffentlicht.

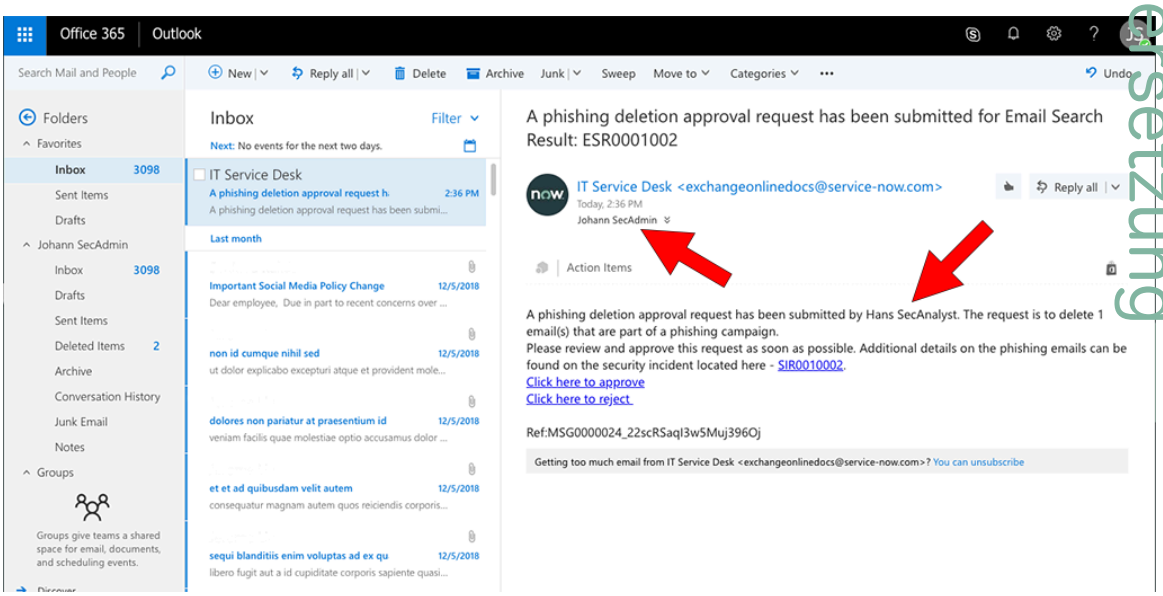
Erforderliche Rolle: sn_si.admin oder alle Mitglieder einer zugewiesenen Genehmigungsgruppe.

## Prozedur

1. Führen Sie die folgenden Schritte aus, um die Löschanforderung aus der E-Mail-Benachrichtigung zu verarbeiten.

   a. Suchen Sie als Genehmiger die Benachrichtigungs-E-Mail in dem E-Mail-Konto, das Sie in Ihrem Now Platform -Benutzerkonto konfiguriert haben.

   In diesem Beispiel sendet der Benutzer mit der Rolle sn_si.analyst (Hans SecAnalyst) eine Anforderung zum Löschen einer E-Mail. John SecAdmin ist Mitglied der Genehmigungsgruppe.



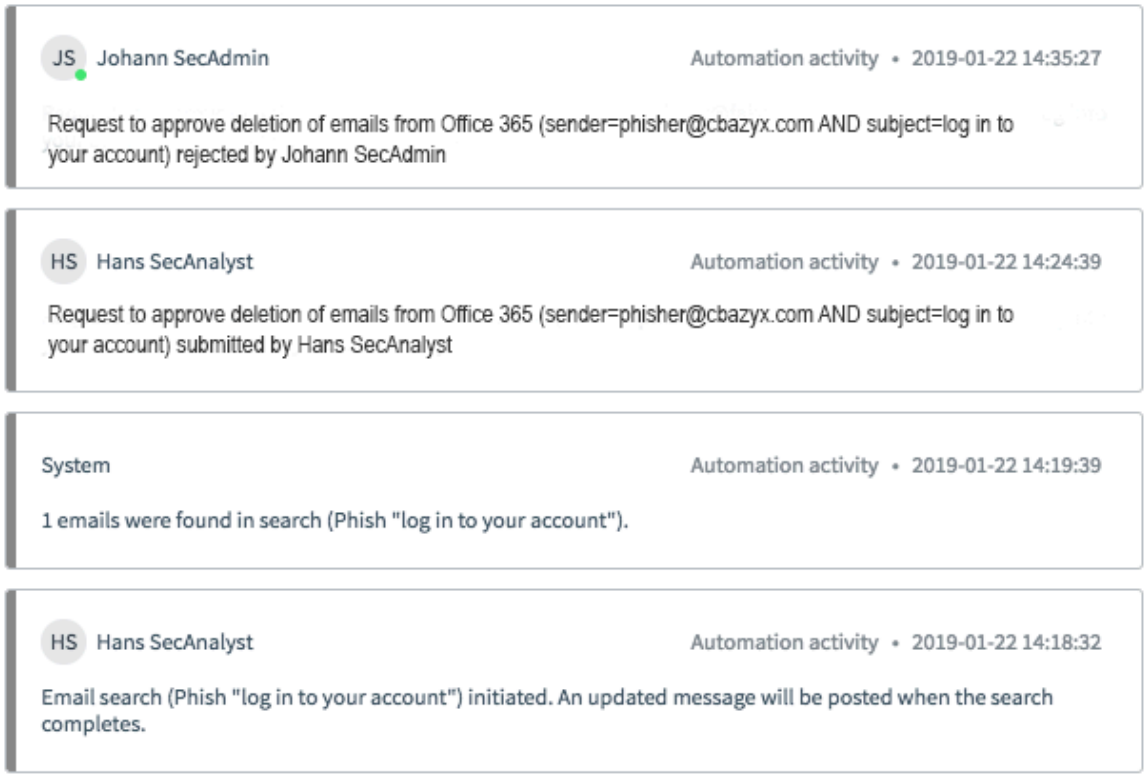

   b. Wählen Sie in der E-Mail-Benachrichtigung eine Option aus, um fortzufahren.

   Die folgende Abbildung zeigt ein Beispiel für den Auditpfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Wenn die Anforderung über die E-Mail-Benachrichtigung von einem Genehmiger abgelehnt wird,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird eine Arbeitsnotiz von der Person veröffentlicht, die die Anforderung abgelehnt hat. Jens SecAdmin lehnt diese Anforderung ab.




In der Instanz Now Platform der Person, die die Anforderung abgelehnt hat (Johann SecAdmin), in **Selfservice > Meine Genehmigungen**, „Abgelehnt“ wird in der Spalte Status angezeigt.

Nachdem eine Anforderung von einem einzelnen Mitglied der Genehmigungsgruppe abgelehnt wurde, müssen Sie als Benutzer mit der Rolle „sn_si.analyst“ eine neue Anforderung zum Löschen dieser E-Mails senden, wenn Sie der Meinung sind, dass sie gelöscht werden sollen.

In diesem Beispiel sendet der Benutzer mit der Rolle „sn_si.analyst“ eine neue Anforderung, nachdem die Anforderung abgelehnt wurde.

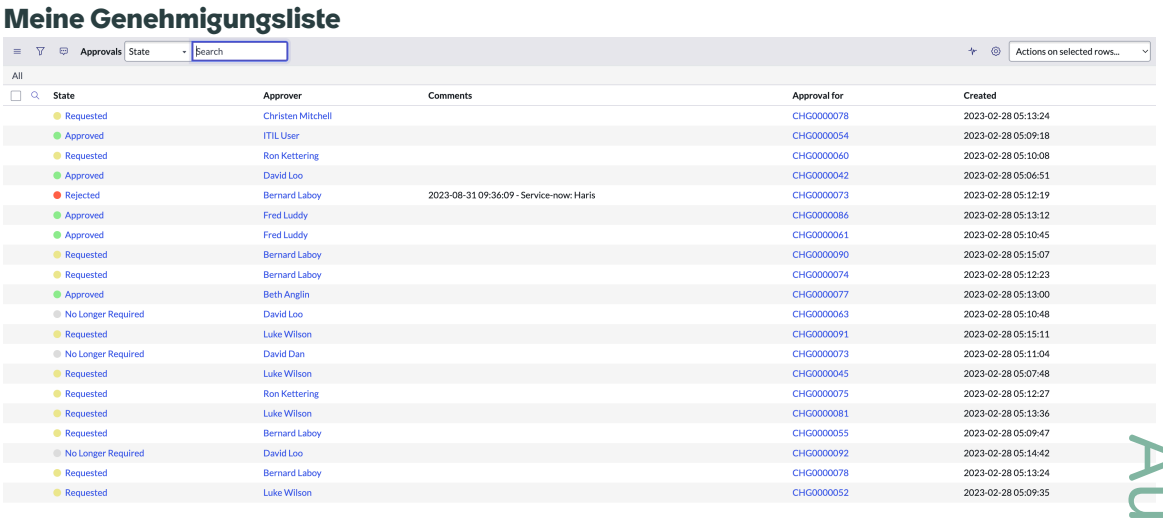
Ein anderes Mitglied der Genehmigungsgruppe, John Approver, erhält eine E-Mail ähnlich der im vorherigen Beispiel. John-Genehmiger kann diese Anforderung auch verarbeiten.

2. Alternativ können Genehmiger zu navigieren **Selfservice > Meine Genehmigungen** in ihren Instanzen Now Platform, um Löschanforderungen anzuzeigen und zu verarbeiten.
   Führen Sie die folgenden Schritte aus, um eine Anforderung aus **Meine Genehmigungen**zu verarbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

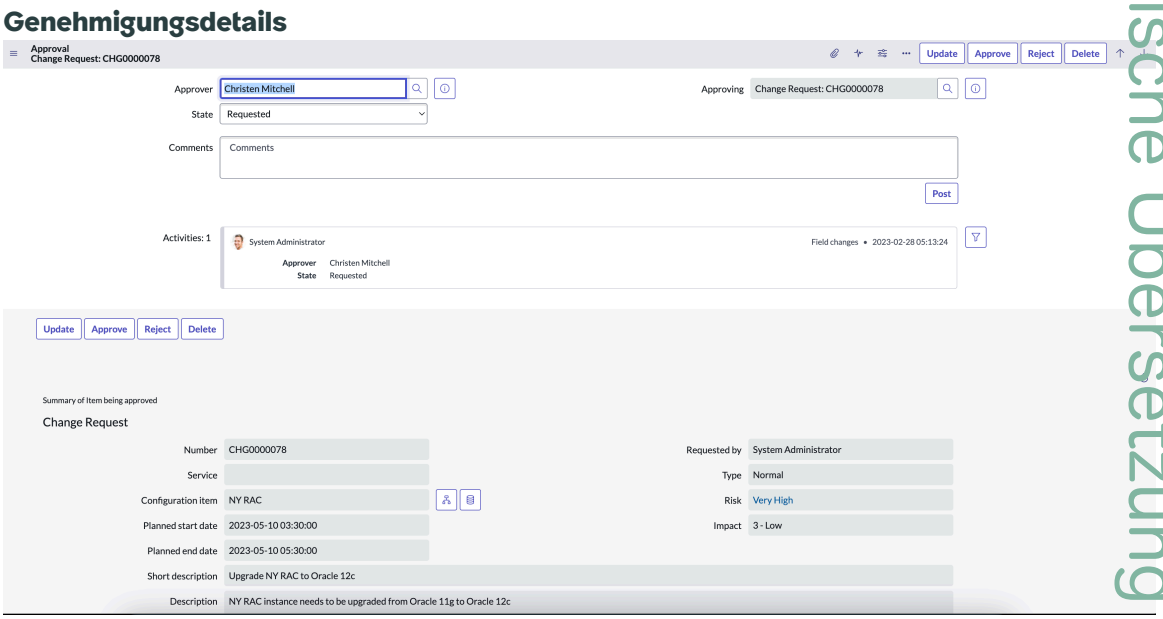
**a.** Navigieren zu **Selfservice > Meine Genehmigungen**.




| State | Approver | Comments | Approval for | Created |
|---|---|---|---|---|
| Requested | Christen Mitchell | | CHG0000078 | 2023-02-28 05:13:24 |
| Approved | ITIL User | | CHG0000054 | 2023-02-28 05:09:18 |
| Requested | Ron Kettering | | CHG0000060 | 2023-02-28 05:10:08 |
| Approved | David Loo | | CHG0000042 | 2023-02-28 05:06:51 |
| Rejected | Bernard Laboy | 2023-08-31 09:36:09 - Service-now: Haris | CHG0000073 | 2023-02-28 05:12:19 |
| Approved | Fred Luddy | | CHG0000086 | 2023-02-28 05:13:12 |
| Approved | Fred Luddy | | CHG0000061 | 2023-02-28 05:10:45 |
| Requested | Bernard Laboy | | CHG0000090 | 2023-02-28 05:15:07 |
| Requested | Bernard Laboy | | CHG0000074 | 2023-02-28 05:12:23 |
| Approved | Beth Anglin | | CHG0000077 | 2023-02-28 05:13:00 |
| No Longer Required | David Loo | | CHG0000063 | 2023-02-28 05:10:48 |
| Requested | Luke Wilson | | CHG0000091 | 2023-02-28 05:15:11 |
| No Longer Required | David Dan | | CHG0000073 | 2023-02-28 05:11:04 |
| Requested | Luke Wilson | | CHG0000045 | 2023-02-28 05:07:48 |
| Requested | Ron Kettering | | CHG0000075 | 2023-02-28 05:12:27 |
| Requested | Luke Wilson | | CHG0000081 | 2023-02-28 05:13:36 |
| Requested | Bernard Laboy | | CHG0000055 | 2023-02-28 05:09:47 |
| No Longer Required | David Loo | | CHG0000092 | 2023-02-28 05:14:42 |
| Requested | Bernard Laboy | | CHG0000078 | 2023-02-28 05:13:24 |
| Requested | Luke Wilson | | CHG0000052 | 2023-02-28 05:09:35 |

**b.** Klicken Sie in der Spalte Status auf das angeforderte Element.

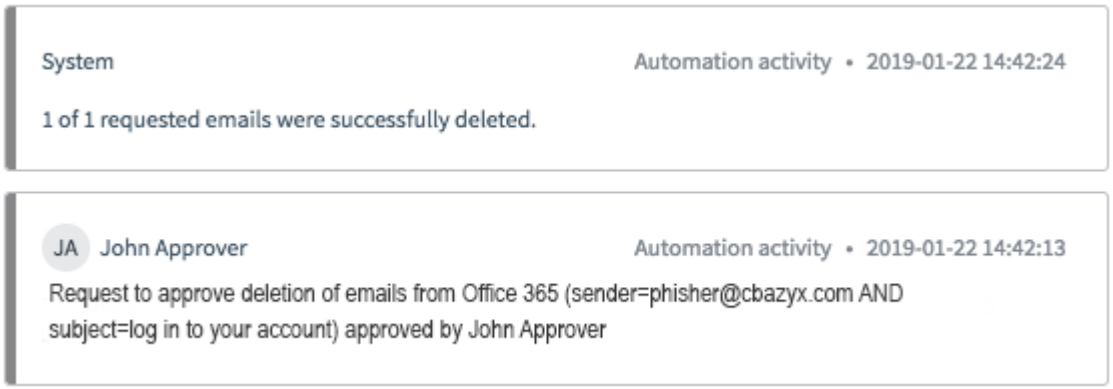
Im angezeigten Genehmigungsdatensatz werden Daten zur Suche, zur Suchanforderung und zu den Suchergebnissen aufgelistet.




**c.** Klicken **Sie** in diesem Datensatz auf Genehmigen, um die Anforderung zu genehmigen. Nachdem die Anforderung genehmigt wurde, initiiert das System den Lösch-Workflow, um die E-Mails zu entfernen. Die folgende Abbildung zeigt ein Beispiel für den Auditpfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Nachdem diese Löschanforderung erneut übermittelt wurde, wird sie genehmigt. Unabhängig davon, welche Methode zum Genehmigen einer Anforderung verwendet wird, wird die Anzahl der erfolgreich gelöschten E-Mails in einer Arbeitsnotiz veröffentlicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nachdem die E-Mails erfolgreich gelöscht wurden, ersetzt das Tag „E- Mail-Löschung – Abgeschlossen “ im zugehörigen Security Incident-Datensatz, wenn Tagging aktiviert ist, das Tag „E- Mail-Löschung – Initiiert “.

Ein **Selfservice > Meine Genehmigungen** Für den Genehmiger (John Approver) ändert sich der Status von Angefordert in Genehmigt.

Ein **Selfservice > Meine Genehmigungen** Für andere Mitglieder der Genehmigungsgruppe, z. B. für „Johann SecAdmin“, ändert sich der Status in „ Nicht mehr erforderlich “, nachdem die Anforderung genehmigt wurde.

**3.** Alternativ können Sie die folgenden Schritte ausführen, um zu bestätigen, dass E-Mails im Datensatz „E-Mail-Suchergebnis“ im zugehörigen Security Incident-Datensatz gelöscht wurden.

**a.** Navigieren zu **Security Incidents > Alle Incidents anzeigen** und suchen Sie den Phishing-bezogenen Security Incident.
Am Ende des Datensatzes werden die zugehörigen Listen angezeigt.

**b.** Klicken Sie auf die zugehörige Liste E- **Mail-Suche**.

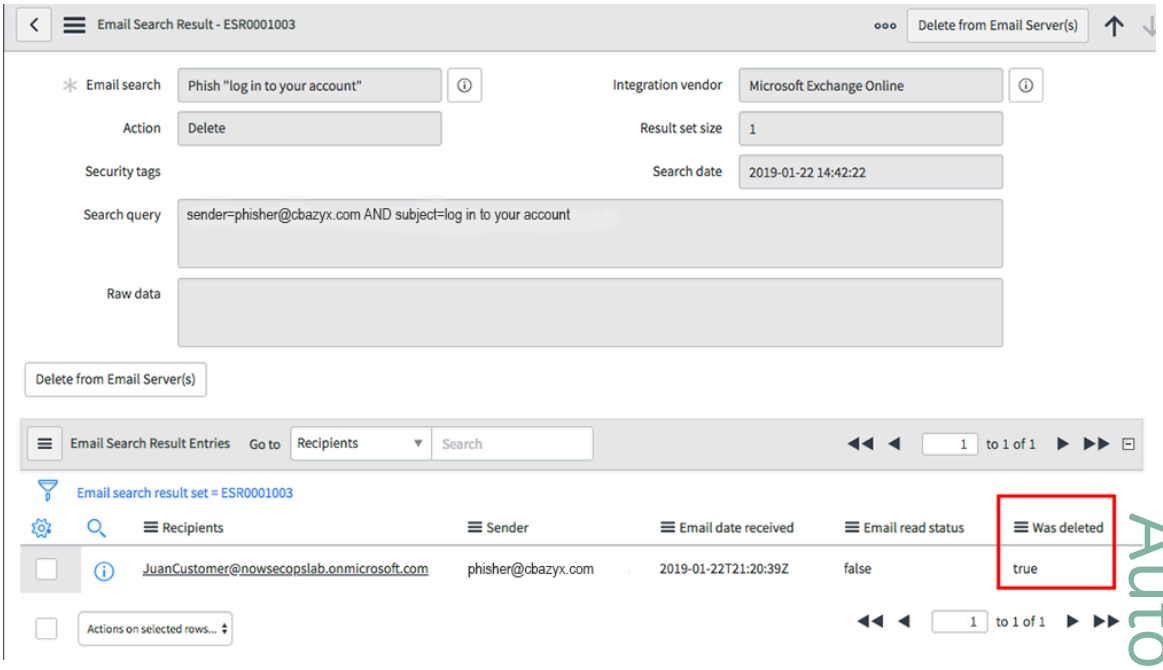
**c.** Klicken Sie auf den Namen der Suche in der E-Mail-Suchspalte (Phishing „bei Ihrem Konto anmelden“).
Der E-Mail-Suchdatensatz wird angezeigt. Wenn die zugehörige Liste E-Mail-Suche nicht sichtbar ist, klicken Sie auf den Link **Alle zugehörigen Listen**anzeigen.

**d.** Klicken Sie auf die zugehörige Liste E- **Mail-Suchergebnisse**.
In der Spalte Suchdatum werden die Such- und Löschaktionen für E-Mails mit den entsprechenden Datumsangaben angezeigt.

**e.** Klicken Sie in der Spalte Suchdatum auf das Element, das der Löschaktion entspricht.
Im angezeigten Datensatz „E-Mail-Suchergebnis“ zeigt der Status der Spalte Was gelöscht an, dass die E-Mail gelöscht wurde (true).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie haben E-Mail-Löschanforderungen erfolgreich aus einer E-Mail-Benachrichtigung und einem Genehmigungsdatensatz genehmigt und bestätigt, dass E-Mails gelöscht wurden. Weitere Informationen zum Suchen des Datensatzes „E-Mail-Suchergebnis“ finden Sie unter Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an.

### Integrationsarchitektur und externe Systemverbindung für die Microsoft Exchange Online -Integration

Die Microsoft Exchange Online -Integrationsarchitektur wurde entwickelt, um die Such- und Löschfunktionen für E-Mail-Bedrohungen im Microsoft Exchange Online -Service zu unterstützen. In dieser Einführung wird erläutert, warum es Setup-Schritte gibt, die Sie in Ihren Microsoft -Konten ausführen müssen, bevor Sie die Anwendung ServiceNow installieren.

Die Integrationsarchitektur basiert auf Bewertungen der derzeit verfügbaren Anwendungsprogrammierschnittstellen und auf der Konsultation des Integrationspersonals von Microsoft. Diese Informationen sowie wichtige Begriffe zu den Services Now Platform und Microsoft Exchange Online werden bereitgestellt, um die konzeptionelle Funktionsweise der Integration zu verdeutlichen.

## Wichtige Begriffe, die für diese Integration verwendet werden

Die folgenden wichtigen Begriffe werden während der Installation und Konfiguration verwendet. Weitere Informationen zu den folgenden Begriffen finden Sie auf der Website der ServiceNow-Produktdokumentation und der Microsoft-Dokumentationswebsite .

[store-future: BEGIN review]

**Now Platform**

Ein Unternehmensprodukt ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere Produkte erstellt werden.

**Security Incident Response (SIR)**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Now Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und dem Abschluss nach dem Incident nachverfolgt.

**Microsoft Exchange Online**

Das E-Mail-Serviceangebot für Microsoft Exchange Online, das Teil der Office 365-Suite von Microsoft -Produkten ist.

**Globale Graph-API**

Die von Microsoft bereitgestellte API, die für den Zugriff auf Postfachinformationen in Microsoft Exchange Onlineverwendet wird.

**[store-future: BEGIN review]Zertifikatbasierte Authentifizierung[End]**

[store-future: BEGIN review]Mit dieser Authentifizierung können Kunden zulassen oder verlangen, dass sich Benutzer für Anwendungen und Browseranmeldung direkt mit X.509-Zertifikaten bei Azure Active Directory (Azure AD) authentifizieren.[End]

**OAuth-Authentifizierung**

Eine im Azure-Portal Microsoft erstellte ID, die zum Sammeln zusätzlicher E-Mail-Nachrichtendetails und zum Löschen von E-Mails in Microsoft Exchange Onlineverwendet wird. Hier werden die Client-ID und der geheime Clientschlüssel von Microsoft zur Authentifizierung der Benutzer verwendet.

**[store-future: BEGIN review]Windows-Host[End]**

[store-future: BEGIN review]Spezifischer Typ des in dieser Integration verwendeten virtuellen Computers.[End]

**[store-future: BEGIN review]MID-Server[End]**

[store-future: BEGIN review]Eine Now Platform -Anwendung, die die Kommunikation und Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services erleichtert. Ein MID Server ist normalerweise für die Integration mit lokalen Technologien erforderlich, aber ein MID Server kann in bestimmten Fällen zwischen Now Platform und einem cloud-basierten Angebot bereitgestellt werden, wenn für die Integration eine vom Kunden bereitgestellte Komponente erforderlich ist. Für diese Microsoft Exchange Online -Serviceintegration erleichtert der MID Server die Kommunikation zwischen Now Platform und dem PowerShell-Server.[End]

**[store-future: BEGIN review]PowerShell-Server[End]**

[store-future: BEGIN review]Der PowerShell-Server ist eine Microsoft-Anwendung, die Ihre Microsoft-Kontoanmeldeinformationen erfordert.[End]

**Security Incident-Administrator (sn_si.admin)**

Benutzer mit der Rolle „sn_si.admin“ überwachen die Konfiguration der Integration mit dem SIR-Produkt in Ihrer Now Platform -Instanz. Benutzer mit dieser Rolle genehmigen standardmäßig auch Löschanforderungen für E-Mails und weisen die Rolle „sn_si.analyst“ nach Bedarf zu. Benutzer mit dieser Rolle haben auch die vollständige Kontrolle über alle Daten von Servicemanagement.

**Security Incident-Analyst (sn_si.analyst)**

Benutzer mit der Rolle „sn_si.analyst“ interagieren mit und analysieren Security Incidents im SIR-Produkt.

[End]

## Verbindung externer Systeme zum Suchen und Löschen von E-Mails

[store-future: BEGIN review]Diese Anwendung verwendet den PowerShell-Service Office 365 Security and Compliance Center und den Global Graph API-Service, um Informationen aus dem Exchange Online-Servicemandanten von Office 365 abzurufen. Eine ausgehende

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTPS-Verbindung vom MID Server zu dieser Umgebung ist erforderlich, damit die Integration ordnungsgemäß funktioniert.[End]

[store-future: BEGIN review]Die Integrationsarchitektur unterstützt die Funktion zum Suchen und Löschen von E-Mails im Service Microsoft Exchange Online. Die Integrationsarchitektur zielt auf Phishing-E-Mails und andere E-Mail-Bedrohungen ab, die die Sicherheit Ihrer Organisation gefährden können. Um E-Mails zu erhalten, die einem bestimmten Suchabfragekriterium entsprechen, stellt Now Platform eine Verbindung zu einem Microsoft Exchange Online -Servicemandanten her und verwendet einen MID Server, auf dem PowerShell auf einem Windows-Server ausgeführt wird.[End]

Diese Anwendung verwendet den REST-basierten Ansatz, um die Daten von Microsoft abzurufen.

Nachdem Now Platform mit dem Service Microsoft Exchange Online ] verbunden wurde, unterstützt die Integration die verschiedenen Ebenen der E-Mail-Suche.

Die aktualisierte Version der Integration von Security Incident Response mit Microsoft Exchange Online ist eine neue und robuste SIR-Integration, bei der Anwendungs-ID, Mandanten-ID (Organisation) und der geheime Clientschlüssel verwendet werden, um ein Bearer-Token (JWT) über REST-APIs zu beziehen. Diese neue Integration erfordert keine MID-Server- oder zusätzlichen PowerShell-Fähigkeiten. Dem in Azure AD erstellten Anwendungsobjekt wird eine Verzeichnisrolle zugewiesen, die sich dann in einem Zugriffstoken widerspiegelt.

[store-future: BEGIN review]

- Die übereinstimmenden Nachrichten: Diese Suche wird über das Microsoft PowerShell-Cmdlet über einen Windows MID Server durchgeführt, der eine Komponente von Now Platformist. Diese Suche basiert auf Kriterien, die Sie in Now Platform aus einem Security Incident konfigurieren. Die erste Komponente der Suche gibt alle E-Mail-Nachrichten zurück, die den von Ihnen konfigurierten Suchkriterien entsprechen, zusätzlich zu den spezifischen Postfachadressen, unter denen diese Nachrichten in Microsoft Exchange Onlinezu finden sind. Die unterstützten Suchparameter sind Betreff, Absender und Empfänger der E-Mail-Nachricht (der Wert, der im Feld An in einer E-Mail-Nachricht angezeigt wird).
- Die Nachrichtendetails: Nachdem die anfängliche PowerShell-Cmdlet-basierte Suche die übereinstimmenden Nachrichten identifiziert hat, ruft diese Suche zusätzliche Nachrichteninformationen mithilfe der Microsoft Global Graph API ab. Die zurückgegebenen E-Mail-Ergebnisse enthalten die folgenden Nachrichtendetails:
  - Lesestatus: Mit dem Status „Wahr“ oder „Falsch“ wird nachverfolgt, wann Benutzer E-Mails gelesen haben.
  - Absenderadresse.
  - Empfängeradresse: Zu diesen Adressen gehören Einzelpersonen, eine Gruppe und Einzelpersonen, die in Nachrichten mit CC und BCC angegeben werden.
  - Löschstatus: Der Status „Wahr“ oder „Falsch“ verfolgt gelöschte E-Mails.
  - Nachrichten-ID: Der alphanumerische Bezeichner von E-Mail-Nachrichten.

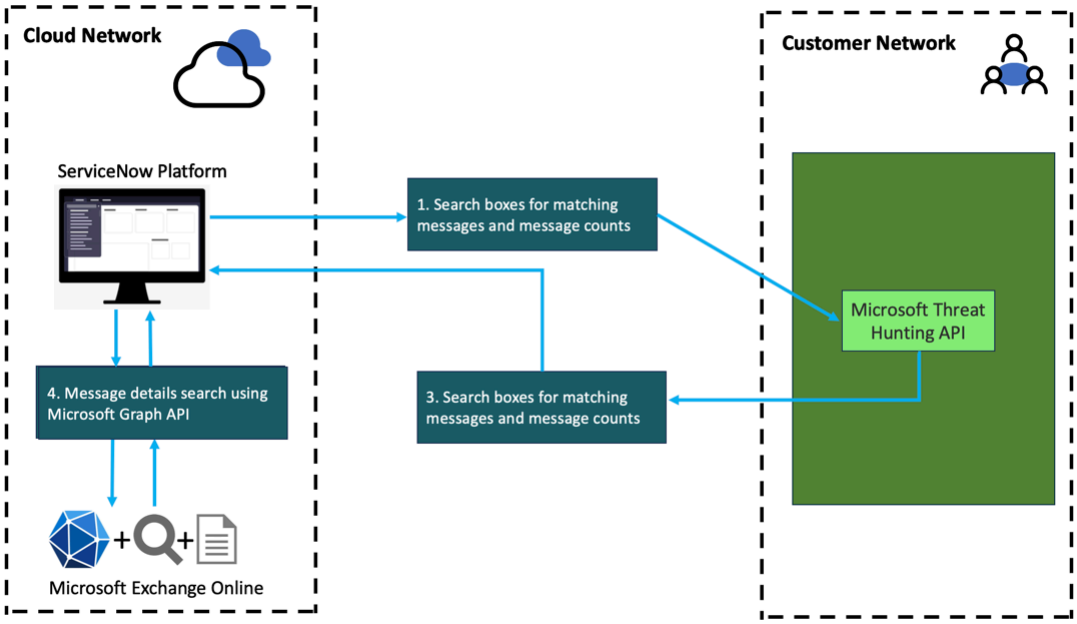
[End]

Der grundlegende Datenfluss der E-Mail-Suchen für die Anzahl der Nachrichten und die Nachrichtendetails ist in der folgenden Abbildung dargestellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### E-Mail-Suche nach der Anzahl der Nachrichten und Nachrichtendetails



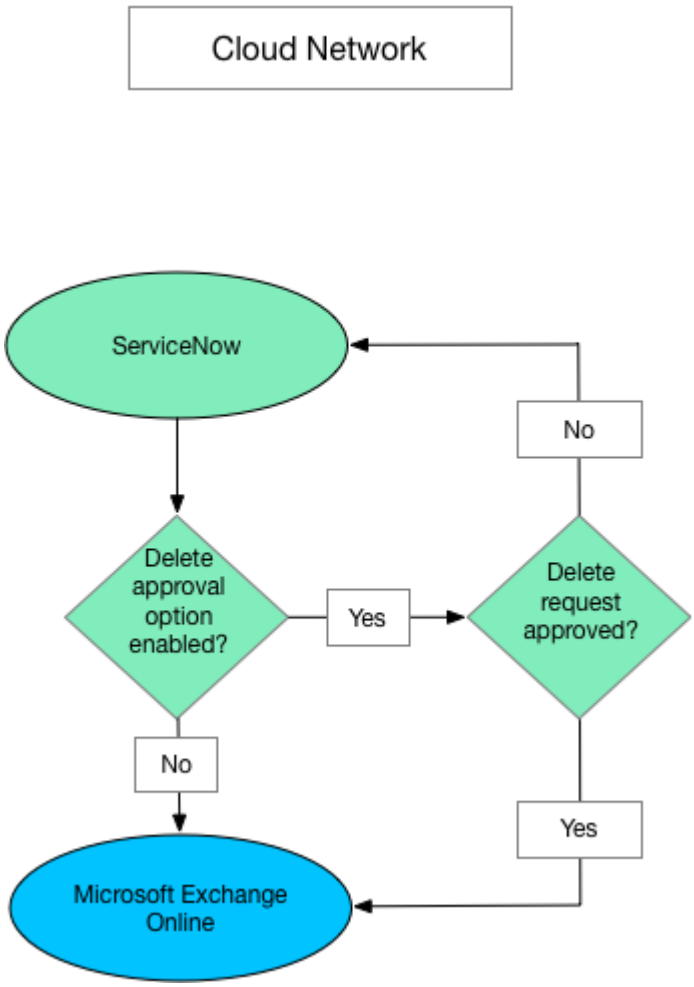

Zum Löschen von E-Mails verwendet die Integration die Global Graph API. Die Wiederherstellung gelöschter E-Mails ist während des Konfigurationsschritts als Option verfügbar und wird in Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanzausführlicher beschrieben.

Der Datenfluss für das Löschen von E-Mails mit dem vorkonfigurierten Genehmigungsprozess ist in der folgenden Abbildung dargestellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**E-Mail löschen**




## Workflows

Die Anwendung Microsoft Exchange Online zum Suchen und Löschen von E-Mails umfasst die folgenden Workflows:

- Exchange Online – E-Mails löschen
- Ruft Exchange Online-E-Mail-Details ab.
- Microsoft Exchange Online E-Mails suchen und löschen.

Weitere Informationen finden Sie unter Erste Schritte mit Workflows .

Sie können jetzt die für die Integration erforderlichen Konten einrichten.

### Stellen Sie gelöschte E-Mails im Service Microsoft Exchange Online wieder her

(Optional) Als Microsoft Exchange-Administrator können Sie gelöschte E-Mails wiederherstellen, wenn die Incident-Korrektur die Wiederherstellung der durch den Workflow dieser Integration gelöschten E-Mails erfordert.

**Vorbereitungen**
Weitere Informationen dazu, wie diese Integration E-Mails löscht, finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanz.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zur Administratorrolle im Office 365-Produkt Microsoft, einschließlich Informationen zum Wiederherstellen gelöschter Elemente in einem Benutzerpostfach, finden Sie unter Informationen zur Exchange Online-Administratorrolle .

Erforderliche Rolle: admin, Microsoft Exchange-Administrator

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie während des Konfigurationsschritts auf der Registerkarte Zusätzliche Einstellungen die Option **Gelöschte E-Mails wiederherstellen** auswählen, aktivieren Sie die Wiederherstellung gelöschter E-Mails in Ihrem Microsoft Exchange Online -Mandanten. E-Mails, die mit dem Lösch-Workflow dieser Integration gelöscht wurden, werden im Unterordner „Gelöschte Elemente“ des Ordners „Wiederherstellbare Elemente“ im Postfach des Benutzers im Service Microsoft Exchange Online abgelegt. Wenn das Konto des Benutzers im Mandanten Microsoft Exchange Online so konfiguriert ist, dass der Benutzer den Ordner „Gelöschte Elemente“ anzeigen kann, kann der Benutzer diese E-Mails mithilfe des Outlook-Diensts Microsoft im Web wiederherstellen. Alternativ kann der Microsoft Exchange Online -Administrator gelöschte E-Mails aus dem Ordner „Gelöschte Elemente“ eines Benutzers wiederherstellen. Weitere Informationen finden Sie unter Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen.

Erforderliche Rolle: Microsoft Exchange Online Administrator oder Microsoft Globaler Administrator, um gelöschte E-Mails wiederherzustellen.

Erforderliche Rolle: sn_si.admin in Now Platform, um die Option „Gelöschte E-Mails wiederherstellen“ zu aktivieren.

Erforderliche Rolle: sn_si.analyst in Now Platform für den Abschluss einer erfolgreichen Suche nach E-Mails und die Überprüfung, ob E-Mails vor der Wiederherstellung erfolgreich gelöscht wurden.

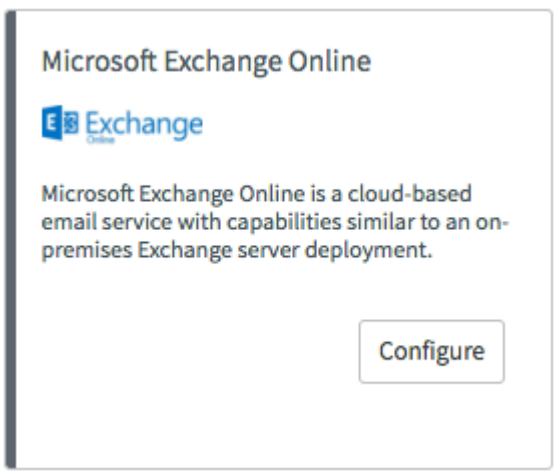
### Prozedur

Führen Sie die folgenden Schritte aus, um die E-Mail-Wiederherstellungsoption zu aktivieren.

**a.** Navigieren zu **Security Operations** > **Integrationen** > **Konfigurationen**.

**b.** Suchen Sie die Kachel Microsoft Exchange Online.

**c.** Klicken Sie auf **Konfigurieren**.

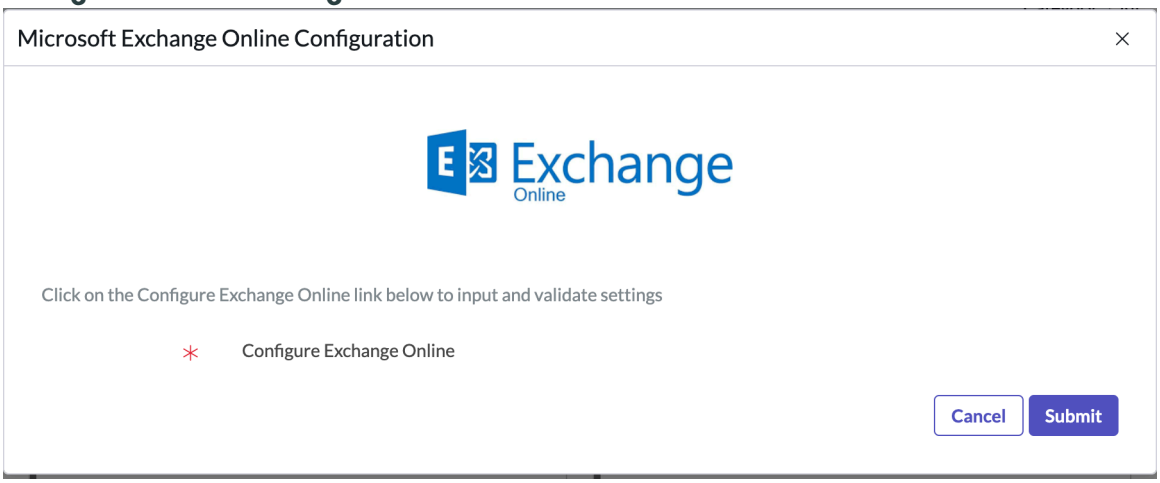



**d.** Klicken Sie im angezeigten Dialogfeld Microsoft Exchange Online Konfiguration auf **Exchange Online konfigurieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

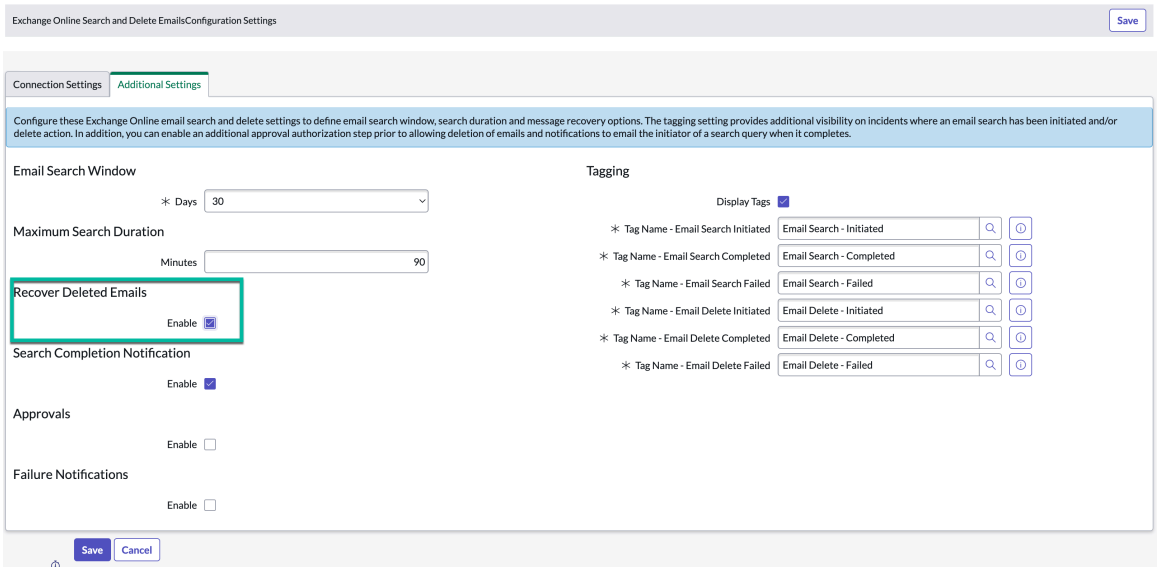

Automatische Übersetzung

**Konfigurieren Sie Exchange Online**




**e.** Aktivieren Sie auf der Registerkarte Zusätzliche Einstellungen unter Gelöschte E-Mails**wiederherstellen** das Kontrollkästchen Aktivieren.

**Gelöschte E-Mails wiederherstellen**




**f.** Überprüfen Sie alle anderen Einstellungen, und klicken Sie auf **Absenden**.

**g.** Um sicherzustellen, dass eine Suche und Löschung von E-Mail-Nachrichten für die E-Mail-Nachrichten, die Sie wiederherstellen möchten, erfolgreich abgeschlossen wurde, navigieren Sie zu dem Security Incident, der die E-Mail-Such- und Lösch-Workflows protokolliert hat.

**h.** Suchen Sie die Arbeitsnotizen, und stellen Sie sicher, dass das System die Nachrichten erfolgreich gelöscht hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Melden Sie sich als Microsoft Exchange Online -Administrator oder globaler Administrator bei Ihrem Microsoft Office 365-Konto an.

j. Führen Sie die unter Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen auf der Dokumentationswebsite Microsoft beschriebenen Schritte aus.

### Bearbeiten Sie Sicherheits-Tags in Now Platform für die Microsoft Exchange Online -Integration

Sie können die Namen und Farben der Sicherheits-Tags in Ihrer Now Platform® -Instanz für die Microsoft Exchange Online -Integration bearbeiten. Mit diesen Sicherheits-Tags können Sie schnell erkennen, wann die E-Mail-Suche entweder abgeschlossen ist oder fehlschlägt. Sie identifizieren auch, wenn Anforderungen zum Löschen von E-Mails initiiert und die E-Mail-Elemente erfolgreich gelöscht wurden.

#### Vorbereitungen

Standardmäßig sind die Sicherheits-Tags in Ihrer Instanz Now Platform® aktiviert, wenn Sie während des Konfigurationsschritts die Option **Tags anzeigen** auswählen. Sie können Tag-Farben und -Namen bearbeiten und Sicherheits-Tag-Gruppen Tags zuweisen, um sie in Ihrer Now Platform® -Instanz zu organisieren. Sie können beispielsweise die Farben von Tags so ändern, dass das Start-Tag einer Fähigkeit eine Farbe und das Abschluss-Tag eine andere Farbe hat, um den anderen Sicherheits-Tags zu entsprechen, die in Ihrer Now Platform® -Instanz aktiviert sind. Anhand dieser verschiedenen Farben können Sie schnell erkennen, wann Workflows gestartet und erfolgreich abgeschlossen wurden. Wenn Sie entscheiden, dass Sie ein bestimmtes Tag nicht benötigen, können Sie auch ein einzelnes Tag aus dem Tag-Datensatz deaktivieren, ohne die Tag-Kennzeichnung für die Integration zu deaktivieren. Wenn diese Option deaktiviert ist, wird dieses Tag nicht mehr in den zugehörigen Security Incidents angezeigt. Weitere Informationen zum Einrichten von Sicherheits-Tag-Gruppen und -Tags finden Sie unter Sicherheits-Tag-Gruppen und -Tags einrichten auf der ServiceNow-Website mit Produktdokumentation .

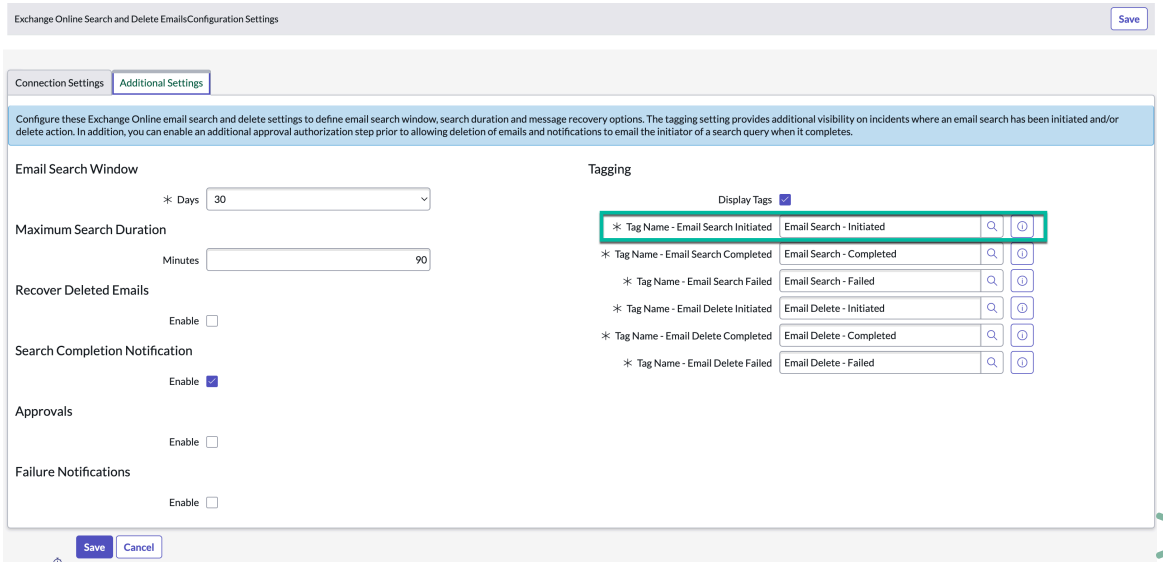
Erforderliche Rolle: sn_si.admin

#### Prozedur

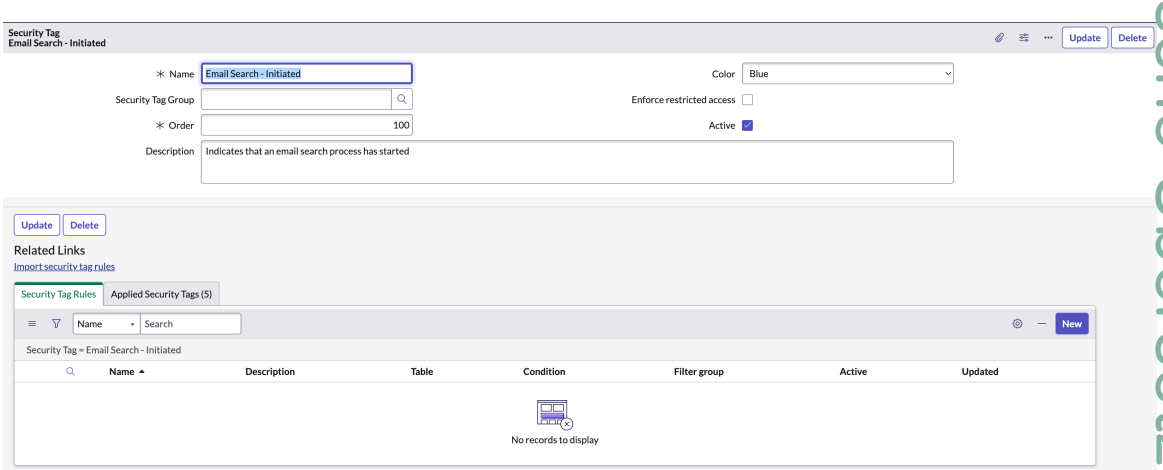
1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Exchange Online-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Zusätzliche Einstellungen**, um sie auszuwählen.
3. Wenn auf der angezeigten Registerkarte die Option **Tags anzeigen deaktiviert** ist, wählen Sie sie aus, um Tag-Namen anzuzeigen.
4. Wenn die Tag-Namen angezeigt werden, klicken Sie rechts neben einem Tag auf das Informationssymbol.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie im angezeigten Dialogfeld Sicherheits-Tag auf **Datensatz öffnen**.
6. Bearbeiten Sie im angezeigten Datensatz die Felder.
7. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.




Sie haben den Tag-Datensatz für ein Sicherheits-Tag jetzt erfolgreich bearbeitet.

## Prüfliste für die Microsoft Exchange Online -Integration

Verwenden Sie diese Prüfliste, um durch die End-to-End-Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle und erwartete Ergebnisse für die Anwendung.

### Vorbereitungen

Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration mit der folgenden Tabelle nach. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jeder Schritt identifiziert die Rollen, die zum Ausführen der Aufgaben erforderlich sind, und verweist auf die nummerierten Themen des Installations- und Konfigurationsleitfadens für diese Integration.

Erforderliche Rollen: Rollen werden für jeden Schritt in der folgenden Tabelle aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

Um Ihren Fortschritt für die Integration nachzuverfolgen, befolgen Sie die Schritte in der Tabelle in der Reihenfolge, in der sie angezeigt werden

### Prüfliste

| | |
|---|---|
| ☐ | Richten Sie als Microsoft Office 365-Administrator Ihr Microsoft Office 365-Konto ein.<br><br>Erstellen Sie ein API-Konto, das den Zugriff auf das Security and Compliance Center in Microsoft Office 365 ermöglicht. |
| ☐ | Richten Sie als Microsoft Azure-Administrator Ihr Microsoft Azure-Konto ein.<br><br>Erstellen Sie einen Account, der eine Anwendungs-ID verwendet, um zusätzliche E-Mail-Nachrichtendetails zu erfassen und E-Mail-Nachrichten zu löschen. Schritte zum Einrichten des Kontos finden Sie unter Richten Sie Ihr Microsoft Azure-Konto für die ServiceNow Microsoft Exchange Online -Integration ein. |
| ☐ | Richten Sie als Now Platform -Administrator Ihre Now Platform -Instanz für die Integration ein.<br><br>Aufgaben und weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die Microsoft Exchange Online -Integration ein.<br><br>**a.** Weisen Sie Now Platform Rollen zu.<br><br>**b.** Installieren Sie die Anwendungen Now Platform (SIR) und Security Operations aus dem ServiceNow Store, und aktivieren Sie sie in Ihrer Instanz.<br><br>**c.** Aktivieren Sie die Funktionen zum Senden und Empfangen von E-Mails.<br><br>**d.** Weisen Sie sn_si.analyst die Rolle „E-Mail lesen und schreiben“ zu.<br><br>**e.** Erstellen Sie eine Genehmigungsgruppe. |
| ☐ | Installieren Sie als Now Platform -Administrator die Anwendung für die -Integration aus dem ServiceNow Store.<br><br>Die Installationsschritte finden Sie unter Installieren Sie die Anwendung Microsoft Exchange Online für die Integration von ServiceNow Microsoft Exchange Online .. |
| ☐ | Füllen Sie als sn_si.admin die Registerkarten mit den Konfigurationseinstellungen aus, um Konnektivität herzustellen und die Such- und Lösch-Workflows zu aktivieren.<br><br>Informationen zu Verbindungs- und Konfigurationseinstellungen finden Sie unter Konfigurieren Sie die Microsoft Exchange Online -Integration mit Ihrer Now Platform -Instanz. |
| ☐ | Richten Sie als sn_si.analyst E-Mail-Suchkriterien ein, und fordern Sie eine Suche nach übereinstimmenden E-Mails auf dem Server Microsoft Exchange Online an. Ein Beispiel finden Sie unter Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im Service Microsoft Exchange Online an. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | **a.** Suchen Sie nach Security Incidents im Zusammenhang mit Phishing-Ereignissen.<br>**b.** Richten Sie E-Mail-Suchkriterien ein.<br>**c.** Fordern Sie eine Suche nach E-Mails an.<br>**d.** Suchen Sie in den zugehörigen Listen des Security Incident nach Suchergebnissen und Nachrichtendetails. |
| ☐ | Löschen Sie als sn_si.analyst E-Mails vom Server Microsoft Exchange Online. Ein Beispiel finden Sie unter Fordern Sie die Löschgenehmigung für E-Mails im Microsoft Exchange-Onlinedienst an.<br>**a.** Suchen Sie nach Security Incidents mit Suchergebnissen.<br>**b.** Löschen Sie E-Mails, oder fordern Sie die Genehmigung zum Löschen von E-Mails an.<br>**c.** Überprüfen Sie, ob E-Mails aus den Ergebnissen gelöscht werden, die in den Arbeitsnotizen und zugehörigen Listen zum Security Incident veröffentlicht werden. |
| ☐ | Verarbeiten Sie als sn_si.admin oder als Mitglied einer Genehmigungsgruppe E-Mail-Löschanforderungen über E-Mail-Benachrichtigungen.<br>Ein Beispiel finden Sie unter Genehmigen Sie E-Mail-Löschanforderungen für die Microsoft Exchange Online -Integration. |

Sie haben die Setup-Schritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration überprüft.

### Problembehandlung bei der Microsoft Exchange Online-Integration

Wenn die Berechtigung ThreatHunting.Read.All nicht sichtbar ist, überprüfen Sie die Microsoft Defender for Office 365-Lizenz.

Weitere Informationen finden Sie unter Sicherheitsvergleich von Microsoft Defender für Office 365 .

## Integration mit Microsoft Exchange lokal

Die Microsoft Exchange On-Premises-Integration bietet Tools für Sicherheitsanalysten, um Phishing- und Spear-Phishing-E-Mail-Bedrohungen in lokalen Instanzen einzudämmen und zu beseitigen.

**Erkunden**

Security Incident Response-Integrationen

**Einrichten**

Erste Schritte mit der Microsoft Exchange On-Premises-Integration

**Verwenden**

Suchen und löschen Sie Phishing-E-Mails

**Entwickeln**

- ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | • Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| **Problembehandlung und Hilfe**<br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

## Erste Schritte mit der Microsoft Exchange On-Premises-Integration

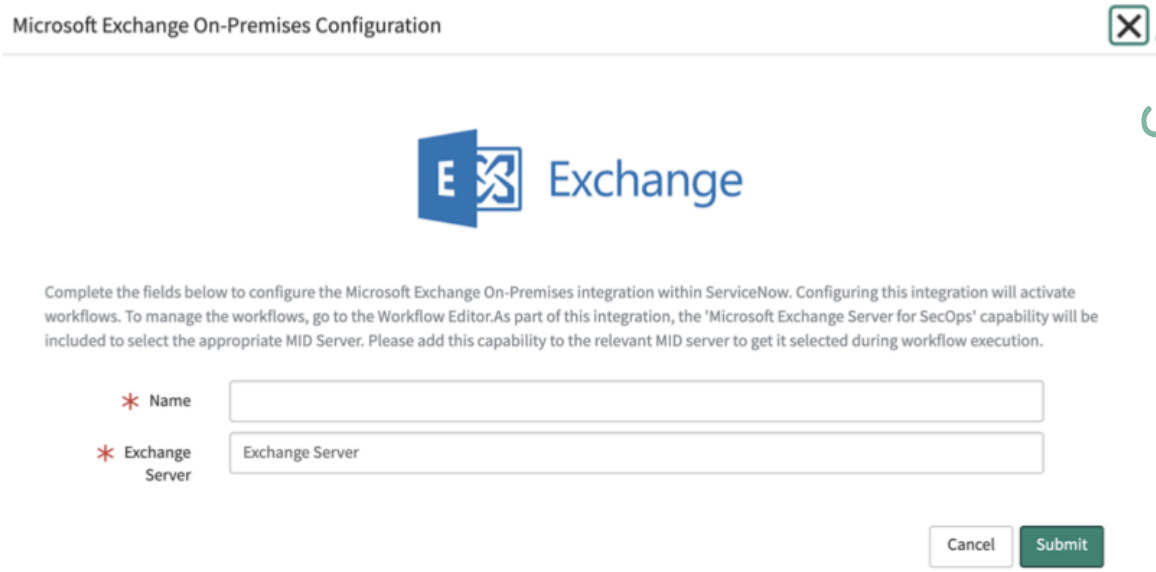
Die Microsoft Exchange On-Premise-Integration bietet Tools für Sicherheitsanalysten, um Phishing- und Spear-Phishing-E-Mail-Bedrohungen in lokalen Instanzen einzudämmen und zu beheben. Bevor Sie die lokale Integration von [ Microsoft Exchange verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechenden Exchange- und MID-Server identifizieren.

### Vorbereitungen

Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie in der Karte Microsoft Exchange Lokales Element auf **Neu**.




Automatische Übersetzung

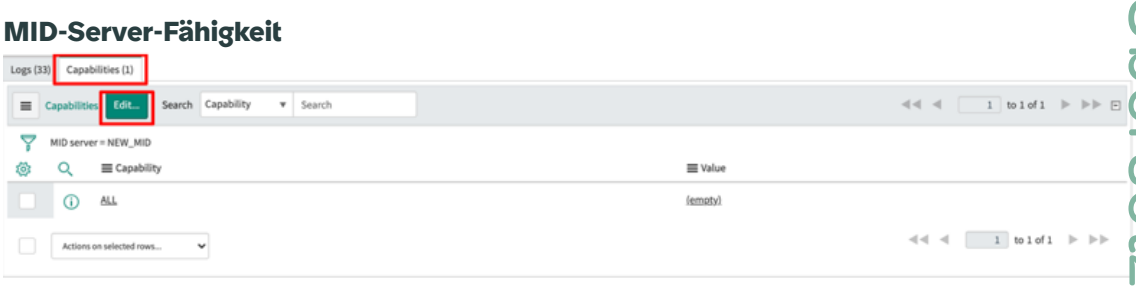
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |
| Exchange Server | Geben Sie den zu verwendenden Exchange-Server an. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

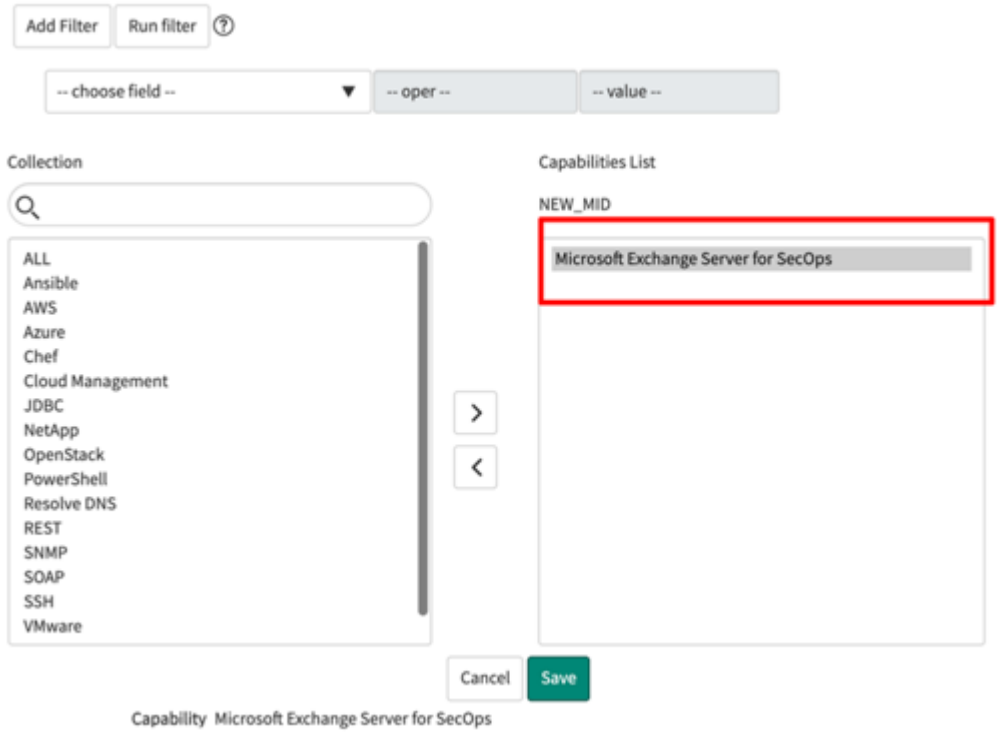
5. Klicken Sie auf **Absenden**.
Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.
8. Navigieren zu **Orchestration** > **MID-Server**.
9. Öffnen Sie den Datensatz, und überprüfen Sie den Status des MID-Servers, der für den Exchange-Server erreichbar ist, und dessen Option **Status** auf **In** Betrieb und **Validiert** auf **Ja**festgelegt ist.
10. Fügen Sie die MID-Server-Fähigkeit hinzu:
    - Wählen Sie den entsprechenden MID-Server aus, um die Fähigkeit hinzuzufügen.
    - Klicken Sie auf die zugehörige Liste **Fähigkeiten** und dann auf **Bearbeiten**.




    - Entfernen Sie **Alle**, und fügen Sie **Microsoft Exchange Server für SecOps hinzu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- Wählen Sie im Abschnitt „ **Zugehörige Listen** “ die **IP-Bereiche** aus, und legen Sie den Wert entweder auf **ALLE** oder einen beliebigen Wert fest.
- Wählen Sie im Abschnitt „ **Zugehörige Listen** “ die **unterstützten Anwendungen** aus, und legen Sie den Wert auf ALLE oder Orchestration fest.
- **Speichern Sie** den Datensatz.

**11.** Validieren Sie die Verbindungen und Anmeldeinformationen.

**12.** Sobald die Anmeldeinformationen validiert wurden, ist die Konfiguration in der ServiceNow-Instanz abgeschlossen und bereit, E-Mail-Such- und -Löschvorgänge mit dieser Integration durchzuführen.

### Microsoft Exchange: E-Mail-Suche und -Löschungs-Workflow ausführen

Wenn der Workflow **„Microsoft Exchange – E-Mail-Suche und -Löschung** durchführen“ ausgeführt wird, wird der Exchange-Server mit der angegebenen Suchabfrage durchsucht und die Details an die lokale Instanz zurückgegeben.

### Vorbereitungen

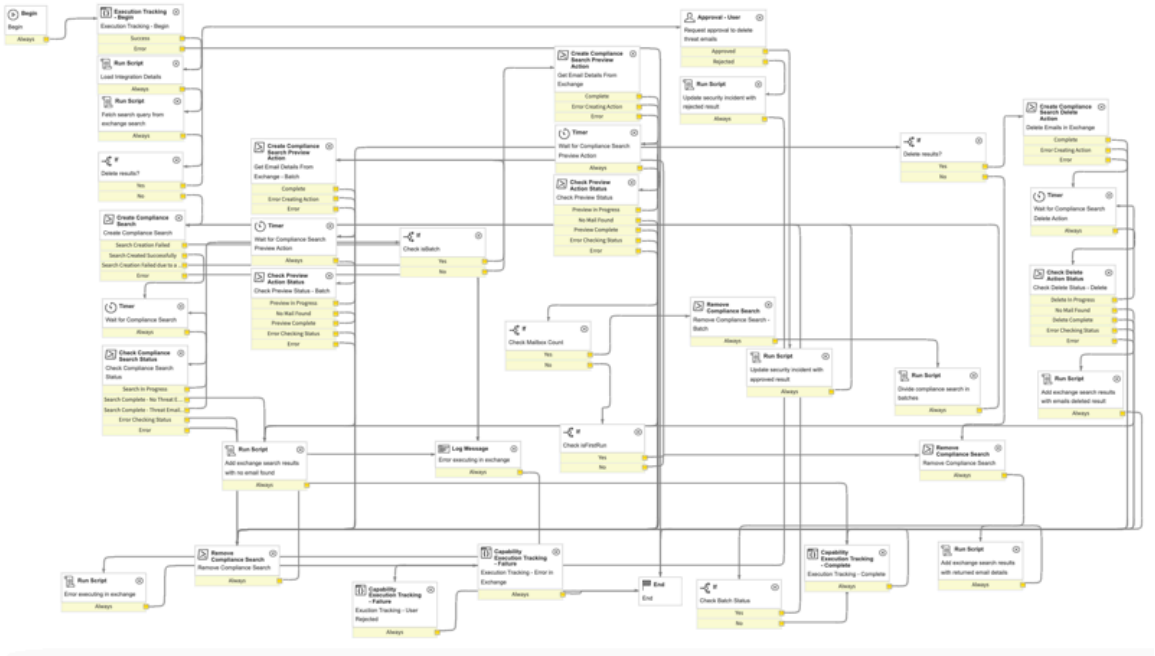
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow „ **Microsoft Exchange – E-Mail-Suche und -Löschung** durchführen“ wird ausgeführt, wenn E-Mail-Suchen eingerichtet sind und die **Schaltfläche Von E-Mail-Servern löschen** oder **Auf E** -Mail-Servern suchen angeklickt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Erstellen Sie eine Compliance-Suchaktivität

Die Aktivität „Compliance-Suche erstellen“ erstellt eine Compliance-Suche für E-Mails auf den angegebenen Exchange-Servern unter Verwendung der definierten Suchabfragen und gibt den Namen der erstellten Compliance-Suche zurück.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| search_query | Obligatorische Suchabfrage, die verwendet wird, um E-Mails in Exchange Server in allen Postfächern zu finden. |
| Exchange-Standort | Obligatorisches Standortfeld, das für die Suche innerhalb des definierten Standorts verwendet wird. Werte sind:<br>• Alle<br>• Name des spezifischen Postfachs |
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Name der erstellten Compliance-Suche. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

#### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Fehler beim Erstellen der Suche | Wenn die Sucherstellung aufgrund einer Ausnahme auf dem Exchange-Server fehlschlägt. |
| Suche erfolgreich erstellt | Wenn die Sucherstellung erfolgreich ist. |
| Fehler beim Erstellen der Suche aufgrund eines Analysefehlers | Wenn die Sucherstellung aufgrund eines Analyseproblems fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Aktivität „Compliance-Suchstatus überprüfen“.

Die Aktivität „Compliance-Suchstatus überprüfen“ überprüft den Status der erstellten Compliance-Suche auf dem Exchange-Server. Wenn der Status abgeschlossen ist, werden die Informationen zur E-Mail-Suche zurückgegeben, die für die Compliance-Suche gefunden wurden.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Enthält den Status der Compliance-Suche und die Anzahl der auf dem Exchange-Server gefundenen E-Mails für die Compliance-Suche. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Suche wird ausgeführt | Wenn der Status der Compliance-Suche in Bearbeitung ist. |
| Suche abgeschlossen – keine Bedrohungs-E-Mails gefunden | Wenn der Status der Compliance-Suche abgeschlossen ist und im Rahmen der Compliance-Suche keine E-Mails gefunden werden. |
| Suche abgeschlossen – Bedrohungs-E-Mails gefunden | Wenn der Status der Compliance-Suche abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden. |
| Fehler beim Überprüfen des Status | Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Erstellen Sie die Aktionsaktivität für die Compliance-Suchvorschau

Die Aktivität „Vorschauaktion für Compliance-Suche erstellen“ erstellt eine neue Compliance-Suchaktion vom Typ „Vorschau“ auf dem Exchange-Server für die erstellte Compliance-Suche.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

#### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Abgeschlossen | Wenn die Compliance-Suchaktion erfolgreich erstellt wurde. |
| Fehler beim Erstellen der Aktion | Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme auf dem Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Aktivieren Sie die Aktivität Vorschau für Aktionsstatus

Die Aktivität „Vorschau-Aktionsstatus“ überprüft den Status der Compliance-Suchaktion vom Typ „Vorschau“ und gibt die Vorschauinformationen der gefundenen E-Mails zurück, z. B. Empfänger, Absender, Betreff, E-Mail-Empfangsdatum.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Enthält den Status der Compliance-Suchaktion und die Vorschauinformationen der im Rahmen der Compliance-Suche gefundenen E-Mail. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Vorschau wird ausgeführt | Wenn der Status der Compliance-Suchaktion ausgeführt wird. |
| Keine E-Mail gefunden | Wenn der Status der Compliance-Suchaktion abgeschlossen ist und im Rahmen der Compliance-Suche keine E-Mails gefunden werden. |
| Vorschau abgeschlossen | Wenn der Status der Compliance-Suchaktion abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden. |
| Fehler beim Überprüfen des Status | Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Erstellen Sie die Löschaktionsaktivität für die Compliance-Suche

Die Aktivität „Compliance-Suche erstellen – Löschaktion“ erstellt eine neue Compliance-Suchaktion vom Typ „Löschen“ auf dem Exchange-Server für die erstellte Compliance-Suche.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Abgeschlossen | Wenn die Compliance-Suchaktion erfolgreich erstellt wurde. |
| Fehler beim Erstellen der Aktion | Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme auf dem Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Aktivieren Sie die Aktivität „Aktionsstatus löschen“.

Die Aktivität „Aktionsstatus löschen“ überprüft den Status der Compliance-Suchaktion vom Typ „Löschen“ und führt einen Soft-Delete-Vorgang auf dem Exchange-Server für die im Rahmen der Compliance-Suche gefundenen E-Mails durch.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Enthält den Status der Compliance-Suchaktion und die Anzahl der gelöschten E-Mails, die im Rahmen der Compliance-Suche gefunden wurden. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Löschen in Bearbeitung | Wenn der Status der Compliance-Suchaktion ausgeführt wird. |
| Keine E-Mail gefunden | Wenn der Status der Compliance-Suchaktion abgeschlossen ist und keine E-Mails im Rahmen der Compliance-Suche gelöscht werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Austrittsbedingungen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| Löschen abgeschlossen | Wenn der Status der Compliance-Suchaktion abgeschlossen ist und E-Mails im Rahmen der Compliance-Suche gelöscht werden. |
| Fehler beim Überprüfen des Status | Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### Entfernen Sie die Compliance-Suchaktivität

Die Aktivität „Compliance-Suche entfernen“ entfernt die erstellte Compliance-Suche vom Exchange-Server.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

# Integration der Microsoft Graph-Sicherheits-API zur Warnungserfassung

Verwenden Sie die Microsoft Graph-Sicherheits-API -Integration, um Warnungen von Microsoft Graph-Sicherheitsanbietern zu erfassen und automatisch Security Incidents zu erstellen.

## Übersicht

Microsoft Graph-Sicherheits-API ist ein intermediärer Service (oder Broker), der eine einzelne programmgesteuerte Schnittstelle für die Verbindung mehrerer Sicherheitsanbieter (nativ von Microsoft sowie ServiceNow-Partner) bereitstellt.

Die Microsoft Graph-Sicherheits-API -Integration behebt diese Probleme, indem Microsoft Graph-Sicherheits-API verwendet wird, um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. Warnungen von Microsoft-Sicherheitsanbietern werden erfasst, und Security Incidents werden automatisch in Security Incident Responseerstellt.

## Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erkennung von Microsoft Graph-Sicherheits-API Warnungen, die Kandidaten für Security Incidents sind, und Automatisierung der Erstellung von Security Incidents.
- Zuordnung von Warnungsfeldern zu Security Incident-Feldern.
- Zusammenfassung ähnlicher Warnungen zu vorhandenen offenen Security Incidents, anstatt doppelte Security Incidents zu erstellen.
- Zeigen Sie eine Vorschau der Warnungsfeldwerte an, und validieren Sie ihre Zuordnungen im Security Incident.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatische Aktualisierung des Warnungsstatus für die Erstellung und Schließung von Security Incidents.
- Richten Sie die geplante Erfassung von Warnungen ein, um regelmäßig Security Incidents zu erstellen.

### Richten Sie Ihre Now Platform-Instanz für die Integration der Microsoft Graph Security API ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response zugewiesen haben. | Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform® -Instanz erforderlich.<br>• Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus dem ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.<br>• Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform®:<br>◦ Benennt, erstellt und bearbeitet Warnungsprofile.<br>◦ Wählt die Warnungsdatenfelder der Microsoft Graph-Sicherheits-API aus und ordnet sie den Security Incident-Feldern zu.<br>◦ Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.<br>◦ Plant die laufende Warnungserfassung.<br>◦ Aktiviert Warnungsaktualisierungen, wenn ein Incident Security Incident Response erstellt und geschlossen wird.<br>◦ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.<br>Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Rollen auf der ServiceNow-Website mit Produktdokumentation . |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
|---|---|
| Registrieren Sie Ihre Anwendung im Microsoft Azure -Portal. | Bevor Sie Warnungen erfassen können, müssen Sie Ihre Anwendung im Microsoft Azure -Portal konfigurieren. Details siehe Konfigurieren Sie das Microsoft Azure-Portal. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Event and Alert Ingestion for Security Operations: Diese Anwendung erfordert:<br>○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit<br>○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST<br><br>**Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Event and Alert Ingestion“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport.<br><br>Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

### Konfigurieren Sie das Microsoft Azure-Portal

Um Sicherheitswarnungen für eine Anwendung abzurufen, die im Microsoft Azure-Mandanten mit Microsoft Graph-Sicherheits-APIverfügbar ist, müssen Sie die Anwendung im Portal Microsoft Azure registrieren und Sicherheits-Events Lese- und Schreibzugriff auf die Anwendung gewähren.

#### Vorbereitungen

Erforderliche Rolle:

- Anwendungsentwickler: Erforderlich für die Registrierung der Anwendung.
- Mandantenadministrator: Der Administrator des Mandanten Microsoft Azure muss der Anwendung Berechtigungen erteilen, indem er den Endpunkt der Administratoreinwilligung aufruft.

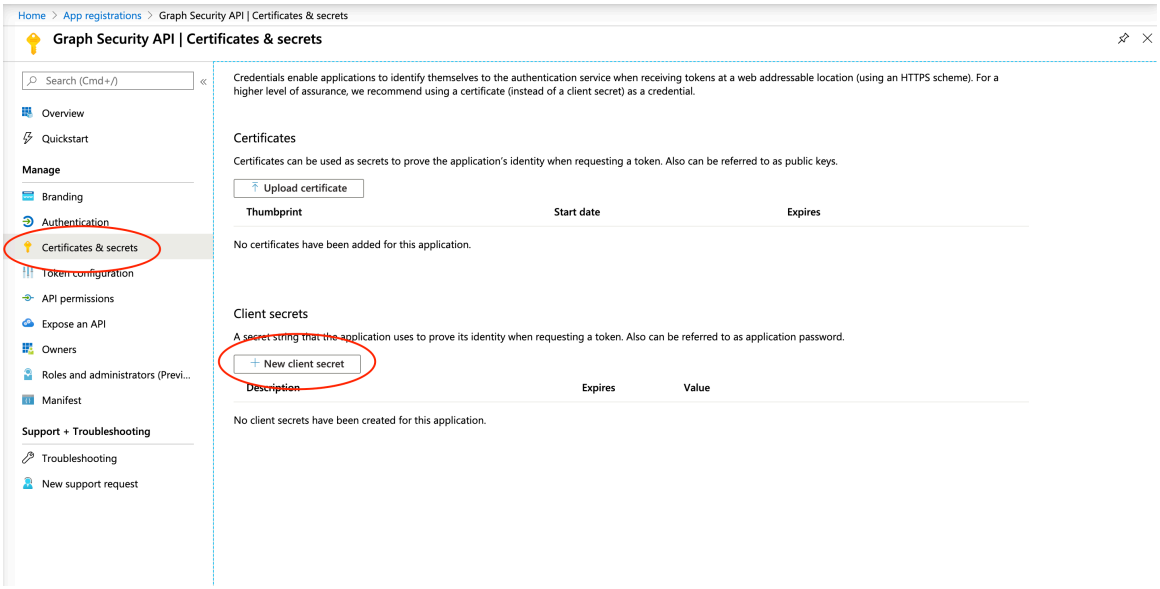
#### Prozedur

1. Melden Sie sich beim Microsoft Azure -Portal an.
2. Geben Sie **App-Registrierungen** in das **Suchfeld** ein.
3. Klicken Sie auf **New registration (Neue Registrierung)**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, z. B. http://localhost, und klicken Sie auf **Registrieren**.
   Der Umleitungs-URI wird verwendet, während die Administratoreinwilligung für die Anwendung erteilt wird.
5. Wählen Sie auf der Seite „App-Registrierungen“ die Anwendung aus, die Sie registriert haben, z. B. Graph Security Demo.
6. Wählen Sie unter **Verwalten**die Option **Zertifikate und geheime Schlüssel**aus.



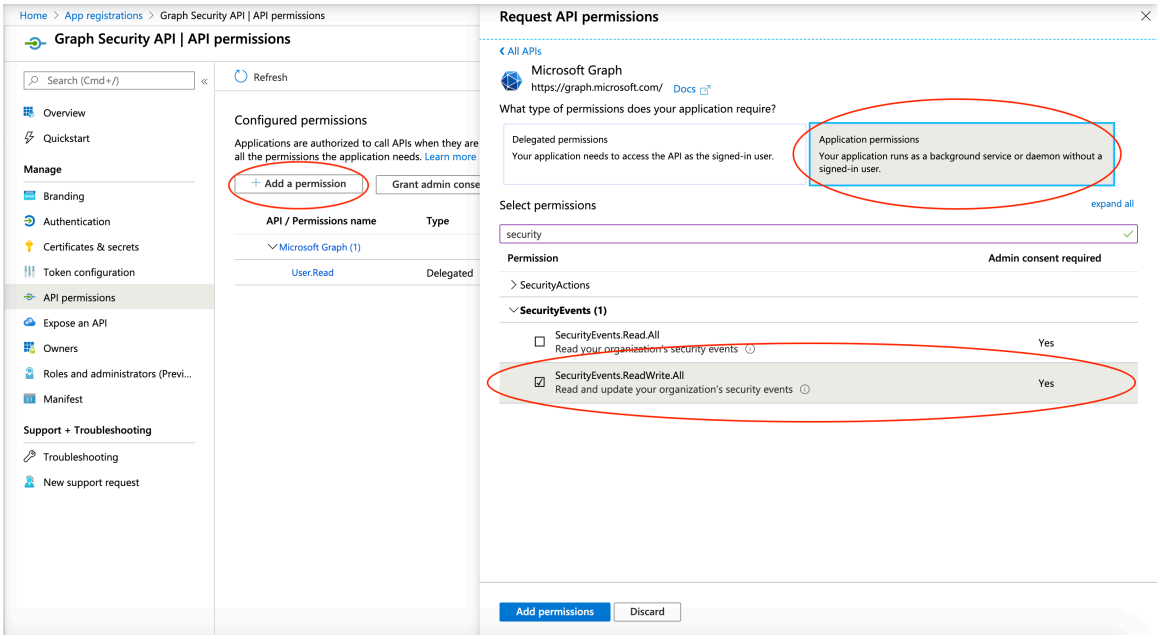

7. Wählen Sie **Neuer geheimer Clientschlüssel** aus, um einen geheimen Clientschlüssel zu erstellen. Kopieren Sie den geheimen Clientschlüssel, und speichern Sie ihn, da er später nicht sichtbar ist. Falls Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen geheimen Clientschlüssel generieren.

   **Hinweis:**
   Wenn Sie den geheimen Clientschlüssel vergessen haben, können Sie einen neuen erstellen, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.

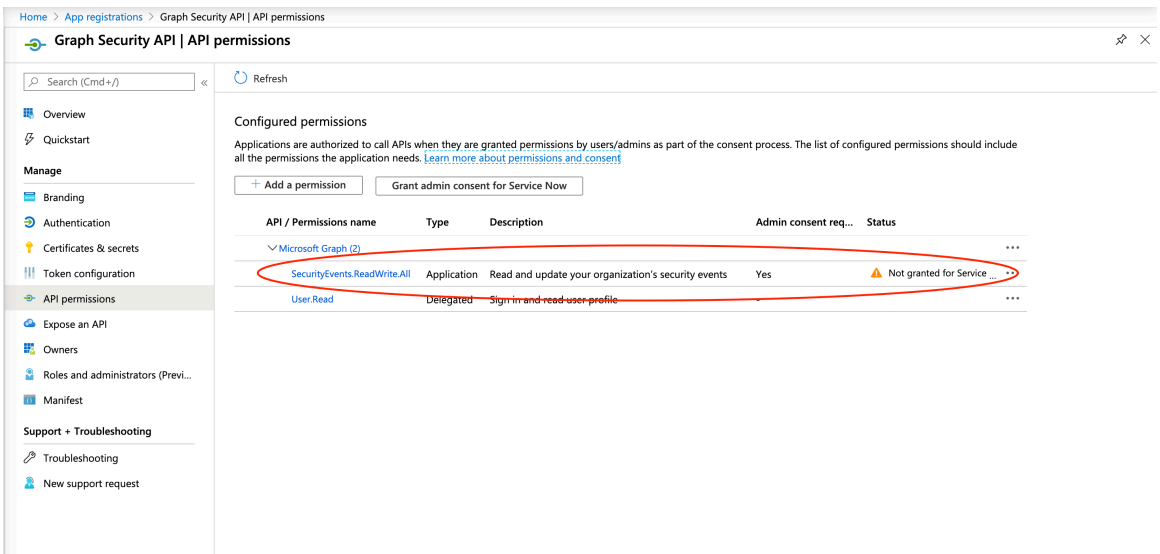
8. Klicken Sie auf der Seite „Übersicht“ auf **API** -Berechtigungen anzeigen.
9. Fügen Sie neue API-Berechtigungen auf Anwendungsebene für SecurityEvents.ReadWrite.All-Sicherheitsevents hinzu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**10.** Erteilen Sie die Einwilligung des Administrators für die neu hinzugefügten API-Berechtigungen. Weitere Informationen finden Sie in der Referenz zu Microsoft Graph-Berechtigungen Microsoft Graph-Berechtigungsmodell.




**11.** Melden Sie sich als Mandantenadministrator an, und geben Sie Ihre Einwilligung für die Anwendung. Die Schritte sind unten aufgeführt:

**a.** Navigieren Sie zur folgenden URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

Geben Sie die APPLICATION_ID der Anwendung ein, die Sie registriert haben.

**12.** Klicken Sie auf **Akzeptieren**, um die von der oben erstellten Anwendung angeforderten Berechtigungen zu akzeptieren.
Anschließend können Sie die Anwendung zum Lesen von Sicherheits-Ereignisse verwenden. Weitere Informationen finden Sie in der Dokumentation zur Microsoft Graph-Sicherheitsautorisierung .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Installieren und konfigurieren Sie die ServiceNow-Anwendung für die Integration von Microsoft Graph Security API-Warnungserfassung

Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform® ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform integriert wird.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Prozedur

1. Wenn Sie die Anwendung Microsoft Graph-Sicherheits-API nicht aus dem ServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die Kachel Microsoft Graph Security API - Alert Ingestion (Microsoft Graph-Sicherheits-API - Warnungserfassung).

3. Um die Anwendung zu konfigurieren, klicken Sie auf **Konfigurieren**.
4. Füllen Sie im angezeigten Dialogfeld „Warnungserfassungskonfiguration“ die Felder aus.
5. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Warnungserfassungen auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.

## Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Warnungsprofil zu erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie ein Profil für die Integration der Warnungserfassung der Microsoft Graph-Sicherheits-API

Als Benutzer mit der Rolle „sn_si.admin“ erstellen Sie ein Warnungsprofil in Ihrer Instanz Now Platform und bestimmen, welche Warnungen Security Incidents verursachen. Bevor Security Incidents aus erfassten Warnungen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform Security Incident angezeigt, sodass Sie eine Vorschau auf die Anzeige des tatsächlichen Security Incident erhalten.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Mit der Integration können Sie verschiedene Arten von Warnungen erfassen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in der Security Operations -Umgebung Ihrer Instanz konfigurieren. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents verursachen.

Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hohes Risiko identifiziert wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen den entsprechenden Feldern in einem Layout von Security Incidents für eine Vorschau zugeordnet. Alle Warnungen, die die Auswahlkriterien in Ihrem Microsoft Azure -Mandanten erfüllen und über den Microsoft Graph-Sicherheits-API verfügbar sind, werden anfänglich in Ihrer Now Platform -Instanz erfasst.

### Identifizieren Sie die Quelle für das Profil

Geben Sie den Namen und die Quelle für das Profil an.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Prozedur

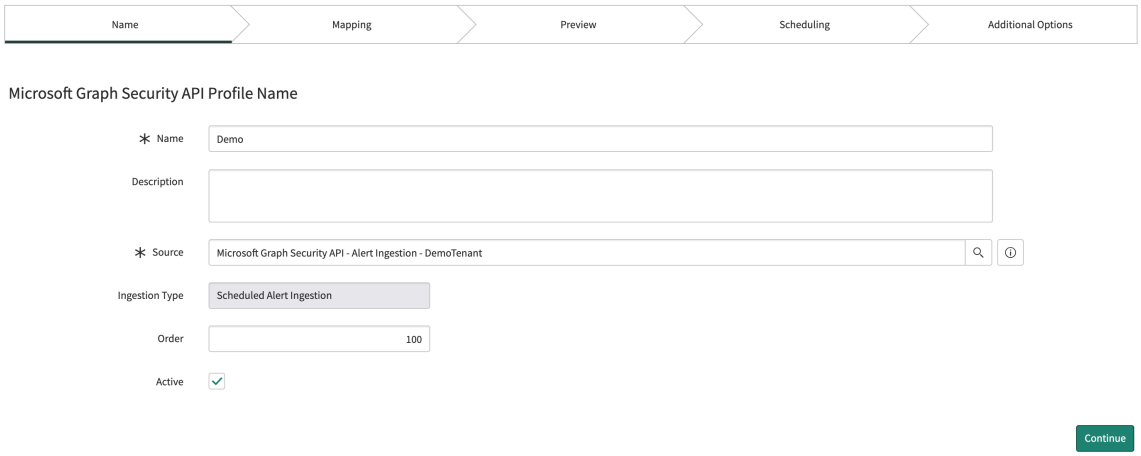
1. Um ein Profil für eine Warnung in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Microsoft Graph-Sicherheits-API-Integration** > **Microsoft Graph-Sicherheits-API-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.




## Nächste Maßnahme

Der nächste Schritt besteht in der Zuordnung der Warnungsfelder.

### Zuordnung von Warnungsfeldern für die Integration der Warnungserfassung der Microsoft Graph-Sicherheits-API

Nachdem Sie die Quellen für die geplante Warnungserfassung identifiziert haben, besteht der nächste Schritt darin, einzelne Warnungsfelder den Feldern in einem Now Platform SIR Security Incident zuzuordnen.

Für den Zuordnungsschritt müssen Sie zuerst Beispielwarnungen aus dem Mandanten Microsoft Azure erfassen. Dann müssen Sie sicherstellen, dass alle relevanten Warnungsfelddaten der entsprechenden Stelle im Incident-Formular SIR zugeordnet sind, und dann den Incident SIR im Vorschaubereich visualisieren.

Die Zuordnung der Beispielwarnungsfelder umfasst Folgendes:

- Erfassen Sie Beispielwarnungen der Microsoft Graph-Sicherheits-API
- Zuordnung von Warnungen zu Security Incident Response-Feldern

### Erfassen Sie Beispielwarnungen der Microsoft Graph-Sicherheits-API

Erfassen Sie Beispielwarnungen aus Ihrem Microsoft Azure -Mandanten.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Prozedur

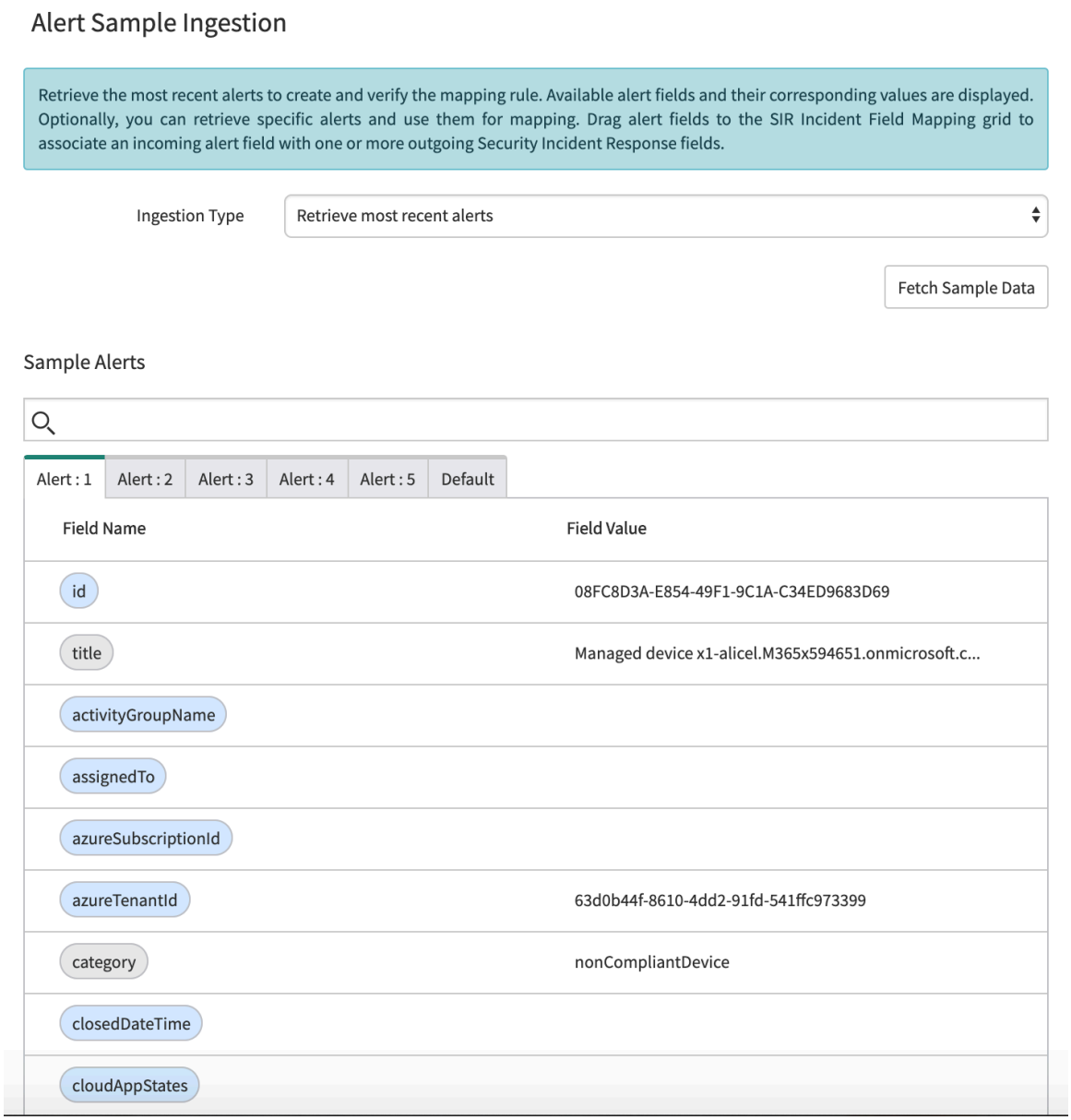
1. Sie können entweder die 5 letzten Beispielwarnungen abrufen oder die eindeutigen Warnungs-IDs für die spezifischen Warnungen angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   **Wählen** Sie in der Auswahlliste „Erfassungseinstellung“ eine der folgenden Optionen aus:
   - Letzte Warnungen abrufen: Die 5 letzten Warnungen werden abgerufen.
   - Wählen Sie Warnungen basierend auf Warnungs-ID aus: Geben Sie die Warnungs-ID für die abzurufenden Warnungen an. Sie können maximal 5 durch Kommas getrennte Warnungs-IDs angeben.
2. Klicken Sie auf **Beispieldaten abrufen**, um die neuesten Beispielwarnungsdaten aus dem Mandanten Microsoft Azure abzurufen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abruf für Beispielwarnungen kann einige Minuten dauern.

Die Beispielwarnungsfeldwerte werden auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Warnungen, die Sie den Security Incident-Feldern SIR zuordnen. Die Ergebnisse der Warnungsfelder und -werte werden als einzelne Registerkarten angezeigt.




Automatische Übersetzung

## Nächste Maßnahme

Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie im nächsten Schritt die Warnungsfelder dem Security Incident zu.

### Zuordnung von Warnungen zu Security Incident Response-Feldern

Ordnen Sie einzelne Warnungsfelder aus ausgelösten Warnungen Feldern in einem Now Platform Security Incident zu.

## Warnungsfeldzuordnung

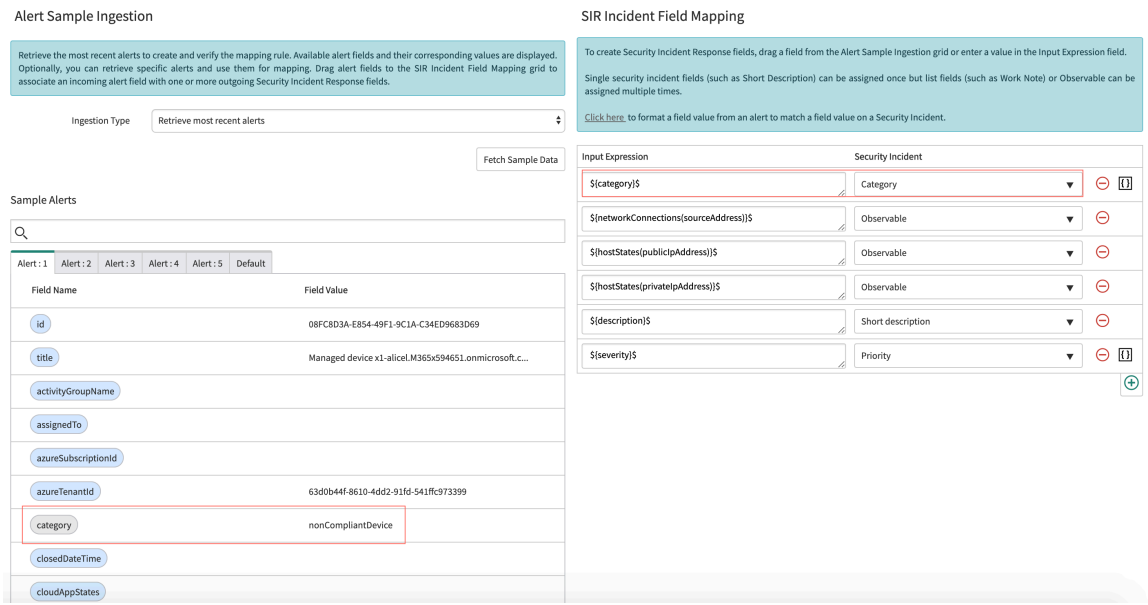
Verwenden Sie als Benutzer mit der Rolle „sn_si.admin“ die Felder aus dem Abschnitt „Beispielwarnungen“ auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der Spalte SIR-Incident-Feldzuordnung im rechten Bereich zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungsfelder von der linken Seite ziehen und sie im Incident-Zuordnungsabschnitt SIR auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Warnungsfeld einem ausgehenden Security Incident-Feld zu.

1. Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie im nächsten Schritt die Warnungsfelder dem Security Incident zu. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.
2. Ziehen Sie den Feldnamen, z. B. Kategorie, in ein Feld in der Spalte Eingabeausdruck neben einem Feldnamen in der Spalte Security Incident.

   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Kategorie dem Feld Kategorie im Security Incident zugeordnet.




Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert während des Vorschauschritts dem Security Incident korrekt zugeordnet wurde.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Warnungsfelder übersehen oder dupliziert werden, sind die Felder farbcodiert. Die Farbcodierung der Warnungsfelder hilft Ihnen, die Warnungswerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Warnungsinformationen nicht zugeordnet wurden.

Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Warnungsfeld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes Warnungsfeld mehr als einem Feld in einem Security Incident zuordnen. Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

**a.** Um manuell einen Wert in das Feld Eingabeausdruck einzugeben, geben Sie ihn im Format ${fieldname}$ ein. Das Warnungsfeld wird dem Security Incident-Feld zugeordnet.

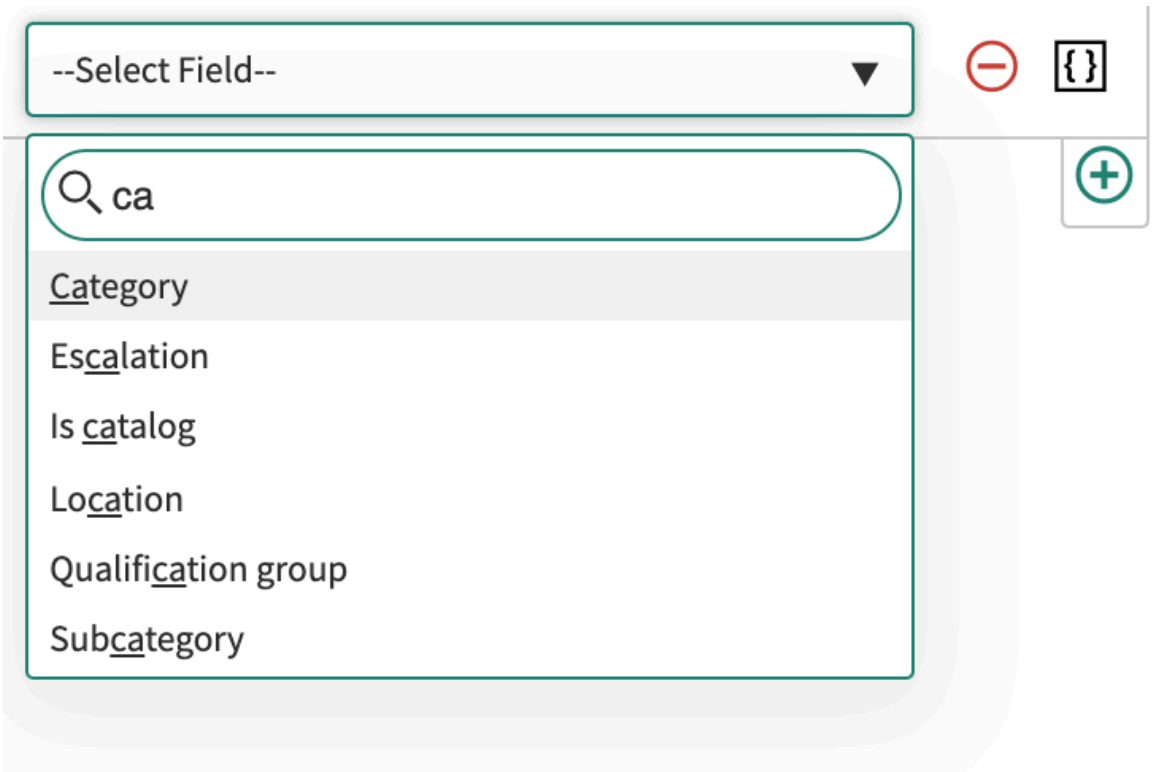
**b.** Sie können erfasste Warnungen nicht den MITRE-ATT&CK Framework-Feldern im Security Incident-Zuordnungsabschnitt zuordnen. Wenn Sie die Felder weiterhin zuordnen, sind die Informationen nicht als Teil der Karte [ MITRE-ATT&CK im Abschnitt MITRE-ATT&CK „ Framework“ im Security Incident-Formular verfügbar. Um die MITRE-ATT&CK -Techniken zuzuordnen, verwenden Sie die automatische Extraktionsfunktion, die als Teil des MITRE-ATT&CK Frameworks im Threat Intelligence -Modul verfügbar ist.

**3.** Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

**a.** Klicken Sie rechts im Formular im Abschnitt SIR Incident-Feldzuordnung am unteren Rand des Rasters auf das Pluszeichen (+). Ein neues Feld wird angezeigt.

**b.** Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat die Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Warnungsfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die bereits zugeordneten SIR Incident-Felder nachzuverfolgen.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

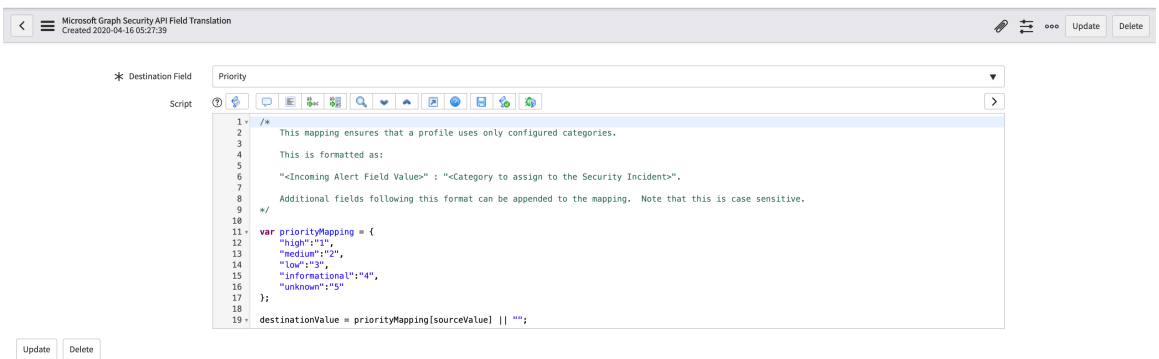
d. Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte Warnungs-ID im Feld Eingabeausdruck auszuwählen. Ordnen Sie es mit der Drag-and-Drop-Funktion neben Ihrem neuen Feld zu.

4. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder daraus entfernen.
5. Nachdem Sie die vorherigen Schritte der Feldzuordnung abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

## Formatfeldübersetzung

In bestimmten Fällen werden Warnungsfeldwerte in Microsoft Graph-Sicherheits-API möglicherweise nicht direkt in die Felder des SIR-Security Incident übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Zum Beispiel kann mit dem Skript-Editor ein Kategoriewert von Malware-Warnung und Virusinfection unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können in eine gemeinsame böswillige Codeaktivität im Feld Kategorie des SIR-Security Incident mit Format übersetzt werden Feldübersetzungsfunktion.

Um den Skript-Editor zu verwenden, klicken Sie auf das Symbol {}. Der Skript-Editor wird angezeigt.




## Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um anzugeben, welche Warnungen Security Incidents erstellen sollen und welche Warnungen herausgefiltert werden sollen, z. B. Warnungen mit niedriger Priorität. Sie



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

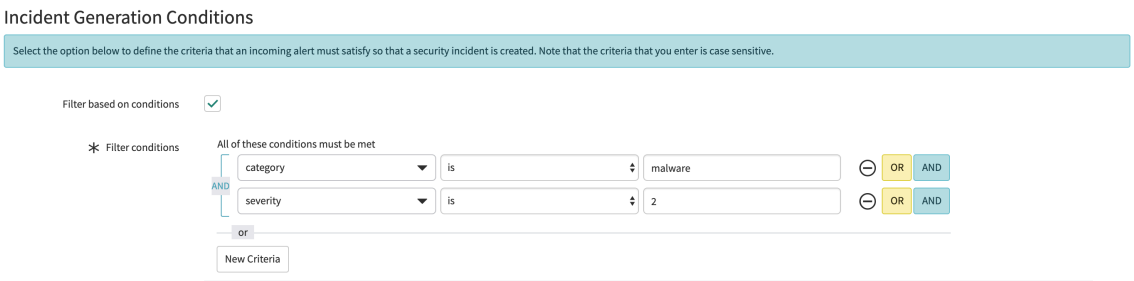
können dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

1. Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und wählen Sie die Option Basierend auf Bedingungen filtern aus. Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Warnungsbeispielerfassung“ für die erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich in Abhängigkeit von der Warnung, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten der Warnung übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu Ihrem Microsoft Azure-Mandanten zurück und überprüfen Ihre Warnungen auf die Stichwörter.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**.
   - Wenn **UND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR**ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.




   Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

   Diese Art der Filterung hilft Ihnen, Sicherheitswarnungen zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn zusätzliche Filterkriterien festgelegt werden, werden nur erforderliche Warnungen erfasst, ohne dass die Abfrage oder die Konfiguration der ausgelösten Warnung geändert werden muss.

## Warnungszusammenfassungskriterien, um ähnliche Warnungen zu behandeln und doppelte Incidents zu verhindern

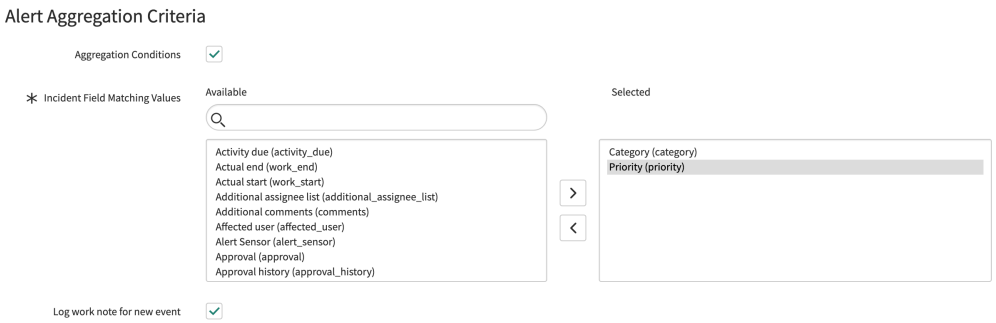
Definieren Sie zusätzliche Warnungszusammenfassungskriterien, die eine eingehende Warnung zu einem vorhandenen SIR Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Warnungsdaten in einem einzigen Security Incident platziert werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

1. Scrollen Sie im Formular zum Abschnitt „Warnungszusammenfassungskriterien“, und wählen Sie die Option Zusammenfassungsbedingungen aus. Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.
2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Now Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt. Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Warnungsfeldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte abgeglichen wird, sind die Bedingungen für die Warnungszusammenfassung nicht erfüllt, und es wird ein neuer Security Incident erstellt. Im Screenshot unten sehen Sie die Zuordnung von Feldern mit mehreren Werten.




Wenn eine neue Warnung mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Warnungen zu einem Security Incident werden in der zugehörigen Liste Zusammengefasste Microsoft Graph-Warnungen angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen zu vorhandenen Security Incidents hinzugefügt werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter Zugehörige Links, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.

3. (Optional) Um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie diese Option. Die Arbeitsnotiz protokolliert, dass eine neue Warnung hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

Sie haben erfolgreich Werte aus einer Warnung zu Feldern in einem SIR Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von Security Incidents mit Filterkriterien zu begrenzen. Sie haben auch Warnungen oder Events an vorhandene SIR Security Incidents angehängt.

4. Klicken Sie auf **Fortsetzen**, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem SIR-Security Incident zugeordnet haben

### Zeigen Sie eine Vorschau des Security Incident für die Microsoft Graph Security API-Integration an

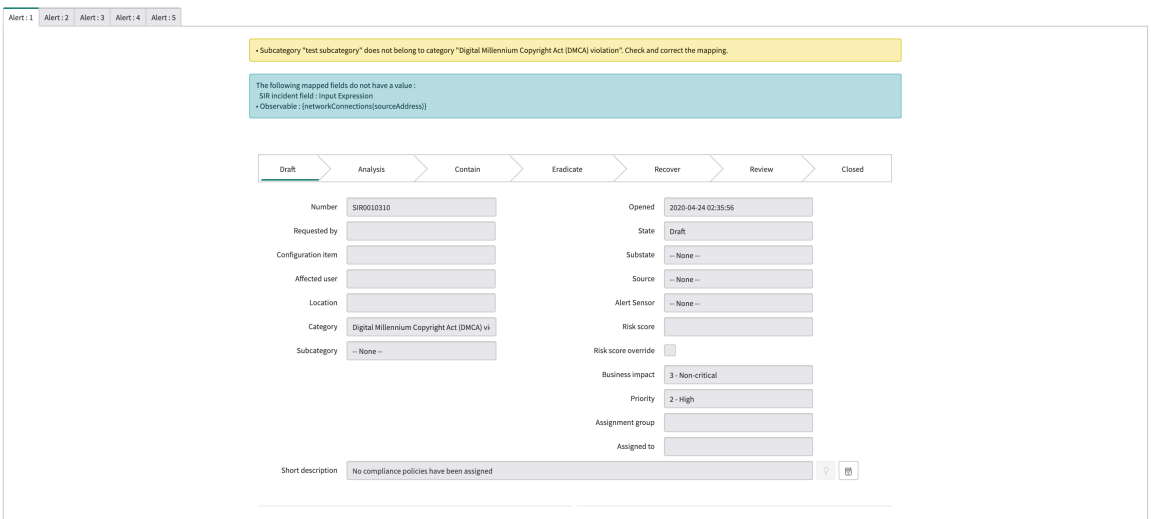
Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Now Platform SIR Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie als Benutzer mit der Rolle sn_si.admin eine Vorschau eines Security Incident an und bearbeiten Sie die Zuordnung bei Bedarf erneut, um fehlerhafte Felder zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

#### Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
   Alle erfassten Warnungen und die auf der Seite „Zuordnung“ definierten Feldzuordnungen werden angezeigt.
2. Klicken Sie auf eine Warnungs-ID, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.




Die obige Abbildung zeigt ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

### Nächste Maßnahme
Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

#### Definieren Sie einen Zeitplan für die Integration der Microsoft Graph-Sicherheits-API

Überprüfen Sie die Standardeinstellungen für den Warnungsabruf, oder ändern Sie die Planung nach Bedarf. Mit diesem Schritt können Sie Ihren Warnungsabruf basierend auf einem Datumsbereich filtern.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Sie können auch auswählen, wie oft zukünftige Warnungen abgefragt werden sollen, die der Konfiguration des Warnungsprofils entsprechen. Bei Profilen für die automatisierte Warnungserfassung überprüfen und ändern Sie die Zeitplanung und den Warnungsabruf, bevor das Profil aktiviert wird. Dieser Schritt ist für geplante Warnungsprofile erforderlich.

Als Benutzer mit der Rolle „sn_si.admin“ konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung der Integration der Microsoft Graph-Sicherheits-API -Warnungserfassung wird durch die unterschiedlichen Abfrageintervalle beeinflusst. Bei der Planung möchten Sie möglicherweise die Systemlast mit der Dringlichkeit von Incidents in Einklang bringen. Für jedes Profil wird ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des Incident und der erwarteten Auslastung Ihres Systems ändern.

### Prozedur
1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie einen aus, um zu planen, wie und wann Warnungen aus dem Mandanten Microsoft Azure abgerufen werden.

3. Klicken Sie auf **Fortfahren**, um zur Seite „Zusätzliche Optionen“ zu navigieren.

#### Automatisieren Sie Warnungsaktualisierungen und -schließungen basierend auf dem SIR-Incident-Status

Die Integration der Microsoft Graph-Sicherheits-API -Warnungserfassung verfügt über eine bidirektionale Schnittstelle, die sowohl Warnungen zum Erstellen von Security Incidents ermöglicht, als auch die Möglichkeit, die Warnungen zu aktualisieren, sobald der Security Incident mit relevanten Incident-Details wie SIR Incident erstellt und/oder geschlossen wurde Nummer, Zuweisungsgruppe, SIR Incident-URL usw. Dieser Abschnitt ist der letzte Teil der Einrichtung der Profilkonfiguration, der optionale Funktionen zum Aktualisieren der Warnungen bereitstellt.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Der Anfangs- und der Abschlusswarnungsstatus werden nur aktualisiert, wenn diese Funktionalität vom Service Provider unterstützt wird. Weitere Informationen finden Sie in der Dokumentation Microsoft Graph-Sicherheits-API und der Dokumentation des Sicherheitsanbieters.

### Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung von Warnungen abzuschließen, wenn der Security Incident erstellt wird.
3. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu verschieben.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um basierend auf Ihrer Planung Warnungen aus dem -Mandanten Microsoft Azure abzurufen. Innerhalb von 24 Stunden können maximal 1.000 Security Incidents erstellt werden.

## Konfigurationseinstellungen für die Microsoft Graph-Sicherheits-API-Integration

Verwenden Sie diese Option, um die Standardsystemeigenschaften der Erfassungsintegration Microsoft Graph-Sicherheits-API zu ändern.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

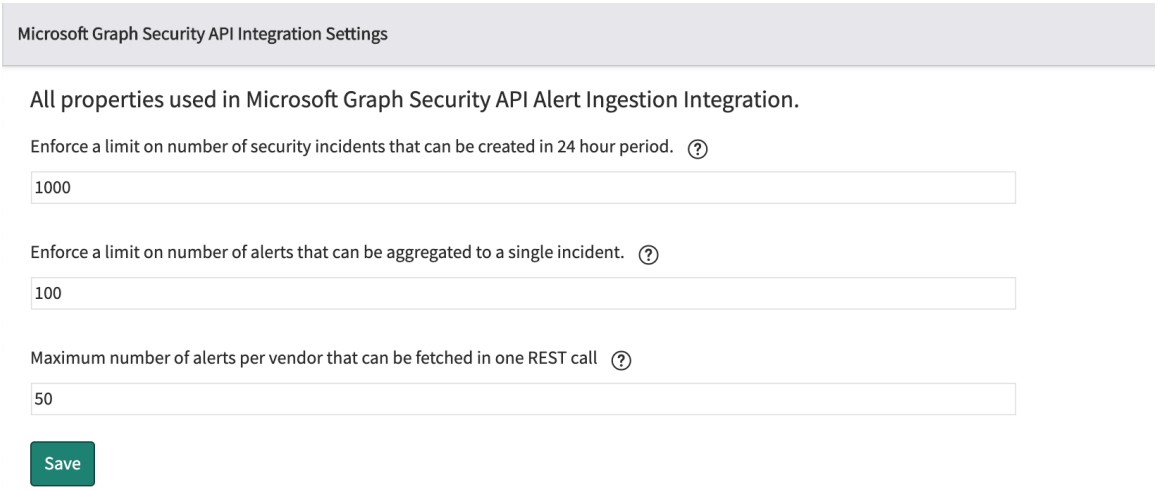
Ändern Sie die Standardkonfigurationseigenschaften, um die Anzahl der Security Incidents zu begrenzen, die innerhalb von 24 Stunden erstellt werden können, oder die Anzahl der Warnungen, die in einem Security Incident zusammengefasst werden können.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Microsoft Graph-Sicherheits-API-Integration** > **Integrationseinstellungen der Microsoft Graph-Sicherheits-API**.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



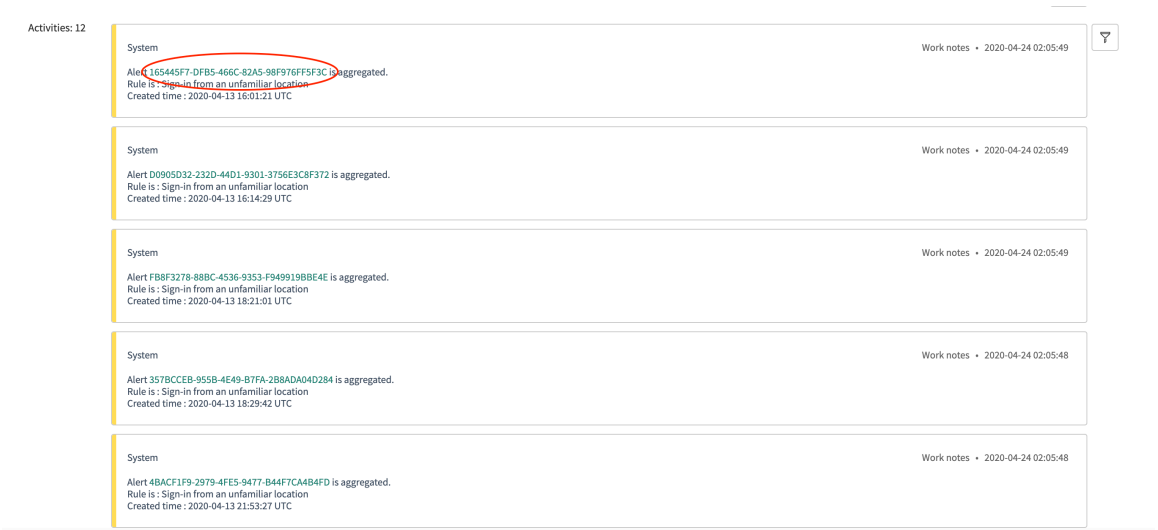

Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

### Security Incident Response-Formular nach der Warnungserfassung

Nachdem eine Microsoft Graph-Sicherheits-API -Warnung erfasst wurde, wird ein Security Incident erstellt und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

## Arbeitsnotiz

Wenn Sie die Option **Arbeitsnotiz für neue Warnung** protokollieren in den Zusammenfassungskriterien der Warnung ausgewählt haben, wie in Zuordnung von Warnungen zu Security Incident Response-Feldernbeschrieben, wird bei der Zusammenfassung der Warnung eine Arbeitsnotiz veröffentlicht.



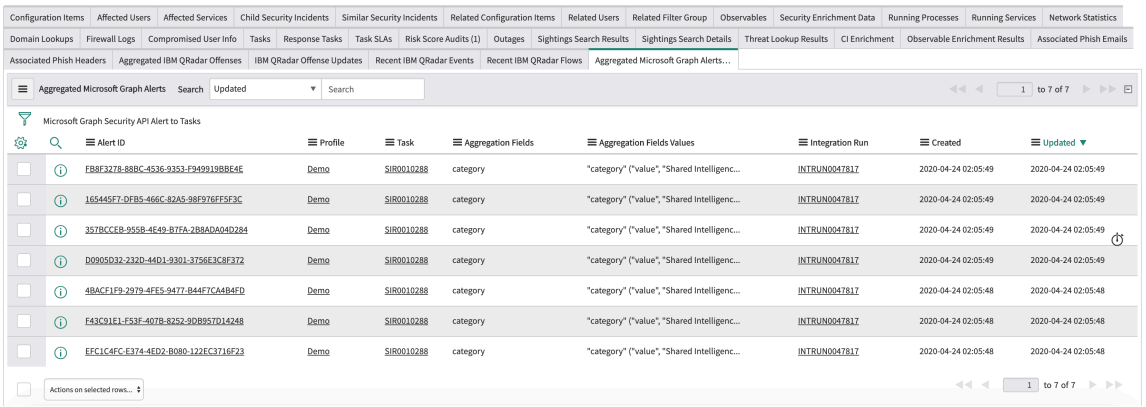

Klicken Sie auf den Warnungslink, um zum internen Warnungsimportdatensatz zu navigieren, der Warnungsrohdaten enthält.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zusammengefasste Warnungen

Klicken **Zugehörige Listen** > **Zusammengefasste Microsoft Graph-Sicherheitswarnungen** , um die zum Security Incident zusammengefassten Warnungen anzuzeigen.




- **Security Incident erstellen**: Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Security Incident erstellen**. Mit dieser Option wird ein neuer Security Incident für die Warnung erstellt, und diese Warnung wird vom übergeordneten Security Incident getrennt.
- **Warnungsdatensatz löschen**: Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf das Menü **Aktionen** und dann auf **Löschen**. Mit dieser Option wird der Warnungsdatensatz gelöscht.

### Optional: Kopieren Sie ein Microsoft Graph-Sicherheits-API-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Profile zu kopieren, um Zeit zu sparen.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Graph-Sicherheits-API-Integration** > **Microsoft Graph-Sicherheits-API-Profil**.
2. Wählen Sie in der angezeigten Liste Microsoft Graph-Sicherheits-API Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.
   Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **Aktiv** auf „false“ gesetzt ist, da das Profil aktiviert werden muss.

### Nächste Maßnahme

Nachdem Sie die Konfigurationsschritte abgeschlossen haben, werden Sie aufgefordert, das neue Profil zu aktivieren.

#### Domänentrennung und Microsoft Graph-Sicherheits-API Warnungserfassung

Domänentrennung wird für diese Anwendung unterstützt. Die Microsoft Graph-Sicherheits-API -Integration erfasst Warnungen von Microsoft Graph-Sicherheitsanbietern und erstellt automatisch Security Incidents. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

### Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

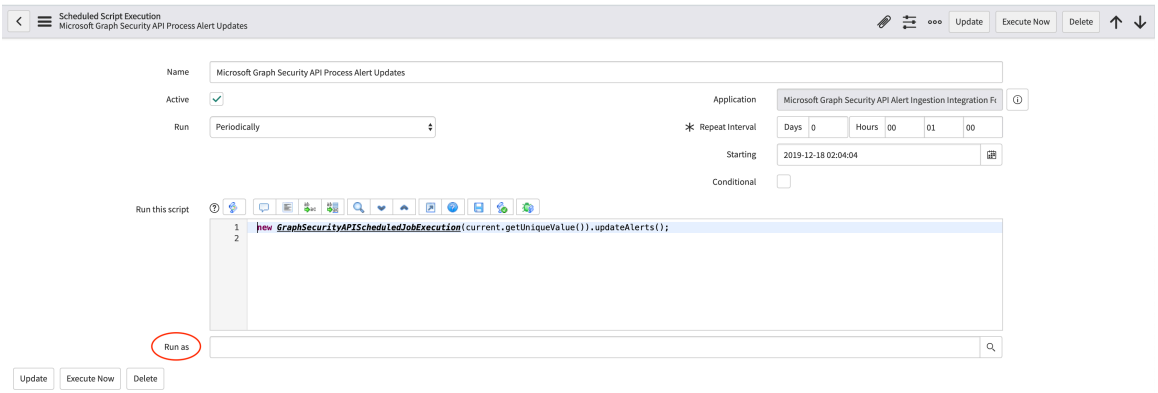
### Funktionsweise der Domänentrennung in der Microsoft Graph-Sicherheits-API

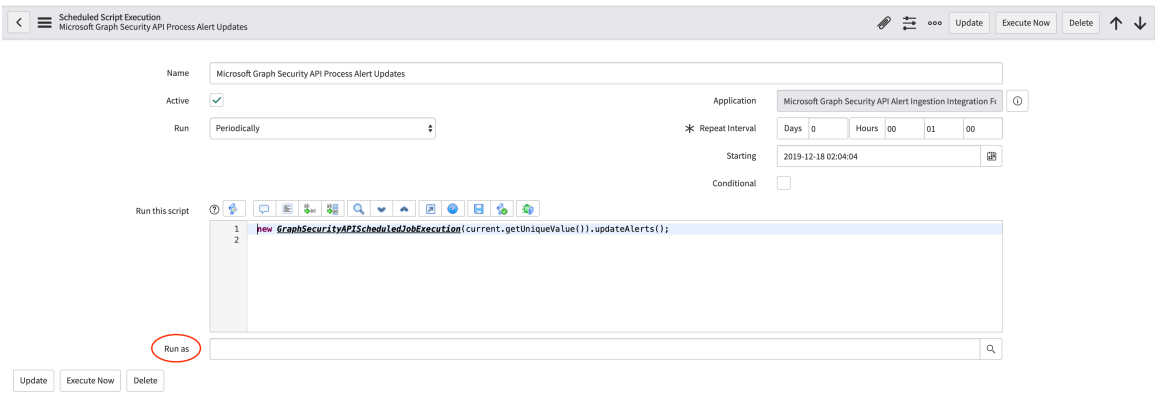
Um eine Domänentrennung zu erreichen, replizieren Sie die regelmäßigen Aufgaben Microsoft Graph-Sicherheits-API „ Profilprozess“ und SIR „ Warnungsaktualisierungen verarbeiten“, und ändern Sie die Benutzer unter „ **Als** ausführen“. Standardmäßig führen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Systembenutzer diese regelmäßigen Aufgaben aus. Ändern **Sie Ausführen als** in einen Benutzer mit der Rolle sn_si.admin in der entsprechenden Domäne, und führen Sie die geplante Aufgabe aus.




### Zugehörige Informationen

Domänentrennung für Service Provider

## Verwendung von Flow Designer und Integration Hub in der Microsoft Graph-Sicherheits-API-Integration

Mit der Funktionalität von Flow Designer und Integration Hub wurden im Rahmen der Microsoft Graph-Sicherheits-API -Integration mehrere Subflows und Aktionen erstellt.

Die folgenden Subflows sind verfügbar:

- Microsoft Graph-Sicherheits-API Konfigurationsvalidierung: Dies wird in der Konfigurationskachel verwendet, um die Anmeldeinformationen beim ersten Setup zu validieren.
- REST-Aufruf für Microsoft Graph-Sicherheits-API: Dies wird für alle Interaktionen mit der Microsoft Graph-Sicherheits-API mithilfe von REST-Aufrufen verwendet.
- Beispielwarnungen abrufen: Dies wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.

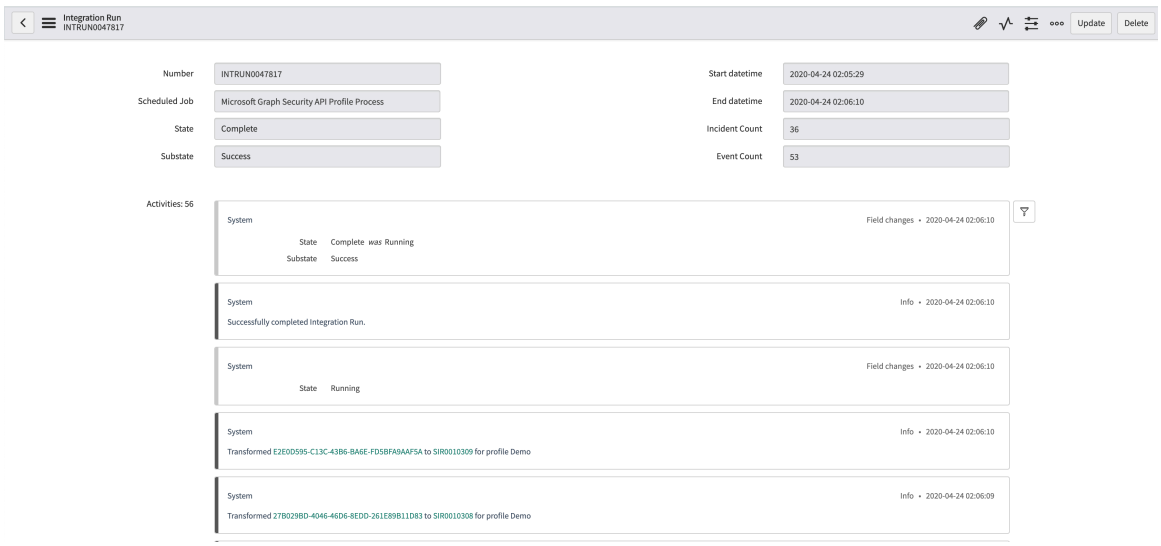
## Problembehandlung bei der Integration der Microsoft Graph-Sicherheits-API

In diesem Abschnitt werden wichtige Tipps zur Fehlerbehebung und häufig gestellte Fragen im Zusammenhang mit der Integration der Microsoft Graph-Sicherheits-API -Warnungserfassung behandelt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Integrationsausführung**: Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Integrationsausführungsdatensatz mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der abgerufenen Warnungen und die Anzahl der Incidents, die in einer geplanten Aufgabe erstellt wurden, werden ebenfalls angezeigt. Benutzer mit der Rolle sn_si.analyst können sehen, ob während der Integrationsausführung Fehler/Profilabrufe fehlgeschlagen sind. Benutzer mit der Rolle sn_si.analyst können die Tabelle sn_event_ingestion_integration_run auf aufgetretene Fehler überprüfen. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Integrationsausführungsdatensätzen für jede Ausführung einer geplanten Aufgabe protokolliert.




- **Unvollständiges Profil**: Während der Konfiguration des Profils müssen Sie im Abschnitt „Zusätzliche Optionen“ (Automatisieren Sie Warnungsaktualisierungen und -schließungen basierend auf dem SIR-Incident-Status) auf die **Schaltfläche** Fertigstellen klicken, um sicherzustellen, dass das Profil in den Status „Warten“ verschoben wird, um anzuzeigen, dass es auf die Erfassung wartet.
- **Profil validieren**: Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die Profilstatus, das Datum des letzten Abrufs des Profils, die Warnungsimporttabelle und die Datensätze der Warnungs-zu-Aufgaben-Tabelle.
- **SSL-Probleme**: Stellen Sie bei der Verbindung über Microsoft Graph-Sicherheits-APIsicher, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in die -Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Weitere Informationen finden Sie in KB0778285 .

## Integration „Palo Alto Networks – AutoFocus“

Das Palo Alto Networks – AutoFocus -Integrationsbasissystem enthält einen Workflow und eine Reihe von Workflow-Aktivitäten, mit denen Sie Palo Alto Networks – AutoFocus in Ihre Instanz integrieren können.

| Erkunden | Einrichten |
| --- | --- |
| Security Incident Response-Integrationen | Aktivieren und konfigurieren Sie die Palo Alto Networks – AutoFocus -Integration |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden

- Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten
- Workflow zum Anreichern von AutoFocus-Sitzungsinformationen abrufen

### Entwickeln

- ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden

### Problembehandlung und Hilfe

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

## Aktivieren und konfigurieren Sie die Palo Alto Networks – AutoFocus -Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich Palo Alto Networks – AutoFocus, schnell aktivieren und einrichten. Bevor Sie Palo Alto Networks – AutoFocusverwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

### Vorbereitungen

Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store herunter.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf die Support-Website von Palo Alto Networks zu, und rufen Sie den API-Schlüssel ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**.
4. Klicken Sie in der Karte Palo Alto Networks AutoFocus auf **Konfigurieren**.
5. Geben Sie den **API-Schlüssel** ein (oder fügen Sie ihn ein), den Sie von der Support-Website von Palo Alto Networks erhalten haben.
6. Klicken Sie auf **Absenden**.

## Workflow zum Anreichern von AutoFocus-Sitzungsinformationen abrufen

Wenn der Workflow **„Security Operations Palo Alto Networks – AutoFocus-Sitzungsanreicherung abrufen“** ausgeführt wird, wird eine Suchabfrage mit AutoFocus in die Warteschlange gestellt, um Informationen zu einer angegebenen Quell-IP zu sammeln. Wenn AutoFocus Wissen über vorherige Sitzungen hat, die von dieser IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

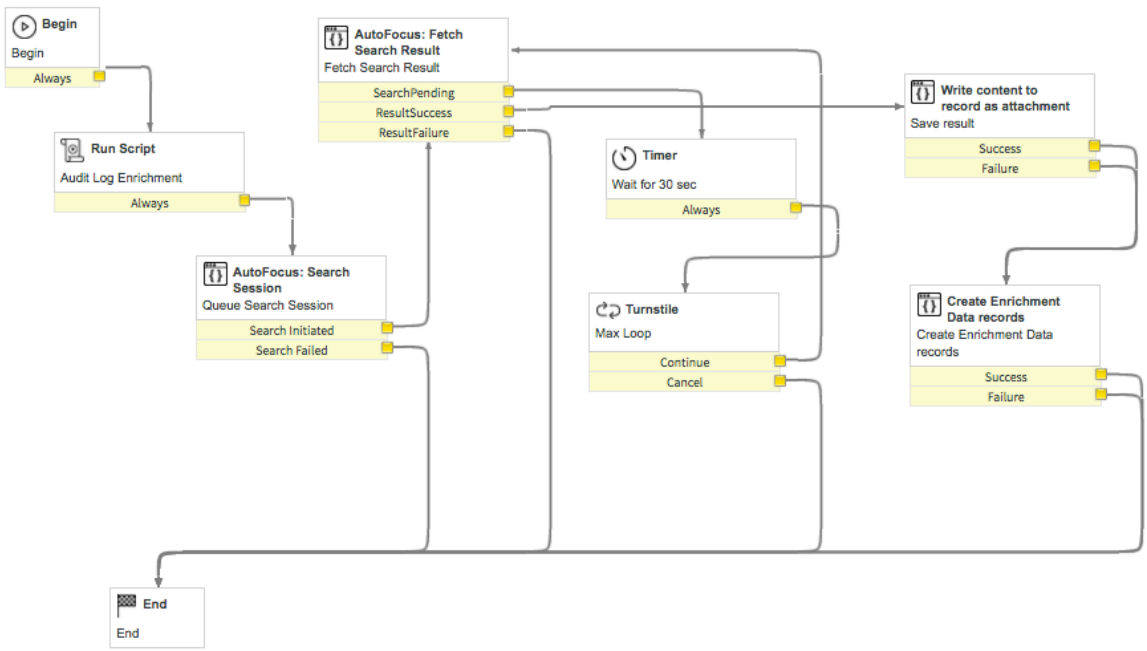


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird
Der Workflow **„Security Operations Palo Alto Networks - AutoFocus-Sitzungsanreicherung abrufen“** wird ausgeführt, wenn das Feld **Quell-IP** in einem Security Incident geändert und der Datensatz aktualisiert wird. Der Workflow ruft die IP-Adresse ab und sendet eine Abfrageanforderung an AutoFocus. Wenn AutoFocus zuvor Sitzungen identifiziert hat, die von der IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

**Security Operations Palo Alto Networks – Wildfire-Datenanreicherungs-Workflow abrufen**




### Prozedur
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Klicken Sie **auf die Registerkarte Kompromittierungsindikatoren** und füllen Sie das Feld **Quell-IP** aus.
3. Klicken Sie auf **Aktualisieren**.
   AutoFocus scannt die Informationen von der IP-Adresse, und eine Textdatei im JSON-Format wird an den Security Incident angehängt.

   Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

#### AutoFocus-Suchsitzungsaktivität
Mit der Workflow-Aktivität **AutoFocus** -Suchsitzung werden Informationen von einer IP-Adresse, die einem Security Incident zugewiesen ist, in AutoFocus hochgeladen und für eine Suchabfrage in die Warteschlange gestellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

**Hinweis:**

Wenn die Aktivität ausgeführt wird, wird eine Suchabfrage mit AutoFocus zum Sammeln von Informationen für eine angegebene Quell-IP in die Warteschlange gestellt. Wenn AutoFocus zuvor Sitzungen identifiziert hat, die von dieser IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| searchSessionQuery [Zeichenfolge] | Die Suchabfrage nach Sitzungsinformationen. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| requestStatus [Boolean] | „True“, wenn eine Suchabfrage für die Ausführung in AutoFocus geplant wurde. |
| Fehler [Zeichenfolge] | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |
| afcookie [Zeichenfolge] | Ein Bezeichner für die AutoFocus-Suchabfrage, die von Aktivität „Suchergebnisse abrufen“. zum Abrufen der Suchergebnisse verwendet wird. |

### Aktivität „Suchergebnisse abrufen“.

Die Workflow-Aktivität „ **Suchergebnisse** abrufen“ ruft Suchergebnisse ab, die durch ein Cookie für die Suchabfrage identifiziert wurden, die von der Aktivität **„AutoFocus** -Suchsitzung“ initiiert wurde.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| afcookie [Zeichenfolge] | Das AutoFocus-Cookie für die von AutoFocus-Suchsitzungsaktivitätgenerierte Suchanforderung. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| searchPending [Boolean] | „True“, wenn die Suchanforderung noch in AutoFocus verarbeitet wird. |
| Ergebnis [Zeichenfolge] | Die Suchergebnisdaten. |
| Status [Boolean] | „True“, wenn die Suche abgeschlossen ist und die Ergebnisse erfolgreich generiert wurden. |
| Fehler [Zeichenfolge] | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |

### Schreiben Sie Inhalte, die als Anhangsaktivität aufgezeichnet werden sollen

Diese Aktivität schreibt den aus einer Eingabe übergebenen Inhalt und erstellt einen bestimmten Anhang zu einem bestimmten Datensatz.

Die Aktivität **Inhalt in Datensatz als Anhang** schreiben kann mit jedem Workflow verwendet werden, um Inhalte zu schreiben und an einen Datensatz anzuhängen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld. |
| sysid [Zeichenfolge] | Der Systembezeichner (sys_id) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld. |
| Nutzlast | Der Nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld. |
| filename | Name der Anhangdatei. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob die Aktualisierung erfolgreich war. |

## Integration „Palo Alto Networks – Firewall“

Um die Integration von Palo Alto Networks – Firewall durchzuführen, stellen Sie sicher, dass MID-Server mit SSH-Anmeldeinformationen eingerichtet ist. Wenn noch keine Firewall eingerichtet ist, fügen Sie eine hinzu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| **Erkunden**<br><br>Security Incident Response-Integrationen | **Einrichten**<br><br>• Aktivieren und konfigurieren Sie die Palo Alto Networks-Firewall-Integration<br>• Richten Sie SSH-Anmeldeinformationen für den MID Server ein |
| **Verwenden**<br><br>Security Operations Integration Palo Alto Networks Firewall-Startprogramm-Workflow | **Entwickeln**<br><br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| **Problembehandlung und Hilfe**<br><br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Richten Sie SSH-Anmeldeinformationen für den MID Server ein

Die Palo Alto Networks-Firewall sendet API-Aufrufe an den MID Server. Stellen Sie daher sicher, dass SSH-Anmeldeinformationen für den MID Server erstellt wurden.

#### Vorbereitungen

- Das Orchestration-Plugin muss aktiviert sein.

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **Orchestration** > **Anmeldeinformationen und Verbindungen** > **Berechtigungen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie im Interceptor-Bildschirm auf **SSH-Anmeldeinformationen**.
4. Füllen Sie die Felder nach Bedarf aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### SSH-Anmeldeinformationen

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie einen Namen für die Anmeldeinformationen ein. |
| Aktiv | Aktivieren Sie diese Checkbox, um diese Anmeldeinformationen zu aktivieren. |
| Betrifft | Wählen Sie **Alle MID Server** oder **Bestimmte MID Server aus**. |
| MID-Server | Wenn Sie **Spezifische MID Server**ausgewählt haben, klicken Sie auf das Sperrsymbol, und wählen Sie die MID Server aus, auf die Sie diese Anmeldeinformationen anwenden möchten. |
| Reihenfolge | Wählen Sie die Reihenfolge aus, in der die Anmeldeinformationen vom Server getestet werden. Kleinere Zahlen werden zuerst versucht. |
| Benutzernamen | Geben Sie den Benutzernamen des Benutzers ein, der diesen Anmeldeinformationen zugeordnet ist, falls vorhanden. |
| Passwort | Wenn Sie einen **Benutzernamen**eingegeben haben, geben Sie das Passwort des Benutzers ein. |
| Tag | Geben Sie ein Tag ein, das für Suchkriterien verwendet werden soll. Das **Tag** -Feld muss den gleichen Wert enthalten wie der **Name**. |

### Aktivieren und konfigurieren Sie die Palo Alto Networks-Firewall-Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich Palo Alto Networks – Firewall, schnell aktivieren und einrichten. Bevor Sie Palo Alto Networks – Firewallverwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

#### Vorbereitungen

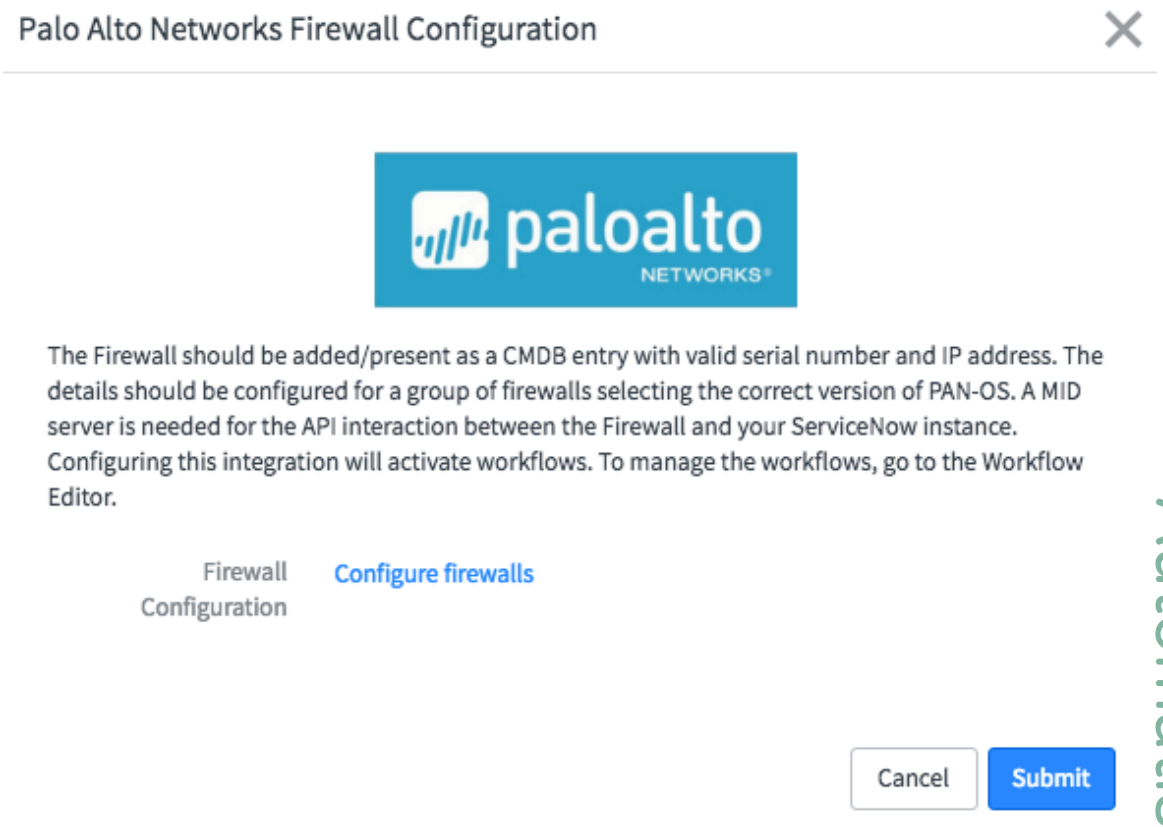
Erforderliche Rolle: sn_si_admin

#### Prozedur

1. Greifen Sie vor der Aktivierung und Konfiguration der Integration auf das Palo Alto Networks-Firewall-Dashboard zu.
   Notieren Sie sich die Namen der dynamischen IP-Liste, der dynamischen URL-Liste oder der dynamischen Domänenliste, die Sie für die Firewall-Blockierung verwenden.
2. Laden Sie die Integration aus dem herunter ServiceNow Store.
3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte „Palo Alto Networks-Firewall“ auf **Konfigurieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie **auf Firewalls konfigurieren**.
6. Klicken Sie im Bildschirm „Firewall-Konfigurationen“ auf **Neu**.
7. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Firewalls | Klicken Sie auf das Sperrsymbol, und wählen Sie die zu konfigurierende Firewall aus. |
| Firewall-Version | Wählen Sie die Version Palo Alto Networks-Firewall aus.**PAN-OS-7.1** ist die empfohlene Version. Die Auswahl früherer Versionen kann zu inkonsistenten Ergebnissen führen. |
| Benutzername | Geben Sie den Benutzernamen ein, der beim Herstellen einer Verbindung zur Firewall über REST-Endpunkte verwendet werden soll. |
| Passwort | Geben Sie das Passwort für den verbindenden Benutzer ein. |
| Dynamische IP-Liste | Geben Sie den Namen der externen dynamischen Liste oder dynamischen Sperrliste ein, die Sie für IP-Adressen verwenden. |
| Dynamische URL-Liste | Geben Sie den Namen der externen dynamischen Liste oder dynamischen Sperrliste ein, die Sie für URLs verwenden. |
| Dynamische Domänenliste | Geben Sie den Namen der externen dynamischen Liste oder dynamischen Sperrliste ein, die Sie für Domänen verwenden. |

8. Klicken Sie auf **Absenden**.

Automatische Übersetzung

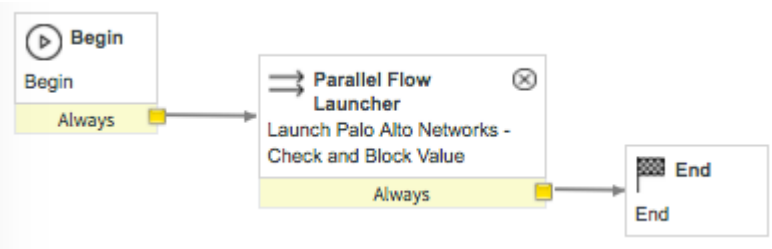
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Operations Integration Palo Alto Networks Firewall-Startprogramm-Workflow

Der Workflow**„Security Operations Integration Palo Alto Networks Firewall Launcher** “ ist die Palo Alto Networks-Firewall-Implementierung, die vom Workflow „ **Security Operations Integration - Block Request** “ gestartet wird.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Zu den Workflow-Prozessaktivitäten gehören:Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten.




### Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten

Während Security Incidents erstellt und selektiert werden, um potenzielle Bedrohungen zu identifizieren, können Sie den Workflow **„Security Operations Palo Alto Networks – Wert** prüfen und blockieren“ verwenden, um IP-Adressen, URLs und Domänen mithilfe von externen dynamischen Listen, die in Palo Alto Networks – Firewalldefiniert sind, automatisch zu überprüfen und zu aktualisieren.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Der Workflow **„Security Operations Palo Alto Networks – Wert überprüfen und blockieren“** wird ausgeführt, wenn Firewall-Blockierungsanforderungen übermittelt werden. Die Blockierungsanforderung gibt die zu verwendende Firewall, den Typ des zu überprüfenden und zu blockierenden erkennbaren Elements (falls erforderlich) und den Blockwert an. Das heißt, die betreffende IP-Adresse, URL oder Domäne.

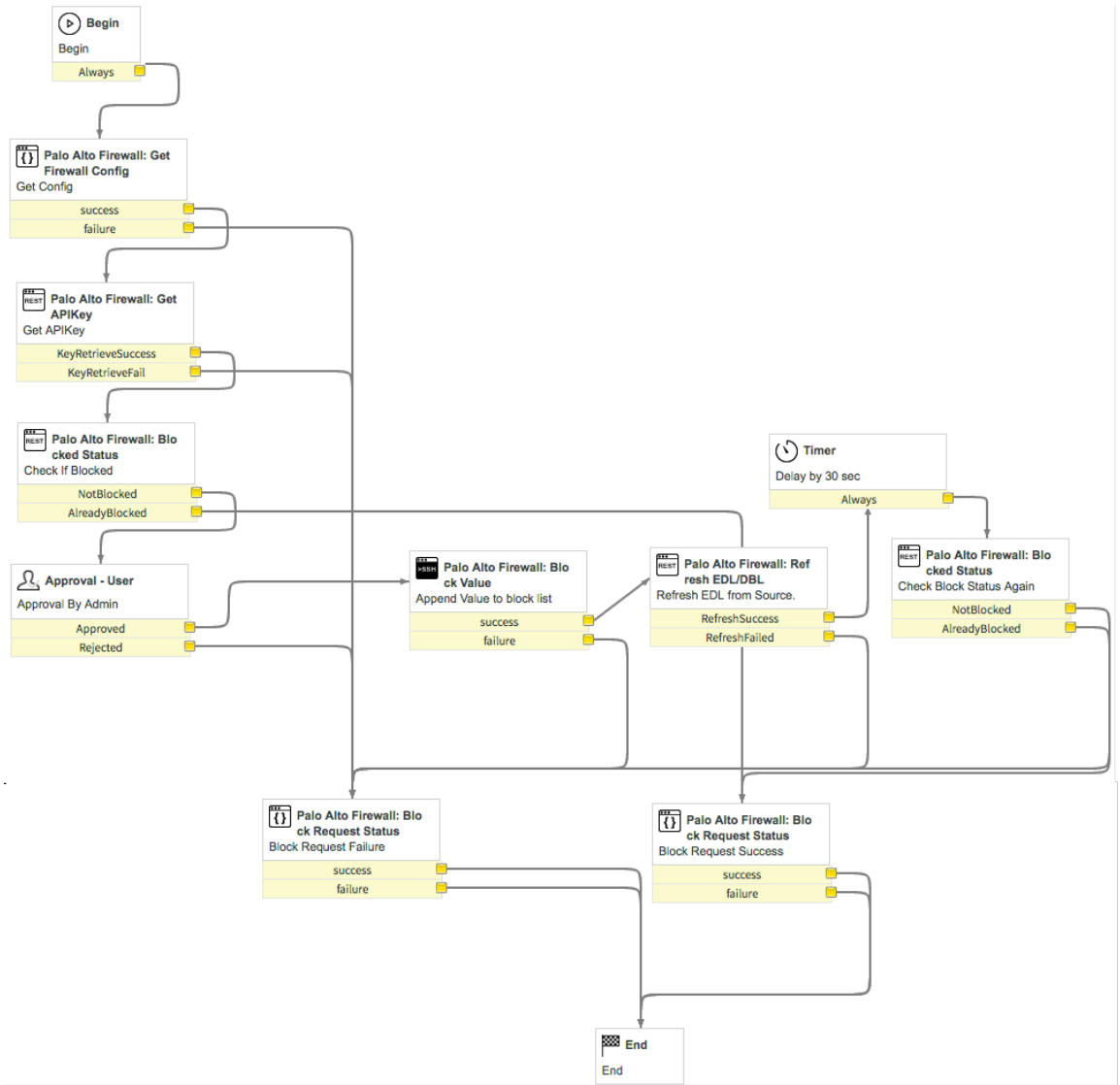
Während der Workflow-Ausführung die unter definierten Befehle **Integration mit Palo Alto Networks** > **Firewall** > **Befehle** werden ausgeführt. Die Typbefehle anzeigen (z. B. Show-IP-ExternalDynamicList) bestimmen, ob der Wert auf der Firewall vorhanden ist. Die Typaktualisierungsbefehle (z. B. Refresh-IP-ExternalDynamicList) fügen der Sperrliste Werte hinzu, die in der Firewall nicht vorhanden sind.

Nachdem die Aktivität „ Blockierter Status “ ausgeführt wurde, ist die Genehmigung durch einen Systemadministrator erforderlich, bevor der Workflow fortgesetzt werden kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten




## Prozedur

1. Navigieren zu **Integration mit Palo Alto Networks** > **Firewall** > **Anforderungen blockieren**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Firewall | Wählen Sie die zu verwendende Firewall aus. |
| Blocktyp | Wählen Sie den Typ des zu prüfenden Werts aus:<br>○ IP<br>○ URL<br>○ DOMAIN |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Blockwert | Geben Sie den Wert des ausgewählten Typs ein, der auf der Firewall überprüft werden soll. |

4. Klicken Sie auf **Absenden**.

### Aktivität „Palo Alto Firewall – Block Request Status“

Diese Aktivität wird von anderen Aktivitäten aufgerufen, um den Status der Firewall-Blockanforderung auf Erfolg oder Fehler festzulegen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| firewallBlockRequestSysid [Zeichenfolge] | Die System-ID der Firewall-Blockierungsanforderung. Diese Eingabevariable ist obligatorisch. |
| Status [Zeichenfolge] | Gibt an, ob der Aktualisierungsauftrag ausgeführt wurde: Erfolg oder Fehler. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob der Aktualisierungsauftrag erfolgreich war oder fehlgeschlagen ist. |

### Palo Alto-Firewall – Aktivität „Blockwert“.

Nachdem der Workflow einen Wert identifiziert hat, der sich nicht in der Firewall befindet, wird der Datensatz zur Genehmigung weitergeleitet. Nach der Genehmigung stellt diese Aktivität über Ihre SSH-Anmeldeinformationen eine Verbindung zum MID Server her und ruft ein Skript auf, das den Wert der externen Sperrliste der Firewall hinzufügt.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Hinweis:**
Sie müssen die Eingabevariablen für diese Aktivität manuell eingeben und dann den Workflow veröffentlichen . Wenn der Workflow nicht veröffentlicht wird, werden die Eingabevariablen für Nicht-Administratoren nicht gespeichert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| toBeBlockedValue [Zeichenfolge] | Der Wert, der der EDL hinzugefügt werden soll, falls noch nicht vorhanden. Diese Eingabevariable ist obligatorisch. |
| typeToBeBlocked [Zeichenfolge] | Der Typ des zu blockierenden Werts: IP, URL oder Domäne. Diese Eingabevariable ist obligatorisch. |
| targetHost [Zeichenfolge] | Der MID Server, auf dem das Skript ausgeführt wird. |
| SSHCredentialTag [Zeichenfolge] | Das auf dem MID-Server definierte SSH-Anmeldeinformations-Tag. |
| scriptCommand [Zeichenfolge] | Das AppendValueToList.sh-Skript, das zum Hinzufügen des Werts zur EDL verwendet wird. Sie erfordert den vollständigen Pfad zum MID Server. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Das an die EDL übergebene Ergebnis. |

#### Palo Alto-Firewall – Aktivität „Blockierter Status“.

Diese Aktivität überprüft, ob der Wert (IP, URL oder Domäne) in der jeweiligen externen dynamischen Liste/dynamischen Sperrliste (EDL/DBL) auf der Firewall enthalten ist. Die EDL/DBL-Details werden mit einem operativen Befehl von der Firewall abgerufen, und eine Routine wird ausgeführt, um zu überprüfen, ob der Wert auf der Firewall blockiert ist.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgeführten Eingabevariableneinträge sind obligatorisch.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| valueToBeChecked [Zeichenfolge] | Der Wert in der Blockanforderung. |
| showEDLDetailsCommand [Zeichenfolge] | Der Befehl „Externe dynamische Liste“, der verwendet wird, um zu bestimmen, ob der Wert auf der Firewall vorhanden ist. |
| FirewallIpAddress [Zeichenfolge] | Die IP-Adresse der verwendeten Firewall. |
| FirewallApiKey [Zeichenfolge] | Der Firewall-API-Schlüssel. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie Daten, die dynamisch mit der Palo Alto Firewall Operational Command-API-Nachricht generiert werden.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| commandResult [Zeichenfolge] | Die Ergebnisse der Firewall für den Befehl show EDL Details. |
| blockiertStatus [Boolean] | „True“ zeigt an, dass blockiert ist. „False“ gibt an, dass der Wert nicht blockiert ist. |
| commandResponse [Zeichenfolge] | Der von der Firewall erhaltene Antwortstatus für den Befehl show EDL Details. |

### Palo Alto-Firewall: Aktivität „API-Schlüssel abrufen“.

Mit dieser Aktivität wird der API-Schlüssel von der Firewall abgerufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgeführten Eingabevariableneinträge sind obligatorisch.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| Benutzername [Zeichenfolge] | Der Benutzername des Firewall-Administrators. |
| Passwort [Zeichenfolge] | Das Firewall-Administratorpasswort |
| FirewallIpAddress [Zeichenfolge] | IP-Adresse der Firewall |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| APIKey [Zeichenfolge] | Der Firewall-API-Schlüssel. |

### Palo Alto-Firewall: Aktivität „Firewall-Konfiguration abrufen“.

Die Workflow-Aktivität **„Palo Alto Firewall:** Firewall-Konfiguration abrufen“ ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der Datenbank ab und stellt sie der nachfolgenden Aktivität zur Verfügung.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| firewallSysid [Zeichenfolge] | System-ID der Firewall Diese Eingabevariable ist obligatorisch. |
| typeOfValueToBeBlocked [Zeichenfolge] | Der Typ des Werts, der auf der Firewall blockiert werden soll: IP, URL oder Domäne. |
| firewallIPAddress [Zeichenfolge] | IP-Adresse der Firewall |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ipEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für IP-Adressen. |
| urlEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für URLs. |
| domainEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für Domänen. |
| firewallVersionSysId [Zeichenfolge] | Die System-ID für die Firewall-Version. |
| refreshEDLCommand [Zeichenfolge] | Der Befehl, der zum Aktualisieren der EDL aus der Quelle verwendet werden soll. |
| ShowEDLDetailsCommand [Zeichenfolge] | Der Befehl, der zum Abrufen der EDL-Details verwendet werden soll. |
| Status [Boolean] | „True“ zeigt Erfolg an. „False“ zeigt einen Fehler an. |
| Fehler [Zeichenfolge] | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |
| Endpunkt [Verschlüsselt] | Der verschlüsselte Endpunkt aus der Datenbank. |

### Palo Alto-Firewall: EDL/DBL-Aktivität aktualisieren

Diese Aktivität führt einen operativen Befehl auf der Firewall aus, um die externe dynamische Liste aus der auf der Firewall konfigurierten Quelle zu aktualisieren. Die Ausgabe dieser Aktivität gibt an, ob der Aktualisierungsauftrag in die Warteschlange gestellt wurde.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgeführten Eingabevariableneinträge sind obligatorisch.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| FirewallIpAddress [Zeichenfolge] | Die IP-Adresse der Firewall, die aktualisiert wird |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eingabevariablen (Fortsetzung)

| Variable | Beschreibung |
|---|---|
| FirewallApiKey [Zeichenfolge] | Der aktualisierte Firewall-API-Schlüssel. |
| FirewallCommand [Zeichenfolge] | Der operative Befehl, der ausgeführt werden soll, um den Aktualisierungsauftrag in die Warteschlange zu stellen. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| activity.Output.result [Zeichenfolge] | Eine Textzeichenfolge, die angibt, ob der Aktualisierungsauftrag zur Ausführung in die Warteschlange gestellt wurde: Erfolg oder Fehler. |

### Workflow „Protokolldaten abrufen“.

Wenn Security Incident Response, Threat Intelligenceund Palo Alto Networks – Firewall aktiviert sind, wird der Workflow „ **Security Operations Palo Alto Networks - Protokolldaten** abrufen“ automatisch ausgeführt, wenn die Quell-IP für erkennbare Elemente in einem Security Incident geändert wird.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

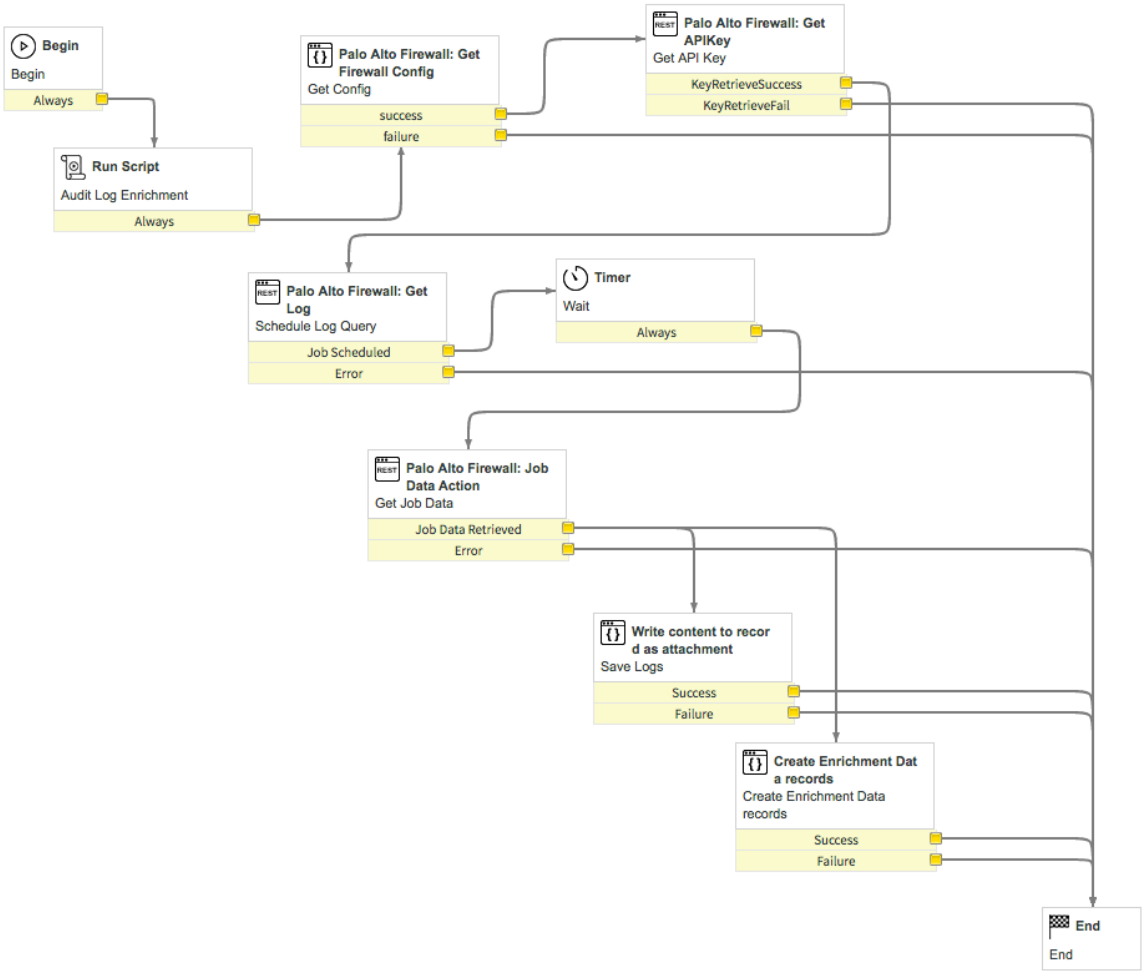
### Warum und wann dieser Vorgang ausgeführt wird

Während der Workflow-Ausführung werden Firewall-Konfigurationsinformationen aus der -Datenbank abgerufen, und der API-Schlüssel wird von der Firewall abgerufen. Die Aktivität Protokoll abrufen setzt eine Suchabfrage auf der Firewall in die Warteschlange. Wenn die Abfrage ausgeführt wird, gibt sie eine Auftrags-ID zurück, die zum Abrufen von Bedrohungsprotokolldaten von der Firewall verwendet wird. Die Protokolldaten werden als XML-Datei an den Security Incident angehängt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow „Security Operations Palo Alto Networks – Protokolldaten abrufen“.**






## Prozedur

1. Navigieren Sie zu einem Security Incident, der erkennbare Elemente enthält.
2. Klicken Sie auf die Registerkarte **Erkennbare Security Incident-Elemente**.
3. Fügen Sie unter **Quell-IP**die IP-Adresse hinzu, oder ändern Sie sie.
4. Klicken Sie auf **Aktualisieren**.
   Der Workflow „ **Security Operations Palo Alto Networks - Protokolldaten** abrufen“ wird ausgeführt, und angereicherte Bedrohungsprotokolldaten werden an den Security Incident angehängt. Die Informationen werden auch analysiert und im Abschnitt „ **Firewall-Protokolle** “ auf der **Registerkarte** „Ergänzungsdaten“ angezeigt.

### Palo Alto-Firewall: Aktivität „API-Schlüssel abrufen“.

Mit dieser Aktivität wird der API-Schlüssel von der Firewall abgerufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgeführten Eingabevariableneinträge sind obligatorisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Benutzername [Zeichenfolge] | Der Benutzername des Firewall-Administrators. |
| Passwort [Zeichenfolge] | Das Firewall-Administratorpasswort |
| FirewallIpAddress [Zeichenfolge] | IP-Adresse der Firewall |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| APIKey [Zeichenfolge] | Der Firewall-API-Schlüssel. |

## Palo Alto-Firewall: Aktivität „Firewall-Konfiguration abrufen“.

Die Workflow-Aktivität **„Palo Alto Firewall:** Firewall-Konfiguration abrufen“ ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der Datenbank ab und stellt sie der nachfolgenden Aktivität zur Verfügung.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| firewallSysid [Zeichenfolge] | System-ID der Firewall Diese Eingabevariable ist obligatorisch. |
| typeOfValueToBeBlocked [Zeichenfolge] | Der Typ des Werts, der auf der Firewall blockiert werden soll: IP, URL oder Domäne. |
| firewallIPAddress [Zeichenfolge] | IP-Adresse der Firewall |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ipEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für IP-Adressen. |
| urlEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für URLs. |
| domainEDLName [Zeichenfolge] | Der Name der externen dynamischen Liste für Domänen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| firewallVersionSysId [Zeichenfolge] | Die System-ID für die Firewall-Version. |
| refreshEDLCommand [Zeichenfolge] | Der Befehl, der zum Aktualisieren der EDL aus der Quelle verwendet werden soll. |
| ShowEDLDetailsCommand [Zeichenfolge] | Der Befehl, der zum Abrufen der EDL-Details verwendet werden soll. |
| Status [Boolean] | „True“ zeigt Erfolg an. „False“ zeigt einen Fehler an. |
| Fehler [Zeichenfolge] | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |
| Endpunkt [Verschlüsselt] | Der verschlüsselte Endpunkt aus der Datenbank. |

### Palo Alto-Firewall: Protokollaktivität abrufen

Die Workflow-Aktivität **Palo Alto Firewall: Protokoll** abrufen plant eine Abfrage auf der Firewall, um Protokolle abzurufen, und gibt eine JobID zurück, die zum Abrufen der Protokolldaten verwendet wird.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| FirewallIpAddress [Zeichenfolge] | IP-Adresse der Firewall Diese Eingabevariable ist obligatorisch. |
| FirewallApiKey [Zeichenfolge] | Der API-Zugriffsschlüssel der Firewall. Diese Eingabevariable ist obligatorisch. |
| FirewallLogType [Zeichenfolge] | Der Typ der abzurufenden Protokolldaten (festgelegt auf Bedrohung). Diese Eingabevariable ist obligatorisch. |
| FirewallLogFilterQuery [Zeichenfolge] | Die Abfrage, die ausgeführt werden soll, um nach Protokollen in der Firewall zu suchen. Diese Eingabevariable ist obligatorisch. |
| LogDirection [Zeichenfolge] | Gibt an, ob Protokolle in der Reihenfolge „Älteste zuerst“ (rückwärts) oder „Neueste zuerst“ (vorwärts) angezeigt werden. |
| LogNumber [Zeichenfolge] | Gibt die Anzahl der abzurufenden Protokolle an. |
| LogSkipCount [Zeichenfolge] | Gibt die Anzahl der Protokolle an, die beim Protokollabruf übersprungen werden sollen. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| QueueJobID [Zeichenfolge] | Die von der Firewall zurückgegebene Job-ID |
| JobScheduled [Zeichenfolge] | Gibt an (Erfolg oder Fehler), ob der Job an die Firewall gesendet wurde. |
| Fehler [Zeichenfolge] | Alle zurückgegebenen Fehler. |

### Palo Alto-Firewall – Aktivität „Auftragsdatenaktion“.

Nachdem die Aktivität „ **Palo Alto Firewall: Protokoll** abrufen“ die Suchabfrage an die Firewall in die Warteschlange gestellt und den Auftrag ausgeführt hat, ruft die Aktivität **„Palo Alto Firewall:** Auftragsdatenaktion“ die Bedrohungsprotokolldaten von der Firewall ab.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle Eingabefelder sind Pflichtfelder.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| FirewallIpAddress [Zeichenfolge] | IP-Adresse der Firewall |
| FirewallApiKey [Zeichenfolge] | Der API-Zugriffsschlüssel der Firewall. |
| Stellen-ID [Zeichenfolge] | Die ID des Auftrags in der Warteschlange. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| commandStatus [Zeichenfolge] | Gibt an (Erfolg oder Fehler), ob Daten von der Firewall abgerufen wurden. |
| JobData [Zeichenfolge] | Die von der Firewall erfassten Daten |
| Fehler [Zeichenfolge] | Alle zurückgegebenen Fehler. |

### Schreiben Sie Inhalte, die als Anhangsaktivität aufgezeichnet werden sollen

Diese Aktivität schreibt den aus einer Eingabe übergebenen Inhalt und erstellt einen bestimmten Anhang zu einem bestimmten Datensatz.

Die Aktivität **Inhalt in Datensatz als Anhang** schreiben kann mit jedem Workflow verwendet werden, um Inhalte zu schreiben und an einen Datensatz anzuhängen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld. |
| sysid [Zeichenfolge] | Der Systembezeichner (sys_id) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld. |
| Nutzlast | Der Nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld. |
| filename | Name der Anhangdatei. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob die Aktualisierung erfolgreich war. |

## Integration „Palo Alto Networks – WildFire“

Palo Alto Networks – WildFire ist eine cloudbasierte Anwendung, die mit der Firewall Ihres Systems interagiert.

**Erkunden**

Security Incident Response-Integrationen

**Einrichten**

Aktivieren Sie Security Operations Palo Alto Networks – WildFire

**Verwenden**

WildFire-Datenanreicherungs-Workflow abrufen

**Entwickeln**

- ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden

**Problembehandlung und Hilfe**

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Aktivieren Sie Security Operations Palo Alto Networks – WildFire

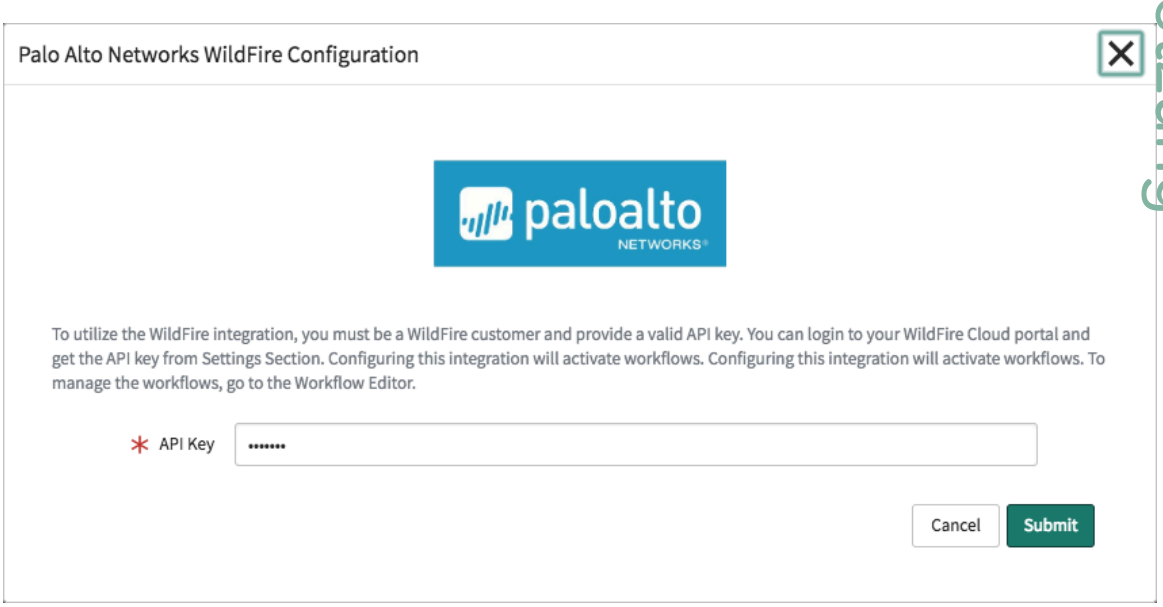
Bevor Sie die Integration von Security Operations Palo Alto Networks - WildFire verwenden können, müssen Sie die Integration aus dem ServiceNow Storeherunterladen.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.

3. Klicken Sie in der Karte Carbon Black auf **Konfigurieren**.




4. Geben Sie den API-Schlüssel ein, und klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integrationskonfigurationskarte wird angezeigt.

5. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

### WildFire-Datenanreicherungs-Workflow abrufen

Wenn der Workflow „ **Security Operations Palo Alto Networks – WildFire-Datenanreicherung** abrufen“ ausgeführt wird, wird eine Hash-Datei in WildFire hochgeladen. Die Daten werden angereichert, und Berichte werden in die Instanz heruntergeladen, um die Verarbeitung potenzieller Malware-Angriffe zu unterstützen.

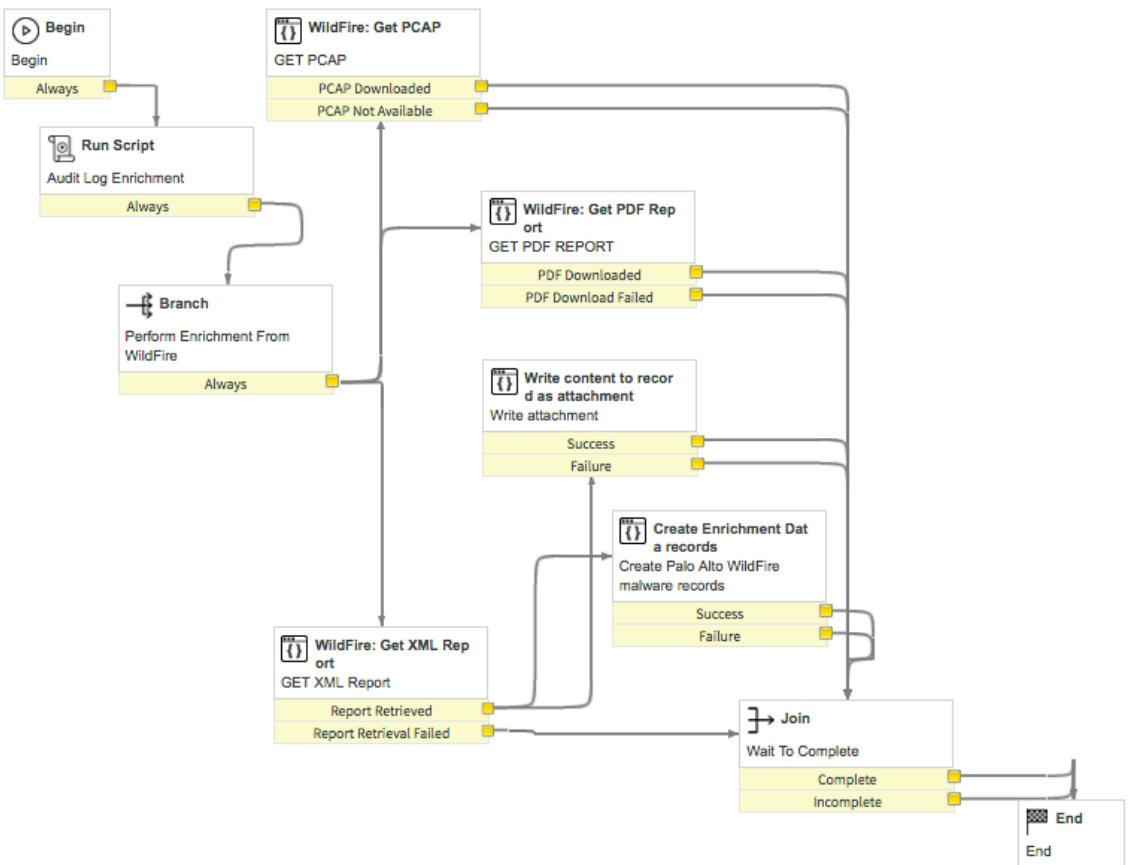
### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow „ **Security Operations Palo Alto Networks - WildFire Data Enrichment** abrufen“ wird ausgeführt, wenn ein Security Incident aus einer Warnung erstellt wird, die von der Anwendung Palo Alto Network Firewall empfangen wurde. Ein Malware-Hash aus der von der Firewall empfangenen E-Mail-Benachrichtigung wird auf der Registerkarte **„IoC** “ des Security Incident eingegeben, und der Datensatz wird aktualisiert.

#### Security Operations Palo Alto Networks – WildFire-Datenanreicherungs-Workflow abrufen




### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**.
2. Suchen und öffnen Sie anhand der von der Firewall erhaltenen E-Mail-Benachrichtigung den erstellten Security Incident.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Klicken** Sie auf die Registerkarte Gefährdungsindikatoren, und füllen Sie den **Malware-Hash** mit dem Hash aus, den Sie in der Warnung erhalten haben.
4. Klicken Sie auf **Aktualisieren**.
   Der Workflow bewirkt, dass die Hash-Datei in WildFire hochgeladen wird, wo die Daten angereichert werden. Berichte im PDF- und XML-Format werden an den Datensatz (Security Incident oder IoC) in Ihrer Instanz angehängt, um die Verarbeitung potenzieller Malware-Angriffe zu unterstützen.

**Hinweis:**
Wenn die angereicherten Daten Paketerfassungsinformationen enthalten, werden auch PCAP-Informationen heruntergeladen. PCAP-Daten erfassen, welche Aktionen die Datei ausgeführt hat. Beispielsweise kann gemeldet werden, welche Server die Datei kontaktiert hat. Zum Anzeigen von PCAP-Dateien benötigen Sie eine Paketanalyse, z. B. Wireshark .

**Beispiel-PDF, generiert von Wildfire**

## 1 File Information

| | |
|---|---|
| **File Type** | PE |
| **File Signer** | None |
| **SHA-256** | ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2 |
| **SHA-1** | 8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc |
| **MD5** | 26cafca052a58bebdeb976e8b9723152 |
| **File Size** | 55296bytes |
| **First Seen Timestamp** | 2016-05-04 17:53:43 UTC |
| **Verdict** | Malware |
| **Antivirus Coverage** | VirusTotal Information |

## 2 Static Analysis

### 2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Automatische Übersetzung

### WildFire: PCAP-Aktivität abrufen

Die Workflow-Aktivität **„WildFire: PCAP abrufen** “ ruft die Paketerfassungsinformationen (PCAP) ab, die während der Analyse eines angegebenen Datei-Hashs in WildFire generiert wurden. Das Ergebnis dieser Aktivität wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| FileSHA256Hash [Zeichenfolge] | Der Hash der Datei, der von der Anwendung Palo Alto Network Firewall empfangen wurde. |
| Tabellenname [Zeichenfolge] | Die betroffene Tabelle. |
| Datensatz-ID [Zeichenfolge] | Der Security Incident oder IoC, der aktualisiert wird. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| commandStatus [Boolean] | „True“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde. |
| errorMessage | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |

### WildFire: Aktivität „PDF-Bericht abrufen“.

Die Workflow-Aktivität **WildFire: PDF-Bericht** abrufen ruft den Bericht ab, der während der Analyse eines angegebenen Datei-Hashs in WildFire im PDF-Format generiert wurde. Das Ergebnis dieser Aktivität wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Die betroffene Tabelle. |
| FileSHA256Hash [Zeichenfolge] | Der Hash der Datei, der von der Anwendung Palo Alto Network Firewall empfangen wurde. |
| Datensatz-ID [Zeichenfolge] | Der Security Incident oder IoC, der aktualisiert wird. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| commandStatus [Boolean] | „True“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde. |
| errorMessage | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |

### WildFire – XML-Berichtsaktivität abrufen

Die Workflow-Aktivität **WildFire: XML-Bericht** abrufen ruft den Bericht ab, der während der Analyse eines angegebenen Datei-Hashs in WildFire im XML-Format generiert wurde. Das Ergebnis dieser Aktivität wird an einen bestimmten Datensatz angehängt, der durch **TableName** und **RecordId**identifiziert wird.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Die betroffene Tabelle. |
| FileSHA256Hash [Zeichenfolge] | Der Hash der Datei, der von der Anwendung Palo Alto Network Firewall empfangen wurde. |
| Datensatz-ID [Zeichenfolge] | Der Security Incident oder IoC, der aktualisiert wird. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| commandStatus [Boolean] | „True“, wenn ein Ergebnis abgerufen und erfolgreich angehängt wurde. |
| errorMessage | Der Fehler, der in der Aktivität aufgetreten ist, falls vorhanden. |

### Schreiben Sie Inhalte, die als Anhangsaktivität aufgezeichnet werden sollen

Diese Aktivität schreibt den aus einer Eingabe übergebenen Inhalt und erstellt einen bestimmten Anhang zu einem bestimmten Datensatz.

Die Aktivität **Inhalt in Datensatz als Anhang** schreiben kann mit jedem Workflow verwendet werden, um Inhalte zu schreiben und an einen Datensatz anzuhängen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld. |
| sysid [Zeichenfolge] | Der Systembezeichner (sys_id) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld. |
| Nutzlast | Der Nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld. |
| filename | Name der Anhangdatei. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob die Aktualisierung erfolgreich war. |

## Integration „Palo Alto Networks Next-Generation Firewall“

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe von EDL-Funktionen (External Dynamic List) mit den -Produkten ServiceNow Security Incident Response (SIR) zu blockieren. Der Security Incident-Analyst erstellt Einträge für eine EDL aus erkennbaren Elementen, die bei ServiceNow SIR Security Incidents als böswillig eingestuft wurden.

Eine EDL ist eine Textdatei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihre Now Platform -Instanz, die es Palo Alto Networks Next-Generation Firewall ermöglicht, Objekte zu importieren, die in der Liste enthalten sind, IP-Adressen, URLs und Domänen, und Richtlinien durchzusetzen.

Um eine Richtlinie für die EDL-Einträge durchzusetzen, wird die Liste in einer Richtlinienregel oder einem Profil referenziert. Wenn die EDL-Einträge geändert werden, importiert die Firewall die Liste dynamisch im konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit für die Firewall. Für diese Integration hat Now Platform eine Tabelle mit EDL-Einträgen erstellt, die von autorisierten Palo Alto Networks Next-Generation Firewallin den konfigurierten Abrufintervallen abgerufen werden.

Die Integration umfasst die folgenden Funktionen:

- Flexibilität beim Erstellen mehrerer EDLs, die für verschiedene Firewall-Verweigerungs- oder -Zulassungsrichtlinien gelten.
- Detaillierte Berichte über die Arten von Websites, die blockiert werden (Phishing, Malware und auf Allow-Listen aufgeführte Websites).
- Tagging von Now Platform Security Incidents mit EDL-Einträgen nach erkennbarem Typ (URL, Domäne, IP-Adresse).
- Konfigurieren von EDL-Ablaufzeiträumen, um die Größe der EDL-Liste beizubehalten, indem ältere Einträge automatisch ablaufen oder entfernt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Suchen, Löschen oder Migrieren von EDL-Einträgen zwischen EDL-Listen.
- Verknüpfen von EDL-Einträgen mit Datensätzen erkennbarer Elemente und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert wird.

Für die Integration müssen die Plugins „“ (com.snc.security_incident) und „“ (com.snc.secops.orchestration) aus dem Produkt Security Incident Response aktiviert werden.

Diese Integration unterstützt nur Palo Alto Networks (PAN-OS 8.x). Frühere Versionen werden nicht unterstützt.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von Now Platform®kompatibel.

**Hinweis:**
Die folgenden Themen sind nummeriert. Um eine reibungslose Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse zu gewährleisten, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

### Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-Generation Firewall

Für die Integration ist ein Zertifikatprofil erforderlich, um die sichere Verbindung zwischen dem Server Now Platform® und dem Server Palo Alto Networks Next-Generation Firewall zu validieren und zu authentifizieren.

#### Vorbereitungen
Erforderliche Rolle: Palo Alto Networks Next-Generation Firewall Administrator

#### Warum und wann dieser Vorgang ausgeführt wird
Ein Palo Alto Networks Next-Generation Firewall authentifiziert sich bei einer Now Platform® -Instanz, ruft EDL-Einträge aus der Datenbanktabelle ab und integriert die Einträge in die entsprechenden Firewall-Richtlinienregeln. Dieser Abruf erfordert die API-Benutzerkontorolle in der Instanz Now Platform®, die vom PAN-Firewall-Administrator für den Zugriff auf die API Now Platform® verwendet wird.

Der Palo Alto Networks Next-Generation Firewall -Administrator erstellt ein Zertifikatprofil in Palo Alto Networks. Dieses Zertifikat validiert und authentifiziert die sichere Verbindung zwischen dem Now Platform® -Server und dem Palo Alto Networks -Firewall-Server.

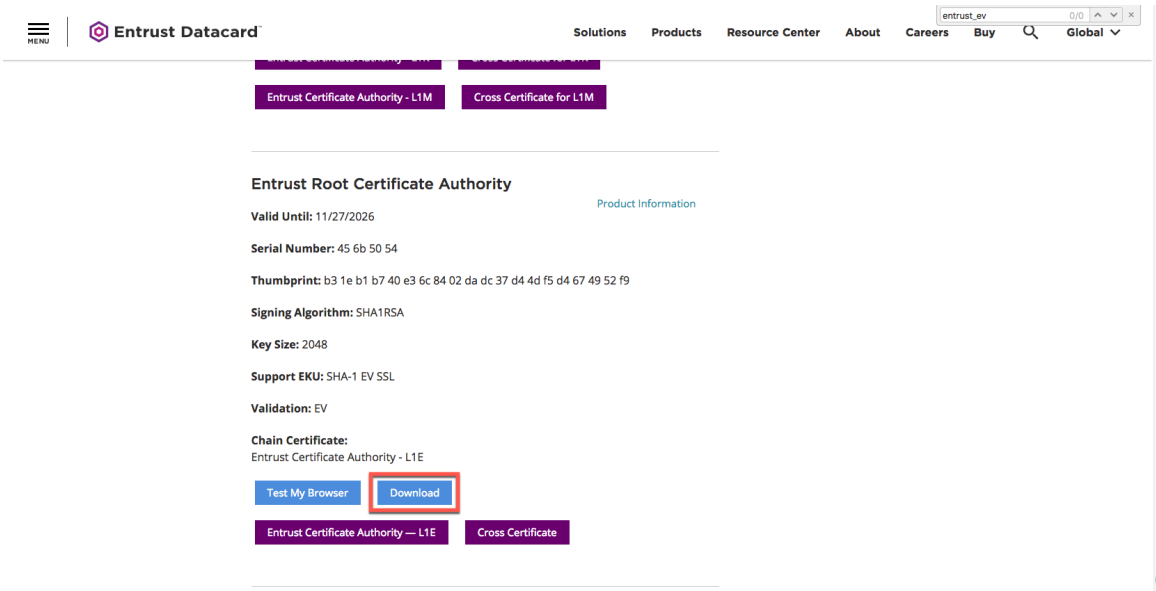
Now Platform® verwendet Entrust als Zertifizierungsstelle, und das erforderliche Zertifikatprofil wird mit dem Zertifikat `entrust_ev_ca.cer` erstellt. Dieses Zertifikat steht auf der EntrustData-Karte ™ -Website zum Download zur Verfügung. Um sicherzustellen, dass Sie die aktuellen Versionen erhalten, laden Sie diese Zertifikate direkt von der Entrust-Website herunter.

#### Prozedur

1. Navigieren Sie zu Stammzertifikate Download .
2. Scrollen Sie auf der Entrust-Website zum Zertifikat der Entrust- **Stammzertifizierungsstelle** (siehe folgende Abbildung).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie auf **Herunterladen**.
   Der Name der heruntergeladenen Datei lautet **entrust_ev_ca.cer**.
4. In der Dokumentation Palo Alto Networks erfahren Sie, wie Sie das Zertifikatprofil konfigurieren, nachdem Sie es heruntergeladen haben.
   Die Anforderungen finden Sie auf der Website Palo Alto Networks.

### Zugehörige Informationen

„Zertifikatprofil konfigurieren“ im Administratorleitfaden für PAN-OS 10.0

## Einrichten und installieren Palo Alto Networks Next-Generation Firewall

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation erforderlich.

### Vorbereitungen

Erforderliche Rolle: (admin)

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Ihnen die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen sind. | Die folgenden Rollen sind erforderlich:<br>• Der Systemadministrator (admin) installiert die App und weist die Rolle Security Incident Administrator (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und erstellt, aktiviert und entfernt EDLs. Diese Rolle weist auch die Rolle sn_si.analyst zu.<br>• Der (administrator) weist die API-Kontorolle Now Platform® (sn_sec_panfw.api_account_access) zu, die ausschließlich für die Eingabe von Anmeldeinformationen verwendet wird, |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | die für die Authentifizierung auf Palo Alto Networks erforderlich sind, damit die Firewalls EDLs von Now Platform® abrufen können.<br>• (sn_si.analyst) oder Security Operations Center (SOC)-Analyst erstellt EDL-Einträge und arbeitet mit Security Incidents. |
| Vergewissern Sie sich, dass Sie Palo Alto Networks Next-Generation Firewall Version-OS 9.x und 10.x verwenden. | Diese Integration unterstützt nur Palo Alto Networks Next-Generation Firewall OS 9.0 und höher. |
| Richten Sie alle EDL-Profile, Sicherheitsrichtlinienregeln und Zertifikatprofile in Palo Alto NetworksPalo Alto Networks ein , wie in der Dokumentation von [] empfohlen. | Weitere Informationen finden Sie in der allgemeinen Dokumentation und den Anforderungen von Palo Alto Networks auf der Palomarto Networks-Dokumentationswebsite . |
| Vergewissern Sie sich, dass Sie das Zertifikat der Entrust™ -Stammzertifizierungsstelle heruntergeladen und konfiguriert haben. | Für die Integration ist dieses Zertifikat erforderlich, um die sichere Verbindung zwischen dem Server Now Platform und dem Server Palo Alto Networks Next-Generation Firewall zu validieren und zu authentifizieren. Weitere Informationen zum Einrichten des Zertifikats finden Sie unter „Zertifikatprofil konfigurieren“ im Administratorleitfaden für PAN-OS 10.0 . Informationen zum Herunterladen finden Sie unter Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-Generation Firewall und Stammzertifikate herunterladen . |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Anforderungen für Madrid und spätere Releases<br><br>Für das Madrid-Release und spätere Familien-Releases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | **1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |
| Wenn Ihre Organisation über Now Platform® Change-Management- und Genehmigungsprozesse für die Löschung von E-Mails verfügt, stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails aktiviert ist. | Um zu überprüfen, ob die Funktion zum Senden/Empfangen von E-Mails in Ihrer Now Platform® -Instanz aktiviert ist, navigieren Sie zu **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**. Überprüfen Sie unter „Konfiguration ausgehender E-Mails“, ob E- **Mail-Senden** und **E-Mail-Empfangen** ausgewählt sind. |

### Prozedur

Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.

#### Erstellen Sie die API-Kontorolle für Palo Alto Networks Next-Generation Firewall

Für diese Integration ist in Ihrer Now Platform® -Instanz eine API-Kontorolle erforderlich. Der Benutzername und das Passwort, die diesem Konto zugeordnet sind, werden in Now Platform® erstellt und in Palo Alto Networks eingegeben, sodass sich Now Platform® beim Abrufen von EDL-Einträgen mit Palo Alto Networks Next-Generation Firewall authentifiziert.

### Vorbereitungen
Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird
Der Now Platform® -Administrator erstellt eine API-Kontorolle (sn_sec_panfw.api_account_access). Dieses Konto wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung bei Palo Alto Networks erforderlich sind, damit die Firewalls EDLs von Now Platform®abrufen können. Dieses Konto ist ein separates, eindeutiges API-Benutzerkonto in der Instanz Now Platform® und wird dem Administrator Palo Alto Networks Next-Generation Firewall zugewiesen.

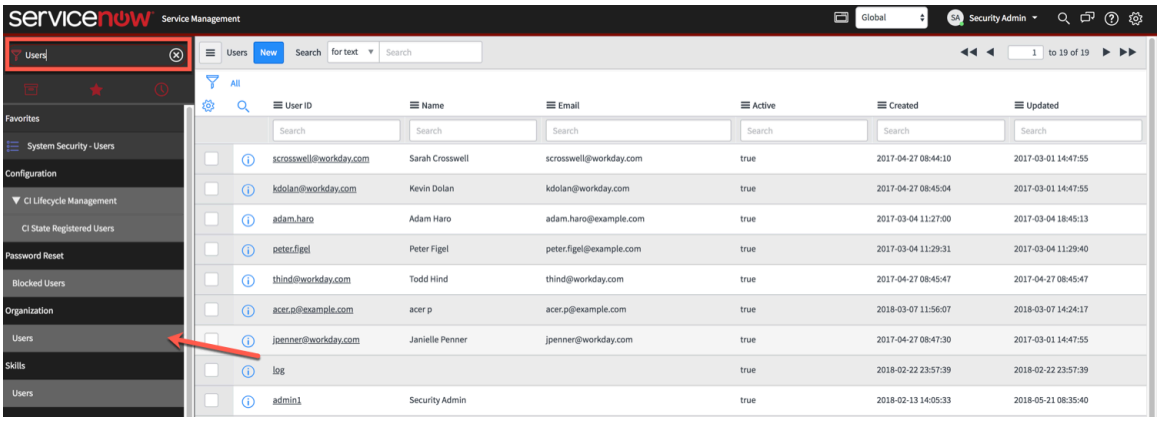
### Prozedur

**1.** Navigieren zu **Alle** > **Organisation** > **Benutzer**.

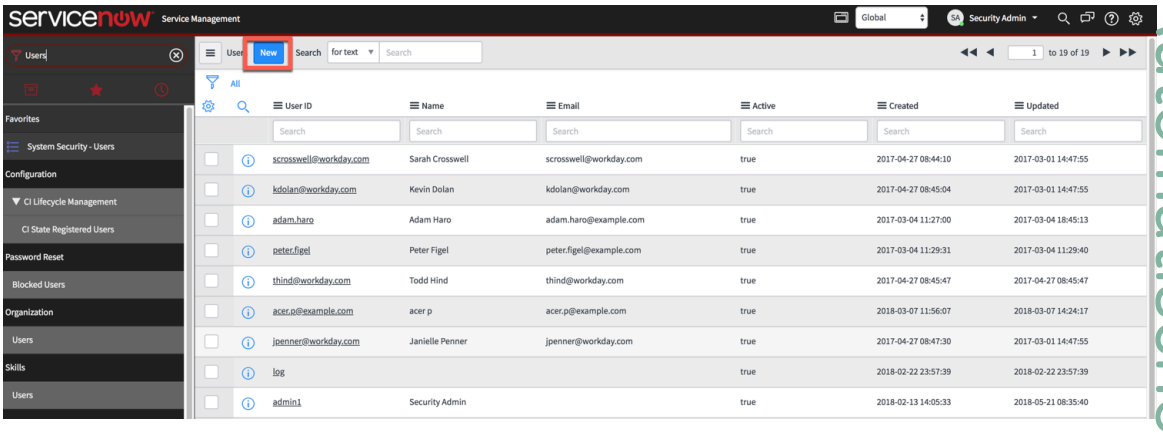
**2.** Klicken Sie auf das Modul **Benutzer**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**3.** Klicken Sie in der angezeigten Benutzerliste auf **Neu**.




Ein neues Benutzerformular wird angezeigt.

**4.** Füllen Sie das Formular aus.

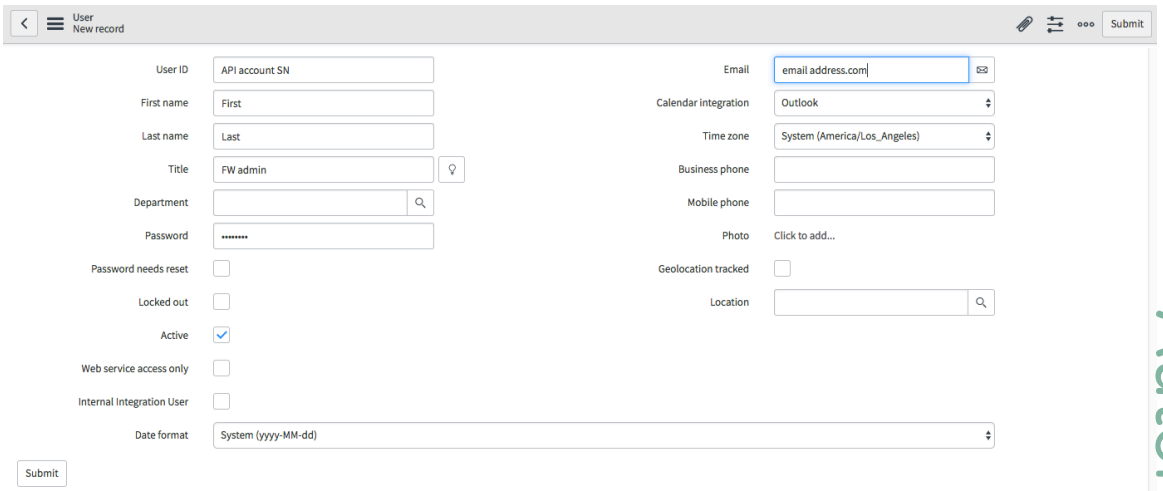
**Hinweis:**
Die Werte für Benutzer-ID-Titel und E-Mail-Adresse in der folgenden Tabelle und Abbildung sind Beispielwerte.

| Feld | Beschreibung |
|---|---|
| Anwender-ID | Eindeutige Benutzer-ID für die Rolle in Ihrer Now Platform® -Instanz. Diese Benutzer-ID wird in das Feld **Benutzername** im Abschnitt „ **Client-Authentifizierung** “ des Dialogfelds „Externe dynamische Listen“ auf der Website Palo Alto Networks eingegeben. Ein Beispiel ist das `API-Konto SN`. |
| Vorname | Person, die Sie zuweisen. |
| Nachname | Person, die Sie zuweisen. |
| Titel | Stellenbezeichnung, z. B. `FW`-Administrator. |
| Passwort | Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird in das Feld **Passwort** im Abschnitt „ **Client-Authentifizierung** “ des |

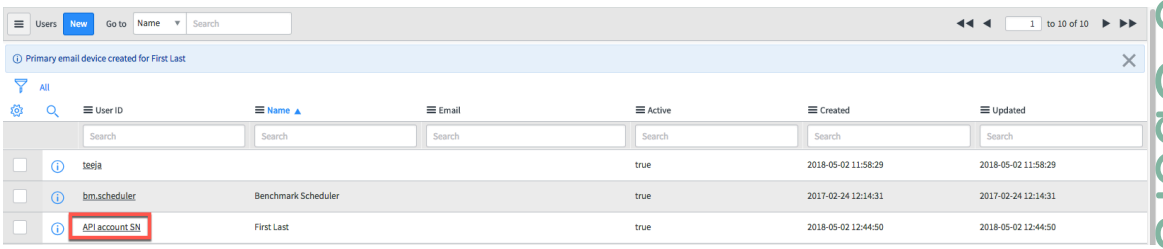
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

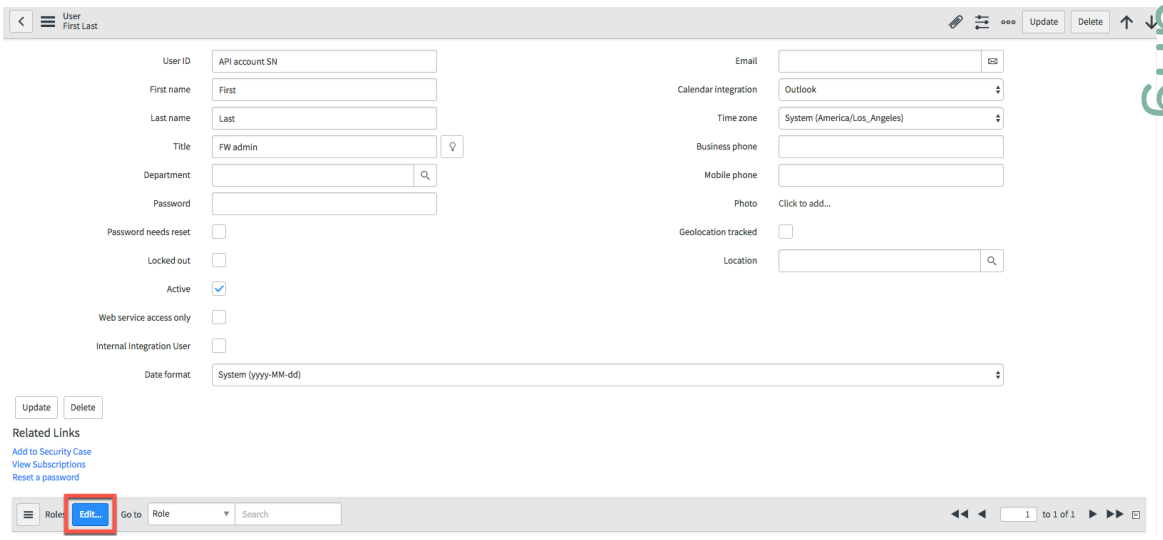
| Feld | Beschreibung |
| --- | --- |
| | Dialogfelds „Externe dynamische Listen“ auf der Website Palo Alto Networks eingegeben. |
| E-Mail | Eindeutige E-Mail-Adresse. |




5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. Klicken Sie in der Benutzerliste in der Spalte **Benutzer-ID** auf den Namen der von Ihnen eingegebenen Benutzer-ID, z. B. API-Konto SN.



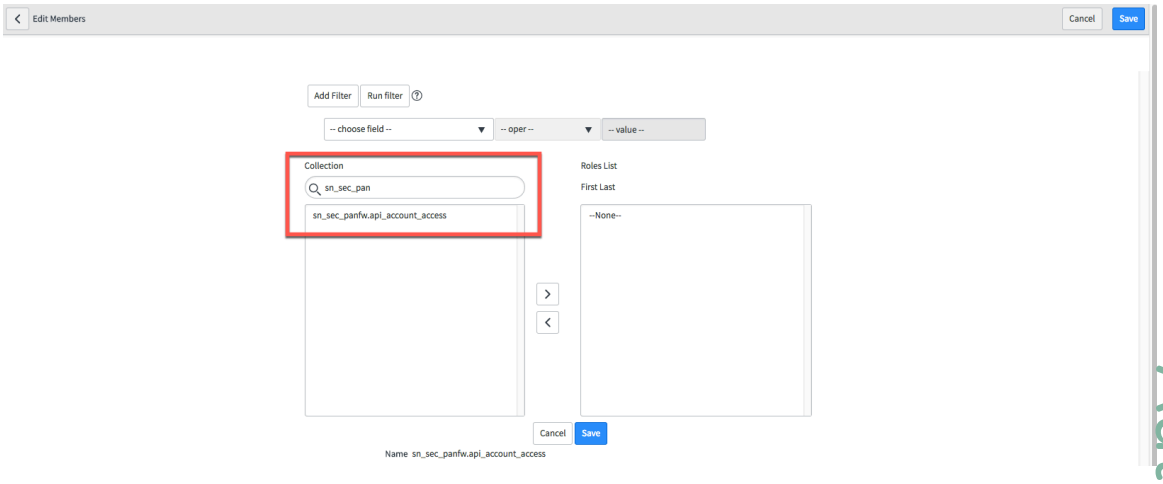

7. Klicken Sie im geöffneten Datensatz im Abschnitt „Rollen“ auf **Bearbeiten**.



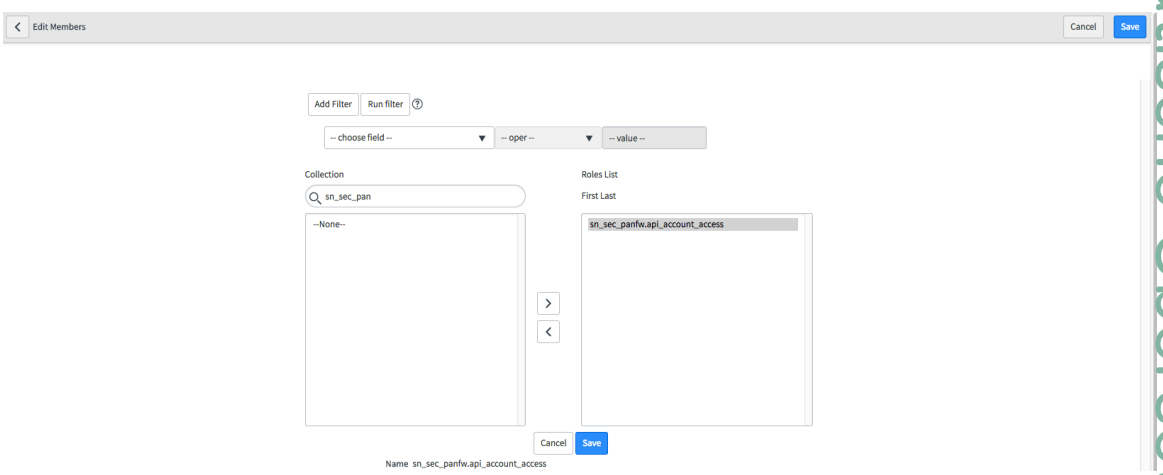

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Geben Sie im angezeigten Formular „ **Mitglieder bearbeiten**“ sn_sec_panfw.api_account_access in das Feld **Sammlung** ein.
   Unterhalb des Felds **Sammlung** wird die Rolle in der Spalte angezeigt.



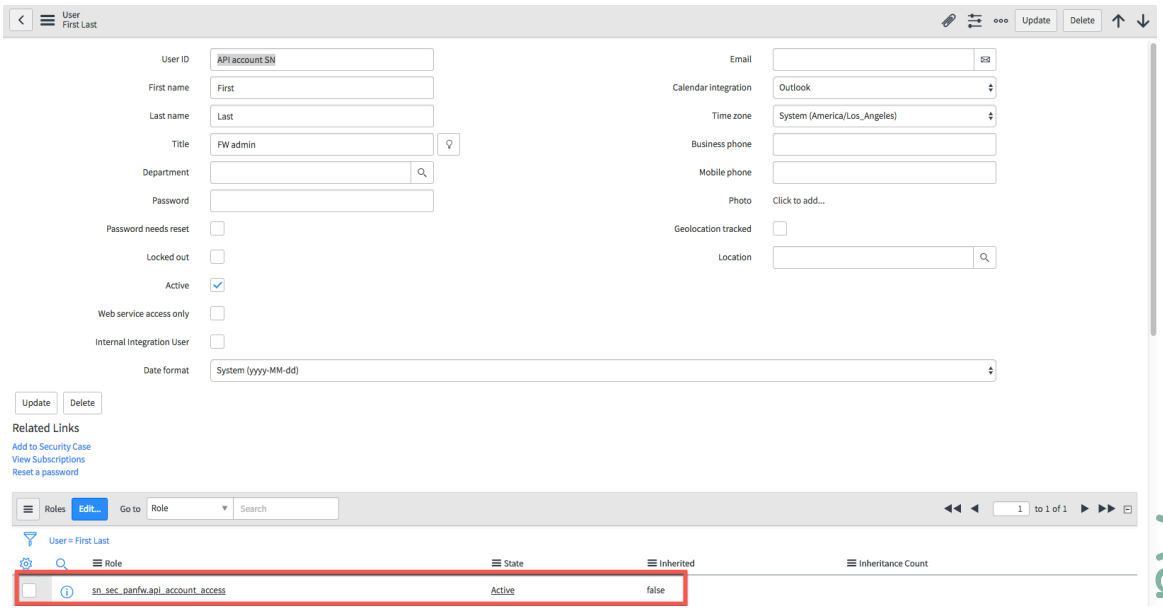

9. Wählen Sie in der Spalte **Sammlung** die Option sn_sec_panfw.api_account_access aus, und verschieben Sie sie in die **Rollenliste**.




10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Benutzer**, und klicken Sie in der Liste in der Spalte **Benutzer** auf den ID-Namen, den Sie für die Rolle erstellt haben (API-Konto SN).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der Benutzerdatensatz wird angezeigt. Dieser Datensatz überprüft, ob der Benutzeraccount zugewiesen wurde. Der **Status** ist aktiv, und die Rolle wird nicht geerbt.

### Unterstützte externe dynamische Listen für Palo Alto Networks Next-Generation Firewall

Die ServiceNow Palo Alto Networks Next-Generation Firewall -Integration unterstützt externe dynamische Listen (EDLs), die erkennbare IP-, URL- und Domänenelemente akzeptieren.

## Unterstützte EDLs und erkennbare Elemente

Eine *externe dynamische Liste* ist eine Textdatei, die auf einem externen *Webserver*gehostet wird, der für diese Integration die Instanz Now Platform ist. Der Palo Alto Networks Next-Generation Firewall kann dann Objekte (IP-Adressen, URLs, Domänen) importieren, die in der Liste enthalten sind, und Richtlinien erzwingen. Um eine Richtlinie für die EDL-Einträge durchzusetzen, wird die Liste in einer Richtlinienregel oder einem Profil referenziert.

Diese Integration unterstützt drei Arten von EDLs:

- IP (Dies umfasst eine einzelne IP-Adresse sowie CIDR-Blöcke (Bereiche) von Adressen.)
- URL
- Domäne

In der folgenden Tabelle sind Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ aufgeführt.

### Unterstützte erkennbare Elemente und Beispielformate

| Erkennbares Element | Beispielformate | Beschreibung |
|---|---|---|
| IP-Adresse | • 95.153.103.54 (IPv4)<br>• (IPv6): 2001:00B8:130F:FE03:0000:0900:980F:130B | Stellt eine einzelne, eindeutige Schnittstellenadresse dar.<br><br>Die Integration unterstützt die Formate IPv4, IPv6 und CIDR. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Unterstützte erkennbare Elemente und Beispielformate (Fortsetzung)**

| Erkennbares Element | Beispielformate | Beschreibung |
|---|---|---|
| | | Die Unterstützung für erkennbare IP-Adresselemente umfasst CIDR-Bereiche (Classless Inter-Domain Routing), z. B. 95.153.100.0/22.<br>Hinweis: Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs blockiert haben. Zum Beispiel ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs, der durch 95.153.100.0/22 (95.153.100.0-95.153.103.255) dargestellt wird. |
| URL | • www.example.com<br>• www.example.com/article.html<br>• beispiel.com<br>• *.example.com | Platzhalterzeichen werden unterstützt. Die Now Platform formatiert URL-Einträge neu, um die EDL-Formatanforderungen von Palo Alto Networks zu erfüllen. |
| Domäne | • www.example.com<br>• beispiel.com<br>• mail.example.com | Platzhalterzeichen werden nicht unterstützt. |

Weitere Informationen zu Formatierungsrichtlinien und EDLs finden Sie unter „Formatierungsrichtlinien für eine externe dynamische Liste“ im PAN-OS 10.0-Administratorhandbuch auf der Website Palo Alto Networks.

### Erstellen Sie eine EDL für Palo Alto Networks Next-Generation Firewall

Erstellen Sie eine externe dynamische Liste (EDL) in Ihrer Instanz Now Platform. Nach der Genehmigung und Aktivierung können Sie Einträge für EDLs aus erkennbaren Elementen erstellen, die bei Now Platform Security Incident Response (SIR)-Incidents als böswillig eingestuft wurden, und die Genehmigung anfordern, um sie zu blockieren.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die EDL in Ihrer Instanz Now Platform, damit die Firewall Objekte (IP-Adressen, URLs, Domänen) aus der Liste importieren und die Richtlinie erzwingen kann. Um eine Richtlinie für die EDL-Einträge durchzusetzen, wird die Liste in einer Richtlinienregel oder einem Profil referenziert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Abbildungen im folgenden Abschnitt werden mit in den Systemeinstellungen **deaktivierten Formularen** mit Registerkarten angezeigt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt „Formulare mit Registerkarten anzeigen“ in Configuring the form layout .

### Prozedur

1. Navigieren Sie nach Abschluss der Installation der Anwendung zu **Integrationen** > **Integrationskonfigurationen**.
2. Suchen Sie die Kachel Palo Alto Networks Next-Generation Firewall, und klicken Sie auf **Konfigurieren**.

3. Klicken **Sie auf Neue EDL-Liste erstellen**.

4. Füllen Sie die Felder des Formulars aus.

**Palo Alto Networks Formular „Externe dynamische Firewall-Liste“**

| Feld | Beschreibung |
|---|---|
| **Name** | Palo Alto Networks Name der dynamischen Firewall-Liste |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Fügen Sie den erkennbaren Typ (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalyst die Absicht der EDL leicht anhand ihres Namens erkennen kann. Der Name sollte auch eindeutig angeben, welcher Firewall-Richtlinie diese EDL-Objekte zugeordnet sind. Einige Beispiele für EDL-Namen sind „Ausgehende Malware-IP“ oder „Ausgehende Phishing-URL“. |
| **Aktiv** | Diese Checkbox ist standardmäßig deaktiviert, um anzuzeigen, dass die EDL inaktiv ist.<br><br>Wenn sie inaktiv ist, kann die EDL keine zusätzlichen Einträge erhalten.<br><br>Wenn das Kontrollkästchen aktiviert ist, ist die EDL aktiviert und für EDL-Einträge verfügbar. |
| **Tag anzeigen** | Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element auf einer EDL blockiert ist. Wenn diese Option ausgewählt ist, sind die Felder Tag-Typ und EDL-Tag für erkennbare Elemente im Formular verfügbar.<br><br>**Hinweis:**<br>Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie in das Feld **Name** mit einem *EDL*-Präfix eingegeben haben, z. B. EDL-Malware OutBound IP. Sie können den Tag-Namen und die Farbe ändern. Weitere Informationen finden Sie unter: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall. Der Tag-Name wird im Feld EDL-Tag für erkennbare Elemente angezeigt, sobald die EDL gespeichert wurde.<br><br>Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und die Felder Tag-Typ und EDL-Tag für erkennbare Elemente sind im Formular nicht verfügbar. |
| **Erkennbarer Typ** | Wählen Sie einen erkennbaren Typ aus der Auswahlliste aus, den diese EDL akzeptiert: IP (einschließlich CIDR), URL oder Domäne. |
| **Tag-Typ** | Tags, die in der Auswahlliste verfügbar sind. |



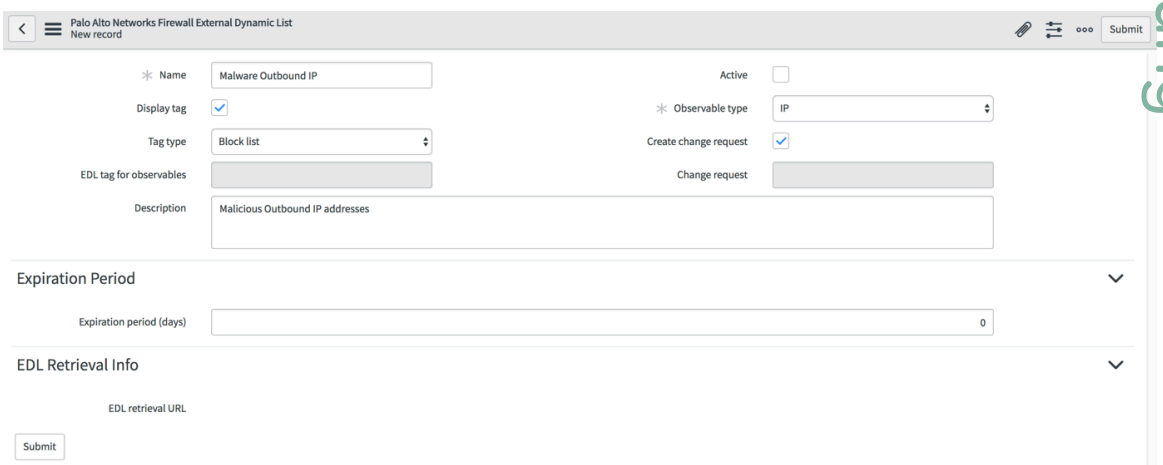
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Eine Sperrliste ist eine Liste der erkennbaren Elemente, die Palo Alto Networks Next-Generation Firewall blockieren soll.<br><br>Eine Allow-Liste ist eine Liste der erkennbaren Elemente, die Palo Alto Networks Next-Generation Firewall zulassen soll.<br><br>Standardmäßig ist die Farbe des Sperrlisten-Tags schwarz und die Farbe des Allow-Listen-Tags grau. Sie können die Farbe ändern. Weitere Informationen finden Sie unter: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall. |
| **Change-Anforderungen erstellen** | Diese Checkbox ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in Ihrer Now Platform -Instanz zu erstellen, die an den EDL-Datensatz angehängt sind.<br><br>Die Change-Anforderung wird verwendet, um die EDL-Listenabruf-URL auf dem Server Palo Alto Networks Next-Generation Firewall zu konfigurieren.<br><br>Diese Option wird empfohlen, wenn Ihr Firewall-Administrator Now Platform auch für Änderungen an Firewall-Richtlinien oder -Regeln verwendet. Wenn Sie eine Anforderung erstellen, wird die EDL-Liste automatisch aktiviert, nachdem sie geschlossen wurde.<br><br>Deaktivieren Sie die Checkbox, um die EDL manuell zu aktivieren, nachdem Sie per E-Mail vom Firewall-Administrator benachrichtigt wurden, dass die Konfiguration auf Palo Alto Networks abgeschlossen ist.<br><br>Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar. |
| **EDL-Tag für erkennbare Elemente** | Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tag anzeigen aktiviert ist. Das Feld wird automatisch ausgefüllt, nachdem die EDL mit einem Standardwert aus dem Feld Name gespeichert wurde.<br><br>Weitere Informationen zum Ändern des Standard-Tag-Namens und der Standardfarbe finden Sie unter (Optional) |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall |
| **Change-Anforderung** | Wenn das Kontrollkästchen Change Request erstellen aktiviert ist, wird die Change Request-Nummer in der Instanz Now Platform angezeigt, sobald die EDL gespeichert ist.<br><br>Wenn das Kontrollkästchen Change Request erstellen deaktiviert ist, wird dieses Feld nicht angezeigt. |
| **Beschreibung** | Beschreibung der dynamischen Palo Alto Networks-Firewall-Liste. Der Name enthält im Allgemeinen die Arten von Sites und erkennbaren Elementen, die Sie in dieser EDL erwarten würden. Sie können dieses Feld für weitere Details verwenden. |
| **Ablaufzeitraum (in Tagen)** | Ablaufzeitraum der EDL.<br><br>0 (Standard) gibt an, dass der EDL-Eintrag nie abläuft.<br><br>Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Es gibt keinen Höchstwert.<br><br>Wenn Sie beispielsweise 30 Tage am 1. Mai um 14:01 Uhr eingeben, läuft die EDL am 31. Mai um 14:01 Uhr ab.<br><br>Alle Einträge in dieser EDL erben dann diesen Wert standardmäßig, es sei denn, Sie überschreiben den Wert für einzelne Einträge. |

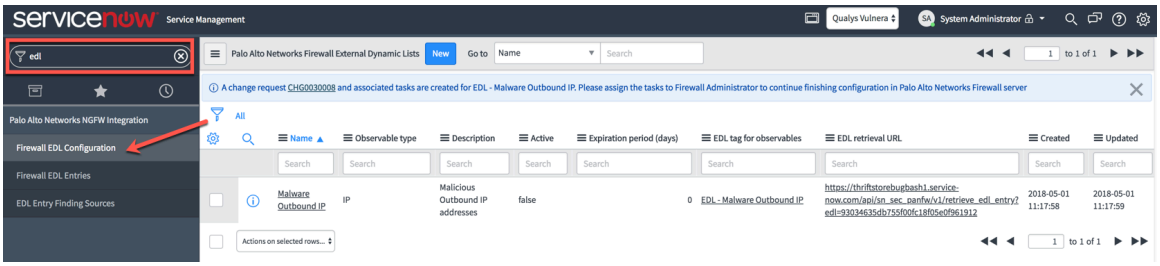



**5.** Klicken Sie auf **Absenden**.

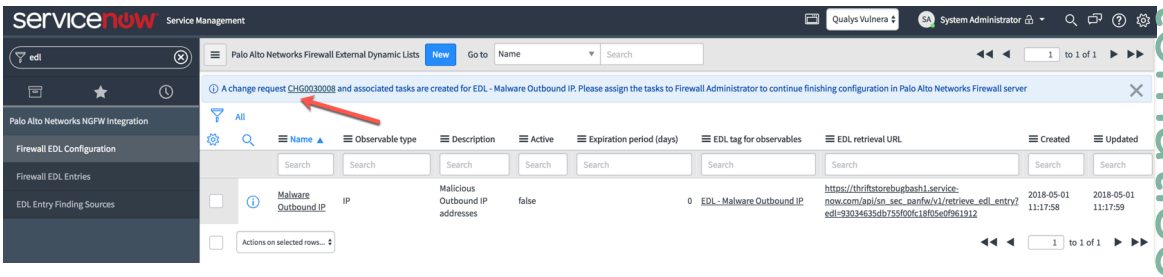
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

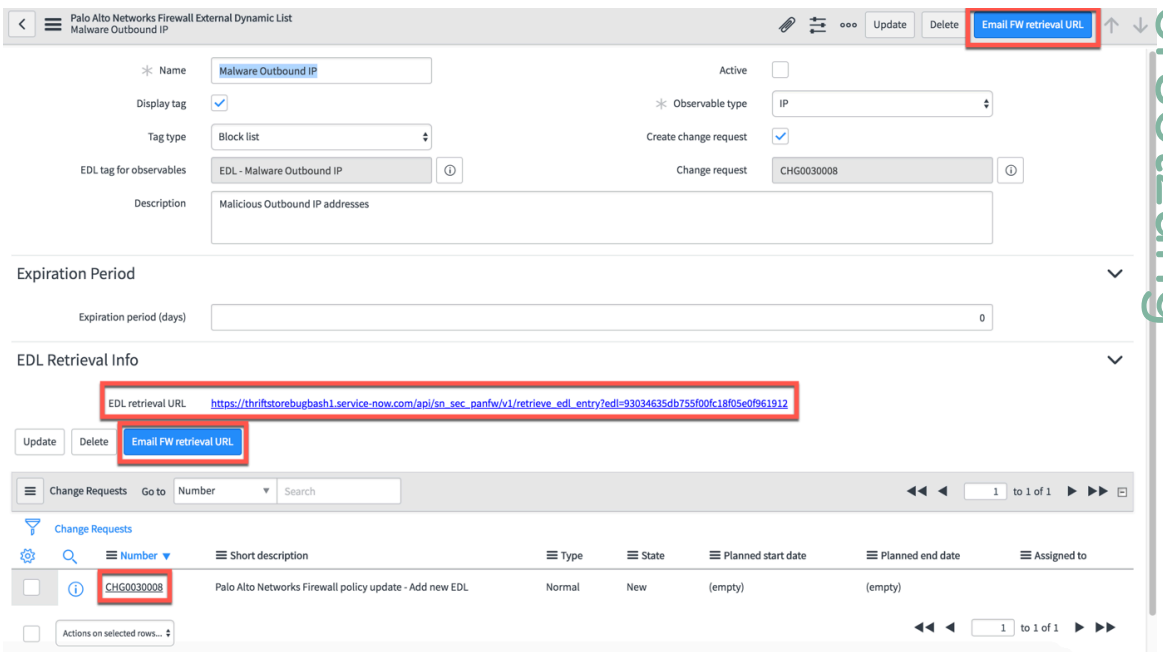
6. Wenn die Liste der externen dynamischen Listen der Palo Alto Networks-Firewall nicht angezeigt wird, navigieren Sie zu **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration** und klicken Sie auf **EDL-Firewall-Konfiguration**.




Die neue EDL wird angezeigt. Der EDL-Status ist noch inaktiv (false), was bedeutet, dass die EDL keine Einträge annehmen kann. Wenn **Change-Anforderung erstellen** konfiguriert wurde, wird eine Nachricht angezeigt, die angibt, dass eine Change-Anforderung und Aufgaben in Ihrer Now Platform -Instanz erstellt wurden.




7. Klicken Sie in der Spalte **Name** auf ein Element, um den Datensatz zu öffnen.
Der EDL-Datensatz wird angezeigt. Dieses Beispiel zeigt eine ausgehende Malware-IP-EDL. Die folgenden Felder, Optionen und Links werden im neuen Datensatz nach der Übermittlung angezeigt und in der folgenden Tabelle beschrieben.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Abruf-URL und Change-Anforderungs-Links im EDL-Datensatz**

| Option | Beschreibung |
|---|---|
| **Abruf-URL für E-Mail-Weiterleitung** | Sendet eine Benachrichtigung per E-Mail, dass der EDL-Link für die Konfiguration für den Firewall-Administrator Palo Alto Networks verfügbar ist. |
| EDL-Abruf-URL | Diese URL wird im Authentifizierungsdialogfeld für externe dynamische Listen auf der Registerkarte **Liste erstellen** auf der Website Palo Alto Networks im Feld **Quelle** platziert.<br><br>Der URL-Link, den der Firewall-Administrator Palo Alto Networks für die Konfiguration in der Firewall Palo Alto Networks verwendet, wird automatisch generiert und angezeigt.<br><br>**Hinweis:**<br>Wenn Sie Ihre Systemeinstellungen auf **Formulare**mit Registerkarten festgelegt haben, wird dieser Link auf der Registerkarte **EDL-Abrufinformationen** am Ende des Datensatzes angezeigt. |
| Now Platform Change-Anforderung | Ein Link zum Change-Anforderungsdatensatz wird im Abschnitt „Change-Anforderungen“ angezeigt, sofern konfiguriert, und die Anforderungsnummer wird im Feld Change-Anforderung angezeigt. |
| **Aktualisieren** | Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder. |
| **Löschen** | Löschen Sie den Datensatz. |

8. Erstellen und fügen Sie nach Bedarf weitere EDLs hinzu.
   Die EDLs werden in der Liste Palo Alto Networks Externe dynamische Listen angezeigt.

### Nächste Maßnahme
Aktivieren Sie eine EDL manuell oder mit einer Now Platform Change-Anforderung.

### Aktivieren Sie eine EDL für Palo Alto Networks Next-Generation Firewall

Nachdem die externe dynamische Liste (EDL) in Now Platform® erstellt wurde und die URL verfügbar ist, konfiguriert der Firewall-Administrator Palo Alto Networks die EDL in Palo Alto Networks Next-Generation Firewall. Die Abruf-URL wird vom Firewall-Administrator Palo Alto Networks verwendet, um die EDL auf dem Server Palo Alto Networks Next-Generation Firewall ] zu konfigurieren. Bevor EDL-Einträge akzeptiert werden können, muss die EDL in [] konfiguriert und in Palo Alto NetworksNow Platform®aktiviert werden.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Nachdem die EDL konfiguriert wurde, können Sie als Security Incident-Administrator die EDL manuell aktivieren, oder die EDL wird nach Abschluss einer Now Platform® Change-Anforderung automatisch aktiviert.

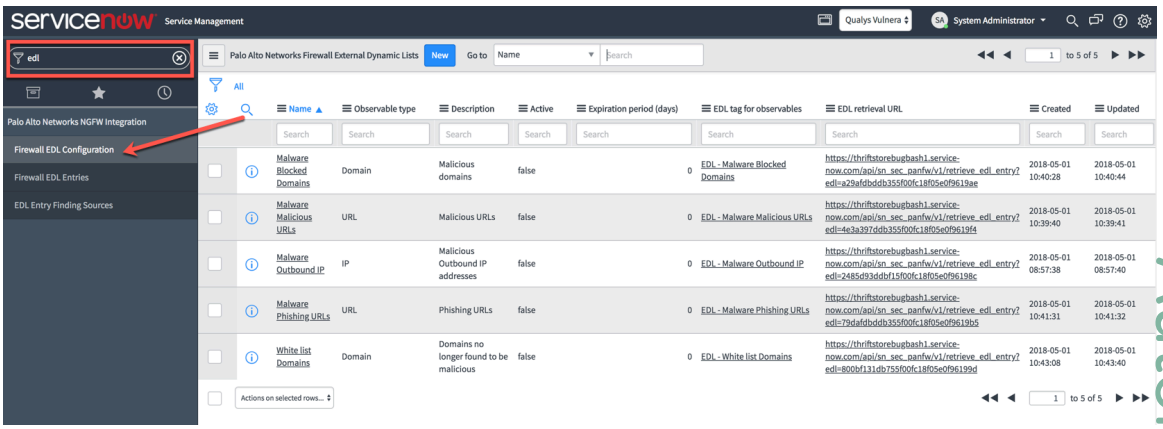


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die EDL muss genehmigt und vom inaktiven Status in den aktiven Status verschoben werden, bevor sie EDL-Einträge akzeptieren kann.

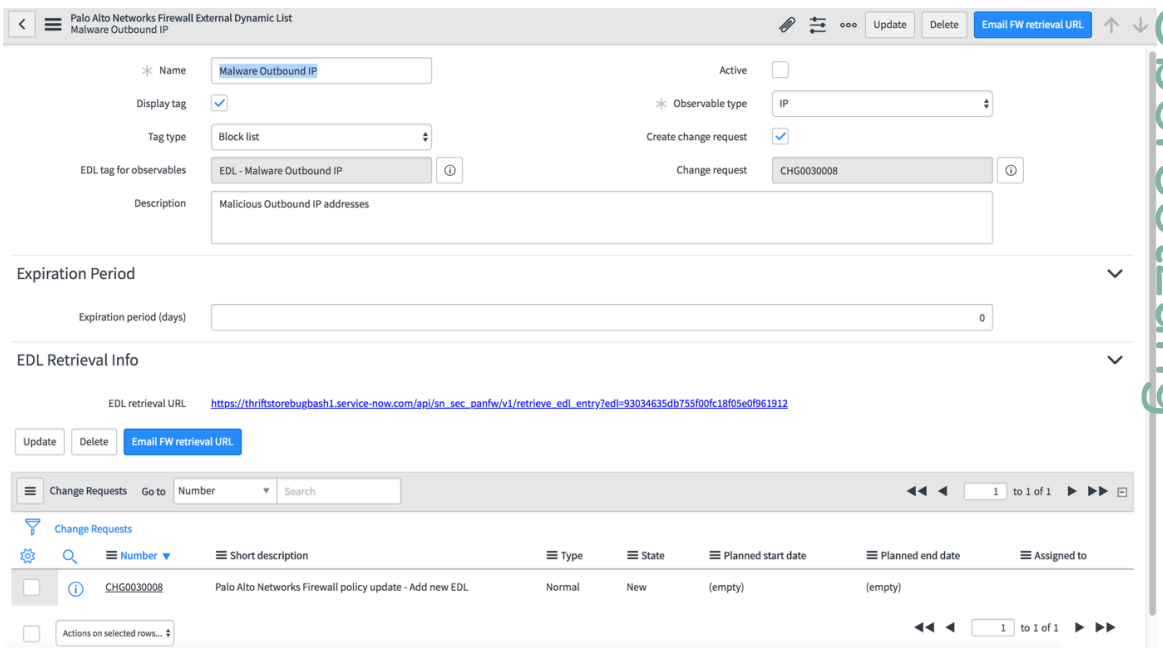
## Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration** und wählen Sie das Modul **„Firewall EDL-Konfiguration** “ aus.




2. Wählen Sie in der angezeigten Liste „Dynamische Listen der Palo Alto Networks-Firewall“ Ihre neue EDL in der Spalte Name aus.

3. Beachten Sie im angezeigten Datensatz die Schaltflächen „ **Email FW-Abruf-URL** “, den aktiven Link „EDL-Abruf-URL“ und, falls konfiguriert, die Change-Anforderung Now Platform® im Abschnitt „Change-Anforderungen“.
Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** deaktiviert ist.




### Hinweis:

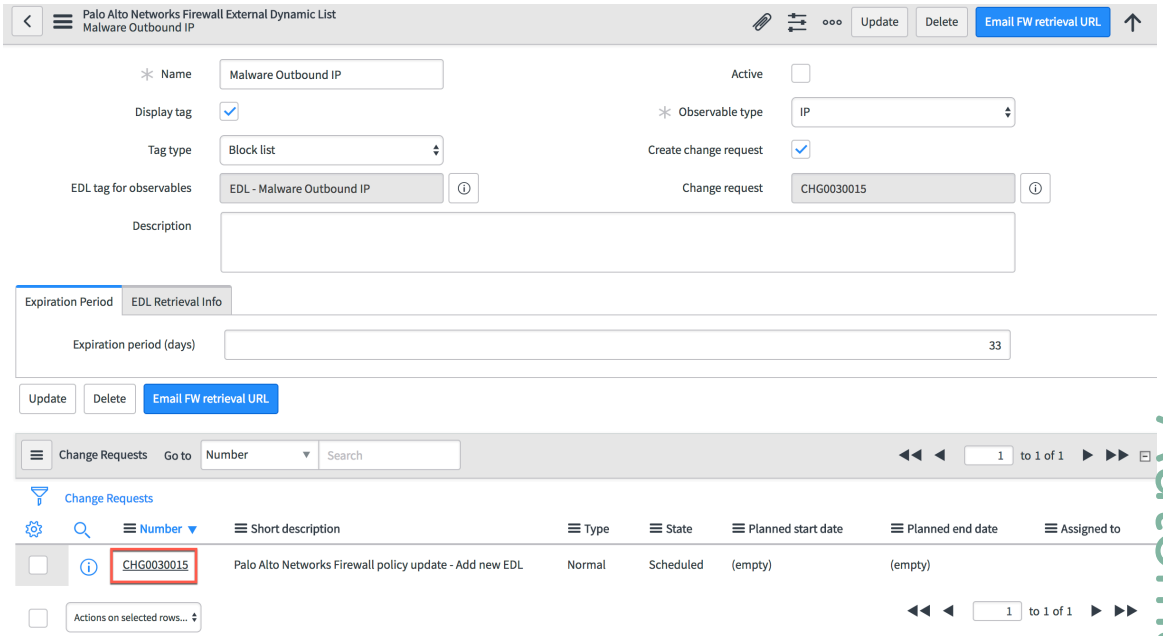
**Wenn Formulare** mit Registerkarten in Ihren Systemeinstellungen deaktiviert sind, wird die EDL-Abruf-URL im Abschnitt **EDL-Abrufinformationen** angezeigt, wie in der vorherigen Abbildung dargestellt.

Die folgende Abbildung zeigt die **EDL-Abrufinformationen** als Registerkarte mit **Formularen** mit Registerkarten, die in Ihren Systemeinstellungen ausgewählt sind. Klicken

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie auf die Registerkarte **EDL-Abrufinformationen**, um die Abruf-URL anzuzeigen. Der Link zum Change Request (**CH0030015**) wird ebenfalls angezeigt.




4. Um die Konfiguration abzuschließen und die EDL von inaktiv in aktiv zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator zu benachrichtigen, dass die Abruf-URL verfügbar ist.
   Nachdem Sie den Firewall-Administrator benachrichtigt haben, dass die Abruf-URL verfügbar ist, und sich vergewissern, dass die EDL in Palo Alto Networkskonfiguriert wurde, müssen Sie als Security Incident-Administrator die EDL aktivieren. Sie aktivieren die EDL entweder manuell oder verwenden, falls konfiguriert, das Change Request-Formular Now Platform, um die EDL zu aktivieren.

### Zugehörige Informationen

Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall

## Aktivieren Sie eine EDL manuell für Palo Alto Networks Next-Generation Firewall

Wenn der Palo Alto Networks-Firewall-Administrator Now Platformnicht verwendet und Sie direkt benachrichtigt werden, dass Palo Alto Networks Next-Generation Firewall konfiguriert ist, können Sie die externe dynamische Liste (EDL) manuell aktivieren.

### Vorbereitungen

Weisen Sie in Palo Alto Networksder von Ihnen erstellten EDL ein EDL-Objekt, eine Richtlinie und die Quell-URL zu. Weitere Informationen zum Konfigurieren der EDL für Palo Alto Networks Next-Generation Firewall in Palo Alto Networksfinden Sie unter Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall.

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

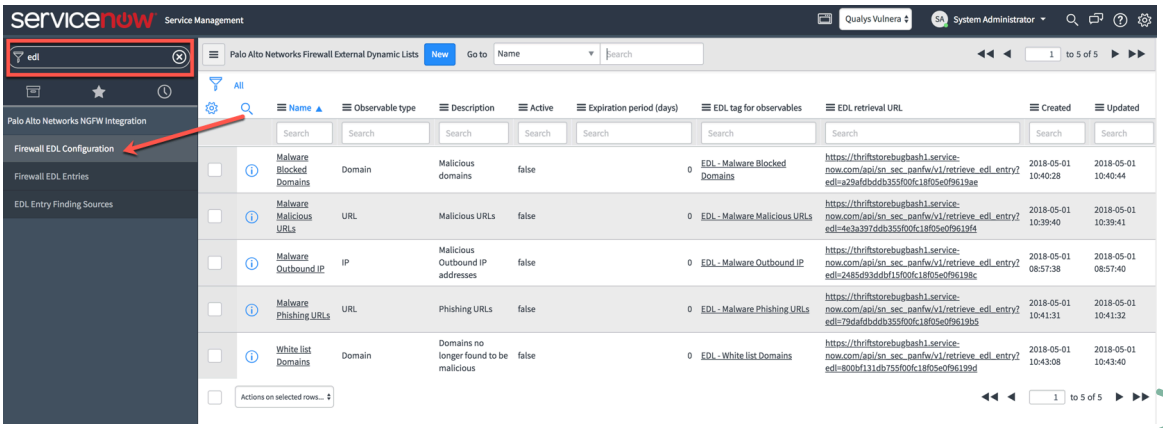
Als Now Platform Security Incident-Administrator werden Sie vom Palo Alto Networks -Firewall-Administrator benachrichtigt, wenn die EDL-Konfiguration in Palo Alto Networks Next-Generation Firewallabgeschlossen ist.

Automatische Übersetzung

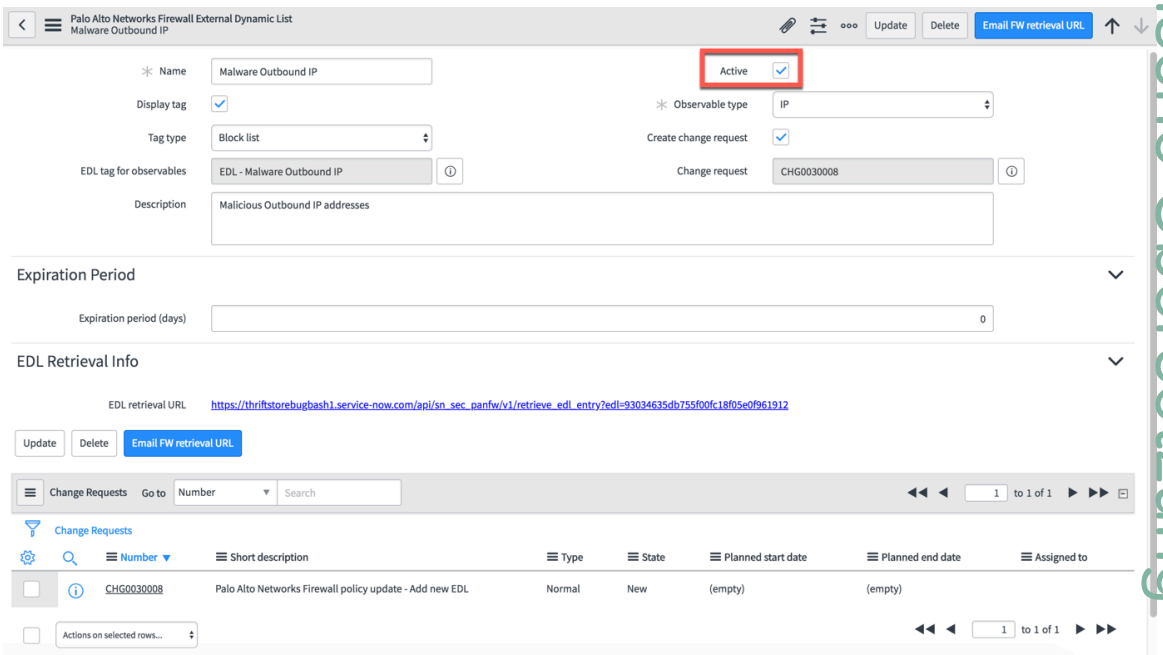
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration**.




2. Wählen Sie das Modul **Firewall EDL-Konfiguration** aus.
3. Klicken Sie in der Liste „Palo Alto Networks-Firewall der externen dynamischen Listen“ auf ein Element in der Spalte **Name**, um sie zu öffnen.
4. Aktivieren Sie im Datensatz, der geöffnet wird, das Kontrollkästchen **Aktiv**.

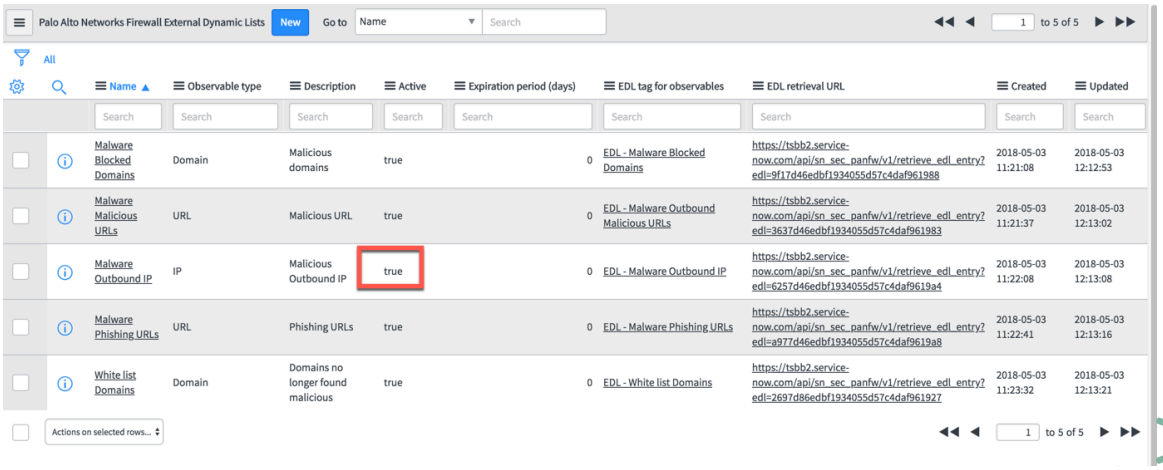



5. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Spalte **Aktiv** der Liste der externen dynamischen Listen der Palo Alto Networks-Firewall wird true für den Status der EDL angezeigt.




## Ergebnisse

Die EDL ist aktiviert und bereit zum Empfangen von EDL-Einträgen

## Nächste Maßnahme

Senden Sie EDL-Einträge aus einem Security Incident oder aus der Sperrliste.

### Konfigurieren Sie eine EDL in Palo Alto Networks Next-Generation Firewall

Der Palo Alto Networks -Firewall-Administrator konfiguriert eine EDL für den Palo Alto Networks Next-Generation Firewall, sobald er benachrichtigt wird, dass die Abruf-URL von Now Platformverfügbar ist. Bevor die EDL EDL-Einträge akzeptieren kann, muss sie in [] konfiguriert und in Palo Alto NetworksNow Platform®aktiviert werden.

## Vorbereitungen

Erforderliche Rolle: Palo Alto Networks Firewall-Administrator

## Warum und wann dieser Vorgang ausgeführt wird

Der Palo Alto Networks Next-Generation Firewall -Administrator erstellt ein EDL-Objekt und weist der EDL die Quell-URL (Abruf) und die Richtlinie zu. Diese Aufgaben werden in Palo Alto Networks ausgeführt, bevor die EDL in Now Platform] aktiviert wird.

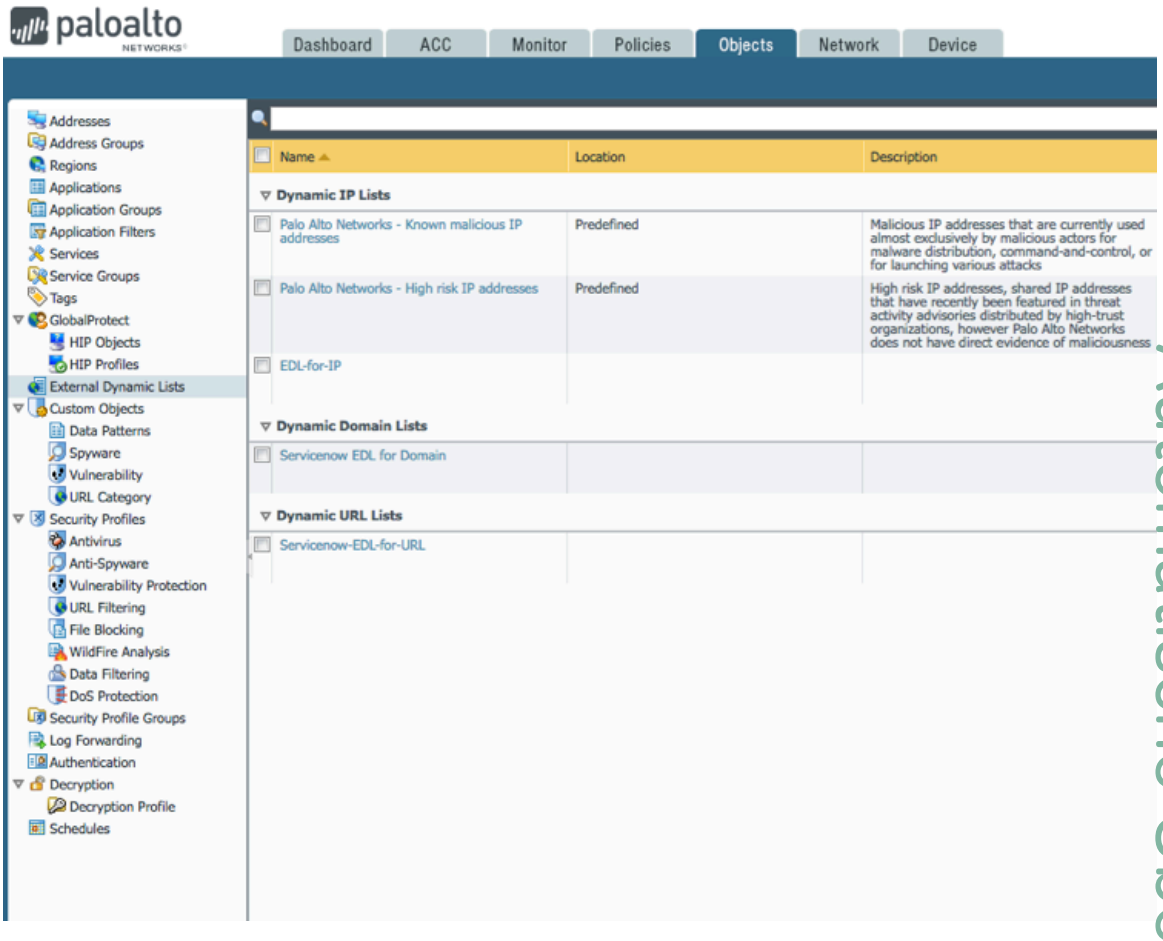
Die Images im folgenden Abschnitt werden mit Erlaubnis verwendet und sind PRIVILEGED und PROPRIETÄR.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

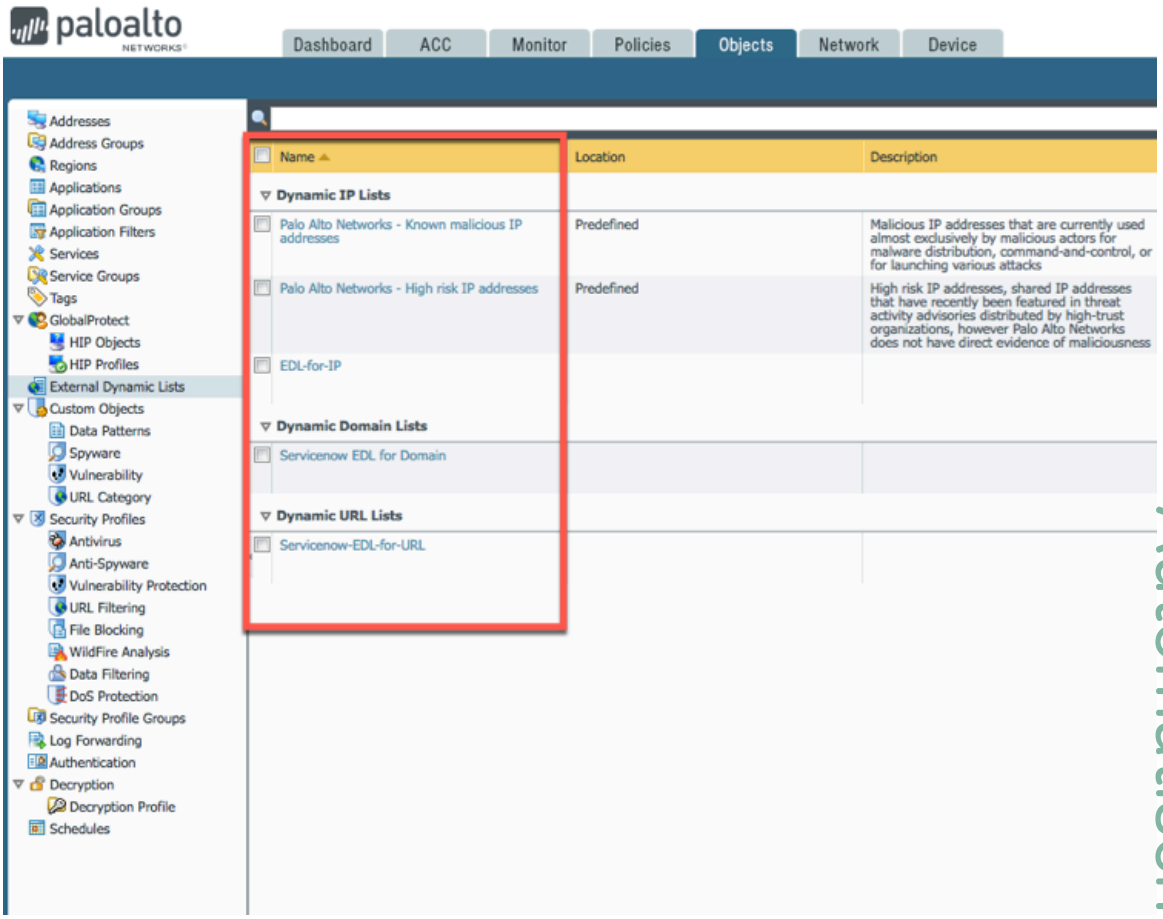
1. Wenn Sie die EDL nicht für die Firewall konfiguriert haben, navigieren Sie zu **Externe dynamische Listen** > **Objekte** in Palo Alto Networks.




2. Wählen Sie in der Spalte **Name** die ServiceNow EDL aus, die Sie konfigurieren möchten, z. B. **ServiceNow EDL für URL**.

Automatische Übersetzung

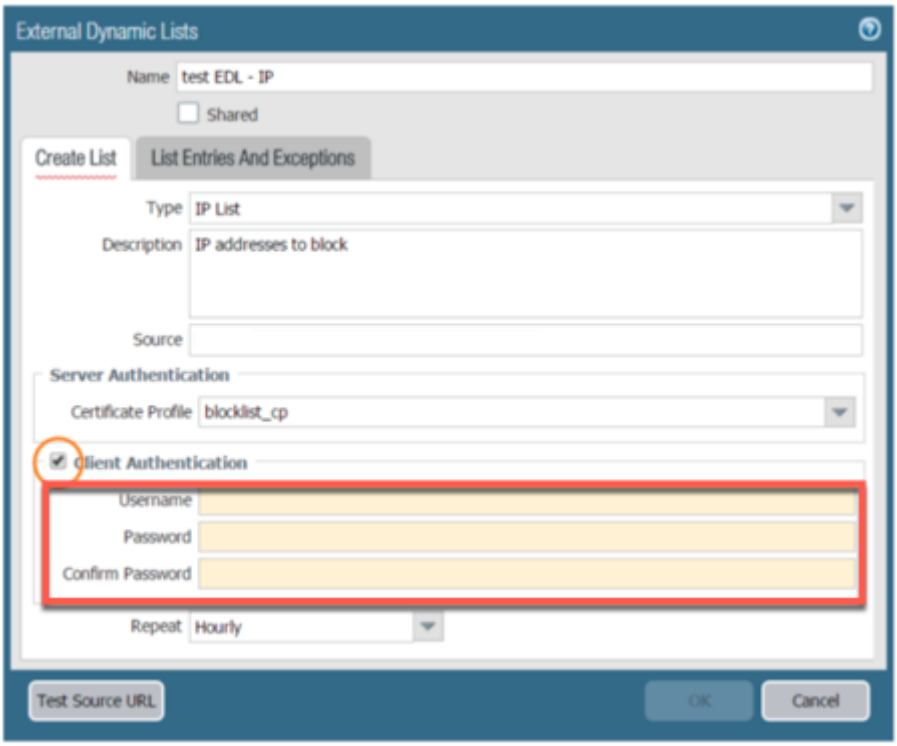
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



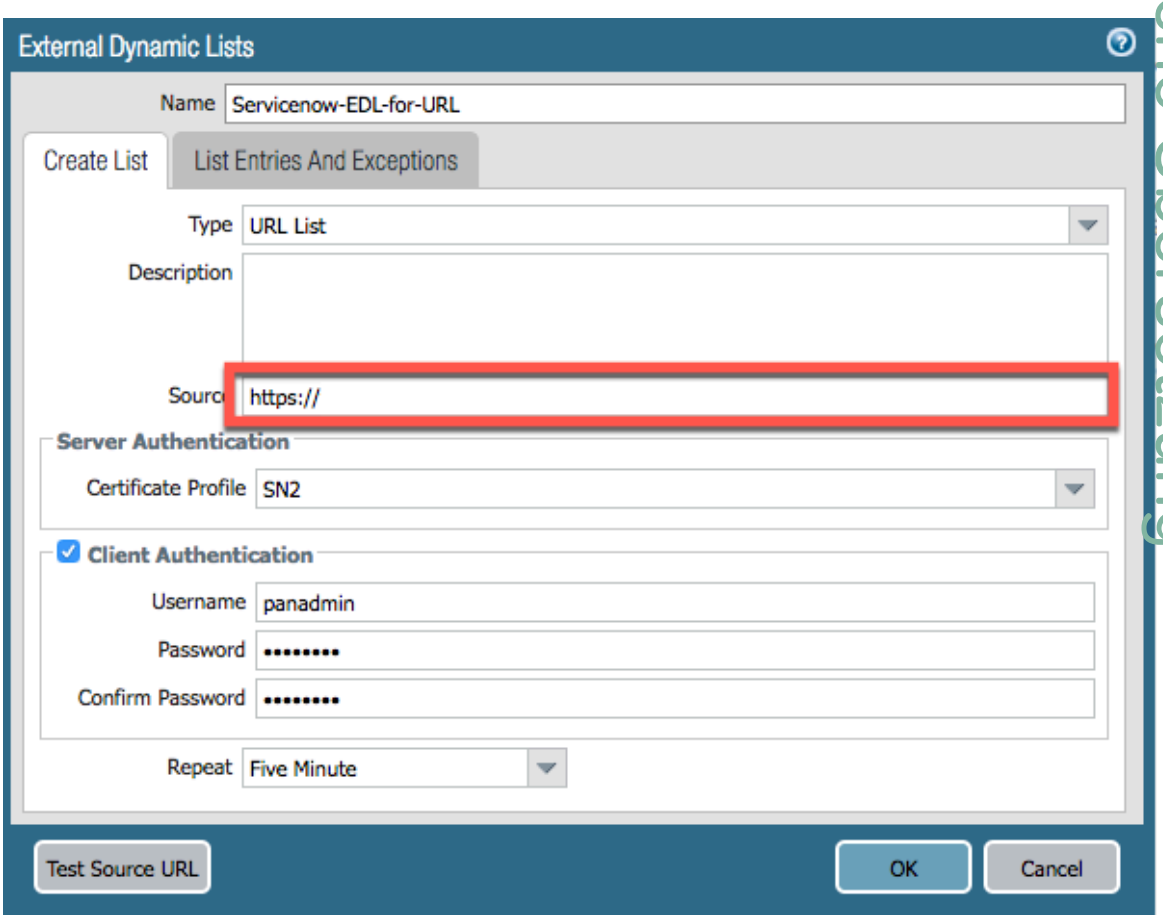

**3.** Geben Sie im Dialogfeld „Externe dynamische Listen“ den Benutzernamen und das Passwort ein, um sich mit dem Now Platform®zu authentifizieren.
Diese Anmeldeinformationen sind der Benutzername und das Passwort, die Sie für die API-Kontorolle (sn_sec_panfw.api_account_access) in Ihrer Instanz ServiceNow erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Geben Sie im Feld Quelle die URL ein, die in der EDL-Liste in Ihrer Instanz ServiceNow generiert wurde.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**5.** Wählen Sie ein Zertifikatprofil aus der Auswahlliste aus, z. B. SN2.

**6.** Klicken Sie auf OK.

### Aktivieren Sie eine EDL für Palo Alto Networks Next-Generation Firewall mit einer Change-Anforderung

Wenn konfiguriert, wird das Change Request-Formular ServiceNow verwendet, um die externe dynamische Liste (EDL) zu aktivieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator Now Platform auch für Änderungen an Firewall-Richtlinien oder -Regeln verwendet. Die EDL wird automatisch aktiviert und ist bereit zum Empfangen von EDL-Einträgen, wenn die Change-Anforderung Now Platform geschlossen wird.

#### Vorbereitungen

**Hinweis:**

Die Abbildungen im folgenden Abschnitt werden mit in den Systemeinstellungen ausgewählten **Formularen** mit Registerkarten angezeigt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt „Formulare mit Registerkarten anzeigen“ in Formularlayout konfigurieren auf der ServiceNow-Website mit Produktdokumentation .

Erforderliche Rolle: sn_si.admin für die Genehmigung der Change-Anforderung und der Change-Aufgaben

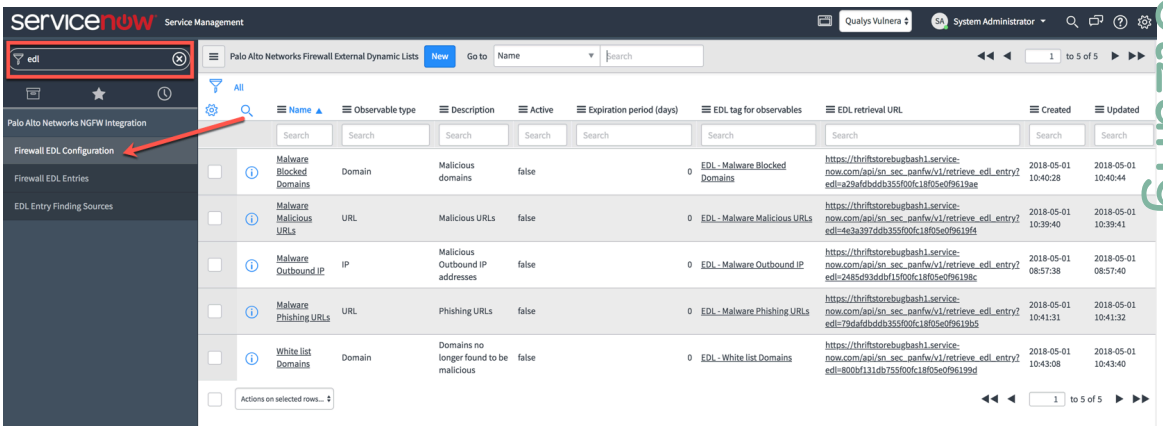
Palo Alto Networks Firewall-Administrator zum Abschließen von Konfigurationsaufgaben in Palo Alto Networks

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn konfiguriert, überwachen Sie Ihre Change-Anforderung Now Platform, und weisen Sie alle Aufgaben zu, die zur Konfiguration von Palo Alto Networks Next-Generation Firewallerforderlich sind. Schließen Sie nach Abschluss dieser Aufgaben die Change-Anforderung Now Platform, um die EDL automatisch zu aktivieren.

#### Prozedur

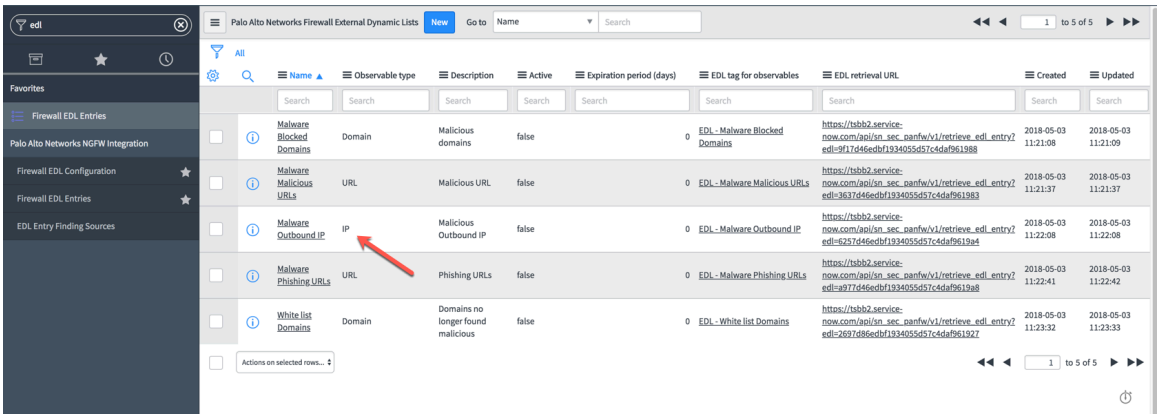
**1.** Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration**.



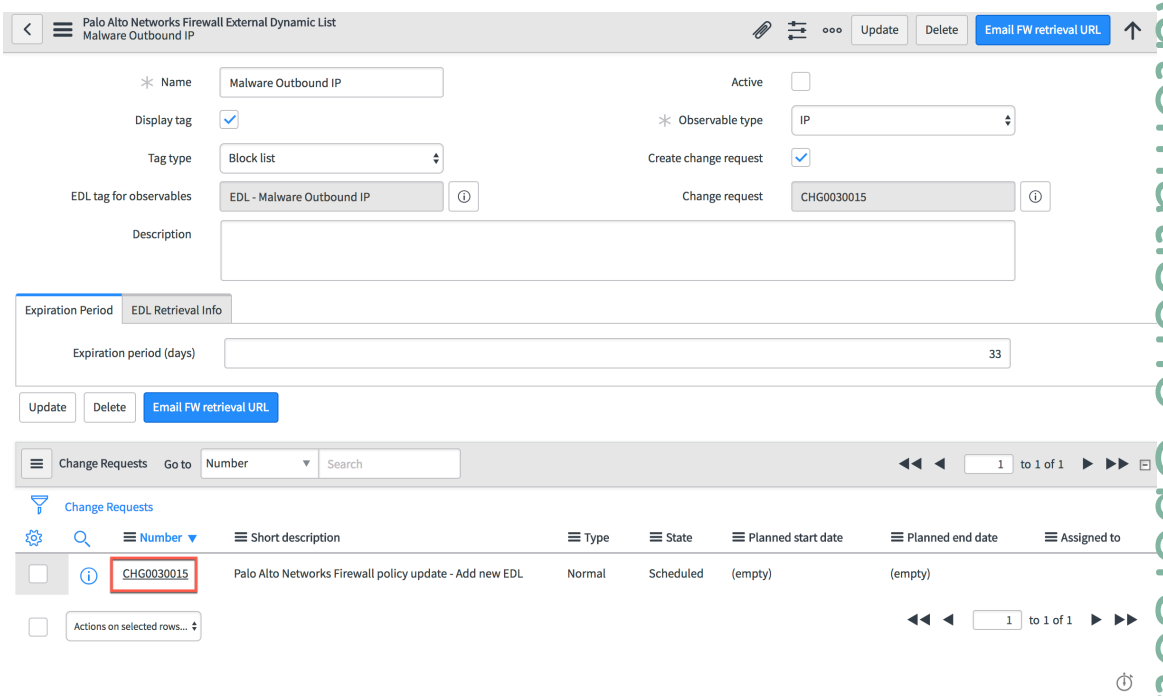

**2.** Wählen Sie das EDL-Modul aus, und klicken Sie in der Spalte **Name** auf eine EDL.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



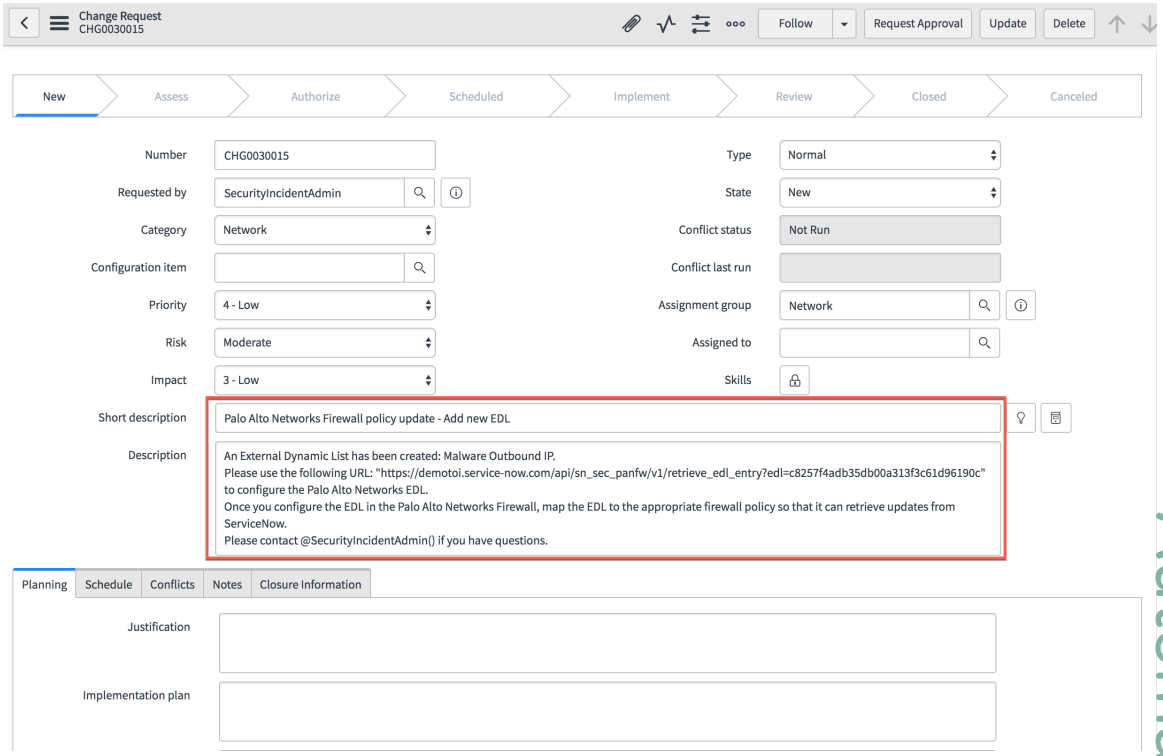

**3.** Klicken Sie im geöffneten EDL-Datensatz in der zugehörigen Liste „Change-Anforderungen“ auf die Nummer der Change-Anforderung.



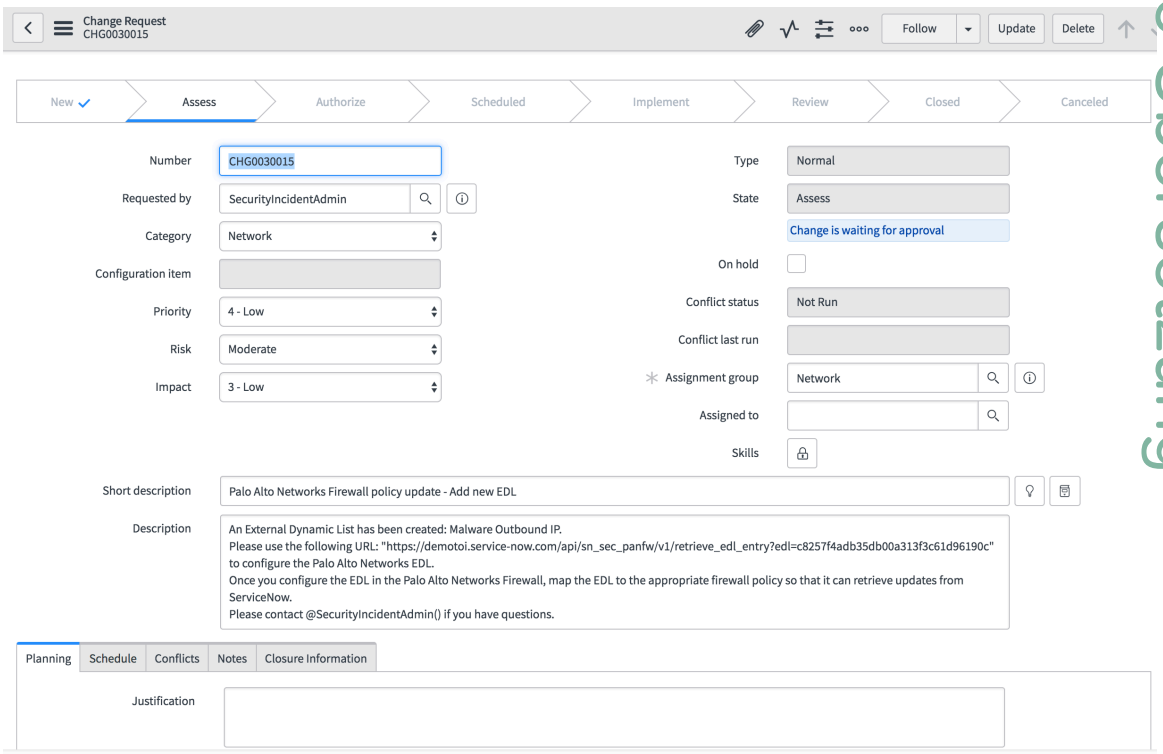

Der Change Request-Datensatz wird angezeigt. Im Feld **Beschreibung** wird die Abruf-URL aufgelistet, die zum Konfigurieren der Palo Alto Networks EDL verwendet wird. Details zur Zuordnung der EDL zur entsprechenden Palo Alto Networks Next-Generation Firewall -Richtlinie sind ebenfalls enthalten. Im Feld **Kurzbeschreibung**gibt ein Kommentar an, dass eine Anforderung zum Hinzufügen einer neuen EDL vorliegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**4.** Klicken Sie in der oberen rechten Ecke des Datensatzes auf **Genehmigung anfordern**.
Der Status ändert sich in Bewerten, und eine Meldung wird angezeigt, dass die Change-Anforderung auf Genehmigung wartet.

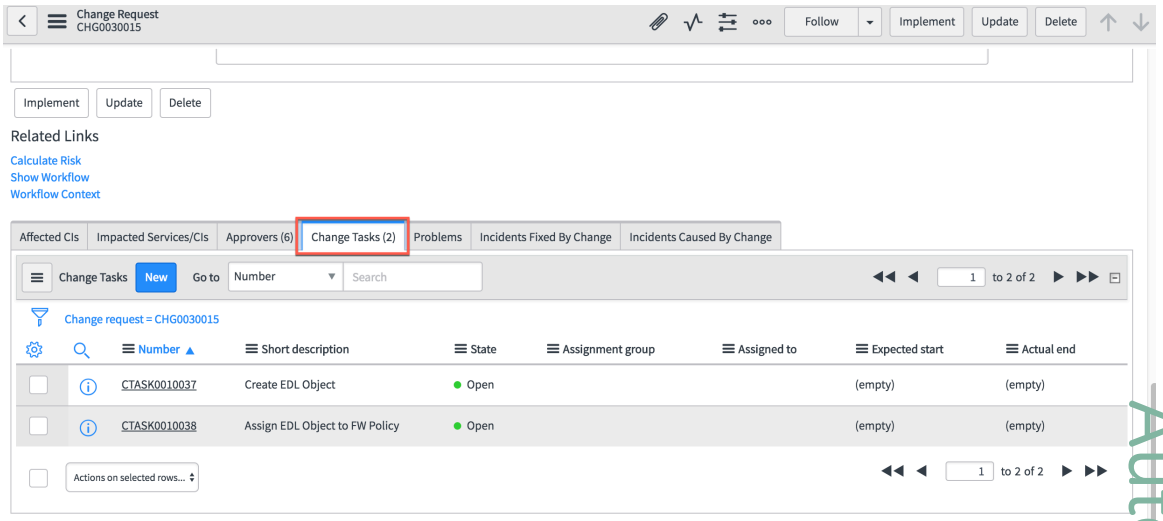



**5.** Um die Change-Anforderung abzuschließen und die EDL zu aktivieren, führen Sie die Schritte zum Zuweisen der Aufgaben aus und schließen die Change-Anforderung.

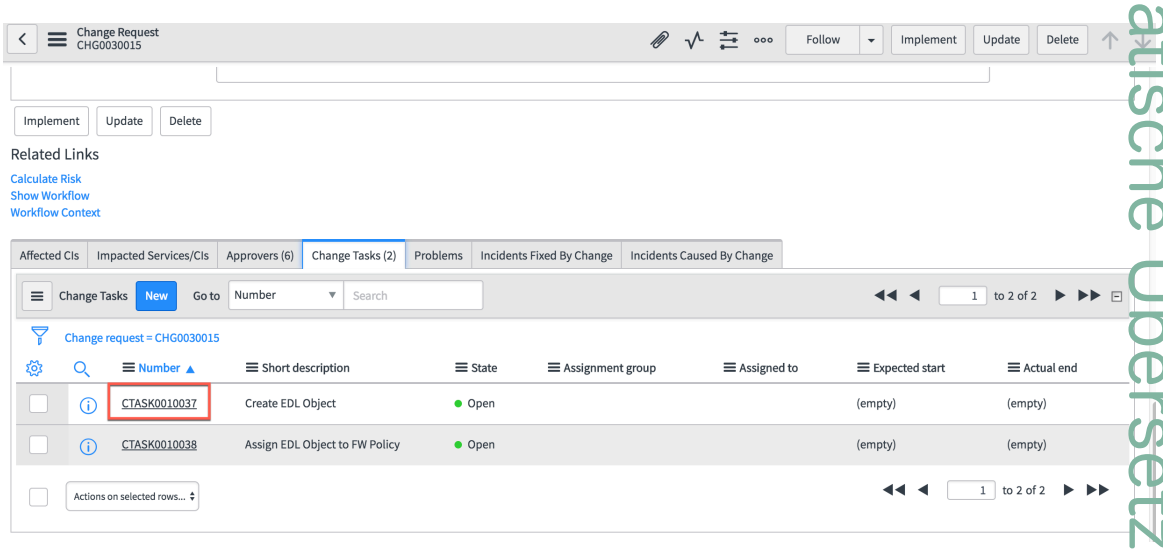
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wenn dies nicht angezeigt wird, öffnen Sie den Change Request, und wählen Sie die Registerkarte **Change-Aufgaben** aus.




**b.** Klicken Sie auf die Aufgabe, die der Erstellung des EDL-Objekts zugeordnet ist, um sie zu öffnen.




**c.** Weisen Sie im angezeigten Datensatz die Aufgabe dem Firewall-Administrator Palo Alto Networks zu, und klicken Sie auf **Aktualisieren**.
Der Firewall-Administrator wird benachrichtigt und erstellt das EDL-Objekt in Palo Alto Networks Next-Generation Firewall.

Um das EDL-Objekt zu erstellen, wird die Abruf-URL Now Platform ] in Palo Alto Networks unter kopiert **Externe dynamische Listen** > **Erstellen Sie Listen** > **Quelle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

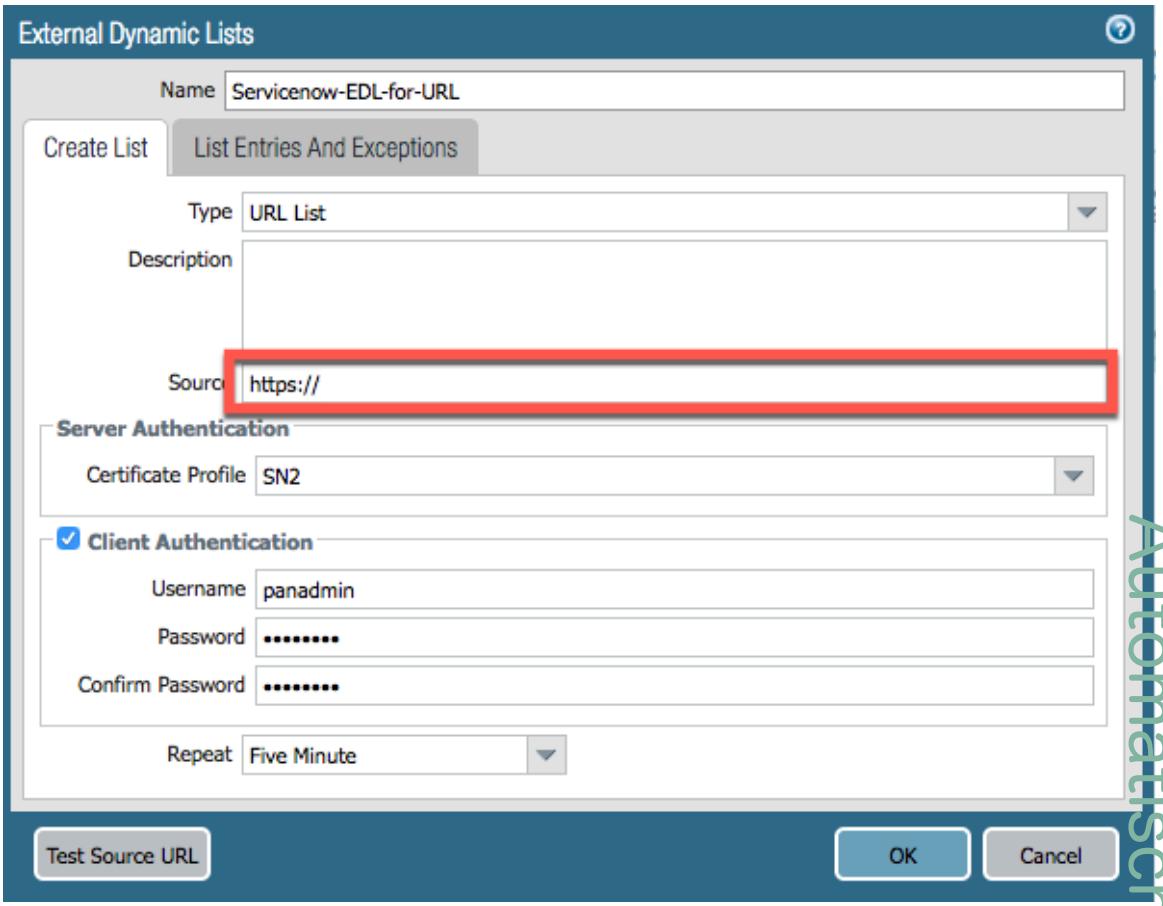



Image wird mit Genehmigung verwendet und ist PRIVILEGED und PROPRIETÄR.

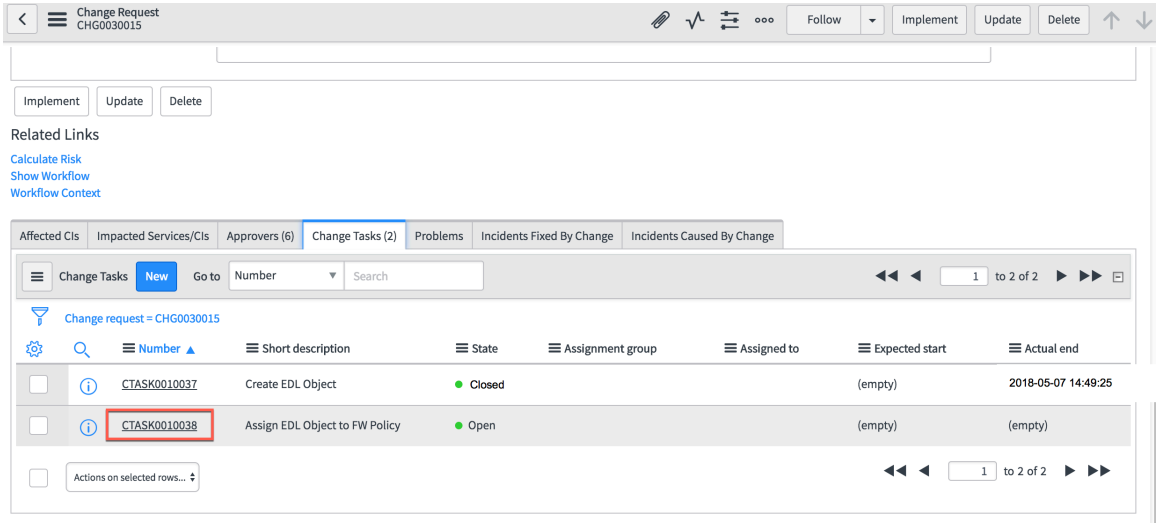
**d.** Nachdem Sie sich vergewissert haben, dass das EDL-Objekt in Palo Alto Networkserstellt wurde, navigieren Sie in Now Platformzu der Change-Anforderung, die der Erstellung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Aufgabe schließen**.

Im Aufgabendatensatz für dieses Beispiel wurde CTASK0010037 für diese Aufgabe geschlossen.

**e.** Navigieren Sie zur Registerkarte Change-Aufgaben, und klicken Sie auf die Aufgabe, um dem EDL-Objekt eine Firewall-Richtlinie zuzuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der Status für CTASK0010037 lautet Geschlossen.

**f.** Öffnen Sie den Datensatz, und weisen Sie die nächste Aufgabe zu.

Nachdem die Aufgabe zugewiesen wurde, navigiert der Firewall-Administrator in Palo Alto Networkszur Registerkarte **Richtlinien**, um die Richtlinie zuzuweisen.

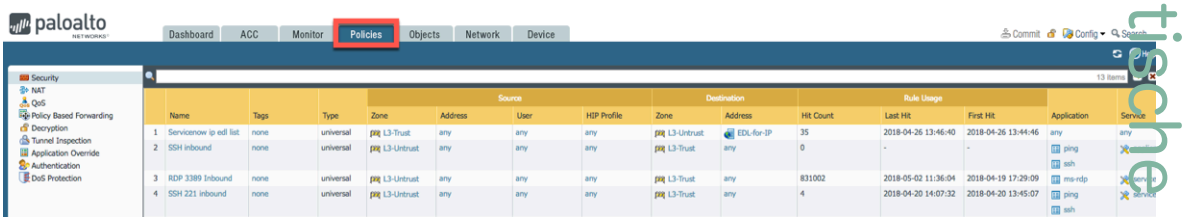



Image wird mit Genehmigung verwendet und ist PRIVILEGED und PROPRIETÄR.

**g.** Suchen Sie in der Spalte **Name** nach der Sicherheitsrichtlinienregel, der Sie die EDL hinzufügen möchten, und klicken Sie darauf, z. B. **ServiceNow ip edl list**.

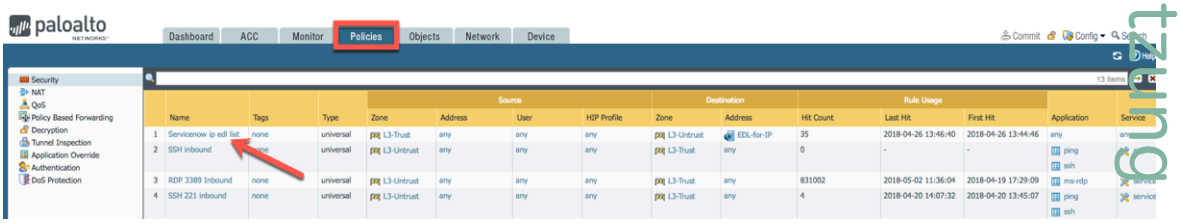



Image wird mit Genehmigung verwendet und ist PRIVILEGED und PROPRIETÄR.

**h.** Wählen Sie im Dialogfeld Sicherheitsrichtlinienregel die Registerkarte **Ziel** aus, um eine **EDL** im Feld Zieladresse hinzuzufügen.

**i.** Um alle verfügbaren EDLs anzuzeigen, klicken Sie auf das Symbol **Hinzufügen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

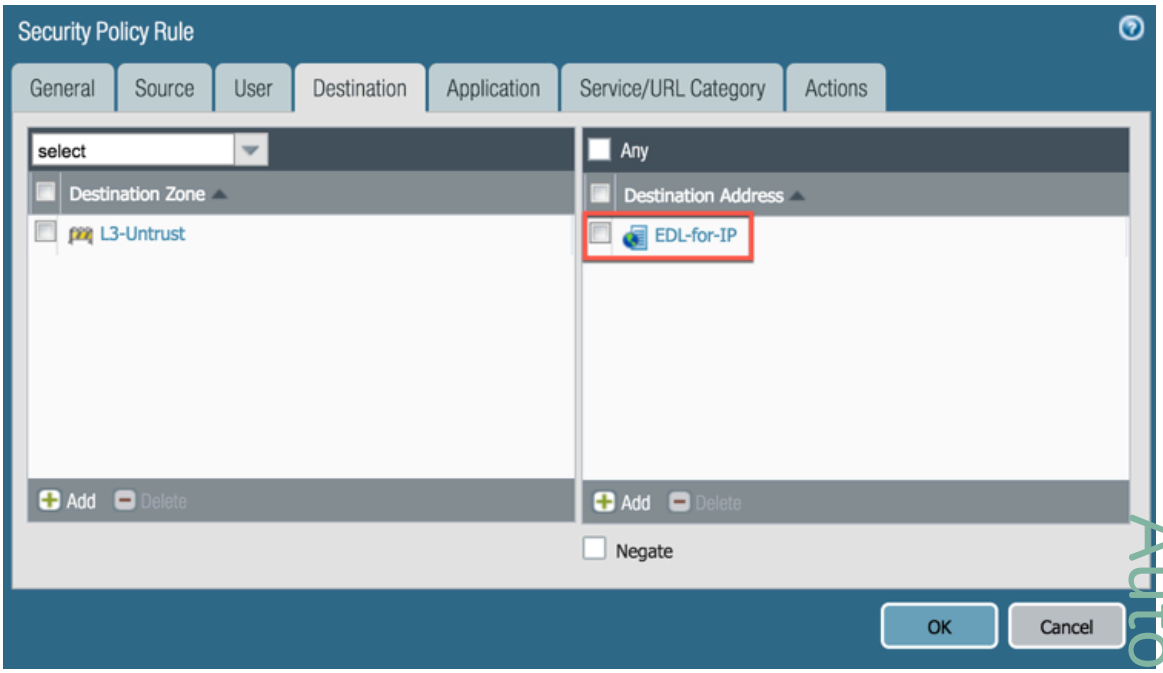



Image wird mit Genehmigung verwendet und ist PRIVILEGED und PROPRIETÄR.

**j.** Klicken Sie auf **OK**.

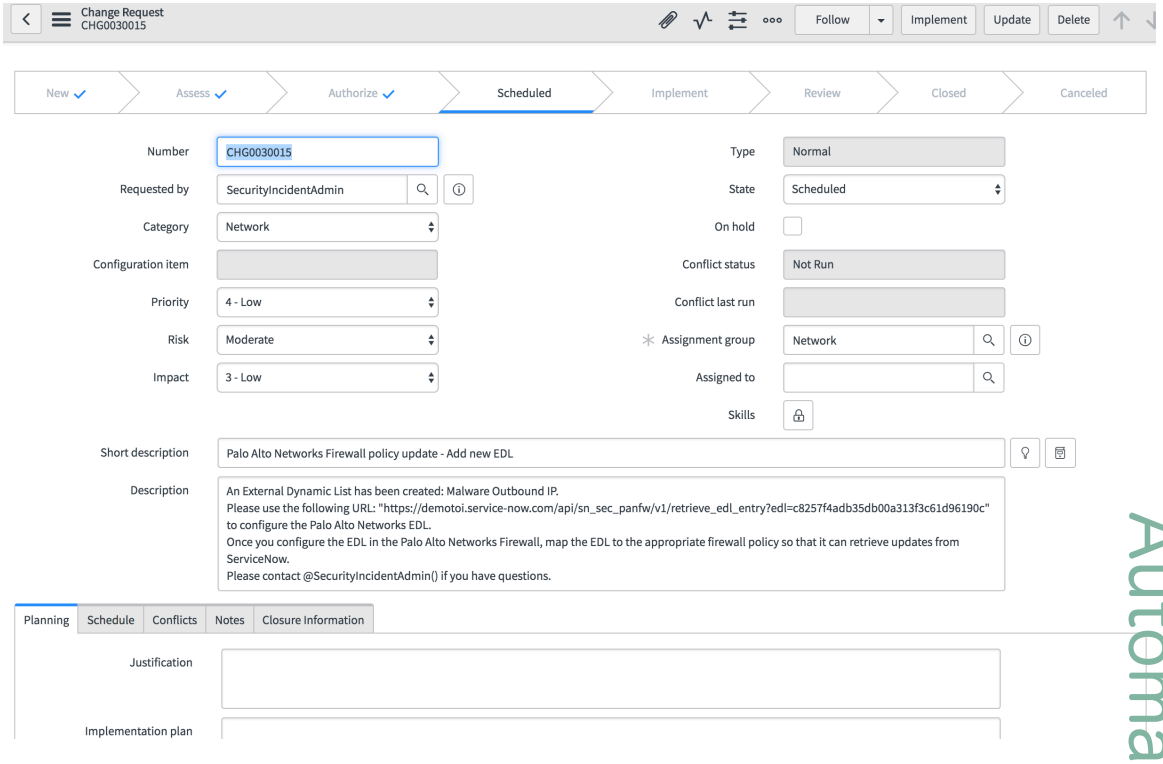
**k.** Nachdem Sie sich vergewissert haben, dass das EDL-Objekt einer Sicherheitsrichtlinie zugewiesen wurde, navigieren Sie in Now Platformzum Change Request, öffnen Sie die Aufgabe, die der Zuweisung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Aufgabe schließen**.
Nachdem beide Aufgaben geschlossen wurden, ist der Change Request zur Genehmigung bereit.

**l.** Klicken Sie im **Datensatz** der Change-Anforderung auf die zugehörige Liste Genehmiger, und wählen Sie ein Element in der **Spalte** Status aus, um die Anforderung zu öffnen, die zum Erstellen der EDL verwendet wird.

**m.** Klicken Sie im geöffneten Genehmigungsanforderungsformular auf **Genehmigen**.
Der Status der Change-Anforderung wird in „Geplant“ verschoben.

Automatische Übersetzung

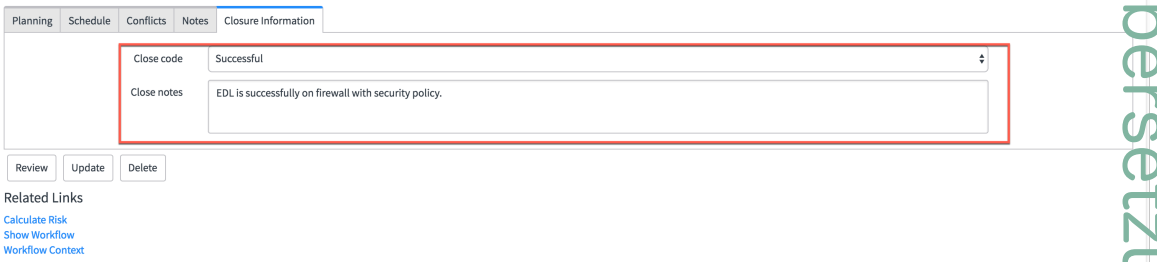
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**n.** Klicken Sie auf **Implementieren**.

**o. Klicken** Sie auf die zugehörige Registerkarte Abschlussinformationen, und geben Sie Notizen ein, um die Anforderung zu schließen.

Ein Eintrag in diesem Feld ist erforderlich, um die Change-Anforderung zu schließen.

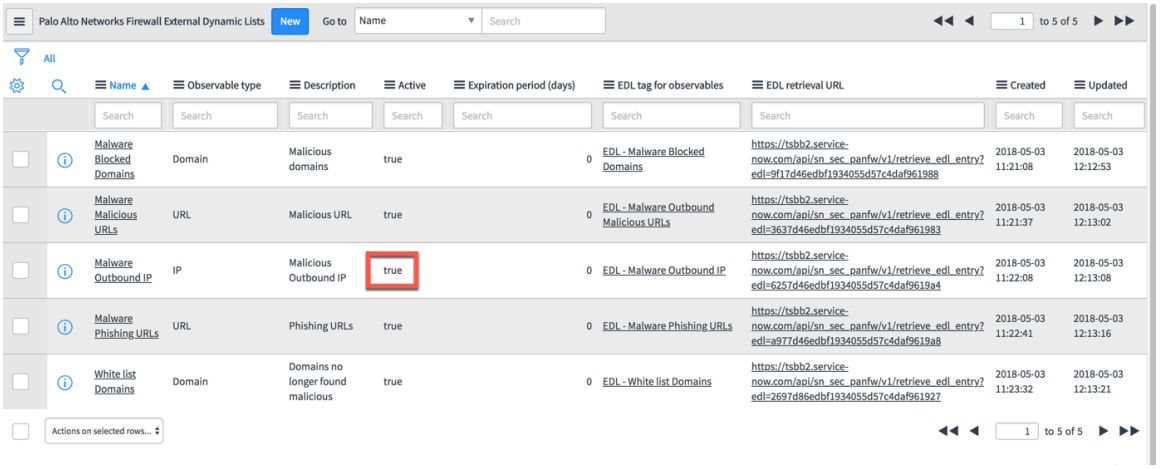



Nachdem die Change-Anforderung geschlossen wurde, wird die EDL automatisch aktiviert. Wenn Sie nicht überprüft haben, ob die EDL aktiviert ist, navigieren Sie zu **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration**.

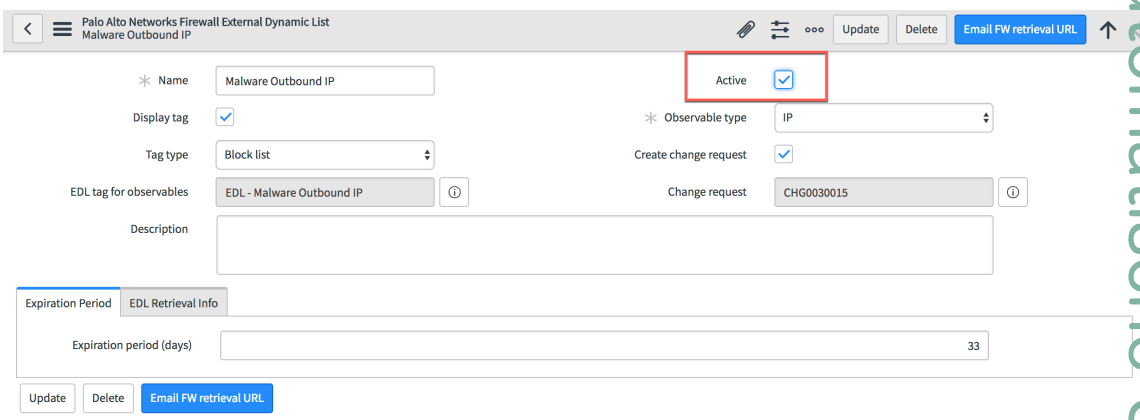
Beachten Sie in der Spalte Aktiv in der Liste, dass der Status für die EDL (true) lautet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Klicken Sie in der Spalte Name auf den EDL-Namen, und beachten Sie im geöffneten Datensatz, dass das Kontrollkästchen **Aktiv** ebenfalls aktiviert ist.




Die EDL ist jetzt bereit, EDL-Einträge zu akzeptieren.

## Nächste Maßnahme

Senden Sie EDL-Einträge aus einem Security Incident oder aus der Sperrliste.

### Senden Sie EDL-Einträge aus einem Security Incident-Datensatz für Palo Alto Networks Next-Generation Firewall

An einen Security Incident-Datensatz angehängte erkennbare Elemente werden als EDL-Einträge (External Dynamic List) an EDLs zur Genehmigung übermittelt. Ein Genehmigungsprozess für EDL-Einträge ist Teil des vorkonfigurierten Workflows. Die Firewall importiert EDL-Einträge (IP-Adressen, URLs, Domänen), die in EDL-Listen enthalten sind, und erzwingt die Richtlinie.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst zum Übermitteln von EDL-Einträgen. So genehmigen Sie EDL-Einträge: Die Genehmigung ist standardmäßig sn_si.admin zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden.

## Warum und wann dieser Vorgang ausgeführt wird

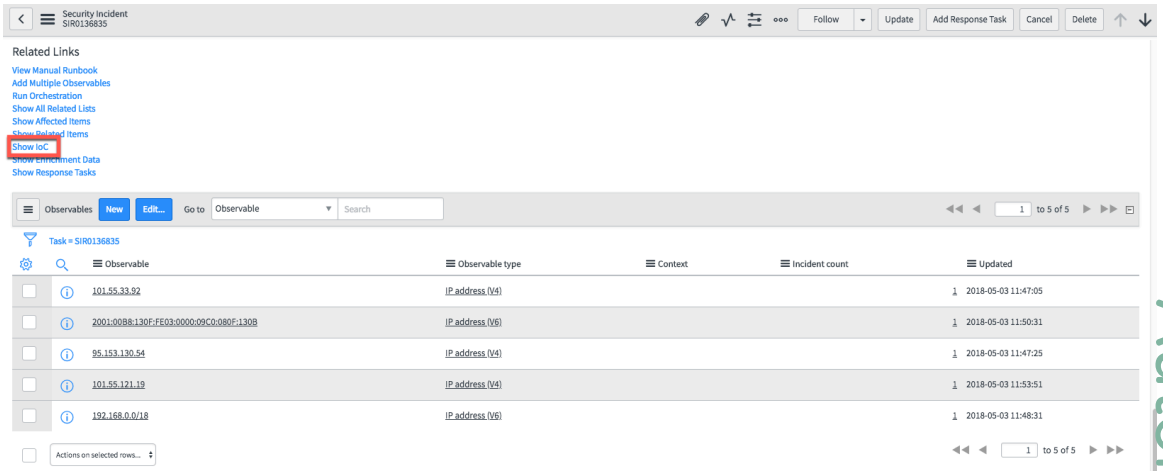
Benutzer mit der Rolle „sn_si.analyst“ übermitteln EDL-Einträge, indem sie eine Sperre für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind. Nach der Übermittlung wird ein EDL-Eintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockanforderung für ein erkennbares URL-Element.

Automatische Übersetzung

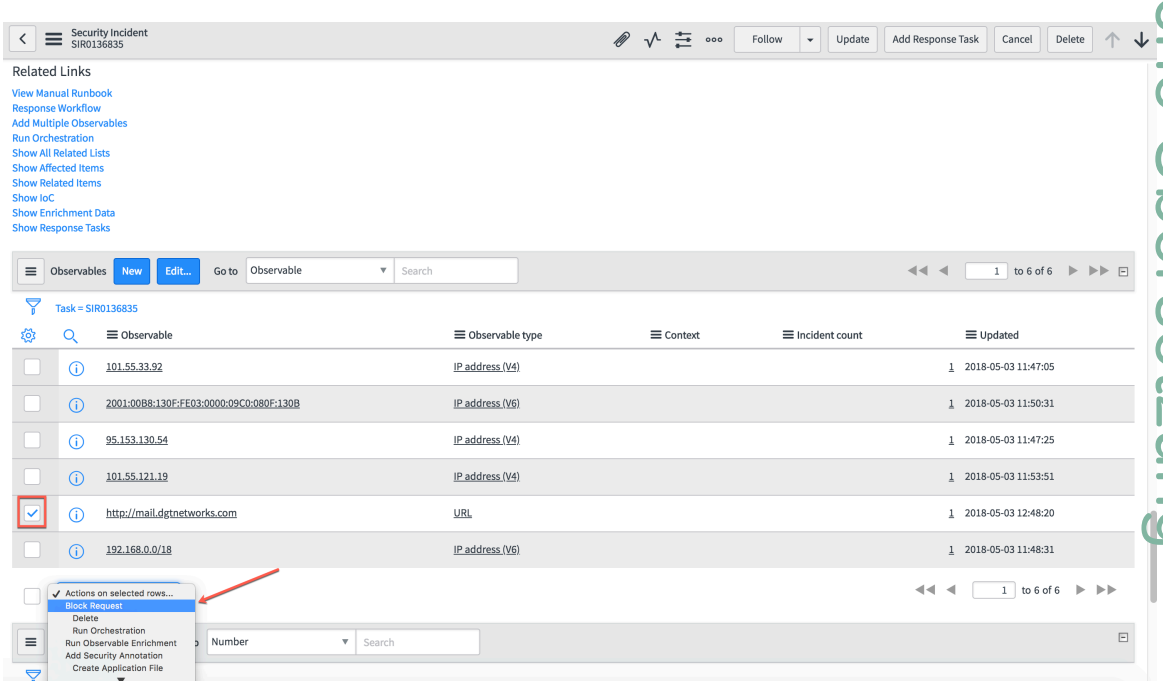
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.




3. Wählen Sie in der zugehörigen Liste „Erkennbare Elemente“ die erkennbaren Elemente aus, die Sie blockieren möchten, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die **Option Anforderung**blockieren aus.

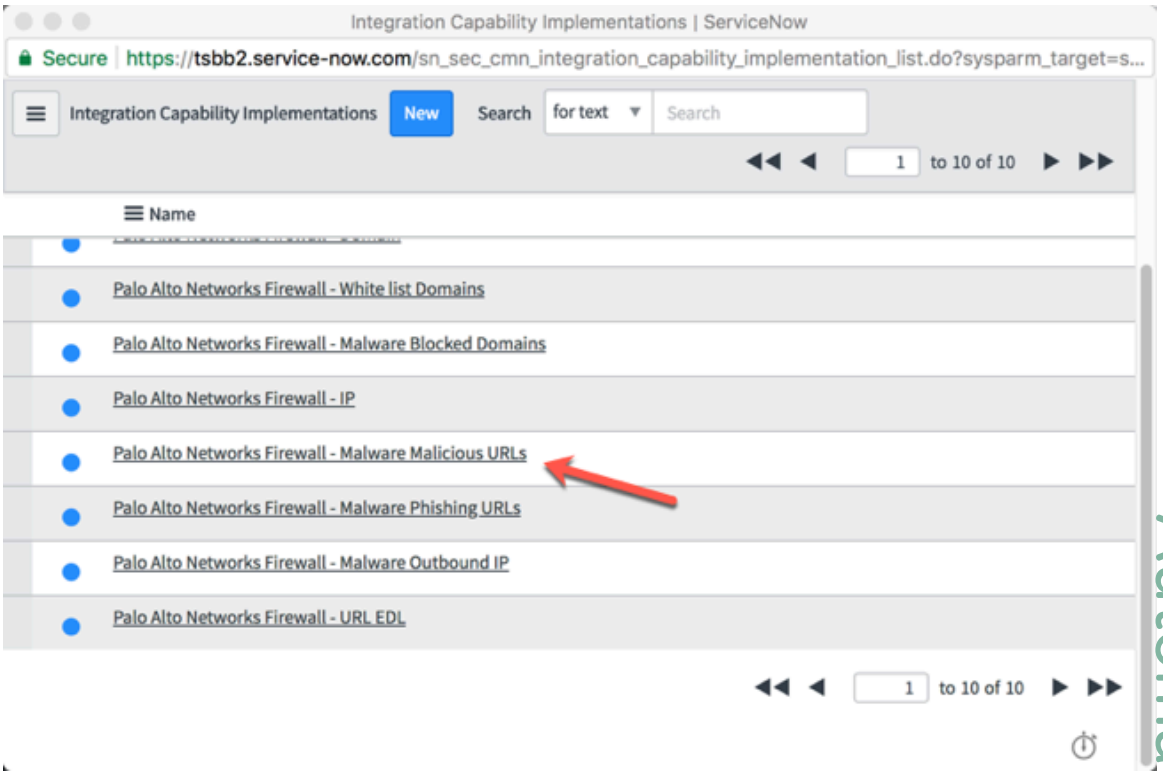



4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( ).
5. Wählen Sie in der angezeigten Liste die EDL aus, an die Sie diesen Eintrag anhängen möchten.

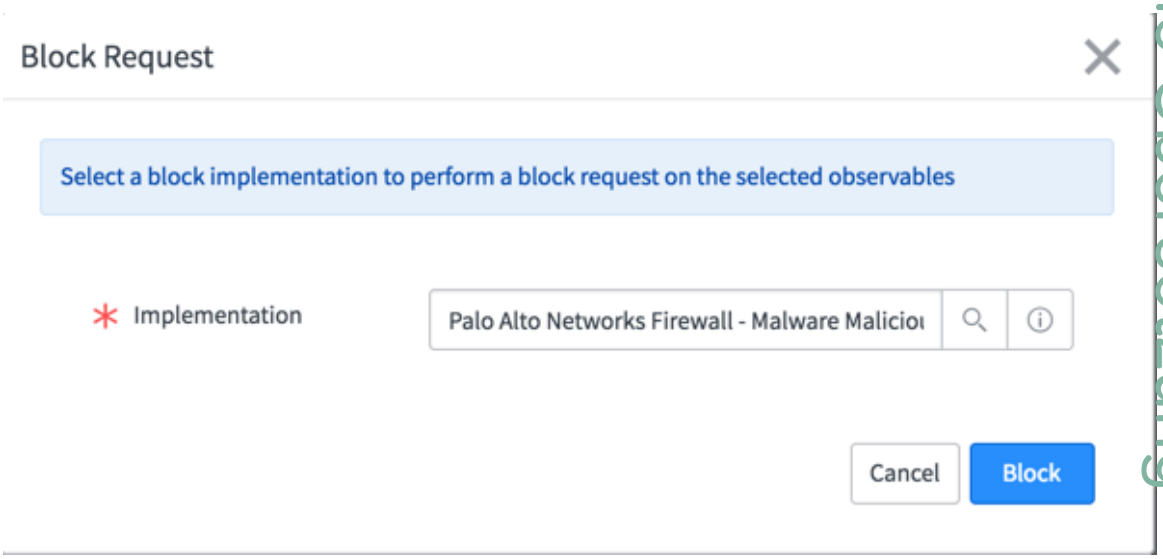
**Hinweis:**
In diesem Beispiel muss der erkennbare Elementtyp (URL) des Eintrags mit dem erkennbaren EDL-Typ (URL) übereinstimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



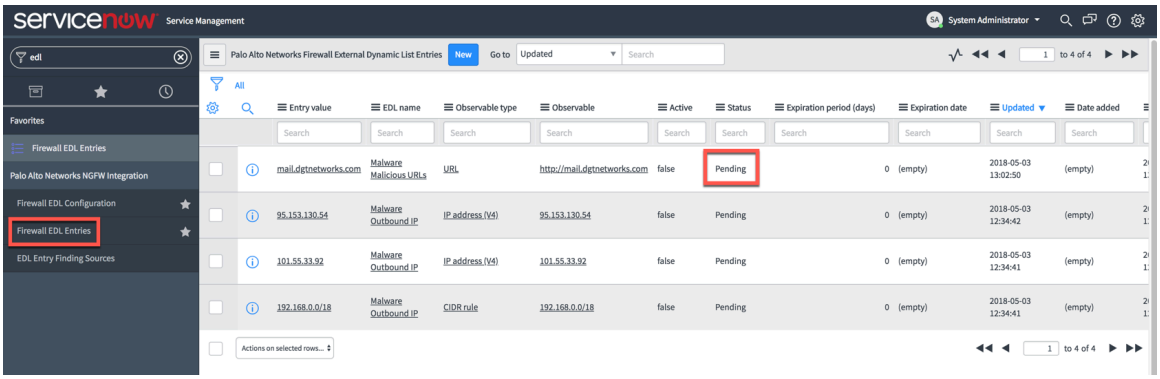

6. Klicken Sie im Dialogfeld „ **Sperranforderung** “ mit dem EDL-Namen im Feld „ **Implementierung**“ auf Sperren.




7. Navigieren zu **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge** und klicken Sie auf **Firewall EDL-Einträge**.

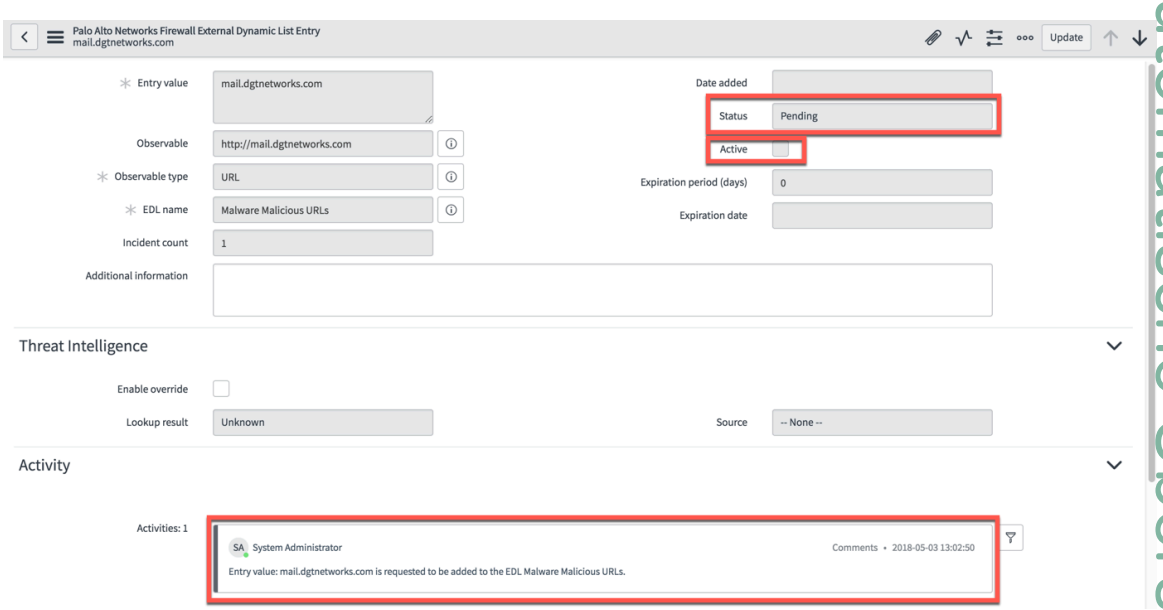
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**8.** Klicken Sie in der Liste Palo Alto Networks-Firewall der externen dynamischen Listeneinträge in der Spalte Eingabewert auf das **erkennbare** Element, um den Datensatz zu öffnen.

In diesem Beispiel wird der Datensatz für **mail.dgtnetworks.com** angezeigt.

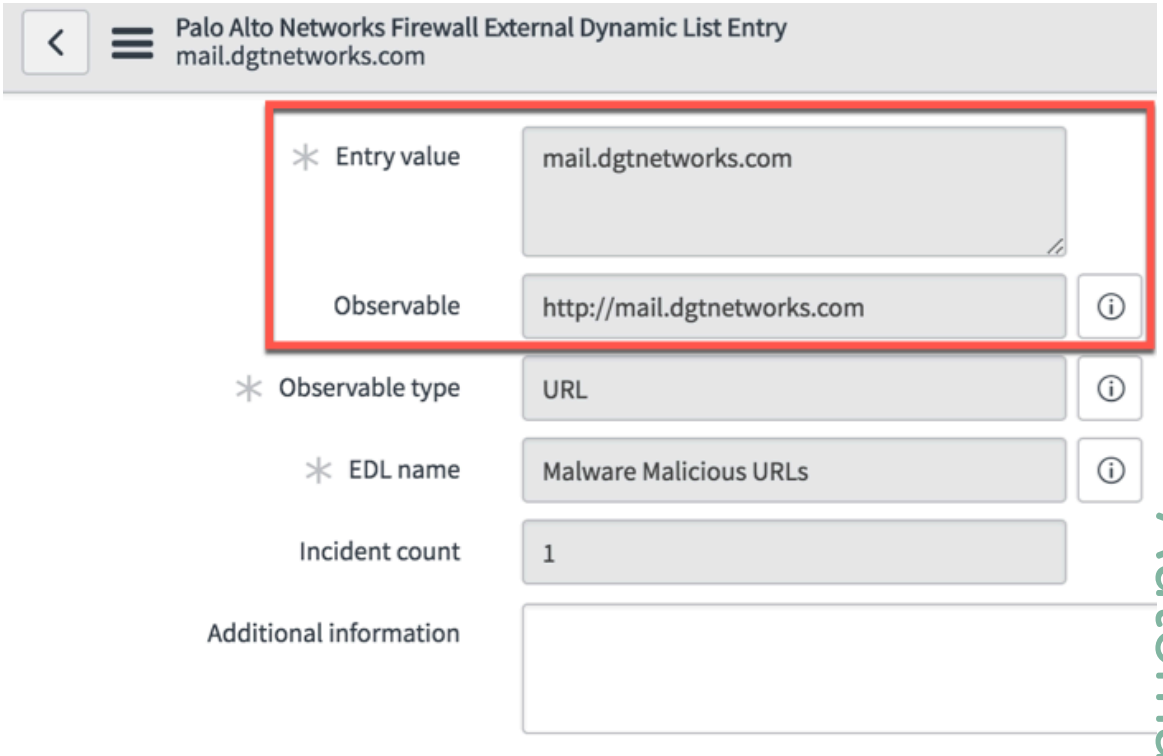



Der Status lautet Ausstehend, das Kontrollkästchen Aktiv ist deaktiviert, und die Arbeitsnotizen zeigen an, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorliegt. Diese EDL-Zutrittsanforderung ist zur Genehmigung bereit.

Die Felder Eingabewert und Erkennbares Element zeigen unterschiedliche Formate für das erkennbare URL-Element an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Symbol neben dem Feld „Erkennbares Element“ ist ein Link zur Tabelle „Erkennbares Element Now Platform® “ .

Der Wert im Feld „Erkennbares Element “ (http://mail.dgtnetworks.com) ist mit der Tabelle „Erkennbares Element“ verknüpft und stimmt mit dem Format überein, das aus dem Incident-auslösenden Event Security Incident Response übernommen wurde.

Now Platform® kann EDL-Einträge automatisch so ändern, dass sie mit dem EDL-URL-Format von Palo Alto Networks kompatibel sind.

In diesem Beispiel wurde das erkennbare Element mit dem Protokoll http:// (http://mail.dgtnetworks.com) erstellt, und dieses Format wird im Feld Erkennbares Element angezeigt. Das Protokoll http:// wird automatisch von Now Platform® aus dem erkennbaren Element entfernt, sodass es mit Palo Alto Networks kompatibel ist und abgerufen werden kann. Daher wird mail.dgtnetworks.com im Feld Eingabewert angezeigt.

## Nächste Maßnahme

Genehmigen Sie EDL-Einträge.

### Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

## Senden Sie EDL-Einträge aus der Sperrliste für Palo Alto Networks Next-Generation Firewall

Für erkennbare Elemente, die als böswillig eingestuft wurden und keinem bestimmten Now Platform Security Incident zugeordnet sind, übermitteln Sie EDL-Einträge (External Dynamic List) aus der Sperrliste.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

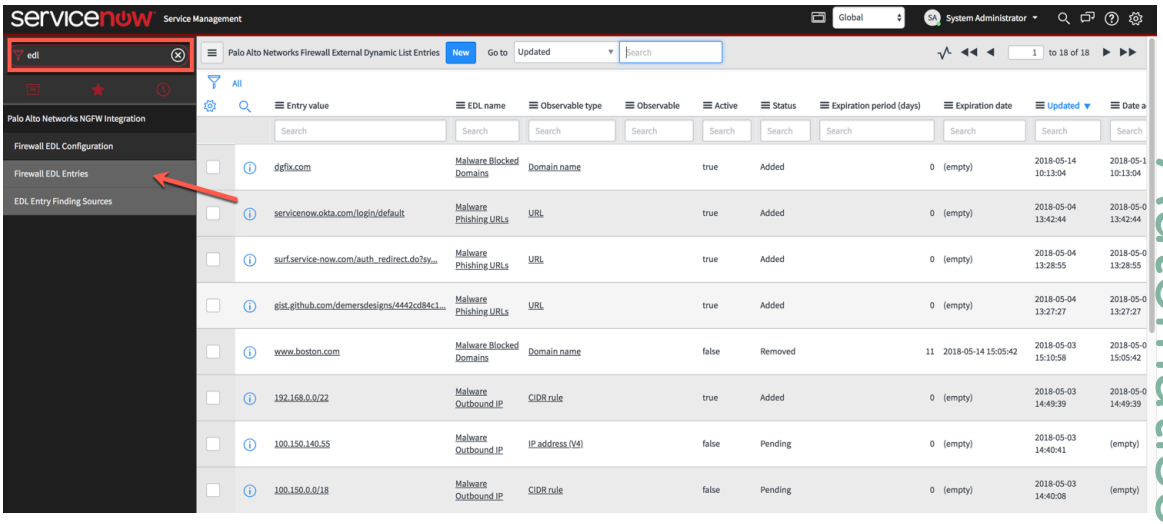
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein erkennbares Element blockieren möchten, von dem Sie festgestellt haben, dass es böswillig ist, oder ein erkennbares Element zulassen möchten, von dem Sie festgestellt haben, dass es nicht böswillig ist, und das erkennbare Element keinem bestimmten Now Platform Security Incident-Datensatz zugeordnet ist, übermitteln Sie EDL-Einträge direkt aus der Sperrliste. Beispiele für diese Arten von EDL-Einträgen können URLs oder Domänen für bestimmte Sites sein.

## Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge**.




2. Klicken Sie auf das Modul **Firewall EDL-Einträge**.
3. Klicken Sie in der Liste Palo Alto Networks-Firewall der externen dynamischen Listeneinträge auf **Neu**.
4. Geben Sie im neuen Datensatz, der angezeigt wird, im Feld **Eingabewert** einen Wert für das erkennbare Element ein.
   Die zwei möglichen Ergebnisse dieses Eintrags:

   **Die verbleibenden Felder im Formular werden automatisch ausgefüllt.**

   Ein übereinstimmendes erkennbares Element wird gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf **Absenden**. Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

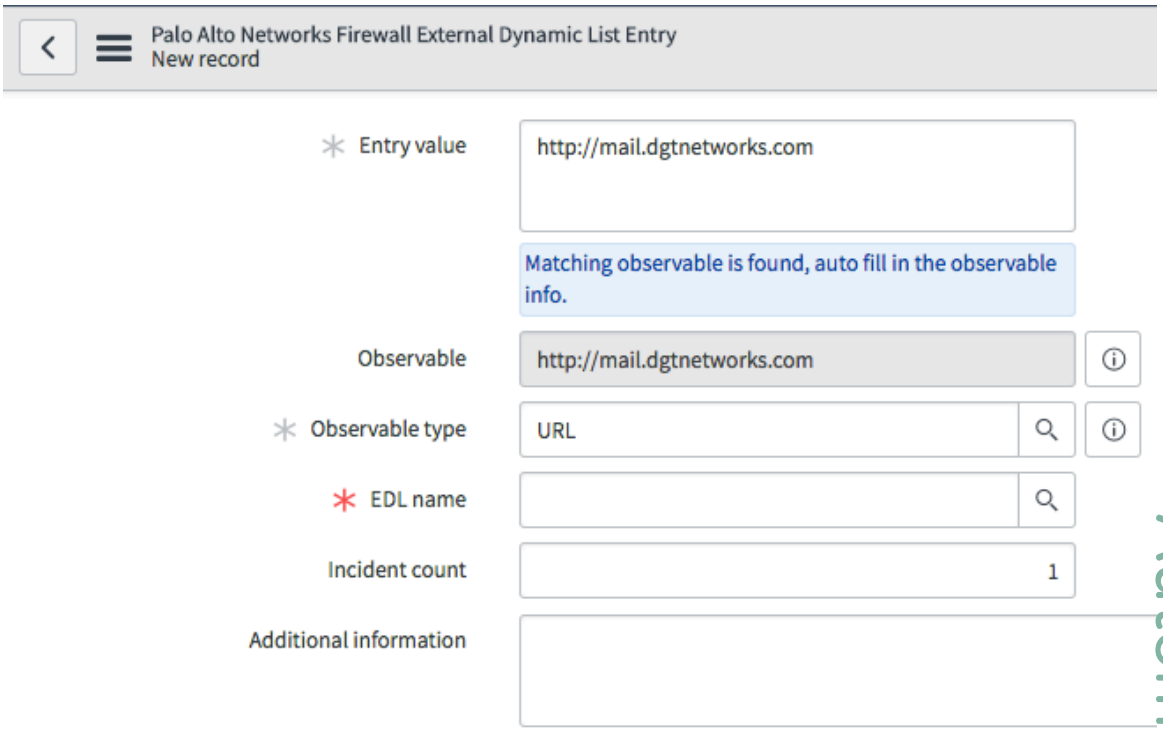
   **Eine Nachricht wird angezeigt, in der Sie aufgefordert werden, das Formular auszufüllen.**

   Es wurde kein passendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Wählen Sie nach Abschluss die EDL aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf **Absenden**. Ein Datensatz für erkennbare Elemente wird erstellt.

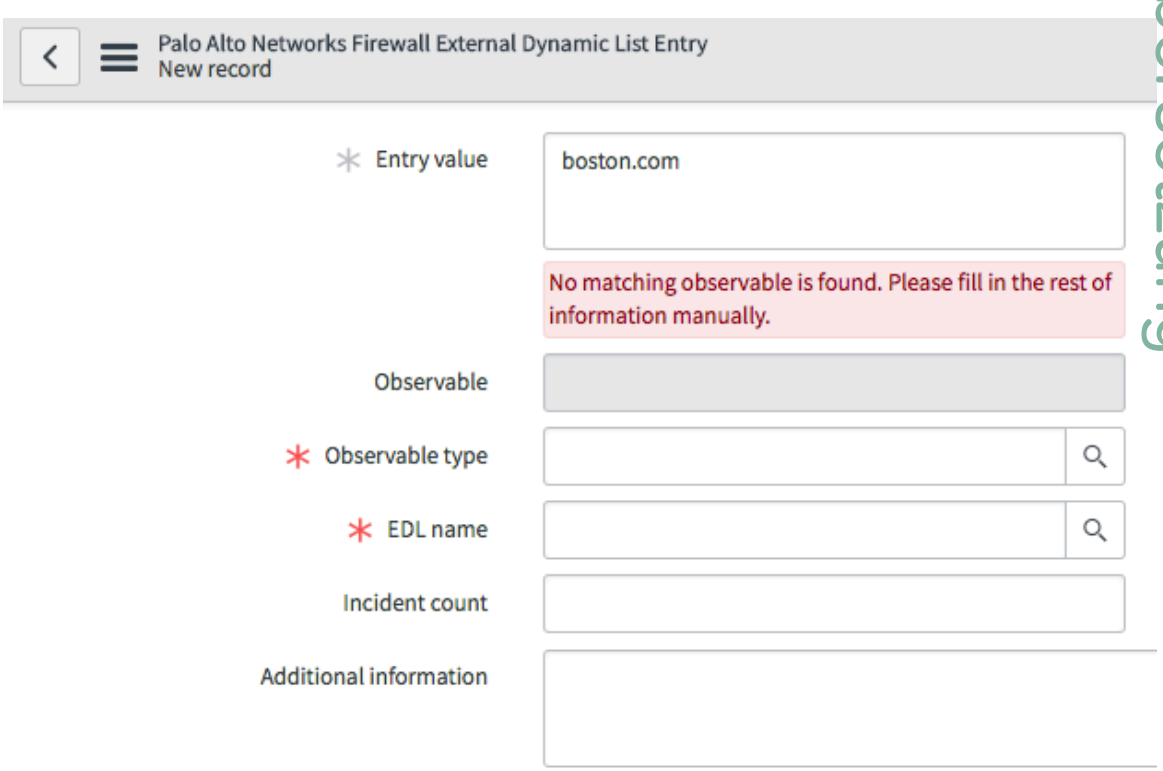
Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



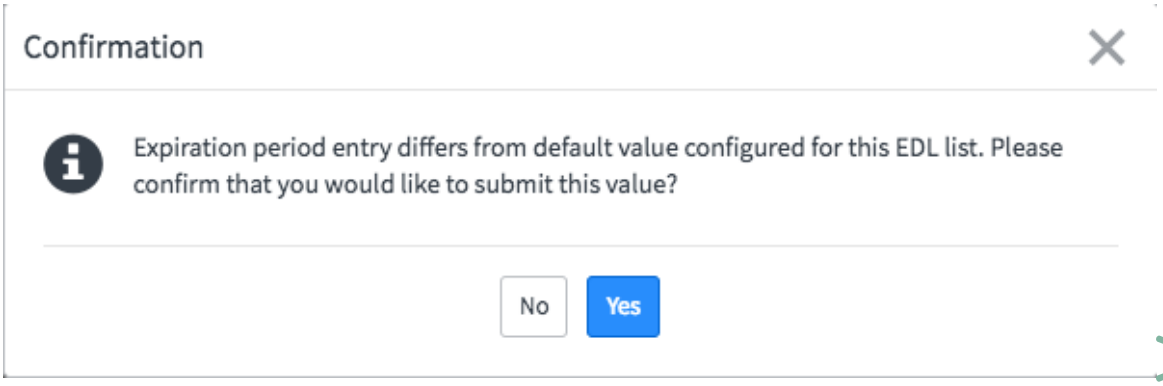

5. Klicken Sie auf das Suchsymbol, um die EDL auszuwählen, an die Sie den Eintrag anhängen möchten.
6. Klicken Sie auf **Absenden**.
   Wenn Sie die E-Mail-Genehmigung in Ihrem Workflow konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
7. Wenn eine Meldung angezeigt wird, in der Sie aufgefordert werden, die restlichen Informationen manuell einzugeben, füllen Sie die Felder aus.




Automatische Übersetzung

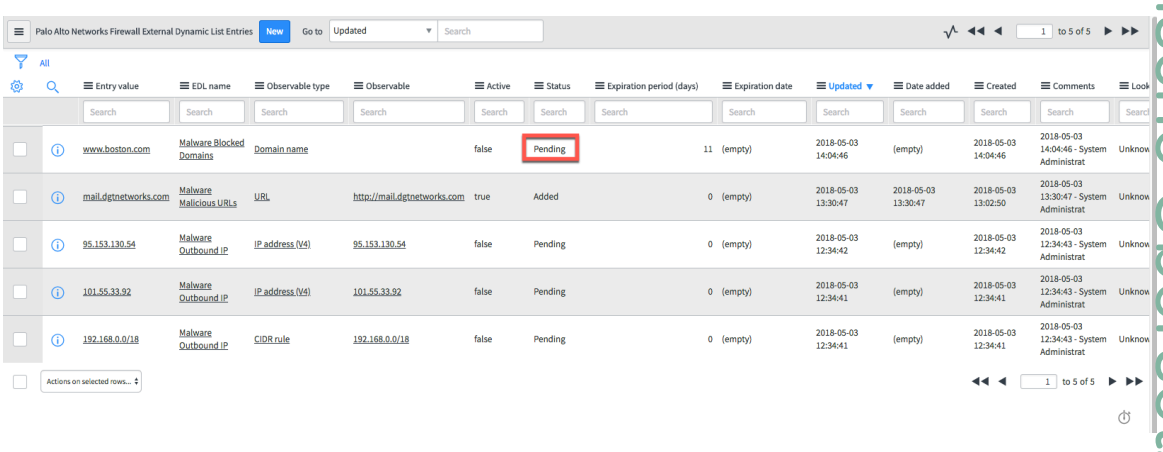
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Absenden**.
   Wenn Sie den standardmäßigen Ablaufzeitraum des EDL-Eintrags geändert haben, wird ein Bestätigungsdialogfeld mit der Warnung angezeigt, dass sich der Zeitraum von dem ausgewählten EDL unterscheidet.




9. Wählen Sie eine Option aus, um den Ablaufzeitraum zu konfigurieren.

10. Wenn nicht angezeigt, navigieren Sie zur **Liste Palo Alto Networks-Firewall der externen dynamischen** Listeneinträge, und beachten Sie, dass der Status für den Eintrag Ausstehend lautet.




Der Eintrag ist jetzt zur Genehmigung bereit.

## Nächste Maßnahme

Genehmigen Sie EDL-Einträge.

### Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

## Genehmigen Sie EDL-Einträge für Palo Alto Networks Next-Generation Firewall

Ein Genehmigungsprozess für EDL-Einträge (External Dynamic List) ist Teil des vorkonfigurierten Workflows. Sie genehmigen EDL-Einträge, bevor die Einträge für EDLs aktiviert werden. Sobald Sie den EDL-Eintrag genehmigt haben, ruft die Firewall den Eintrag ab, und Ihr erkennbares Element ist ab diesem Zeitpunkt blockiert.

## Vorbereitungen

Erforderliche Rolle: Die Genehmigung für EDL-Einträge ist standardmäßig sn_si.admin zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugewiesen werden. Im folgenden Beispiel verfügt der Now Platform -Administrator über Genehmigungsberechtigung.

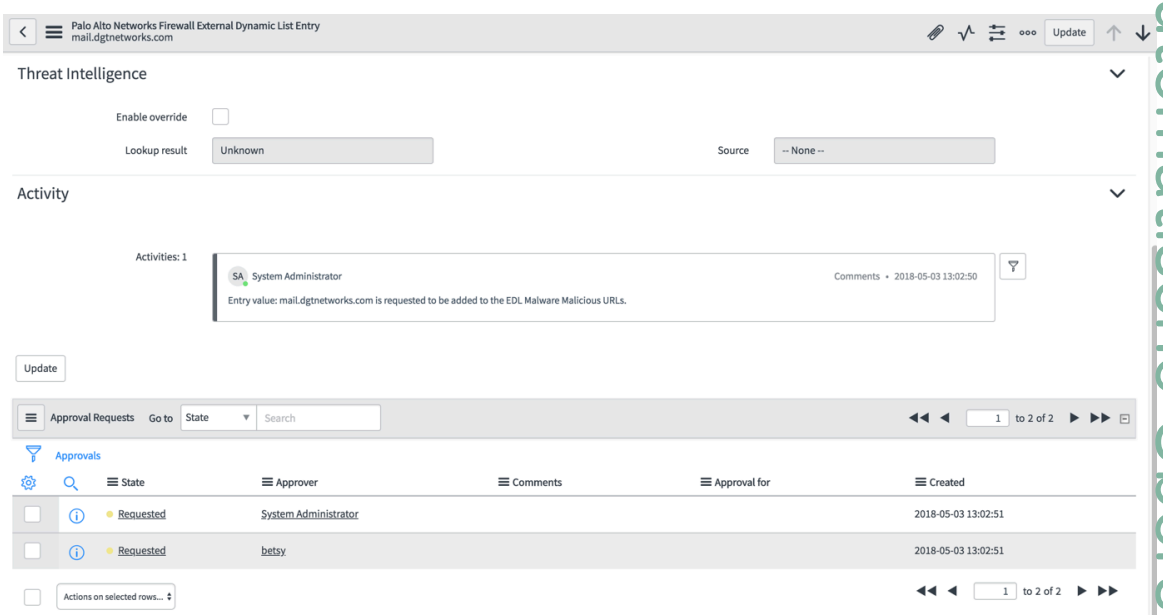
### Warum und wann dieser Vorgang ausgeführt wird

Wenn der Genehmigungsprozess aktiviert ist, wird ein EDL-Eintrag in der EDL erst aktiviert oder deaktiviert, wenn er genehmigt wurde.

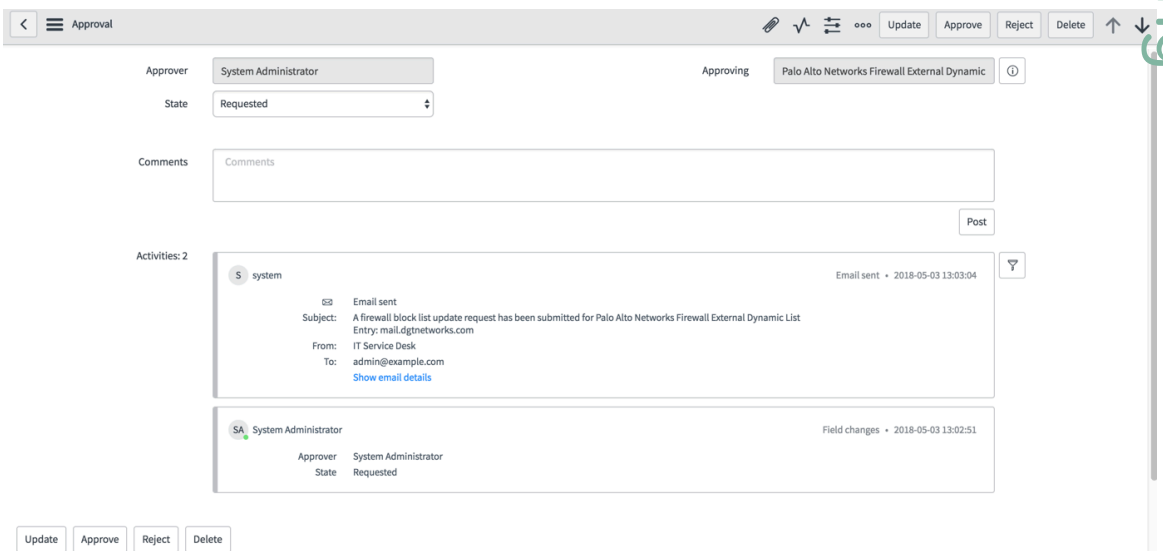
### Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge** und öffnen Sie den EDL-Datensatz.
2. Scrollen Sie im EDL-Datensatz zum Abschnitt „Genehmigungsanforderungen“.

**Hinweis:**
Wenn Sie in den Systemeinstellungen Formulare mit Registerkarten ausgewählt haben, wird der Abschnitt als Registerkarte im Datensatz angezeigt.



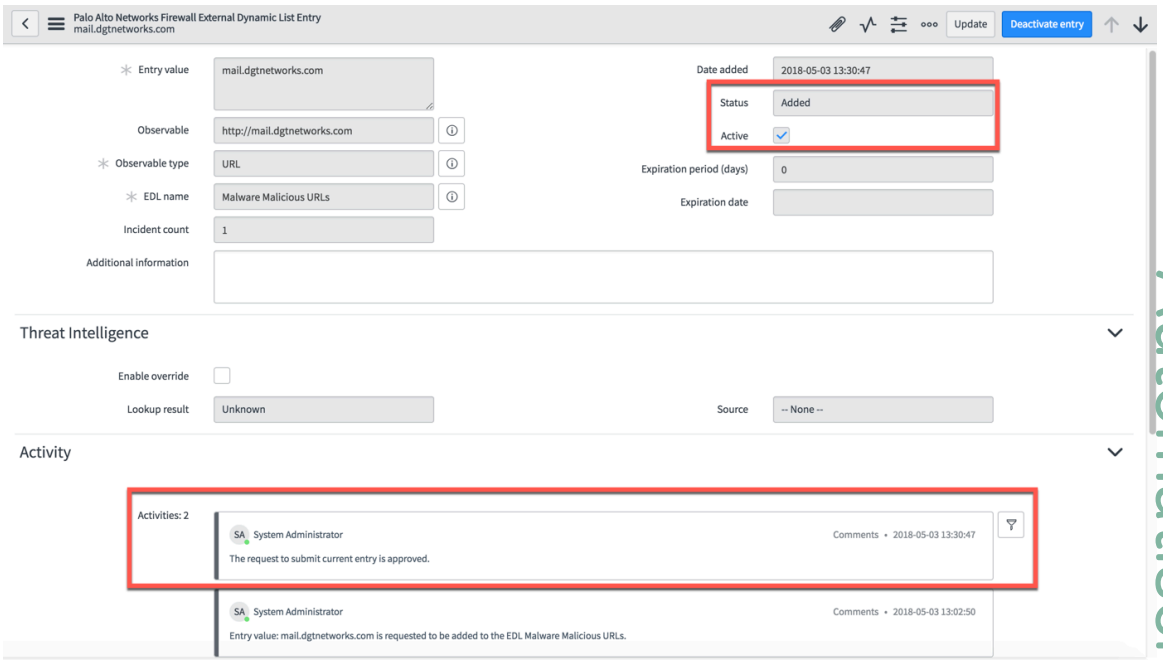

3. Klicken Sie in Genehmigungsanforderungen auf ein Element in der **Spalte** Status, um es zu öffnen. Der Genehmigungsdatensatz wird angezeigt.



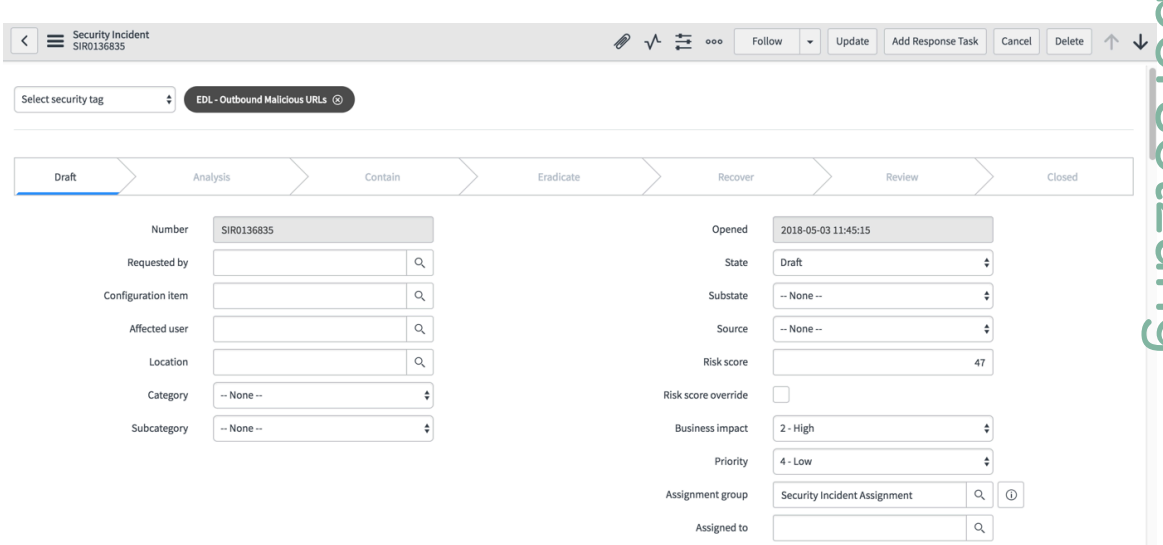

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie eine Option für die Genehmigung des EDL-Eintrags aus.
   Nachdem Sie den EDL-Eintrag genehmigt haben und aktiviert ist, ruft Palo Alto Networks Next-Generation Firewall den EDL-Eintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, ist das erkennbare Element ab diesem Zeitpunkt blockiert. Beachten Sie in der folgenden Abbildung, dass das Kontrollkästchen Aktiv aktiviert ist, der Status Hinzugefügt lautet und die Arbeitsnotizen angeben, dass die Anforderung genehmigt wurde.



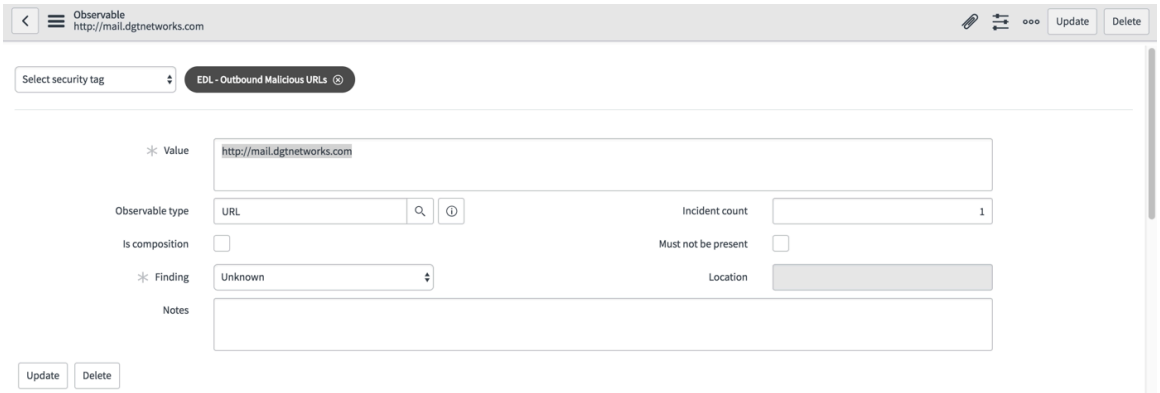

Nachdem der EDL-Eintrag genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag markiert. Das Tag wird oben im Datensatz angezeigt.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



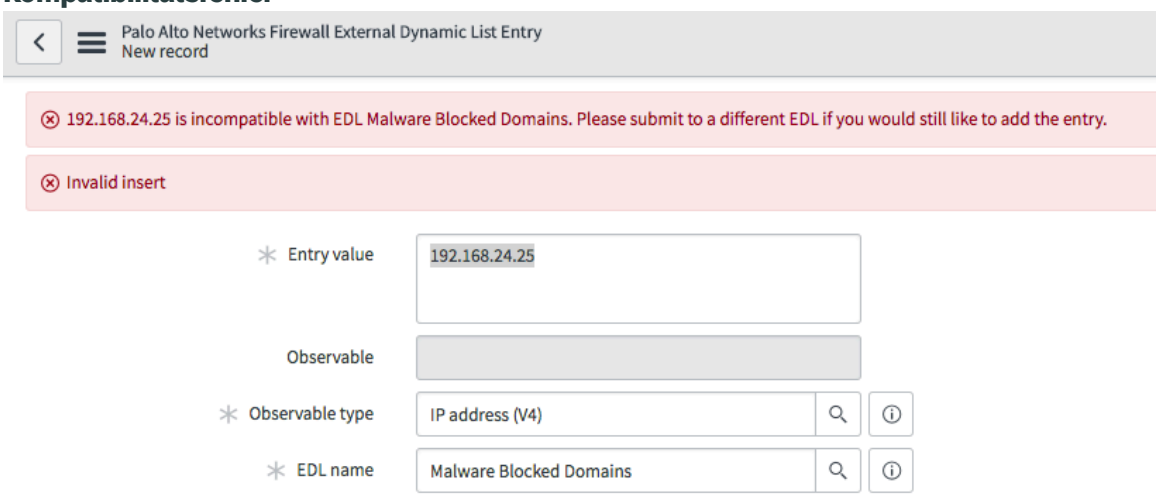

### EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Es gibt Einschränkungen für das Hinzufügen von EDL-Einträgen (External Dynamic List) zu EDLs. Wenn Duplikat-, Kompatibilitäts- oder CIDR-Konflikte (Classless Inter-Domain Routing) auftreten, wenn Sie versuchen, EDL-Einträge zu EDLs hinzuzufügen, werden Fehlermeldungen angezeigt, die Sie bei der Behebung dieser Fehler unterstützen.

## Kompatibilitätsausnahme

Jede EDL akzeptiert nur Einträge, die mit ihrem erkennbaren Typ kompatibel sind. Wenn Sie eine Domänen-EDL erstellen und versuchen, eine erkennbare IP-Adresse an sie anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänen-EDL nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

**Kompatibilitätsfehler**



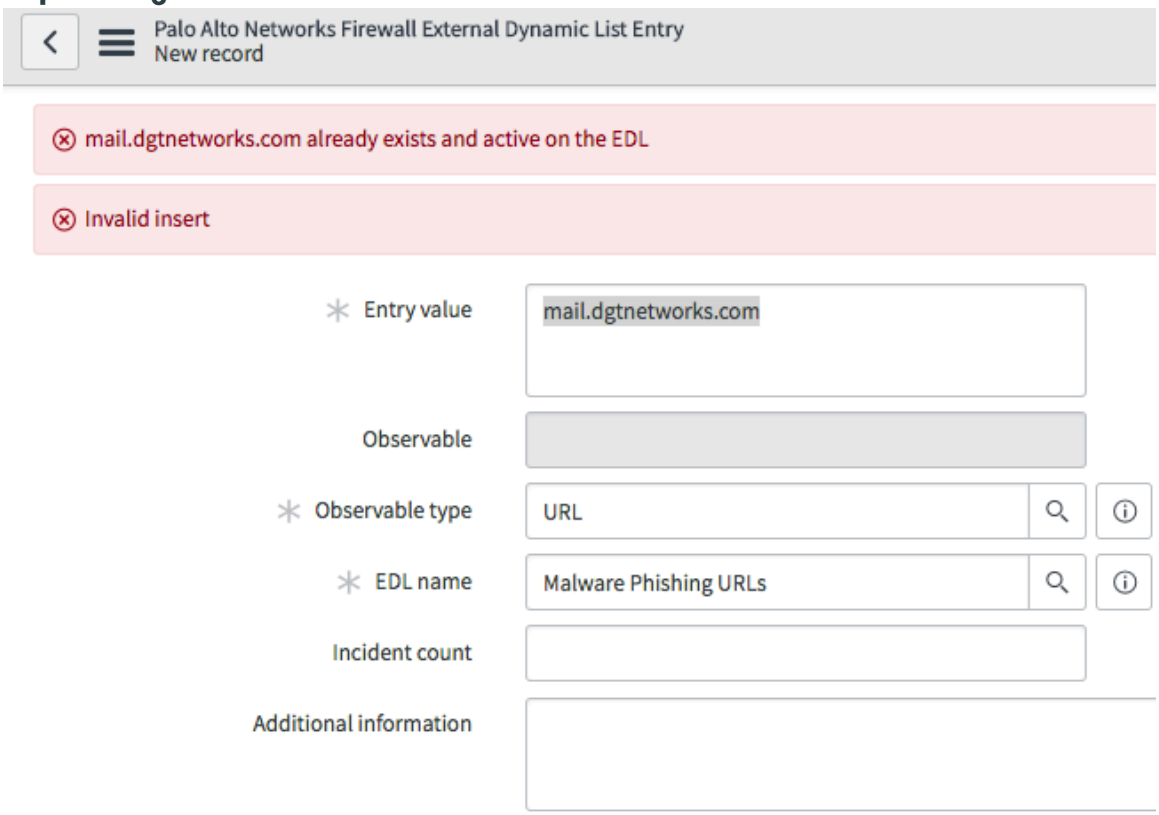

## Duplizierungsausnahme

Ein erkennbares Element kann nicht für mehrere EDLs desselben erkennbaren Typs aktiviert werden. Wenn ein erkennbares URL-Element bereits für eine URL-EDL aktiviert ist und Sie versuchen, dasselbe erkennbare Element für eine Phishing-URL-EDL zu aktivieren, wird eine Duplizierungsfehlermeldung angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Duplizierungsfehler



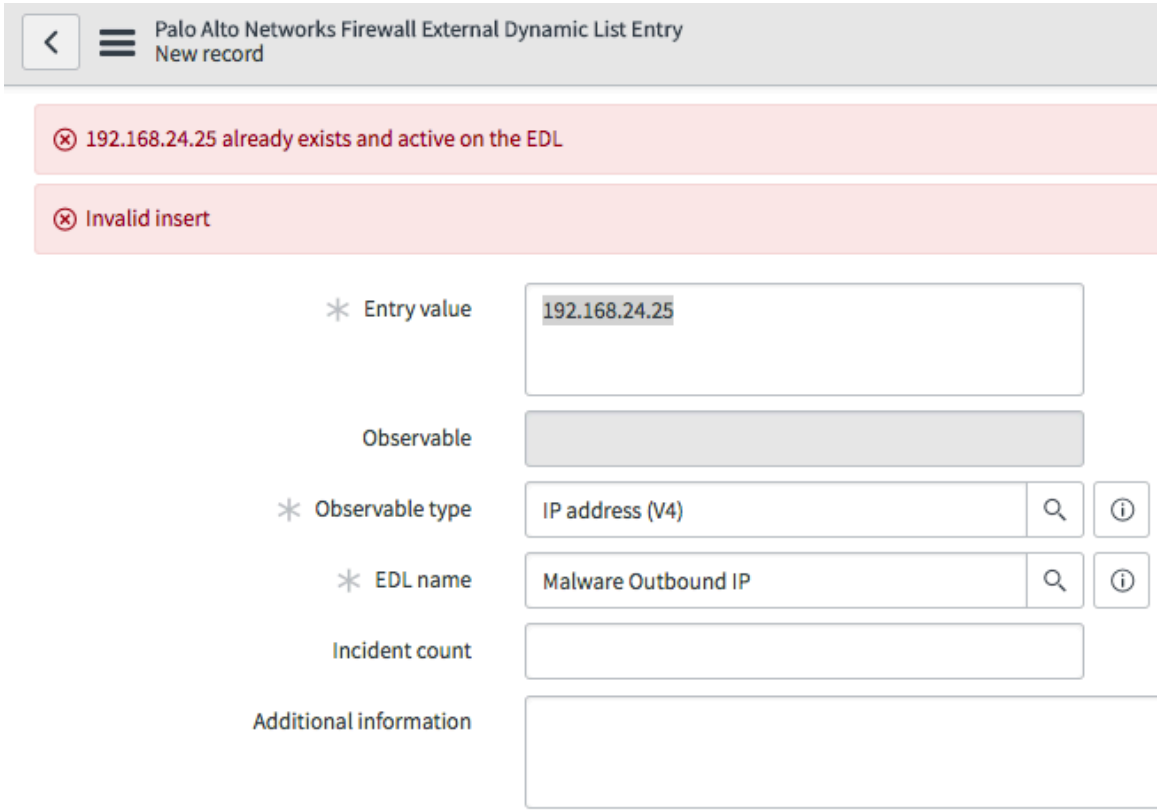

### CIDR-Ausnahme (Classless Inter-Domain Routing).

Wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen, und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits in einer EDL befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler weist darauf hin, dass die einzelne IP-Adresse bereits in der EDL als Teil des erkennbaren CIDR-Elements enthalten ist. Zum Beispiel ist 192.168.24.25 Teil des CIDR-Blocks 192.168.0.0/22.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CIDR-Konflikt**




### (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall

Wenn die **Checkbox Tag anzeigen aktiviert** ist, wenn Sie den EDL-Datensatz (External Dynamic List) erstellen, können Sie die Tag-Namen und Farben der Sicherheits-Tags bearbeiten. Sicherheits-Tags helfen Ihnen, erkennbare Elemente nachzuverfolgen, die bereits blockiert sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

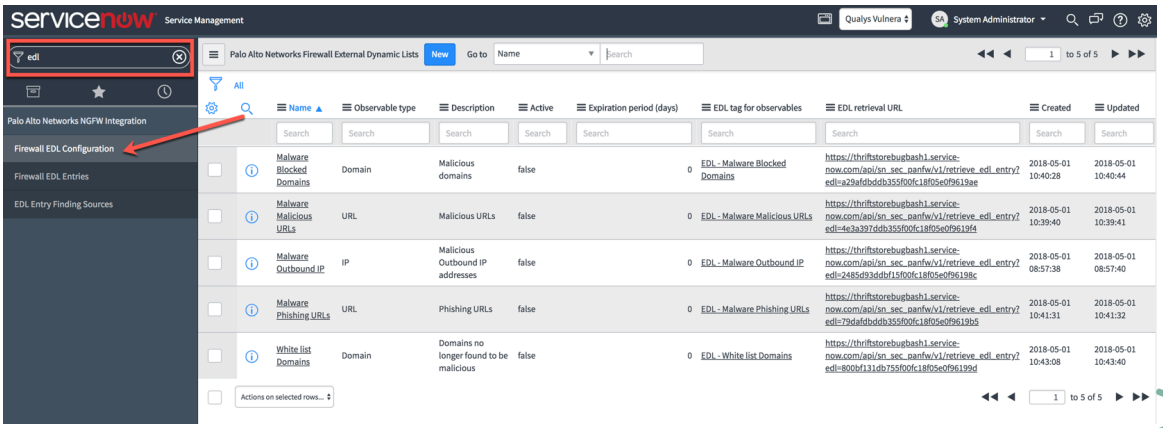
Sicherheits-Tags helfen Ihnen, schnell zu erkennen, welche Security Incidents erkennbare Elemente in einer Sperrliste enthalten. Tags helfen Ihnen auch dabei, zu erkennen, ob ein erkennbares Element bereits blockiert ist oder ob es aus einer EDL entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Sperrlisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, damit Sie bestimmte Tags leichter erkennen können.



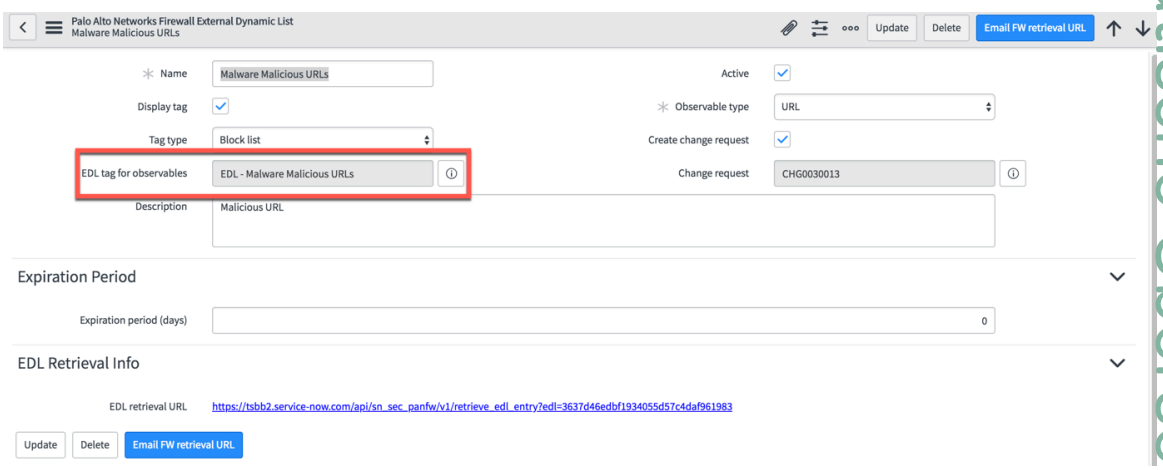
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

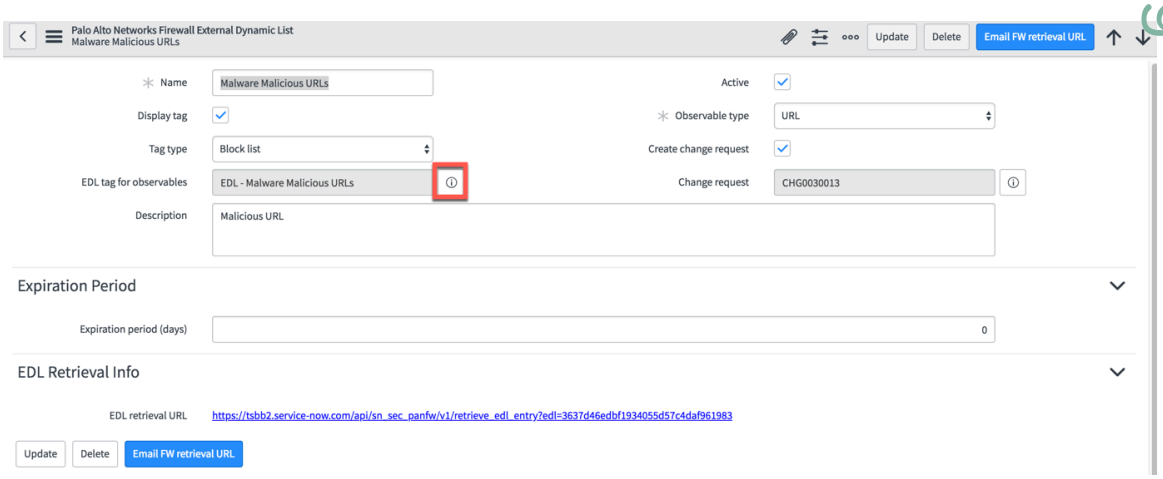
1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **EDL-Firewallkonfiguration**.




2. Klicken Sie auf ein Element in der Spalte **Name**, um es zu öffnen
   Der EDL-Datensatz wird angezeigt. Standardmäßig ist der Name des Sicherheits-Tags derselbe Wert, den Sie im Feld **Name** der EDL eingegeben haben, als Sie sie erstellt haben. Standardmäßig enthält der Name auch ein *EDL* -Präfix, z. B. „EDL – Malware Malicious URLs“.



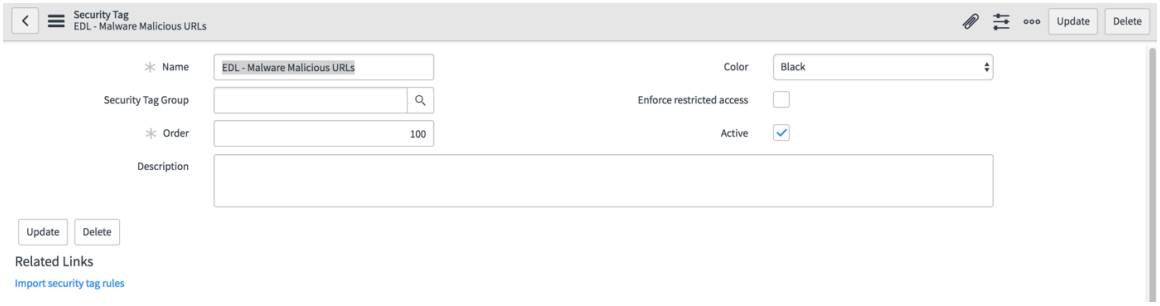

3. Klicken Sie auf das Informationssymbol ( ) neben dem **EDL-Tag für erkennbare Elemente und** dann **auf Datensatz öffnen**.



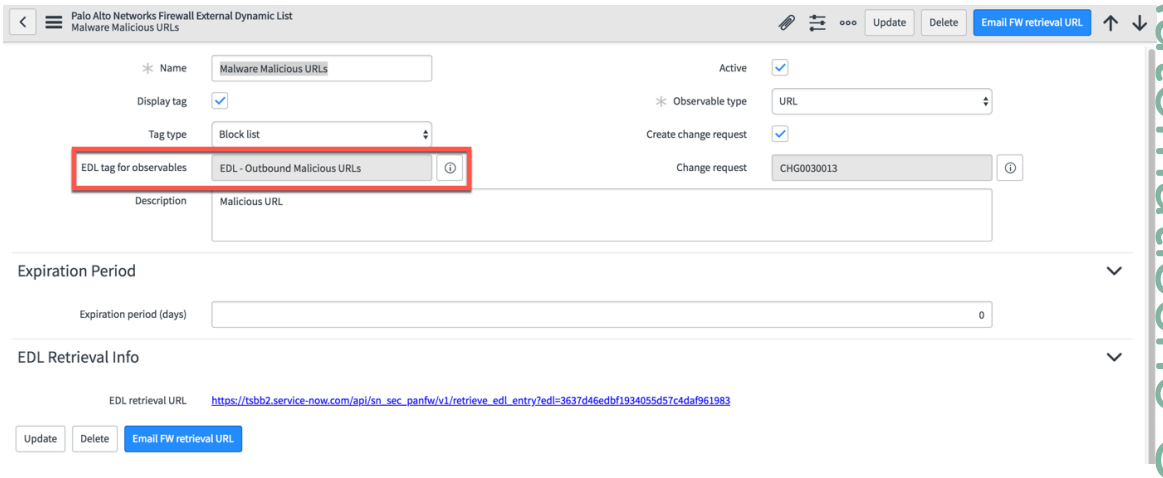

   Das Sicherheits-Tag-Formular wird angezeigt.

Automatische Übersetzung

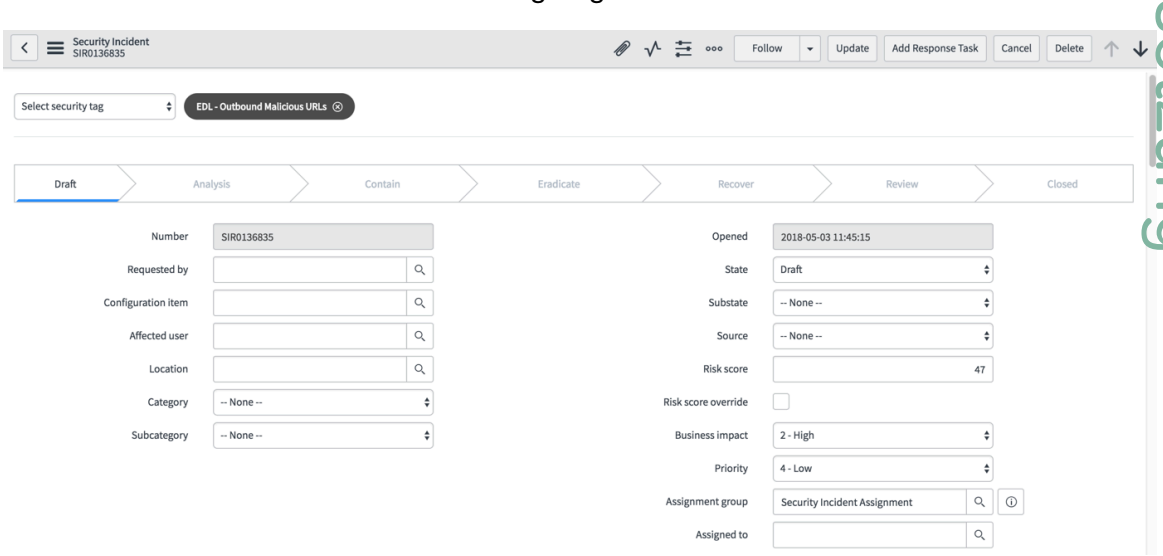
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Ändern Sie im Feld **Name** den Sicherheits-Tag-Namen, und klicken Sie auf **Aktualisieren**.
   Der aktualisierte EDL-Datensatz wird mit dem geänderten Tag-Namen angezeigt. Im folgenden Beispiel wurde dem Tag-Namen Ausgehend hinzugefügt. Behalten Sie das EDL -Präfix in Ihrem neuen Tag-Namen bei, damit Sie leichter erkennen können, dass das Tag der Palo Alto Networks Next-Generation Firewall -Integration zugeordnet ist.




Die Sicherheits-Tags werden für jeden erkennbaren Typ (IP, URL, Domäne) im Security Incident-Datensatz und im Datensatz des erkennbaren Elements angezeigt, jedes Mal, wenn das erkennbare Element einer EDL hinzugefügt wird.




Wenn ein erkennbares Element bereits einer EDL hinzugefügt wurde und ein Sicherheits-Tag für einen Security Incident für dieses erkennbare Element angezeigt wird, wird das EDL-Sicherheits-Tag auch automatisch in allen nachfolgenden Security Incident-Datensätzen angezeigt, die erstellt werden. Diese Duplizierung teilt Ihnen mit, dass

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sich das erkennbare Element bereits in einer Sperrliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In diesem Fall weist kein Sicherheits-Tag darauf hin, dass das Ablaufdatum des erkennbaren Elements möglicherweise abgelaufen ist oder das erkennbare Element für eine EDL deaktiviert wurde.

### Palo Alto Networks Next-Generation Firewall deinstallieren

Wenn Sie Palo Alto Networks Next-Generation Firewall aus Ihrer Instanz von Now Platform deinstallieren und alle Reste aus der Integration entfernen möchten, finden Sie auf der Dokumentationswebsite von ServiceNow Anweisungen zum Deinstallieren von Anwendungen.

#### Vorbereitungen

Erforderliche Rolle: Systemadministrator (admin)

Siehe Anwendungen deinstallieren auf der ServiceNow-Website mit Produktdokumentation .

## Integration „PhishTank“

PhishTank ist ein Community-basiertes Phishing-Verifizierungssystem, in dem Benutzer mutmaßliche Bedrohungen einreichen und andere Benutzer im System darüber abstimmen, ob die Phishing-Bedrohungen berechtigt sind. Bei Integration mit dem Produkt Now Platform Security Operations bieten die Threat Intelligence-Ergebnisse Analysten zusätzliche Einblicke in Phishing-bezogene Security Incidents oder Untersuchungen.

Die PhishTank -Integration führt Suchen nach URLs potenzieller Phishing-Websites durch.

Der Workflow sucht nach neuen erkennbaren Elementen, sobald sie in Security Incidents eintreffen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Als böswillig erkannte erkennbare Elemente werden mit Tags versehen.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von Now Platform®kompatibel.

### PhishTank installieren und konfigurieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendung PhishTank ordnungsgemäß in Now Platform Security Operationsintegriert wird.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Now Platform Rollen für Ihre Instanz zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Systemadministrator (admin) installiert die App und weist die Rolle Security Incident Administrator (sn_si.admin) zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| | • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations. |
| Rufen Sie einen API-Schlüssel ab. | Besuchen Sie die Website PhishTank, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: PhishTank-Website . |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Anforderungen für Madrid und spätere Releases<br><br>Für das Madrid-Release und spätere Familien-Releases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

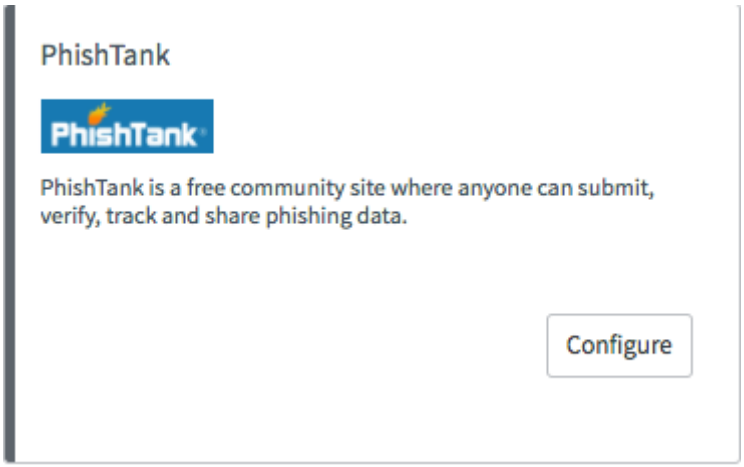
Erforderliche Rolle: admin



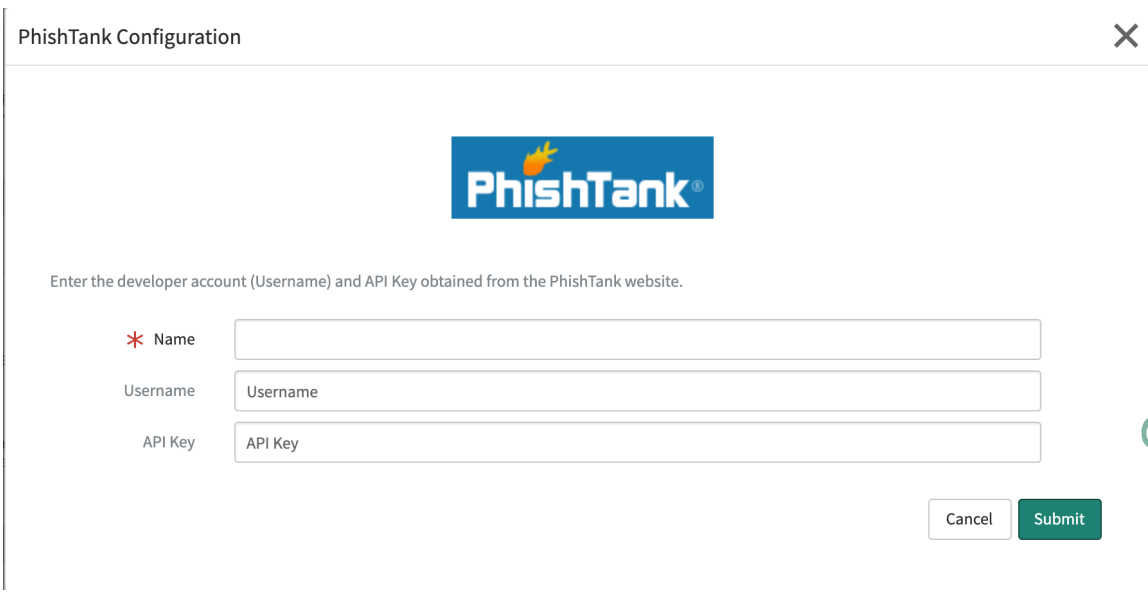
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel PhishTank.
3. Klicken Sie auf **Konfigurieren**.




4. Geben Sie im Dialogfeld „ **PhishTank-Konfiguration** “ den Namen der Konfiguration, den Benutzernamen (in PhishTank erstellter Entwickleraccount) und den API-Schlüssel ein, den Sie von der Website PhishTank erhalten haben, und klicken Sie auf **Absenden**.




5. Vergewissern Sie sich, dass die Konfiguration erfolgreich war.
   Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird.

**Trouble?**

Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel PhishTank möglicherweise ungültig.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Überprüfen Sie die erwarteten Ergebnisse für PhishTank

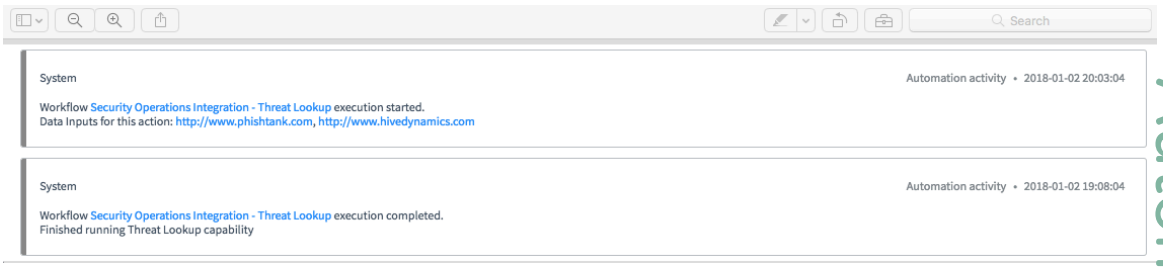
Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchergebnisse werden auf der Registerkarte Ergebnisse der Bedrohungssuche am unteren Rand des Security Incident-Datensatzes angezeigt.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Prozedur

1. Öffnen Sie das Security Incident-Formular, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

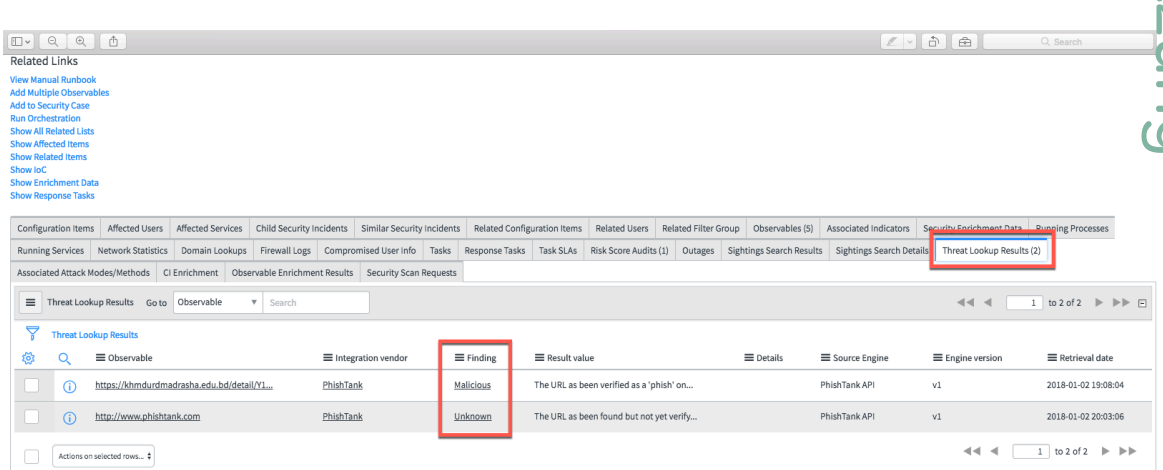



   Nachdem die Anwendung konfiguriert wurde, wird der Workflow automatisch bei der Incident-Erstellung gestartet. Der Ausführungs- und Abschlussstatus der Suche wird dann in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweisen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.

   **Hinweis:**
   Die Abbildungen in den folgenden Schritten werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der rechten oberen Ecke des Bannerframes auf das Zahnradsymbol für Einstellungen. Klicken Sie im angezeigten Dialogfeld „ **Systemeinstellungen** “ auf **Formulare**, und überprüfen Sie, ob **Formulare** mit Registerkarten und **Mit dem Formular** ausgewählt sind.



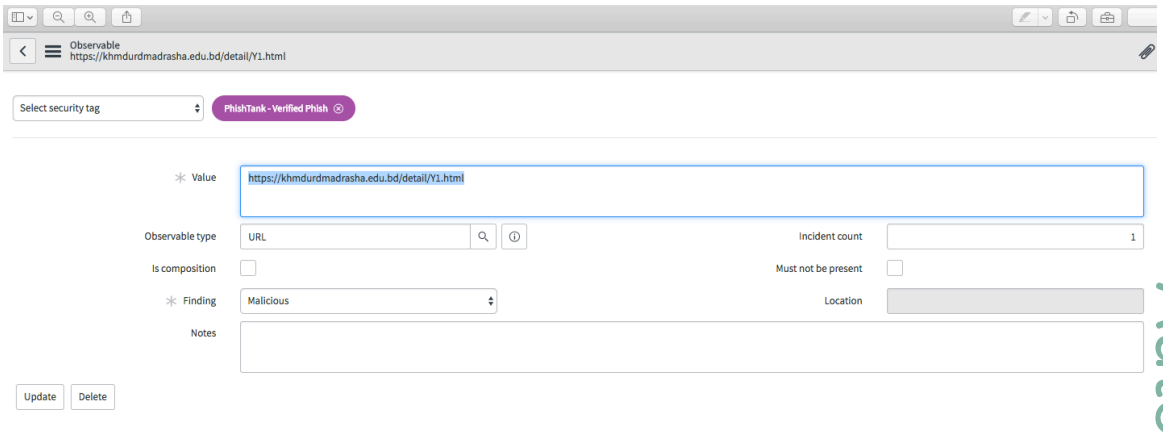

   Auf der Registerkarte **Ergebnisse der Bedrohungssuche** am unteren Rand des Security Incident-Datensatzes werden die Suchergebnisse angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der **Spalte** „Ergebnis“ wird für Datensätze, die nicht als schädlich eingestuft wurden, Unbekannt angezeigt. Für Ergebnisse, die mit „böswillig“ übereinstimmen, wird „Böswillig “ in der **Spalte** „Ergebnis“ angezeigt.

4. **Klicken** Sie in der Spalte Erkennbares Element auf ein erkennbares Element, um einen Datensatz zu öffnen und weitere Informationen anzuzeigen.

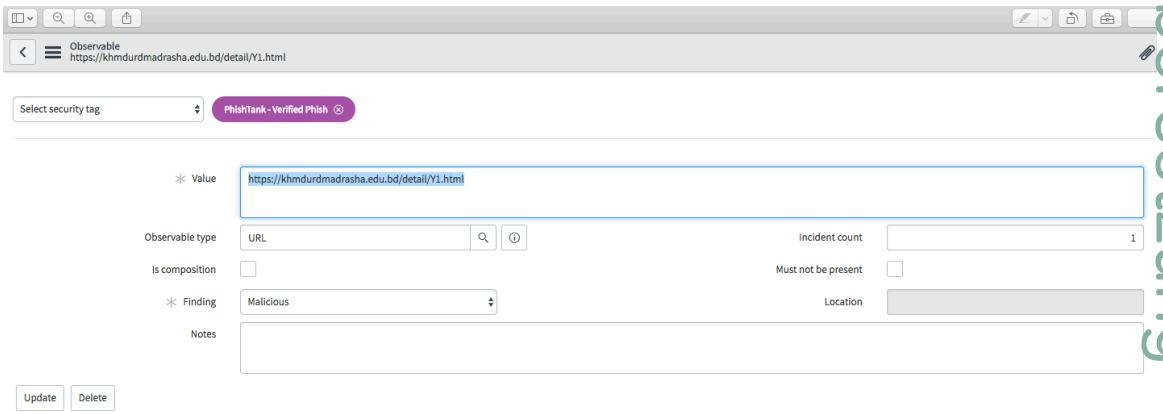



Im Datensatz des erkennbaren Elements wird für Suchvorgänge, die mit „böswillig“ übereinstimmen, „Böswillig “ im Feld „Ergebnis“ **angezeigt**. Das erkennbare Element ist mit der Quelle Threat Intelligence gekennzeichnet, die es als schädlich befunden hat, in diesem Fall die Anwendung PhishTank.

5. Um Rohdaten anzuzeigen, navigieren Sie zurück zum Security Incident und klicken auf das blaue Informationssymbol neben einem erkennbaren Element.



6. Klicken Sie im angezeigten Fenster auf **Datensatz öffnen**.




Der von der API erstellte Link und das Feld „ **Suche** “ werden mit den Ergebnissen angezeigt.

### Trouble?

Wenn auf der Registerkarte Ergebnisse der **Bedrohungssuche keine Ergebnisse** angezeigt werden, stellen Sie sicher, dass das erkennbare Element ein Typ ist, der für die Suche von der Integration unterstützt wird.

## (Optional) Hängen Sie ein erkennbares Element für manuell an PhishTank

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie hängen erkennbare Elemente manuell an, wenn Sie eine Bedrohungssuche für erkennbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

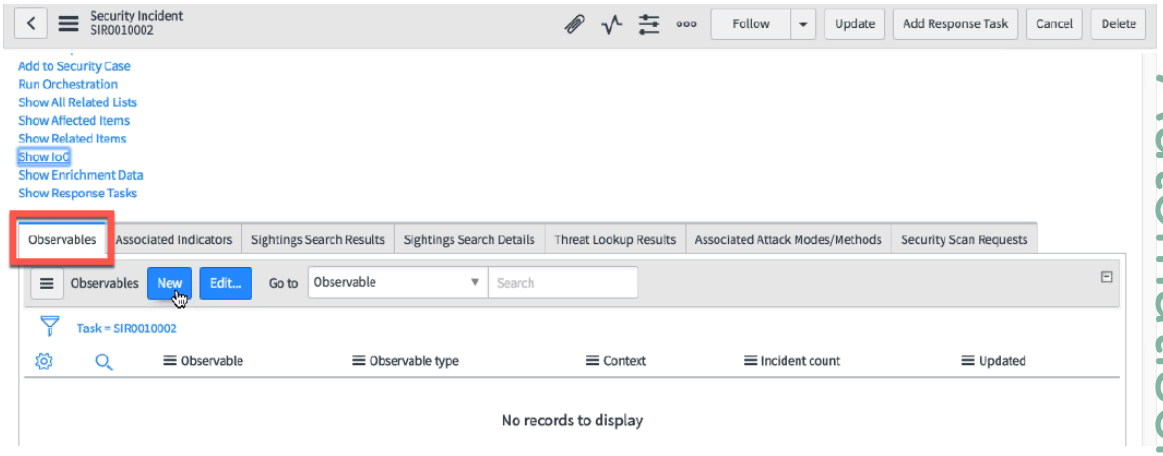
durchführen möchten, die beim ersten Event-Auslöser nicht an einen Security Incident angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Prozedur

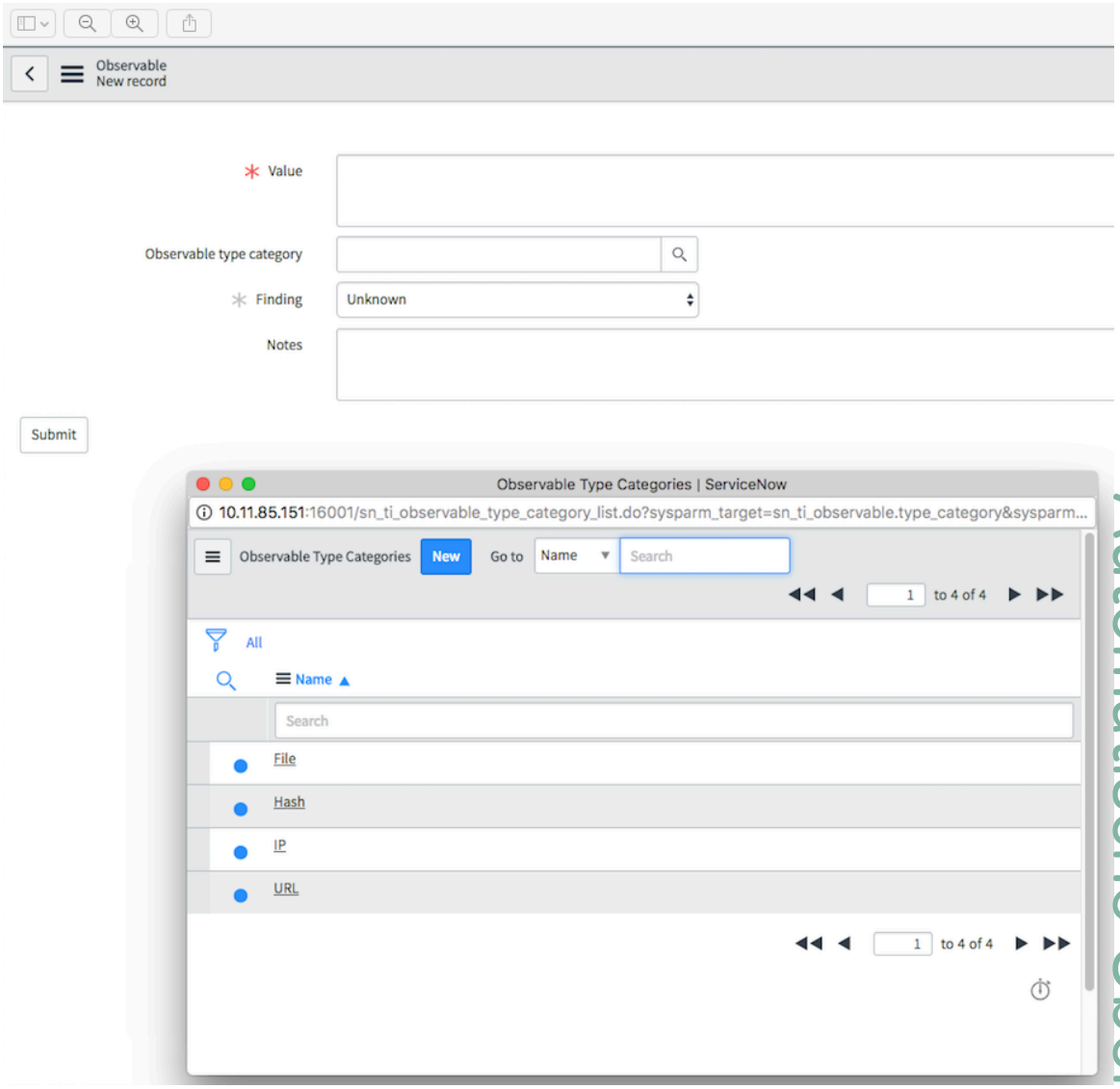
1. Navigieren Sie zu Ihrem offenen Security Incident.
2. Klicken Sie im geöffneten Security Incident-Datensatz auf den Link **IoC**anzeigen unter **Zugehörige Links**, um die Registerkarte **„Erkennbare** Elemente“ anzuzeigen.



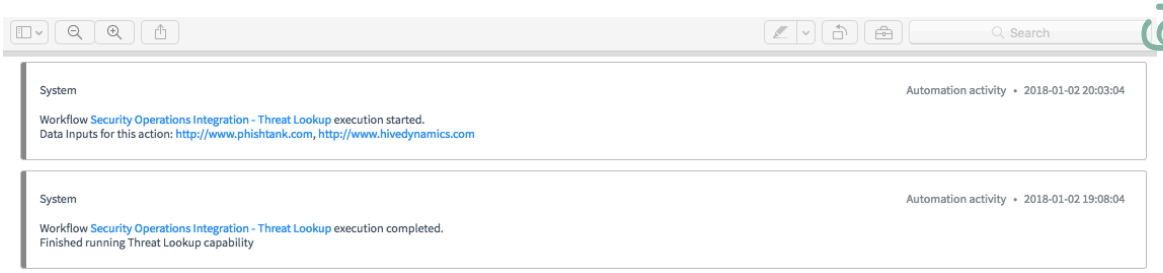

3. Klicken Sie auf **Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** eine URL ein.
5. Klicken Sie auf das **Suchsymbol**, und klicken Sie im Dialogfeld „Kategorien erkennbarer Typen“ in der Liste auf **URL**, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



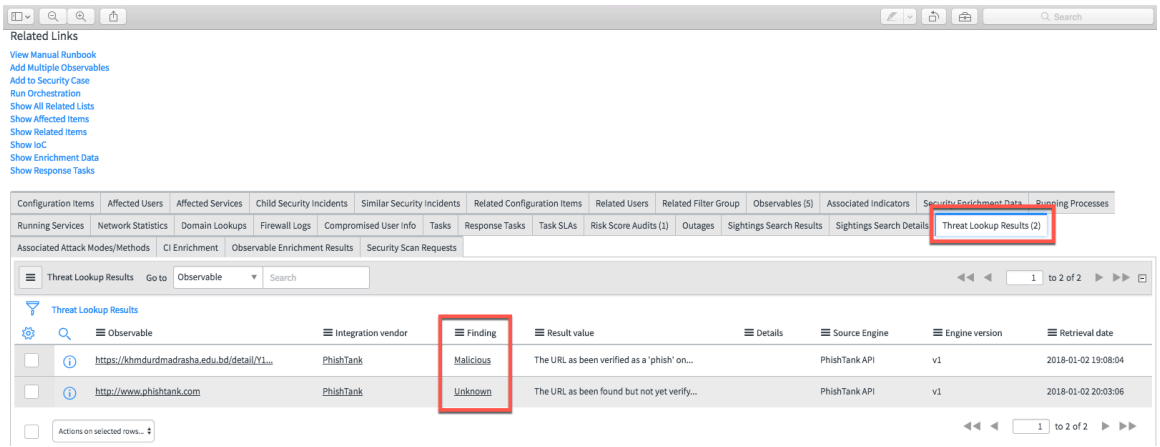

6. Klicken Sie auf **Absenden**.
   Der Workflow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ im Security Incident-Datensatz angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.




8. Klicken Sie unten im Security Incident auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.
9. Klicken Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche**, um die Ergebnisse anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




10. **Klicken** Sie in der Spalte „Erkennbares Element“ auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.



11. Klicken Sie im angezeigten Dialogfeld auf **Datensatz öffnen**.

**Trouble?**
Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweisen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

## Integration „Reverse Whois“

Reverse Whois ist ein Service, der Suchvorgänge in Domänennamen durchführt, die von Einzelpersonen oder Organisationen registriert wurden.

Führen Sie Domänensuchen mit Suchbegriffen in erkennbaren Elementen durch, die Sie an einen Security Incident anhängen. Die Reverse Whois -API durchsucht Domänendatensätze basierend auf den von Ihnen eingegebenen Suchbegriffen und gibt alle Datensätze zurück, die diesen Begriffen entsprechen.

Analysten verwenden diese Integration manchmal zusammen mit der Whois -Integration für Security Incident-Forschung. Die Whois -Integration bietet zusätzliche Ergänzungsinformationen basierend auf den Domänensuchen aus der Reverse Whois -Integration.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von Now Platform®kompatibel.

### Reverse Whois installieren und konfigurieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendung Reverse Whois ordnungsgemäß in das Produkt Security Operations ] integriert wird.

### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie die erforderlichen ServiceNow Rollen zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Systemadministrator (admin) installiert die App und weist die Rolle Security Incident Administrator (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration. Der Security Incident-Administrator weist auch die Rolle „Security Incident-Analyst“ (sn_si.analyst) zu.<br>• Der Security Incident Analyst (sn_si.analyst) führt Domänensuchen mit Reverse Whois durch und analysiert und bearbeitet Security Incidents. |
| Rufen Sie einen API-Schlüssel ab. | Besuchen Sie die WhoisXML-API-Website, um Informationen zu API-Schlüsseln zu erhalten und ein Konto zu erstellen: WhoisXML-API-Website . Die Konfiguration erfordert die Eingabe der API-Schlüssel. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Anforderungen für Madrid und spätere Releases<br>Für das Madrid-Release und spätere Familien-Releases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br>**1.** Security Incident Response<br>**2.** Security Integration Framework |



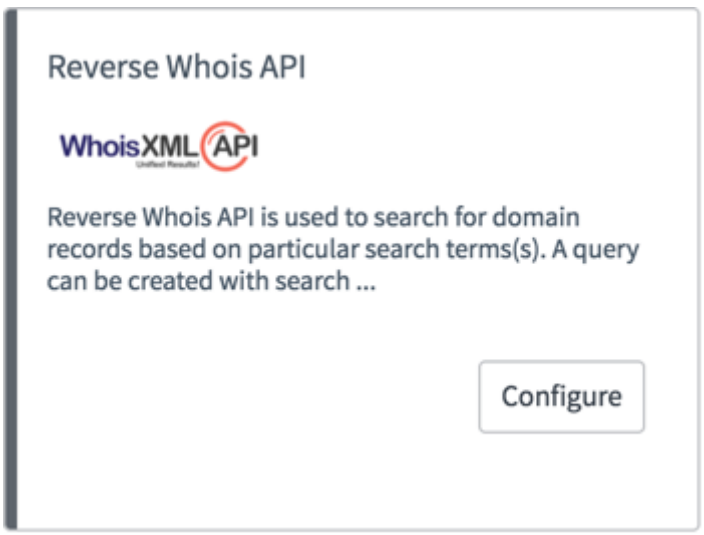
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| | **3.** Security Support Common<br>**4.** Security Support Orchestration<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

Erforderliche Rolle: admin

### Prozedur

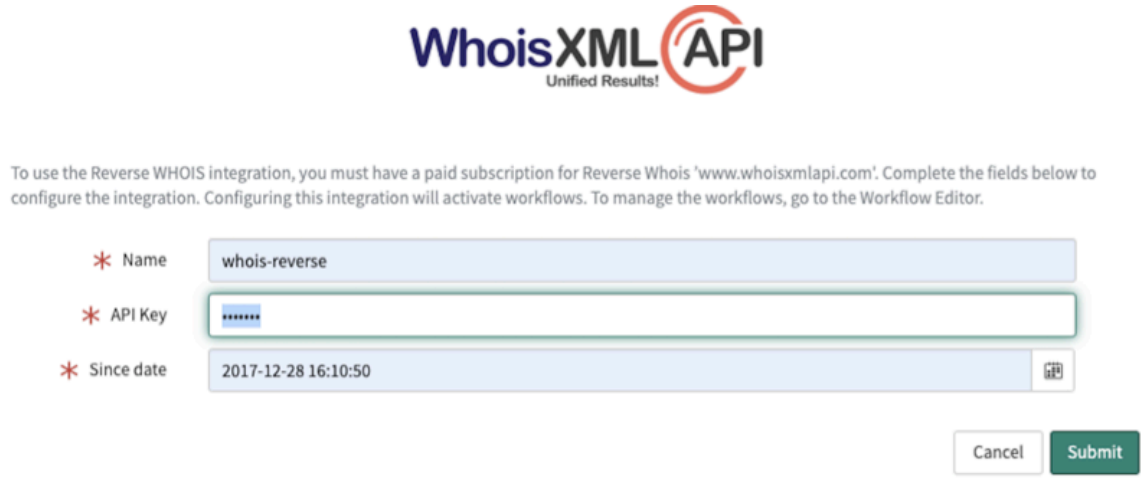
1. Wenn Sie die Anwendung Reverse Whois bereits installiert und konfiguriert haben, führen Sie die folgenden Schritte aus:
   a. Löschen Sie die vorhandene Konfiguration.
   b. Installieren Sie und erstellen Sie eine neue Konfiguration mit dem API-Schlüssel, den Sie erhalten haben.
2. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
3. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die Kachel API Reverse Whois.
4. Klicken Sie auf **Konfigurieren**.




5. Geben Sie im Dialogfeld **Reverse Whois API-Konfiguration** den API-Schlüssel ein, den Sie von der Whois XML API-Website erhalten haben.
6. Wählen Sie eine Option in der folgenden Tabelle aus, um Domänensuchen nach Ihren Suchbegriffen zu filtern.
   Diese Konfigurationseinstellungen bleiben gespeichert, bis Sie sie ändern, und gelten für alle Reverse Whois API-Suchen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Klicken Sie auf **Absenden**.
   Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird.

**Trouble?**
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

**Fehlermeldung**

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

### (Optional) Installieren und konfigurieren Sie Whois

Installieren Sie das Plugin Whois, um zusätzliche Ergänzungsinformationen für Ihre Domänensuchen über die API Reverse Whois ] bereitzustellen. Diese Suche stellt zusätzliche Ergänzungsdaten für die Domäne bereit, z. B. das Registrierungsdatum, den Namen der Registrierungsstelle und das Herkunftsland.

### Vorbereitungen

1. Wenn Sie keine Berechtigung für die Anwendung angefordert haben, finden Sie weitere Informationen zur Anwendung Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations abWhois aus dem ServiceNow Store unter [].
2. Rufen Sie Anmeldeinformationen für den API-Schlüssel Whois von der Produktwebsite ab: WHOIS-API-Website .

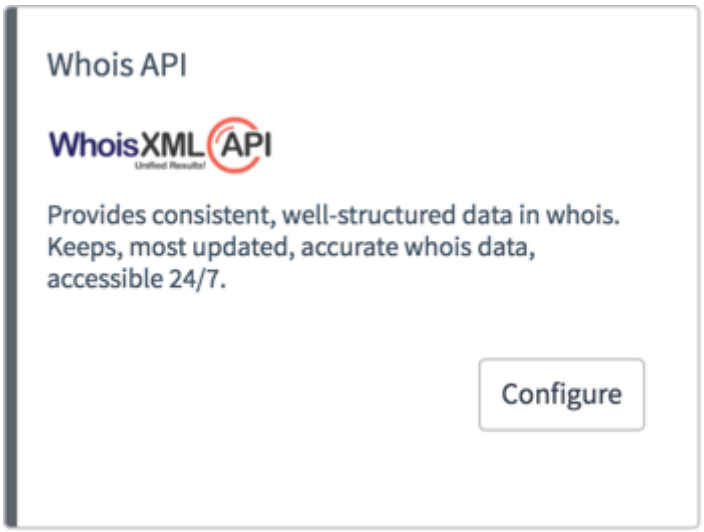
Erforderliche Rolle: admin

### Prozedur

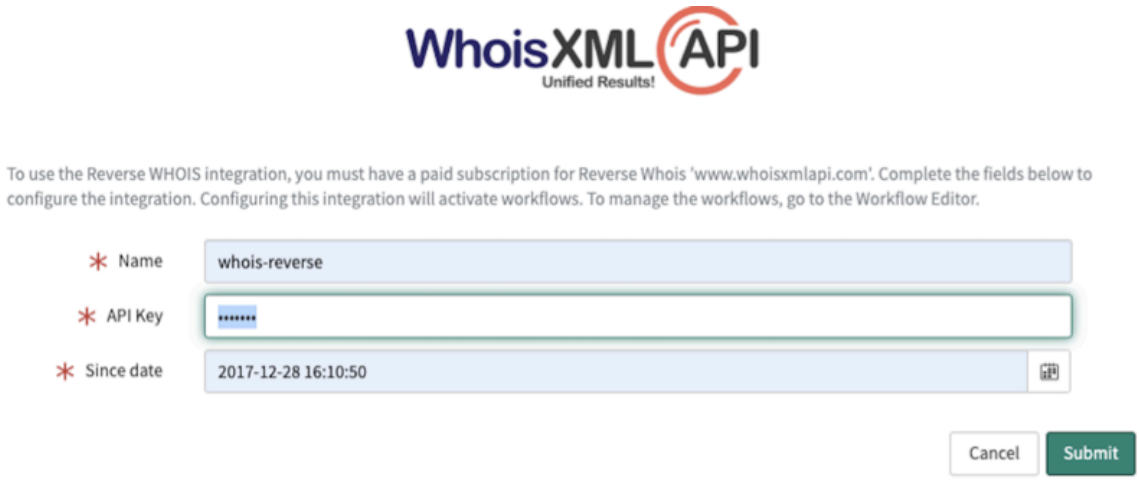
1. Wenn Sie die Anwendung nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die Kachel API Whois.
3. Klicken Sie auf **Konfigurieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



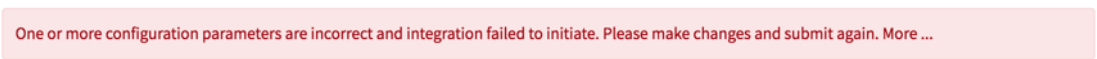

4. Geben Sie im Dialogfeld **Whois-API-Konfiguration** den API-Schlüssel ein, den Sie von der Produktwebsite erhalten haben.




5. Klicken Sie auf **Absenden**.
   Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird. Sie können jetzt Ergänzungssuchen für die Domänen ausführen, die von der Reverse Whois -Integration zurückgegeben werden.

**Trouble?**
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

**Problembehandlung**




## Initiieren Sie die Suche nach Reverse Whois

Initiieren Sie Domänensuchen mit Suchbegriffen in erkennbaren Elementen, die Sie manuell an einen Security Incident-Datensatz anhängen.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

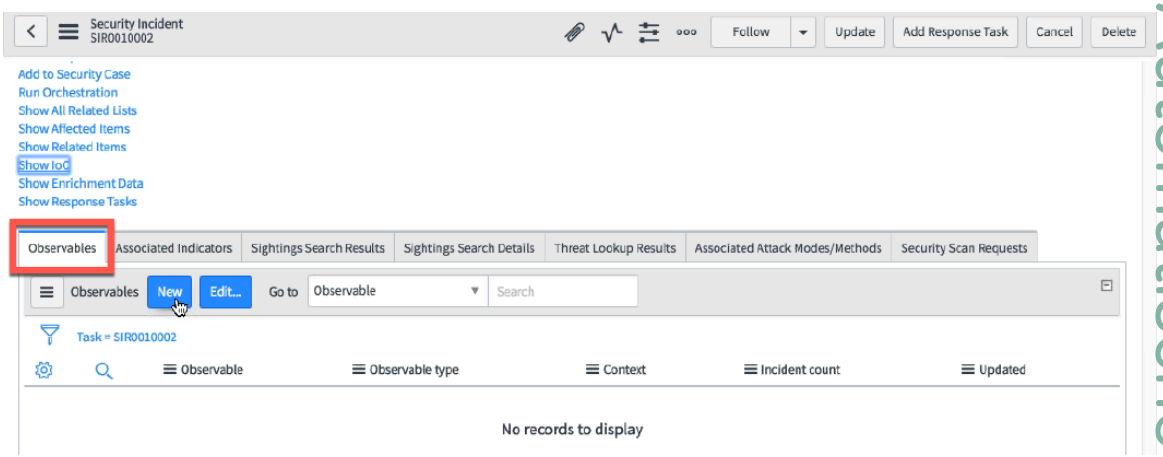
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn nicht geöffnet, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie den Security Incident, an dem Sie arbeiten.
2. Klicken Sie unten im Datensatz auf den zugehörigen Link **IoC** anzeigen, um die Registerkarte „Erkennbare Elemente“ anzuzeigen.

### Hinweis:

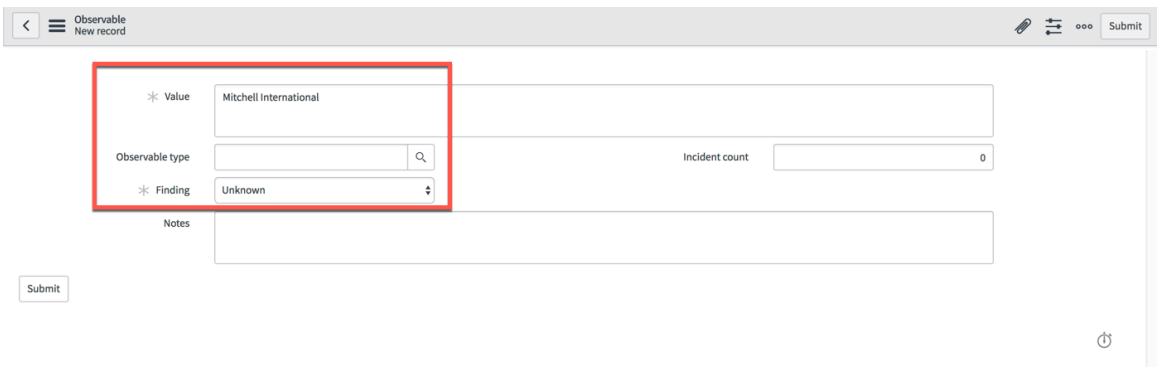
Die Abbildungen in den folgenden Schritten werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt. Wenn beim Security Incident keine Registerkarten angezeigt werden, klicken Sie in der oberen rechten Ecke des **Bannerframes** auf das Zahnradsymbol für Einstellungen. Klicken Sie im angezeigten Dialogfeld „ **Systemeinstellungen** “ auf **Formulare**, und überprüfen Sie, ob **Formulare** mit Registerkarten und **Mit dem Formular** ausgewählt sind.




3. Klicken Sie auf der Registerkarte Erkennbare Elemente auf **Neu**.
4. Füllen Sie die Felder aus.

### Pflichtfelder im neuen Datensatz

| Feld | Beschreibung |
|---|---|
| Wert | Eindeutiger Suchbegriff für eine Domäne. |
| Erkennbarer Typ | Dieses Feld wird automatisch gelöscht. |
| Ergebnis | Dieses Feld wird automatisch auf **Unbekannt**gesetzt. |




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Sie kehren zum Security Incident-Datensatz zurück, und der Workflow initiiert die Suche.

## Nächste Maßnahme

Überprüfen Sie die Suchergebnisse für den Security Incident. Weitere Informationen finden Sie unter Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois.

### Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

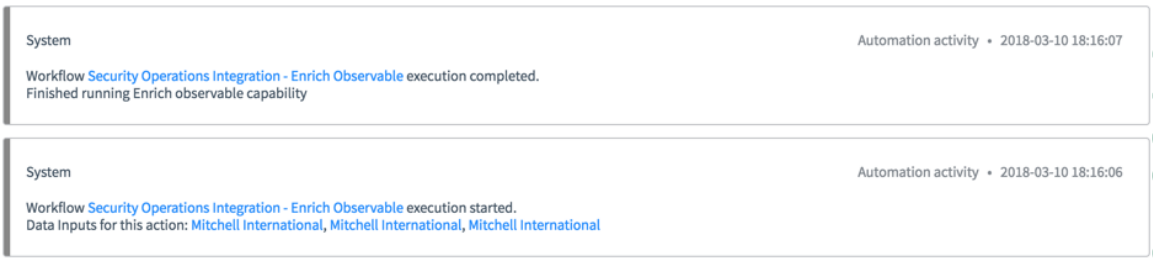
Die Ergebnisse der Anreicherung werden auf der Registerkarte **ReverseWhois-Domänen** am unteren Rand des Security Incident-Datensatzes angezeigt. Suchen Sie die Suchergebnisse, um sicherzustellen, dass die Suche erfolgreich ausgeführt wurde.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

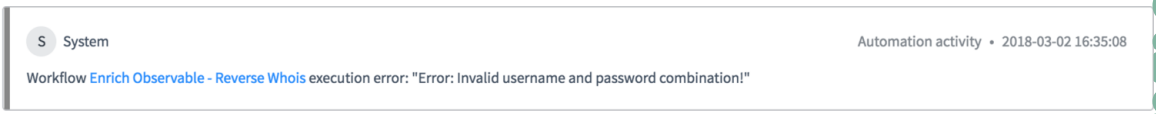
## Prozedur

1. Wenn noch nicht geöffnet, navigieren Sie zu **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, an dem Sie arbeiten.




   Nachdem die Anwendung konfiguriert wurde und Sie ein erkennbares Element angehängt haben, wird der Workflow automatisch gestartet. Die Arbeitsnotizen im Security Incident-Datensatz zeigen die Ausführung und den Abschlussstatus der Suche an.

2. Wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde, finden Sie in den Arbeitsnotizen weitere Informationen zum weiteren Vorgehen.

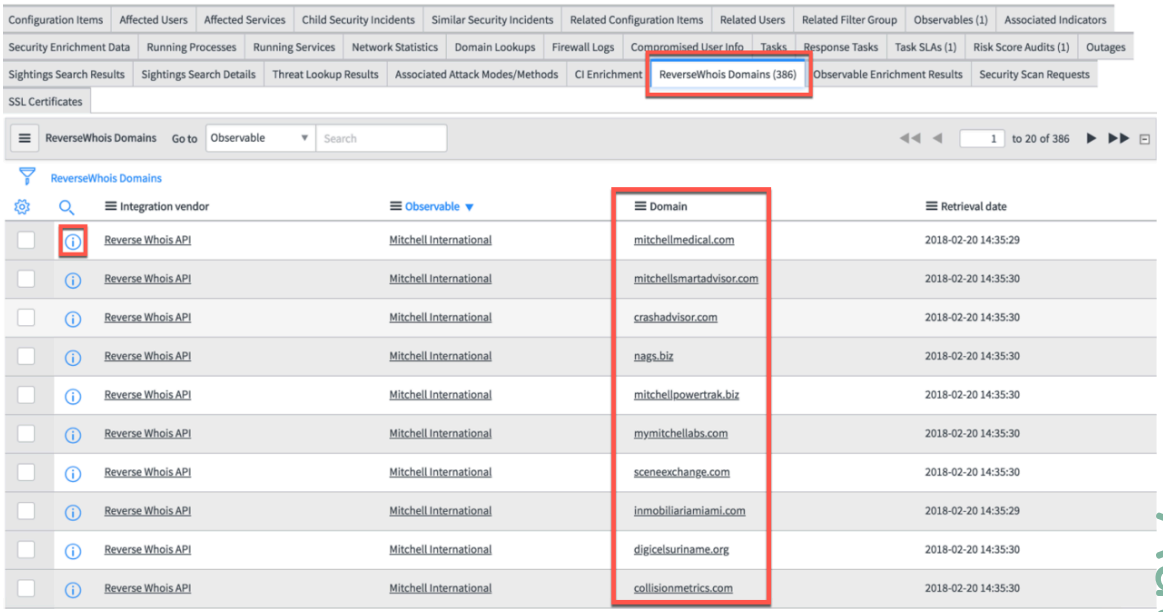



3. Navigieren Sie zum Ende des Security Incident, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.

**Hinweis:**
Für die in der folgenden Abbildung gezeigten gefilterten Suchergebnisse wurden die Konfigurationseinstellungen in der API-Konfigurationskachel Reverse Whois mit **der Eingabe 1991-06-01** im Datumsfeld **Seit** gespeichert.

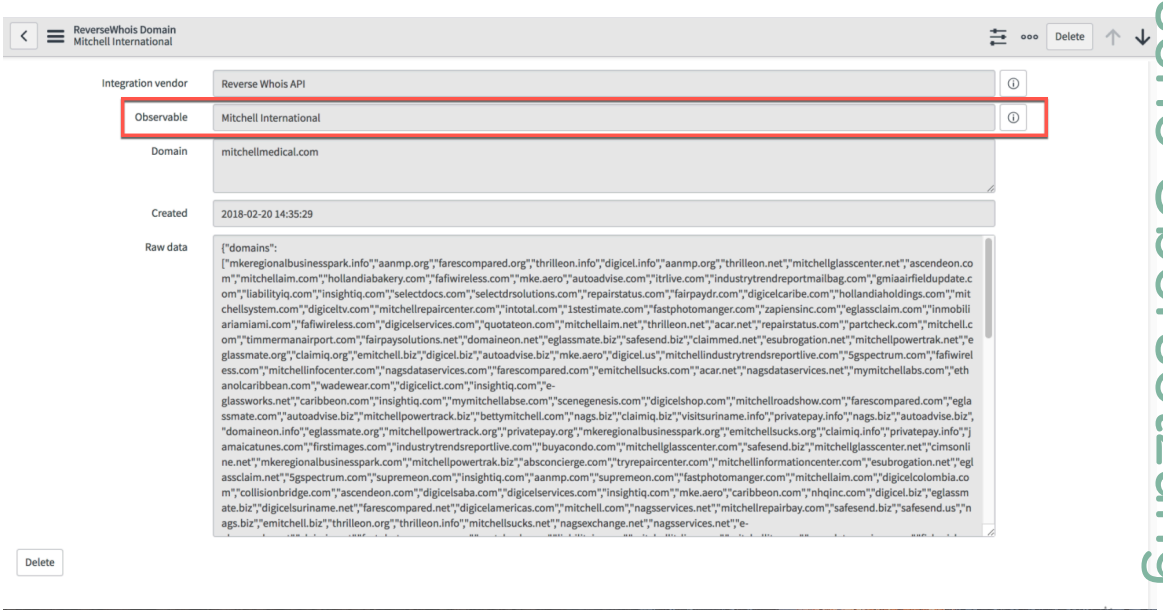
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die Ergänzungsergebnisse werden auf der Registerkarte **ReverseWhois-Domänen** angezeigt. Die aktiven Domänen für dieses erkennbare Element werden in der Spalte **Domäne** angezeigt.

4. Klicken Sie auf das blaue Informationssymbol neben einem Element, und klicken Sie dann im angezeigten Dialogfeld auf **Datensatz öffnen**.

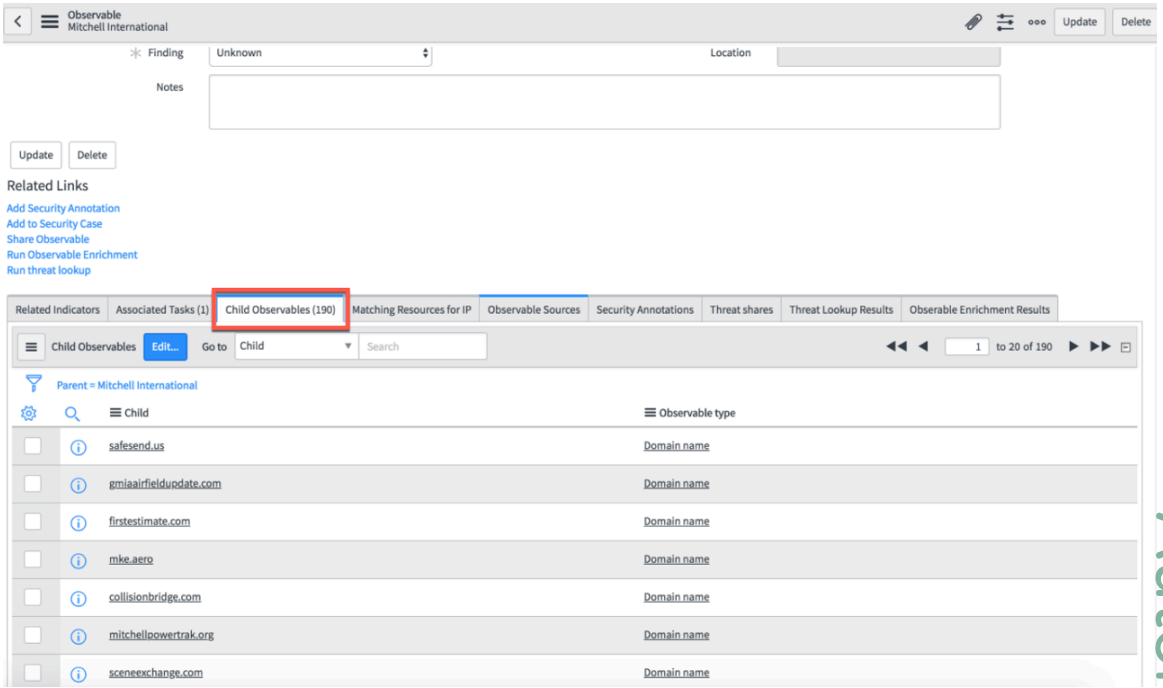



Der Datensatz wird mit Ergänzungsdetails angezeigt, einschließlich der Rohdaten.

5. Navigieren Sie zurück zum Security Incident, und klicken Sie bei ausgewählter Registerkarte **ReverseWhois-Domänen** in der Spalte Erkennbares Element auf ein erkennbares **Element**, um einen Datensatz zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die untergeordneten erkennbaren Elemente werden auf der Registerkarte **Untergeordnete** erkennbare Elemente im Datensatz „Erkennbares Element“ angezeigt. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn die Anwendung Reverse Whois Domänen zurückgegeben hat.

### Trouble?

Wenn die Suche nicht erfolgreich abgeschlossen wird, überprüfen Sie, ob die von Ihnen eingegebenen Suchbegriffe von der Integration unterstützt werden. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen.

### Nächste Maßnahme

Um weitere Ergänzungsdaten in den Domänensuchergebnissen zu erhalten, können Sie die Integration Whois ausführen, um Ergänzungssuchen für die von der Integration Reverse Whois zurückgegebenen untergeordneten erkennbaren Elemente durchzuführen. Diese Ergänzungsdaten zu den untergeordneten erkennbaren Elementen enthalten Informationen zum Registrierungsdatum, zum Namen des Registrars und zum Herkunftsland.

## (Optional) Führen Sie eine Ergänzungssuche aus, und überprüfen Sie die erwarteten Ergebnisse für Whois

Führen Sie die Whois -Integration aus, um Ergänzungssuchen in den Domänen durchzuführen, die von der Reverse Whois -Integration zurückgegeben werden.

### Vorbereitungen

Vergewissern Sie sich, dass Sie die Plugins Reverse Whois und Whois installiert und konfiguriert haben. Führen Sie diese Schritte erst aus, nachdem Sie die Domänensuche mit dem Plugin Reverse Whois erfolgreich ausgeführt haben.

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

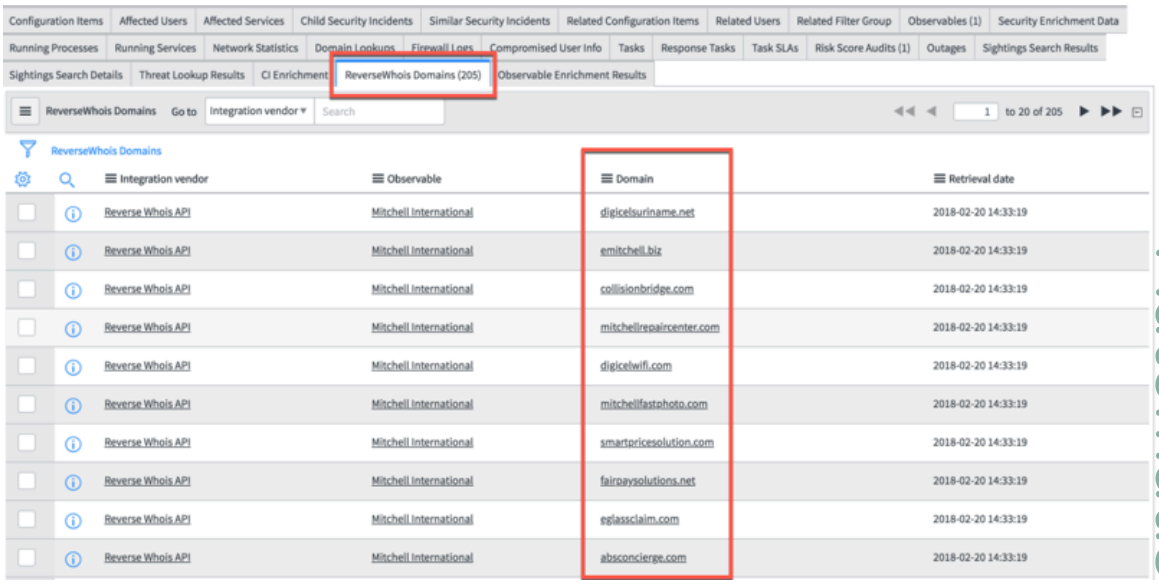
Die Ergebnisse werden auf der Registerkarte **„Anreicherung erkennbarer** Elemente“ im Datensatz „Erkennbares Element“ angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

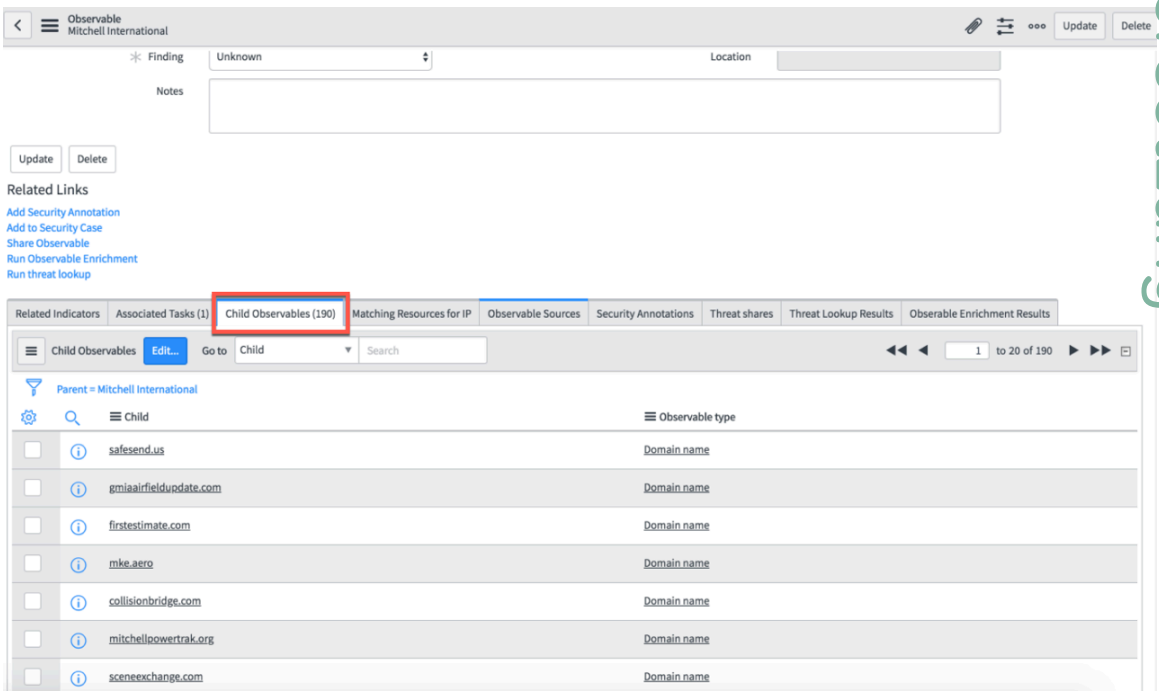
## Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** und suchen Sie den Security Incident, an dem Sie arbeiten und für den die Domänensuche erfolgreich ausgeführt wurde.
2. Öffnen Sie den Datensatz, und klicken Sie auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.
3. Wählen Sie am unteren Rand des Datensatzes die Registerkarte **Reverse Whois Domains** aus.




In der Spalte **Domänen** wird die Liste der zurückgegebenen Domänen angezeigt.

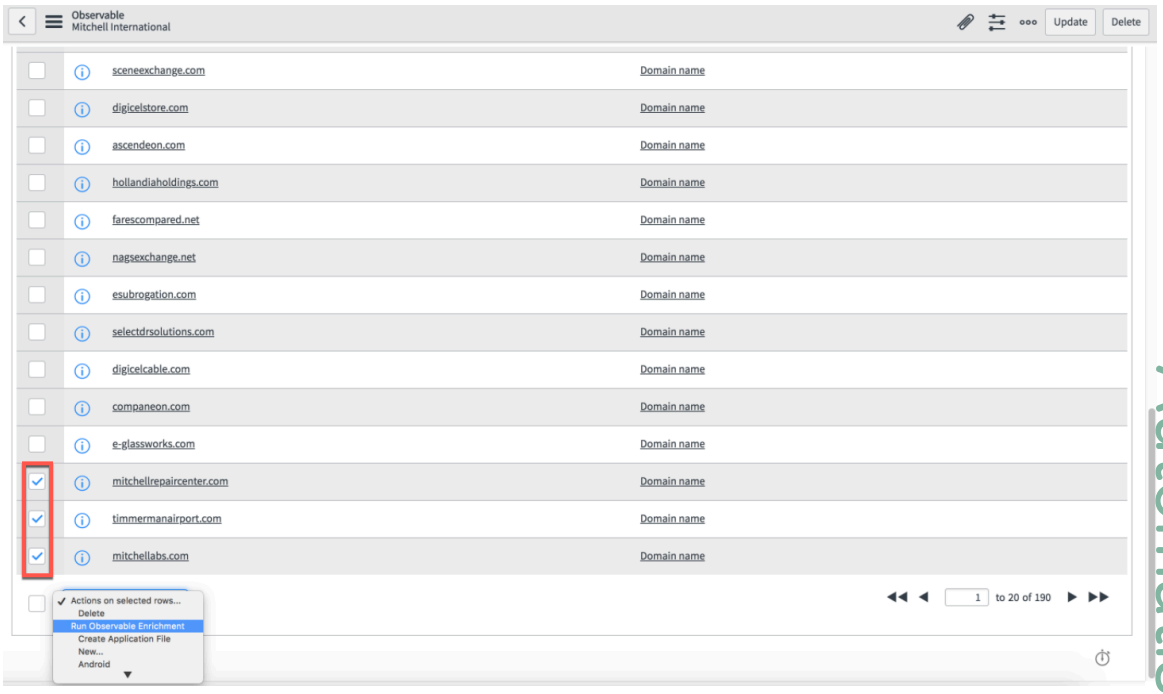
4. **Klicken** Sie in der Spalte Erkennbares Element auf ein erkennbares Element.
   Auf der Registerkarte **Untergeordnete erkennbare** Elemente werden die untergeordneten erkennbaren Elemente angezeigt. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn der erste Scan des erkennbaren Elements durch die Anwendung Reverse Whois Domänen zurückgegeben hat.




Automatische Übersetzung

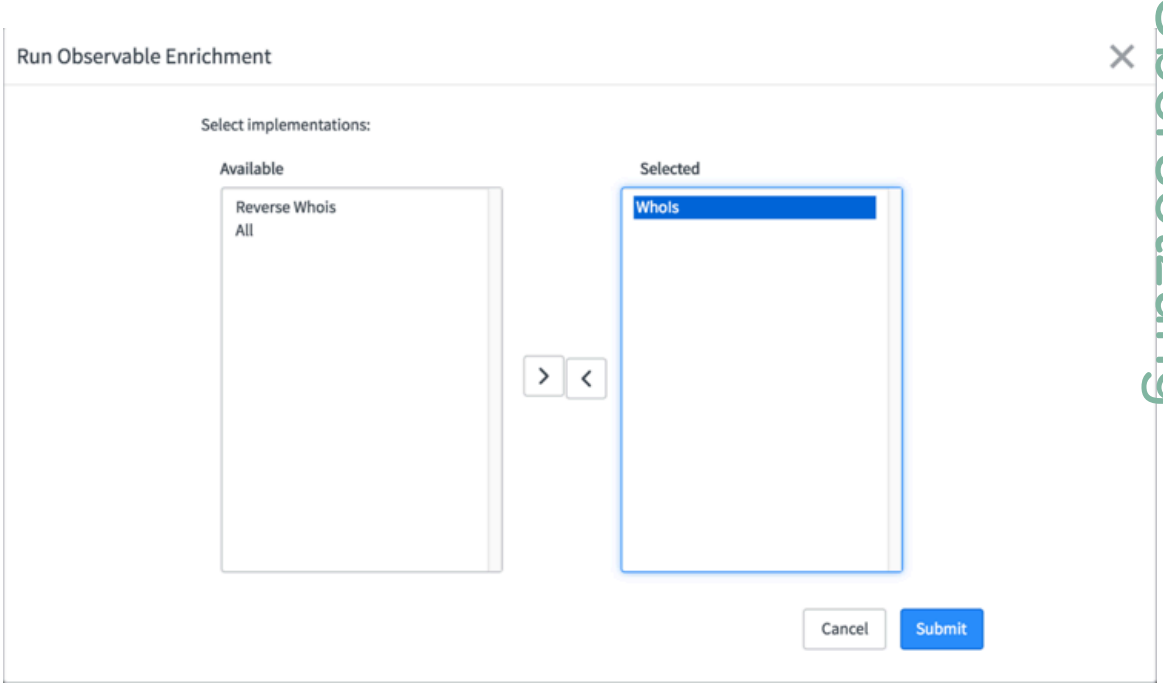
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie die untergeordneten erkennbaren Elemente aus, für die Sie die Ergänzung erkennbarer Elemente ausführen möchten, und wählen Sie in der Auswahlliste **Aktion für ausgewählte Zeilen** die **Option Ergänzung erkennbarer Elemente ausführen**aus.




Das Dialogfeld „ **Anreicherung erkennbarer Elemente** ausführen“ wird angezeigt.

6. Verschieben Sie die Whois -Integration von „ **Verfügbar** “ zu „ **Ausgewählt** “, und klicken Sie auf **Absenden**.

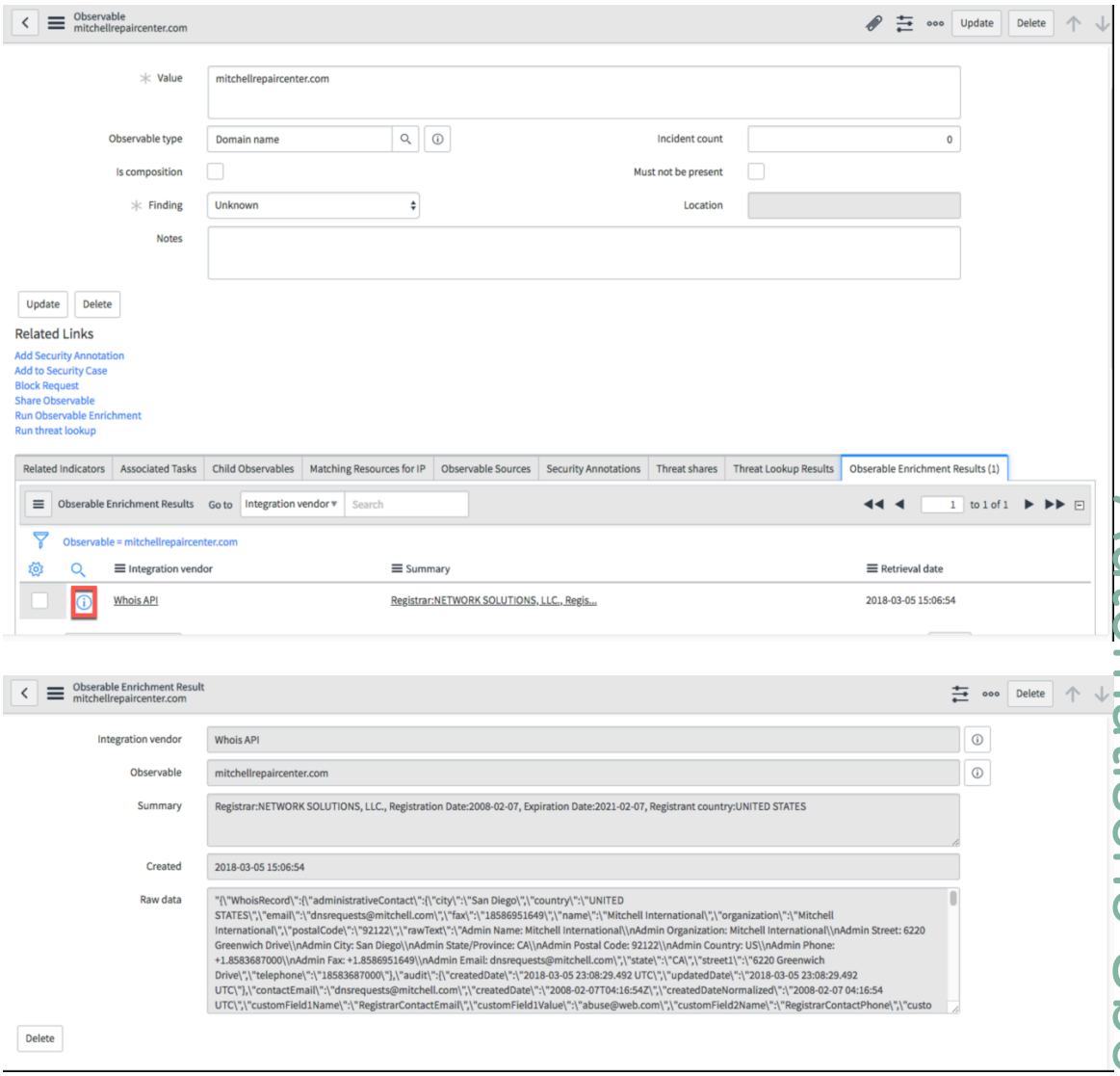



Die Ergebnisse werden auf der Registerkarte **„Anreicherung erkennbarer Elemente“** – Ergebnisse des Datensatzes „Erkennbares Element“ angezeigt.

7. Klicken Sie auf das blaue Informationssymbol und dann im angezeigten Dialogfeld auf **Datensatz öffnen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Weitere Informationen und Rohdaten im Zusammenhang mit der ursprünglichen Domänensuche werden angezeigt, z. B. das Registrierungsdatum, der Name der Registrierungsstelle und das Herkunftsland.

**Trouble?**
Wenn Sie keine untergeordneten erkennbaren Elemente oder Ergänzungsergebnisse finden können, stellen Sie sicher, dass die Reverse Whois -Integration erfolgreich ausgeführt wurde und Domänen zurückgegeben hat. Weitere Informationen finden Sie auch in den Arbeitsnotizen im Datensatz.

**Zugehörige Informationen**

Reverse Whois installieren und konfigurieren

Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

## Integration von RISKIQ und WHOISIQ

Durch die Integration der APIs RISKIQ und WHOISIQ mit dem Produkt Now Platform® Security Operations erhalten Sicherheitsanalysten zusätzliche Ergänzungsdaten und Einblicke in die Gültigkeit von Websites.

Die RISKIQ SSL Certificates-API führt Suchvorgänge für SSL-Zertifikate durch, die Details zur ausstellenden Zertifizierungsstelle, zu Organisationen, die Zertifikate anfordern, zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Entitätszertifikaten, an die ausgestellt werden, und zur Domäne enthalten. SSL-Zertifikatsuchen werden automatisch ausgeführt, wenn Security Incidents erstellt werden.

Die RISKIQ WHOISIQ -API sucht nach anderen erkennbaren Typen wie Domäne, E-Mail, Nameserver, Organisation, Adresse und Telefonnummer. Erkennbare URL- und Domänenelemente werden automatisch erweitert, wenn Security Incidents erstellt werden.

Für die Integration sind die Produkte Security Incident Response und Threat Intelligence erforderlich.

Diese Integration ist mit Rome oder späteren Releases von Now Platform®kompatibel.

### Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

Die RISKIQ API unterstützt die automatische SSL-Zertifikatsuche für erkennbare Elemente wie IP-Adresse, Datei-Hash, Zertifikat-Seriennummer, Domäne und URL. Erkennbare URL- und Domänenelemente werden automatisch mit der WHOISIQ -API angereichert. Für die Ergänzung erkennbarer Elemente für andere Arten von erkennbaren Elementen mit der WHOISIQ -API erstellen Sie erkennbare Elemente und führen Suchvorgänge manuell in der Tabelle „Erkennbare Elemente“ aus.

## Unterstützte erkennbare Elemente

In der folgenden Tabelle sind der Typ der in dieser Integration verwendeten APIs und die von jeder API unterstützten erkennbaren Elemente aufgeführt. Die Tabelle gibt auch an, ob eine Suche automatisch erfolgt, wenn Security Incidents erstellt werden, oder ob die Suche manuell über die Tabelle „Erkennbare Elemente“ ausgeführt wird.

**Unterstützte erkennbare Elemente und Suche**

| API | Unterstützte erkennbare Elemente | Suche (automatisiert oder manuell) |
|---|---|---|
| RISKIQ SSL-Zertifikat-API | • IP-Adresse<br>• Datei-Hash (Zertifikat-Fingerabdruck). In der folgenden Abbildung sehen Sie ein Beispiel für einen Datei-Hash.<br>• Zertifikat-Seriennummer oder Seriennummer. Diese Zeichenfolge ist eine eindeutige ID für die Entität. In der folgenden Abbildung sehen Sie ein Beispiel für eine Zertifikat-Seriennummer.<br>• Domäne (www.site.comoder site.com) | Automatisierte Suche, wenn Incidents erstellt werden.<br><br>Die Ergebnisse werden auf der Registerkarte **SSL-Zertifikate** des Security Incident-Datensatzes angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Unterstützte erkennbare Elemente und Suche (Fortsetzung)**

| API | Unterstützte erkennbare Elemente | Suche (automatisiert oder manuell) |
|---|---|---|
| | • URL<br>**Hinweis:** Automatische Scans werden für das URL-Format mit dem Protokoll `https://` ausgeführt, z. B. `https://example.com/index.html` | |
| RISKIQ WHOISIQ -API | • Domäne<br>• URL | Automatisierte Suche, wenn Incidents erstellt werden.<br>Die Ergebnisse werden auf der Registerkarte **„Anreicherung erkennbarer Elemente** – Ergebnisse“ im Security Incident-Datensatz angezeigt. |
| RISKIQ WHOISIQ -API | • E-Mail-Adresse<br>• Organisationsname<br>• Telefonnummer<br>• Postanschrift | Die manuelle Suche wird über die Tabelle „Erkennbare Elemente“ ausgeführt.<br>Die Ergebnisse werden auf der Registerkarte **„Anreicherung erkennbarer** Elemente“ im Datensatz „Erkennbares Element“ angezeigt. |

## Beispiel für einen Datei-Hash und eine Zertifikat-Seriennummer

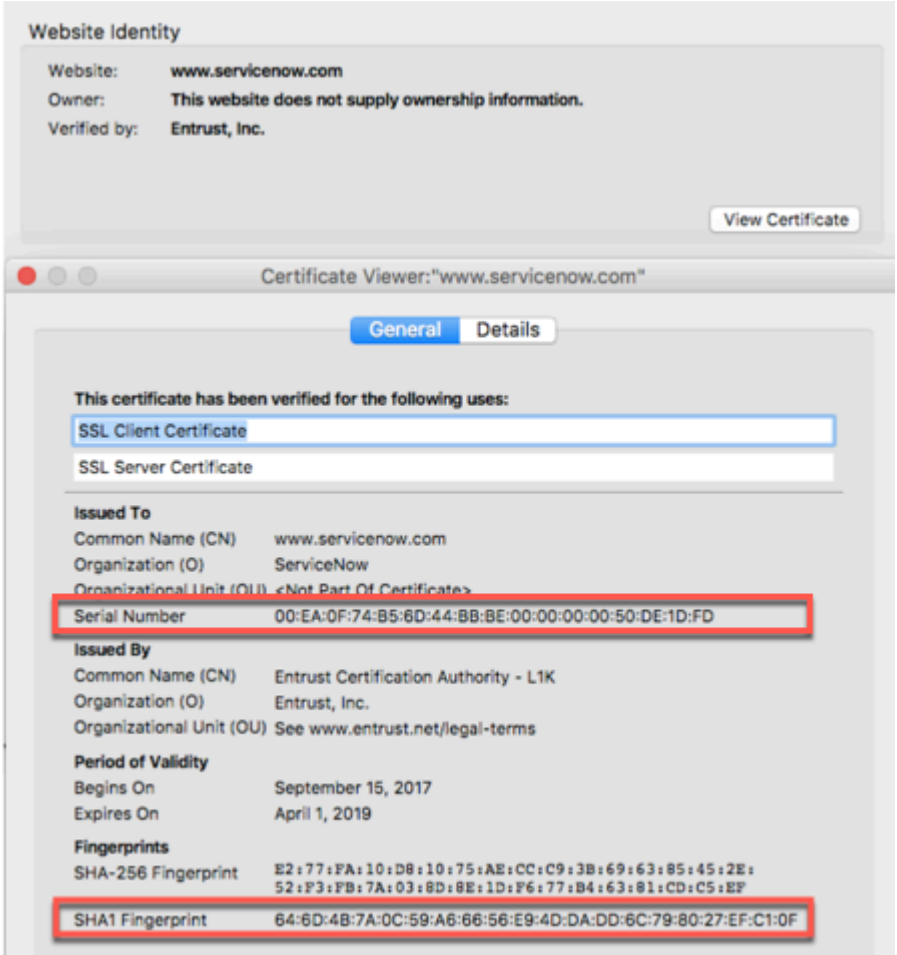
Diese Abbildung zeigt ein Beispiel für die erkennbaren Elemente Datei-Hash und Zertifikat-Seriennummer, die für die SSL-Zertifikatsuchen für diese Integration verwendet werden. Der Datei-Hash verweist auf einen SHA-1-Fingerabdruck. Dieser Wert wird in Ihrer Instanz Now Platform ohne Doppelpunkt-Trennzeichen angezeigt. Beispiel: `646D4B7A0C59A66656E94DDADD6C798027EFC10F`.

Das erkennbare Element der Zertifikatseriennummer bezieht sich auf die eindeutige ID oder Seriennummer für die Entität. Dieser Wert wird auch ohne Doppelpunkt-Trennzeichen angezeigt. Beispiel: `00EA0F74B56D44BBBE0000000050DE1DFD`.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Datei-Hash und Seriennummer des Zertifikats




## RISKIQ und WHOISIQinstallieren und konfigurieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendungen RISKIQ und WHOISIQ ordnungsgemäß in Now Platform Security Operationsintegriert werden können.

### Vorbereitungen

Erforderliche Rolle: admin, RISKIQ und WHOISIQ admin.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

| Setupaufgabe | Beschreibung |
|---|---|
| Stellen Sie sicher, dass Sie die erforderlichen Rollen zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Systemadministrator (admin) installiert die App und weist die Rolle Security Incident Administrator (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

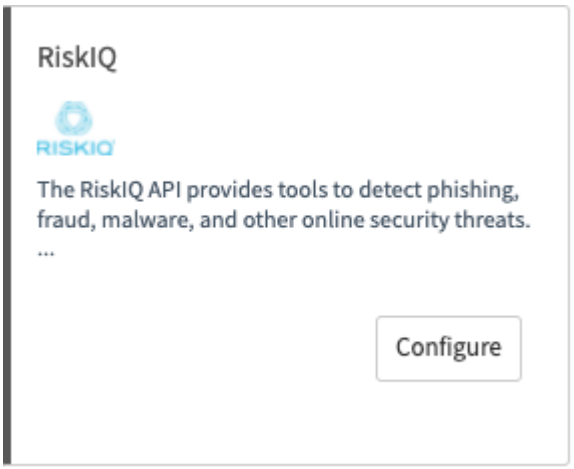
| Setupaufgabe | Beschreibung |
| --- | --- |
| | Modul Security Operations und weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>• Security Incident Analyst (sn_si.analyst) arbeitet mit Security Incident-Datensätzen. |
| Rufen Sie einen Benutzernamen und einen API-Schlüssel ab. | Besuchen Sie die Website, um Informationen zum API-Schlüssel und zum Erstellen eines Kontos zu erhalten: RISKIQ-Website . Die Konfiguration erfordert die Eingabe des API-Schlüssels. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Anforderungen für Madrid und spätere Releases<br>Für das Madrid-Release und spätere Familien-Releases ist das Plugin Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br>1. Security Incident Response<br>2. Security Integration Framework<br>3. Security Support Common<br>4. Security Support Orchestration<br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |



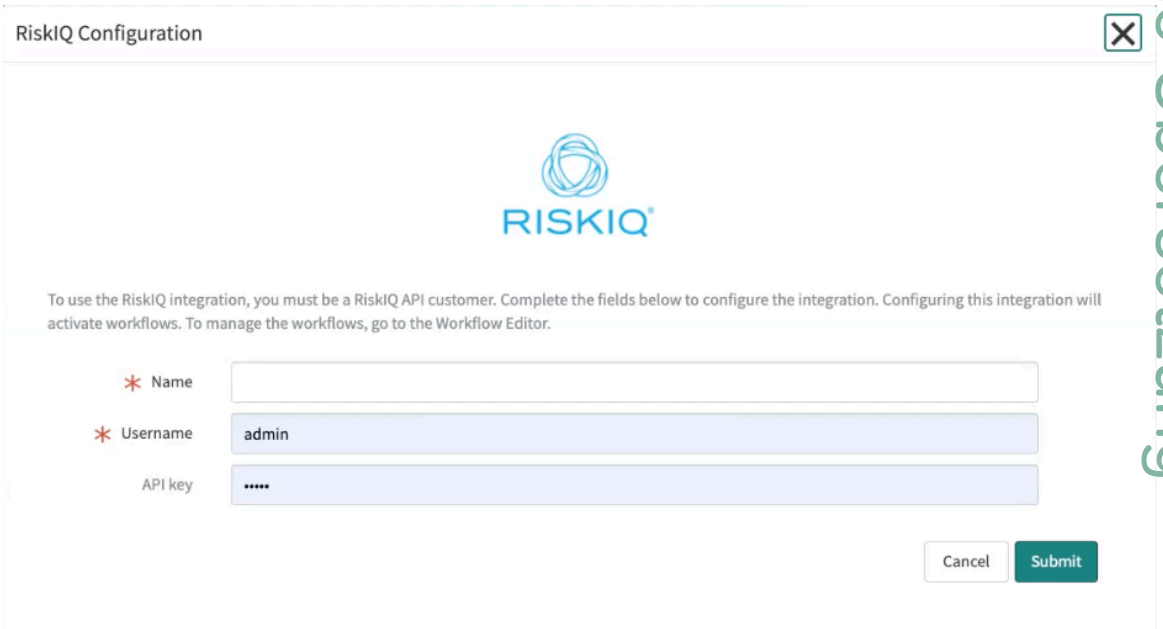
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die API-Kachel.
3. Klicken Sie auf **Konfigurieren**.




4. Geben Sie im angezeigten Dialogfeld „RiskIQ-Konfiguration“ den **Benutzernamen** und den **API-Schlüssel**ein.



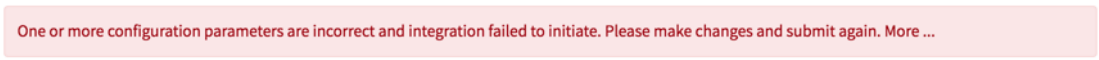

5. Klicken Sie auf **Absenden**.
6. Vergewissern Sie sich, dass die Konfiguration erfolgreich war.
   Nach erfolgreicher Konfiguration wird die Seite „Security Integrations“ (Sicherheitsintegrationen) mit den Integrationskacheln angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Trouble?**
Wenn eine Fehlermeldung angezeigt wird, ist der Benutzername oder API-Schlüssel möglicherweise ungültig. Vergewissern Sie sich, dass Ihr Benutzername und der API-Schlüssel korrekt sind:

**Problembehandlung**




### Überprüfen Sie die erwarteten Ergebnisse für RISKIQ SSL-Zertifikatsuchen

Wenn ein Security Incident erkennbare Elemente für URLs, Domänen, IP-Adressen, Zertifikatdatei-Hashes (SHA-1-Fingerabdruck) und Zertifikat-Seriennummern generiert, verwenden Security Incident-Analysten die Ergebnisse der SSL-Zertifikatsuche, um zu überprüfen, ob Websites über Zertifikate verfügen, die von einem vertrauenswürdigen ausgegeben wurden öffentliche Zertifizierungsstelle (CA).

## Vorbereitungen
Erforderliche Rolle: sn_si.analyst

## Warum und wann dieser Vorgang ausgeführt wird
Für unterstützte erkennbare Elemente scannt Now Platform nach dem letzten Vorkommen von URLs, Domänen, IP-Adressen, Zertifikatdatei-Hashes (SHA-1-Fingerabdruck) und Zertifikat-Seriennummern. Dies sind mögliche Ergebnisse des Scans:

**Es wurde eine exakte Übereinstimmung gefunden**

Ein gültiger Aussteller eines SSL-Zertifikats wird im Security Incident-Datensatz aufgeführt.

**Es wurden keine Zertifikatergebnisse gefunden**

Im Security Incident-Datensatz werden keine Ergebnisse aufgeführt.

**Für ein selbstsigniertes oder intern generiertes Zertifikat wird eine exakte Übereinstimmung gefunden**

Die Ergebnisse für ein intern generiertes SSL-Zertifikat werden im Security Incident-Datensatz angezeigt.

**Für ein primäres SSL-Zertifikat wurde keine exakte Übereinstimmung gefunden**

Ein Suchwert gibt mehrere Einträge zurück, und ein primäres Zertifikat kann nicht identifiziert werden. Eine Zusammenfassungsnachricht wird im Security Incident-Datensatz angezeigt.

## Prozedur

1. Um die erkennbaren Elemente anzuzeigen und die Suchergebnisse zu überprüfen, öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und suchen Sie die Arbeitsnotizen.

   **Example**
   Um Beispiele für die möglichen Suchergebnisse für diese Integration zu veranschaulichen, nehmen Sie an, dass ein Security Incident mit den folgenden erkennbaren Elementen generiert wurde:

   - community.servicenow.com
   - ungültige Subdomäne.servicenow.com
   - mail.dgnetworks.com
   - servicenow.com



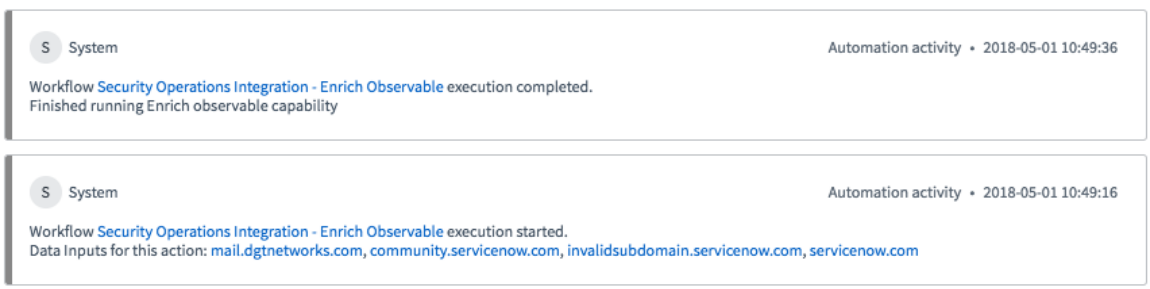
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erkennbare Elemente und Speicherort der Suchergebnisse

| Erkennbares Element (Beispiel) | Scan-Ergebnisse | Beschreibung und Standort |
|---|---|---|
| community.servicenow.com | Zertifikat mit SHA1-Hash gefunden. | Es wird eine exakte Übereinstimmung gefunden, und ein gültiger Aussteller eines SSL-Zertifikats wird aufgelistet. Die Ergebnisse für die genaue Übereinstimmung werden auf der Registerkarte **SSL-Zertifikate** im Security Incident-Datensatz angezeigt. |
| ungültige Subdomäne.servicenow.com | Keine Zertifikate gefunden. | Eine Zusammenfassung, die angibt, dass keine Zertifikatergebnisse gefunden wurden, wird auf der Registerkarte **Anreicherung erkennbarer Elemente – Ergebnisse** des Security Incident-Datensatzes angezeigt. |
| mail.dgnetworks.com | Zertifikat mit SHA1-Hash gefunden. | Eine genaue Übereinstimmung wird für ein selbstsigniertes oder intern generiertes Zertifikat aufgelistet. Die Ergebnisse werden auf der Registerkarte **SSL-Zertifikate** im Security Incident-Datensatz angezeigt. |
| servicenow.com | Die Suche ergab 138 Zertifikate, und ein einzelnes primäres Zertifikat konnte nicht identifiziert werden. | Für ein primäres SSL-Zertifikat wird keine exakte Übereinstimmung gefunden, da ein Suchwert mehrere Zertifikate zurückgibt. Eine Zusammenfassung, die angibt, dass kein primäres Zertifikat gefunden wurde, wird auf der Registerkarte **Anreicherung erkennbarer Elemente – Ergebnisse** des Security Incident-Datensatzes angezeigt. |

Nachdem die Anwendung konfiguriert wurde, wird der Workflow automatisch gestartet. Der Suchstatus und die erkennbaren Elemente werden in den Arbeitsnotizen angezeigt.

2. Stellen Sie sicher, dass die Suche erfolgreich ausgeführt wurde.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Trouble?**
Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, stellen Sie sicher, dass das erkennbare Element von der SSL-Zertifikatsuche für die Integration unterstützt wird.

**Zugehörige Informationen**

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

### RISKIQ SSL-Zertifikatsuchen, die eine exakte Übereinstimmung zurückgeben

RISKIQ Ergebnisse der SSL-Zertifikatsuche für eine exakte Übereinstimmung werden auf der Registerkarte **SSL-Zertifikate** im Security Incident-Datensatz angezeigt. Eine exakte Übereinstimmung liefert einen gültigen Zertifizierungsstellennamen, der einem Security Incident-Analysten hilft, die Gültigkeit einer Website zu bestimmen.

## Example: Genaue Übereinstimmung mit einem gültigen SSL-Zertifikat

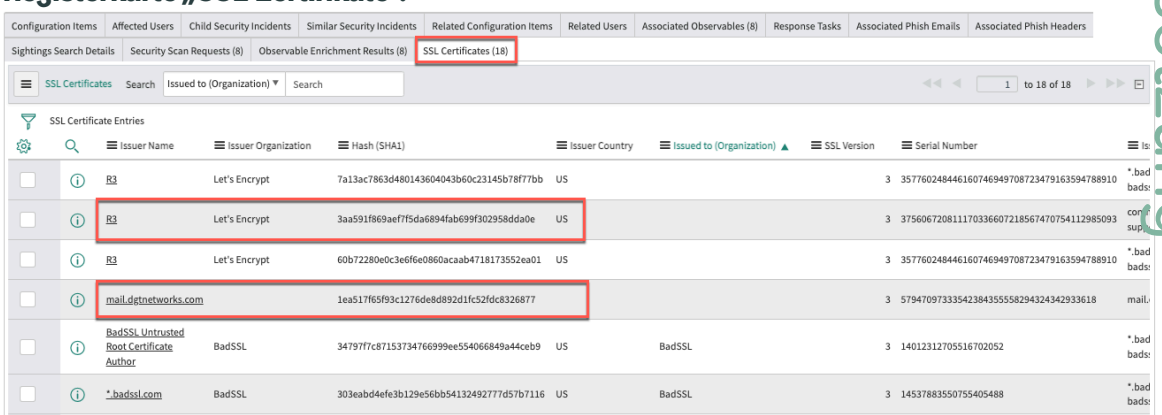
Das folgende Beispiel zeigt einen gültigen Aussteller eines SSL-Zertifikats aus einer genauen Übereinstimmung in den Suchergebnissen. Befolgen Sie die Schritte, um die Ergebnisse und Rohdaten anzuzeigen.

**Hinweis:**
Die Abbildungen in den folgenden Beispielen werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt. Wenn Ihr Bildschirm nicht mit der unten gezeigten Ansicht übereinstimmt, befolgen Sie die Schritte zum Festlegen von Formularen mit Registerkarten.

1. Klicken Sie in der oberen rechten Ecke des Bannerframes auf das Symbol für Einstellungen.
2. Klicken Sie im angezeigten Dialogfeld „ **Systemeinstellungen** “ auf **Formulare**, und überprüfen Sie, ob **Formulare** mit Registerkarten und **Mit dem Formular** ausgewählt sind.

1. Klicken Sie im Security Incident-Datensatz auf die Registerkarte **SSL-Zertifikate**.

**Registerkarte „SSL-Zertifikate“.**




Informationen über den Namen des Zertifikatausstellers, die Organisation des Ausstellers und die Person, für die das Zertifikat ausgestellt wurde (Organisation), werden zusammen mit anderen Daten angezeigt.

In der Spalte **Ausstellername** werden 18 Elemente angezeigt. Das zweite Element (R3) gibt einen gültigen Zertifizierungsstellennamen (Let's Encrypt) in der Spalte **Ausstellerorganisation** an.

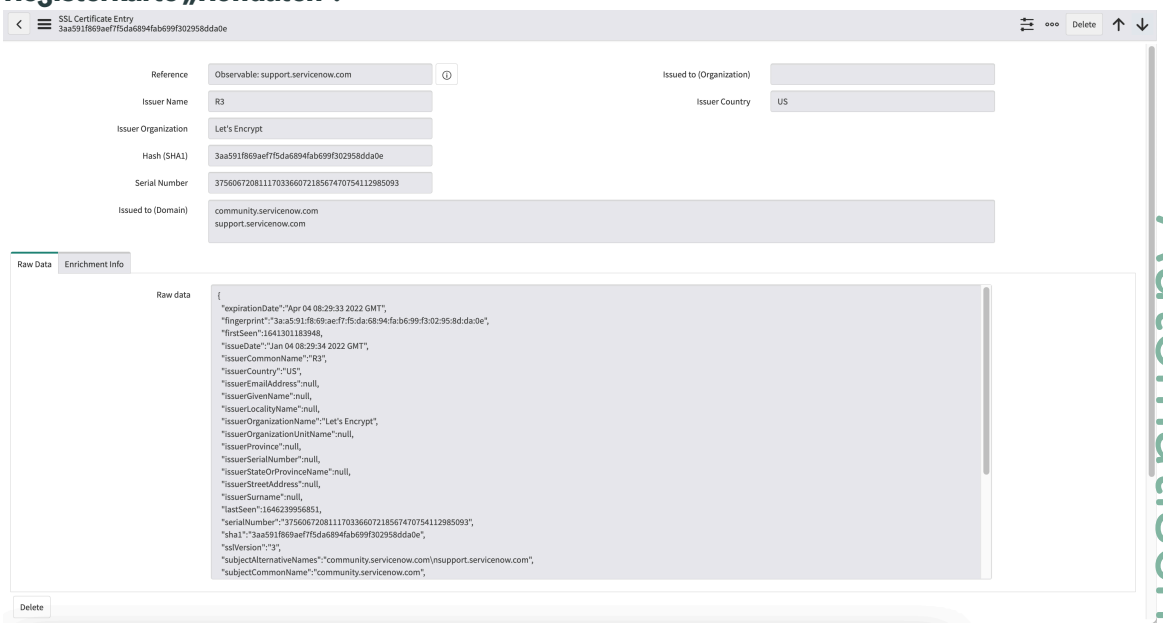
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für das zweite Element ( **mail.dgtnetworks.com** ) werden keine Informationen in den SpaltenAusstellerorganisation und **Ausgestellt an**angezeigt.

2. Klicken Sie auf das zweite Element in der Spalte **Ausstellername**(**R3**), um den Zutrittsdatensatz zu öffnen. Alternativ können Sie auf das Informationssymbol neben dem Element und anschließend auf **Datensatz öffnen**klicken.
3. Wählen Sie die Registerkarte **Rohdaten** aus.

**Registerkarte „Rohdaten“.**




Der Datensatz „SSL-Zertifikateintrag“ enthält das erkennbare Element auf der Registerkarte „ **Rohdaten** “ unter der Spalte „ **Entitätsname“** sowie andere Daten.

Hinweis: In der Spalte **Kategorie** entsprechen Subjectund Issuer erkennbaren Entitäten in der Spalte **Entitätsname**. Der Aussteller dieses Zertifikats ist höchstwahrscheinlich gültig und stammt von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle. Beachten Sie auch, dass Subjectund Issuer unterschiedliche Entitäten sind. Diese separaten Entitäten weisen darauf hin, dass das Zertifikat kein intern signiertes Zertifikat einer unbekannten Zertifizierungsstelle ist.

## Example: Genaue Übereinstimmung mit einem selbstsignierten SSL-Zertifikat

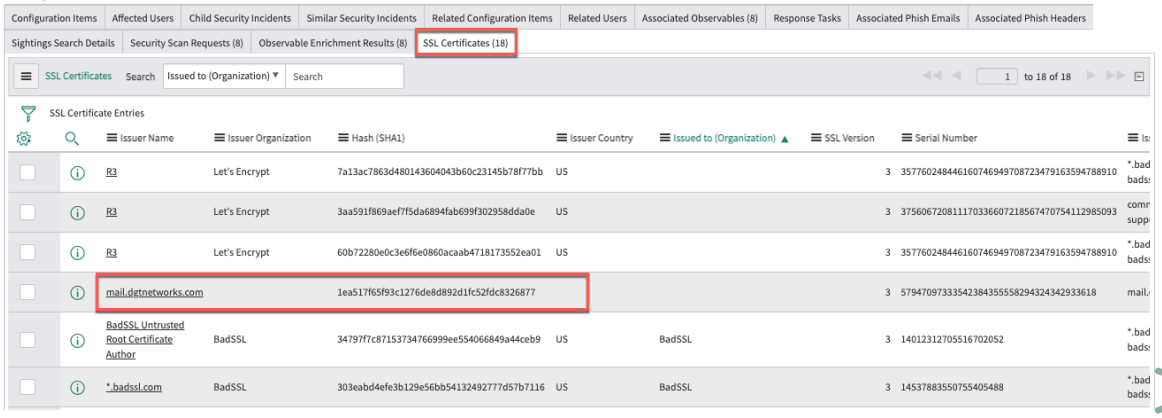
Das folgende Beispiel zeigt Ergebnisse für ein selbstsigniertes SSL-Zertifikat aus der Suche. Befolgen Sie die Schritte, um die Ergebnisse und Rohdaten anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

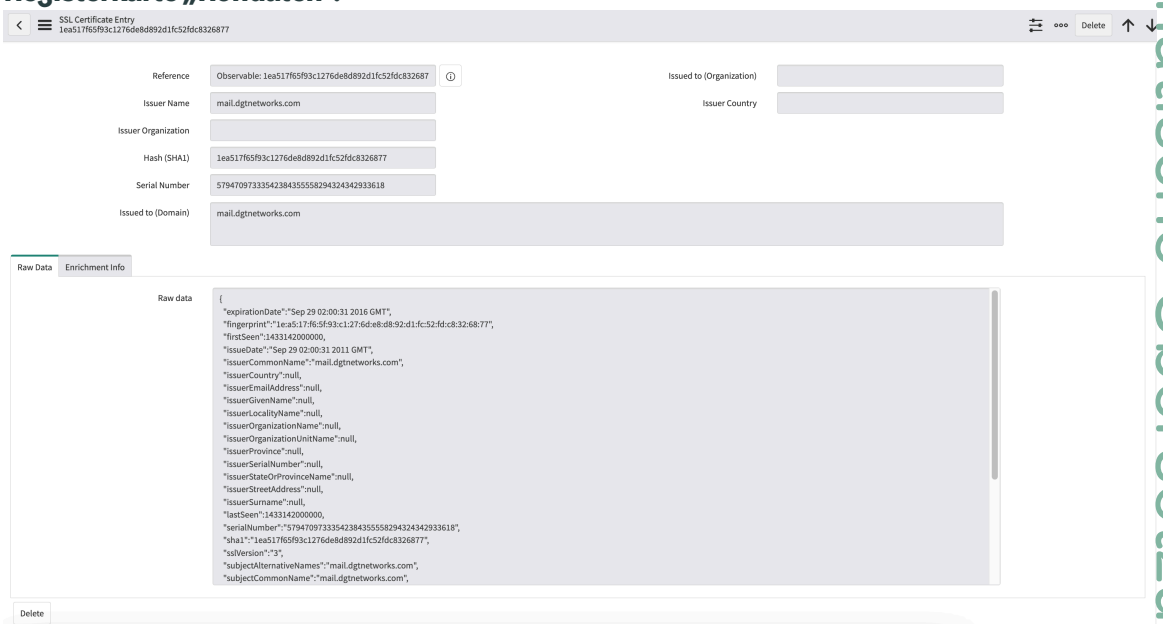
1. Navigieren Sie zurück zum Security Incident-Datensatz. Klicken Sie in der Spalte**Ausstellername auf das andere Element (mail.dgtnetworks.com)**.

**Registerkarte „SSL-Zertifikate“.**




2. Wählen Sie im geöffneten Datensatz die Registerkarte **Rohdaten** aus.

**Registerkarte „Rohdaten“.**




Die Spalte **Kategorie** gibt an, dass derAussteller ( mail.dgtnetworks.comunddgtsbs.DgtNetworks.local) keine vertrauenswürdigen öffentlichen Zertifizierungsstellen sind. Beachten Sie auch,dass Aussteller und Betreff dieselbe Entität sind ( dgtsbs.DgtNetworks.local) und jeweils den Namen des erkennbaren Elements (dgtsbs) enthalten. Dieses Zertifikat ist möglicherweise ein selbstsigniertes Zertifikat. Selbstsignierte Zertifikate erfordern möglicherweise weitere Untersuchungen, da diese Zertifikate nicht von einer bekannten Zertifizierungsstelle ausgestellt werden.

### RISKIQ SSL-Zertifikatsuchen, die mehrere Zertifikate oder keine Zertifikate zurückgeben

Ein Security Incident-Analyst kann mehrere SSL-Zertifikatergebnisse verwenden, um zu bestimmen, ob eine Site Teil einer gemeinsamen, erkennbaren Entität ist. Keine SSL-Zertifikatergebnisse weisen möglicherweise darauf hin, dass Sites mit obskuren oder verdächtigen Namen keine vertrauenswürdigen Zertifikate haben. Suchergebnisse für erkennbare Elemente, die keine SSL-Zertifikate zurückgeben oder mehrere SSL-Zertifikate

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

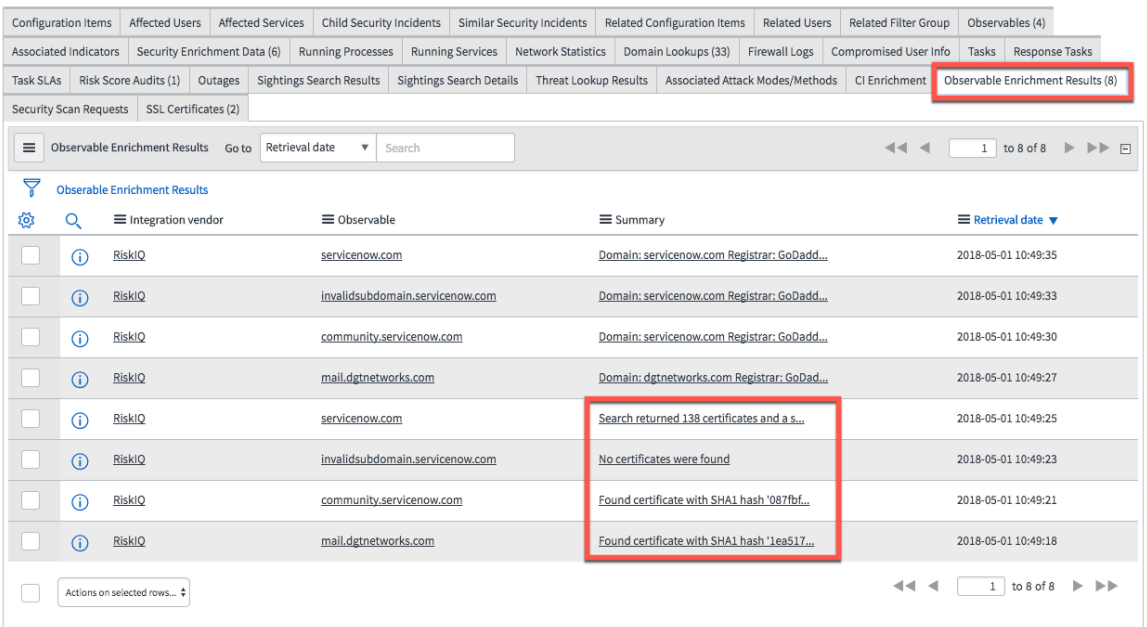
zurückgeben, werden auf der Registerkarte Anreicherung erkennbarer Elemente im Security Incident-Datensatz angezeigt.

### Example: Keine SSL-Zertifikatergebnisse oder mehrere SSL-Zertifikatergebnisse

Führen Sie die Schritte aus, um die Ergebnisse für erkennbare Elemente anzuzeigen, die keine SSL-Zertifikate zurückgeben oder mehrere Zertifikate zurückgeben.

1. Klicken Sie im Security Incident-Datensatz auf die Registerkarte **Anreicherung erkennbarer Elemente – Ergebnisse**.

**Registerkarte „Anreicherung erkennbarer Elemente“ – Ergebnisse**

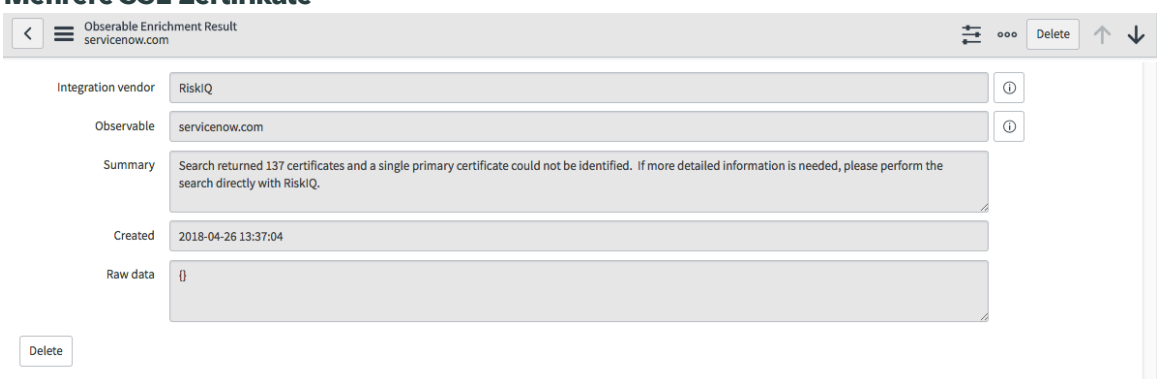



Die Ergebnisse der Ergänzung erkennbarer Elemente für die Suche RISKIQ und WHOISIQ werden angezeigt.

In der Spalte „Erkennbares Element“ entspricht servicenow.com**der** Nachricht „ Suche hat 138 Zertifikate zurückgegeben “ in der Spalte „ **Zusammenfassung** “. In ähnlicher Weise entspricht invalidsubdomain.servicenow.com In der Spalte **Zusammenfassung**wurden keine Zertifikate gefunden. Diese Zusammenfassungen geben an, dass mehrere SSL-Zertifikate gefunden wurden und dass keine genauen Übereinstimmungen für SSL-Zertifikate gefunden wurden.

2. Klicken Sie in der Spalte **„Erkennbares Element“ auf servicenow.com.**

**Mehrere SSL-Zertifikate**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zusammenfassungsnachricht, die im Datensatz angezeigt wird, gibt an, dass mehrere Ergebnisse für SSL-Zertifikate für servicenow.com zurückgegebenwurden und kein primäres SSL-Zertifikat abgeglichen werden konnte. Diese Nachricht wird häufig bei Suchen zurückgegeben, die allgemeine Domänennamen enthalten, z. B. servicenow.com.

Wenn Sie weitere Informationen zu einer gemeinsamen Domäne benötigen, können Sie die Suche direkt mit der RISKIQ -API durchführen.

3. Navigieren Sie zurück zur Registerkarte **Anreicherung erkennbarer Elemente – Ergebnisse**, und klicken Sie in der **Spalte** „Erkennbares Element“ auf ungültige **Subdomäne.servicenow.com**.

**Keine SSL-Zertifikate**

**Hinweis:**

- Wenn für das aktuelle erkennbare Element keine SSL-Zertifikate gefunden werden, wird im Feld Zusammenfassung die Meldung Es wurden keine Zertifikate gefundenangezeigt.
- Wenn für das aktuelle erkennbare Element keine aktiven SSL-Zertifikate gefunden werden, wird im Feld Zusammenfassung die Meldung Es wurden keine aktiven Zertifikate gefundenangezeigt.

### Überprüfen Sie die erwarteten Ergebnisse für WHOISIQ URL-Suchen

Wenn ein Security Incident erkennbare Elemente für URLs oder Domänen generiert, führt die WHOISIQ -API die Ergänzung erkennbarer Elemente automatisch bei der Erstellung des Security Incident durch. Die Suchergebnisse werden auf den Registerkarten **„Anreicherung erkennbarer Elemente“** und **„SSL-Zertifikate** “ im Security Incident-Datensatz angezeigt.

## Vorbereitungen

**Hinweis:**

Die Abbildungen in den folgenden Schritten werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt.

Erforderliche Rolle: sn_si.analyst

## Warum und wann dieser Vorgang ausgeführt wird

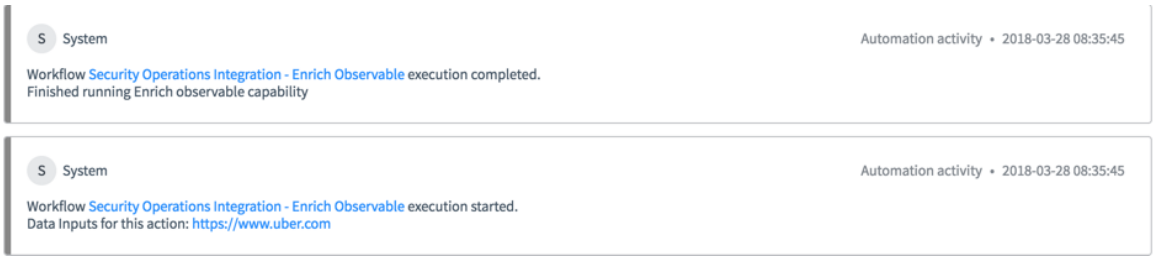
Die Ergebnisse der Ergänzung erkennbarer Elemente werden auf der Registerkarte **Ergebnisse** der Ergänzung erkennbarer Elemente am unteren Rand des Security Incident-Datensatzes angezeigt. Für unterstützte erkennbare Elemente wird auch eine SSL-Zertifikatsuche ausgeführt, und die Ergebnisse werden auf der**Registerkarte SSL-Zertifikate**angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

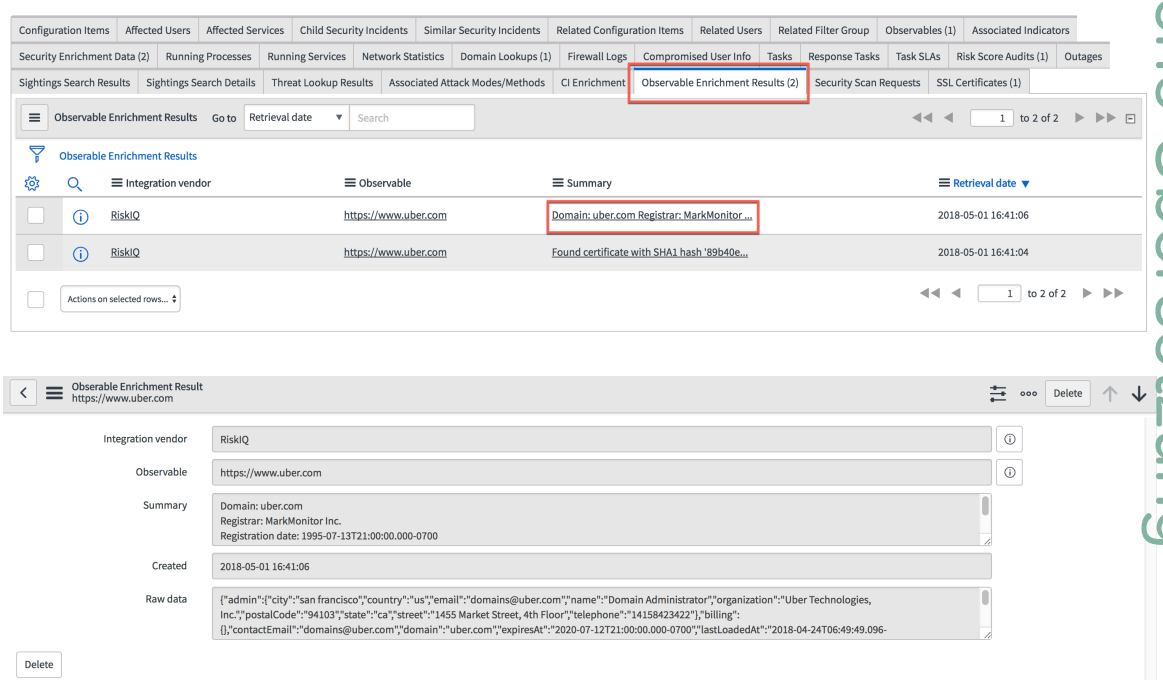
## Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und vergewissern Sie sich, dass die Suche in den Arbeitsnotizen erfolgreich ausgeführt wurde.




   Sobald die Anwendung konfiguriert ist, wird der Workflow automatisch bei der Incident-Erstellung gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde, finden Sie in den Arbeitsnotizen weitere Informationen zum weiteren Vorgehen.
3. Klicken Sie im offenen Security Incident auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.
4. Klicken Sie auf die Registerkarte Ergänzung erkennbarer Elemente – **Ergebnisse**, um sie auszuwählen.
5. Klicken Sie in der Spalte **Zusammenfassung** auf das erste Element, **Domäne: uber.com Registrar: Markmonitor...**.

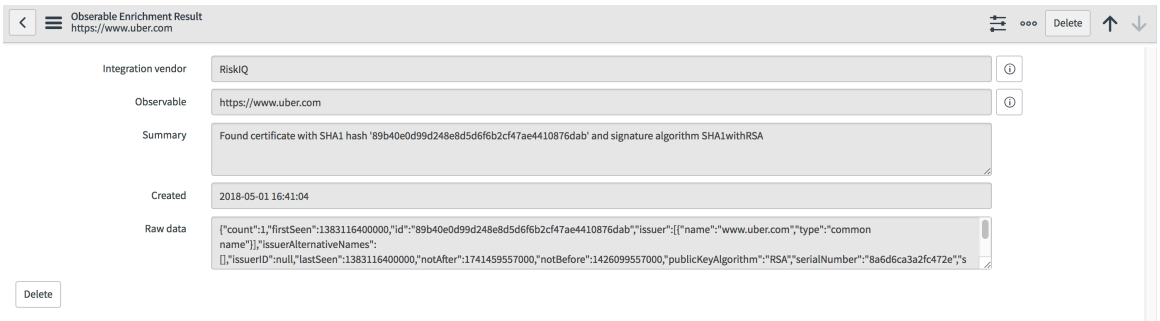



   Der angezeigte Datensatz enthält Informationen zur Domäne.

6. Navigieren Sie zurück zur Registerkarte **Anreicherung erkennbarer Elemente – Ergebnisse**, und klicken Sie in der Spalte **Zusammenfassung** auf das zweite Element, Certificate with SHA1 hash... ( **Zertifikat mit SHA1-Hash gefunden...**).

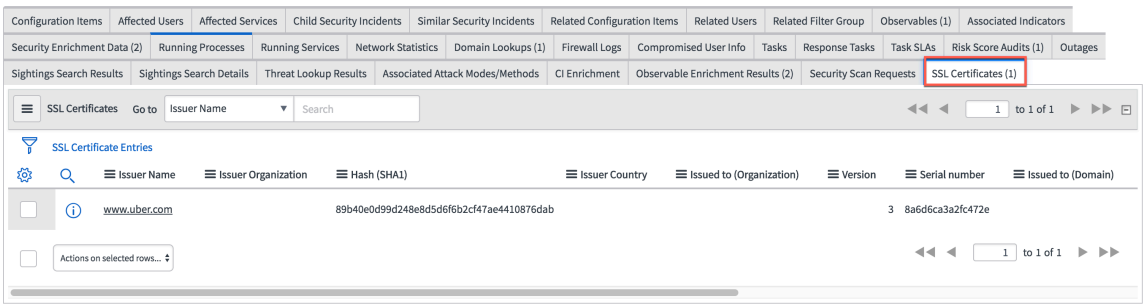
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Dieser Datensatz gibt an, dass ein SSL-Zertifikat mit einem Datei-Hash gefunden wurde.

7. Navigieren Sie zurück zum Security Incident-Datensatz, und klicken Sie auf die Registerkarte **SSL-Zertifikate**.




Die SSL-Zertifikatergebnisse für den Datei-Hash werden auch hier angezeigt.

### Trouble?

Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, überprüfen Sie die Arbeitsnotizen. Stellen Sie außerdem sicher, dass das erkennbare Element für die Suche durch die Integration unterstützt wird.

### Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

## Erstellen Sie ein erkennbares Element für manuelle WHOISIQ Suchvorgänge

Security Incident-Analysten verwenden Informationen aus der Ergänzung erkennbarer Elemente mit der WHOISIQ -API, um mehr über die E-Mail-Adressen, Namen und Telefonnummern von Organisationen zu erfahren.

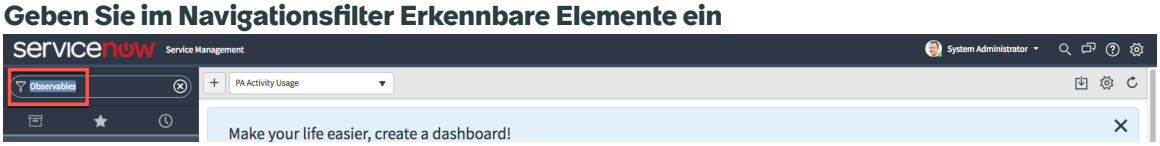
### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente**.

**Geben Sie im Navigationsfilter Erkennbare Elemente ein**

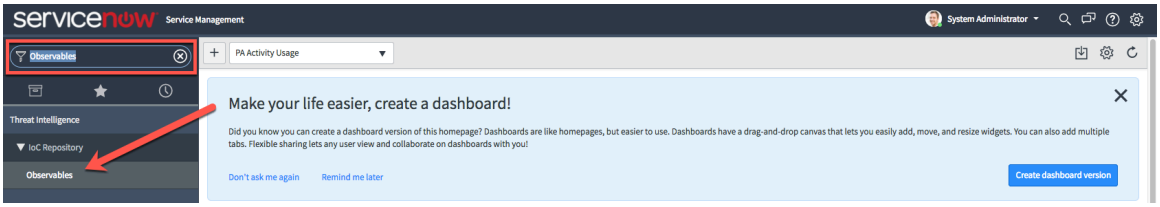



Unter dem Navigationsbereich wird das Modul „Erkennbare Elemente“ angezeigt.

Automatische Übersetzung

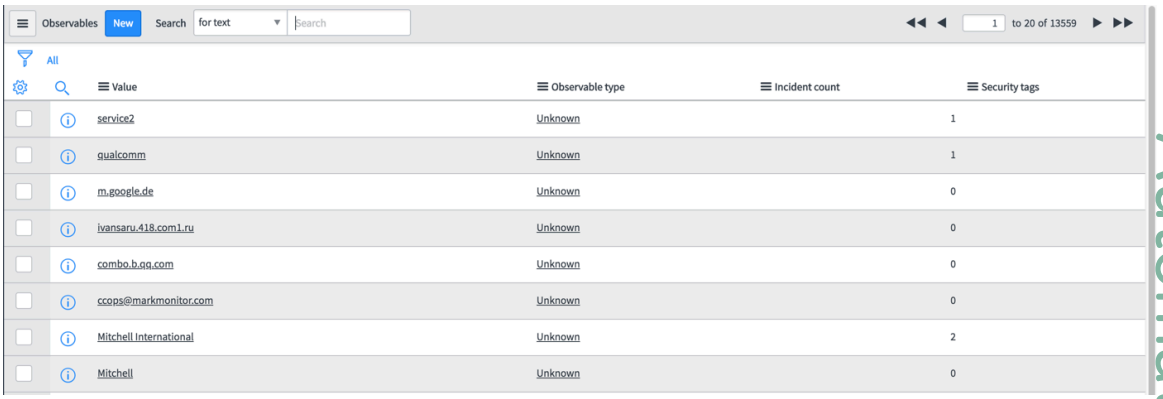
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Modul „Erkennbare Elemente“.




**2.** Klicken Sie auf das Modul **„Erkennbare** Elemente“, um die Liste der erkennbaren Elemente anzuzeigen.

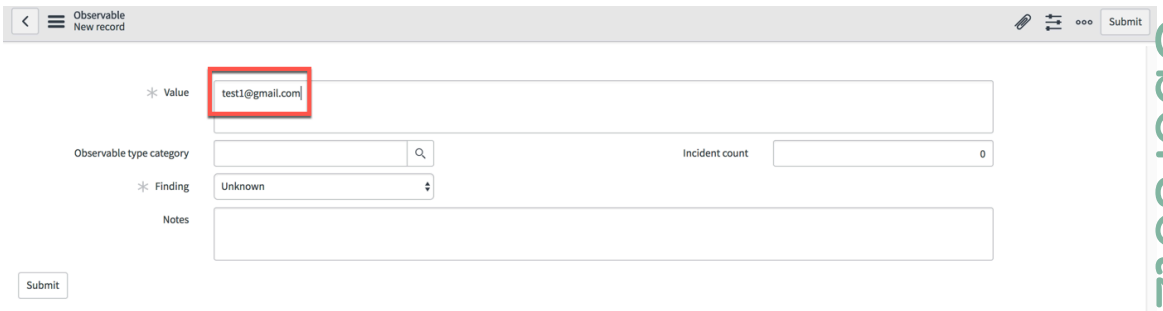
### Liste der erkennbaren Elemente




**3.** Klicken Sie auf **Neu**, um ein neues erkennbares Element zu erstellen.

**4.** Füllen Sie die Felder im Formular „Erkennbares Element“ aus.

### Erstellen Sie ein neues erkennbares Element




**5.** Klicken Sie auf **Absenden**.
Sie kehren zur Liste „Erkennbare Elemente“ zurück. In der Spalte **Wert** wird Ihr neues erkennbares Element angezeigt.

> **Hinweis:**
> Wenn Sie Ihr erkennbares Element im angezeigten Teil der Liste nicht finden können, verwenden Sie die Suchfunktion, um es zu finden.

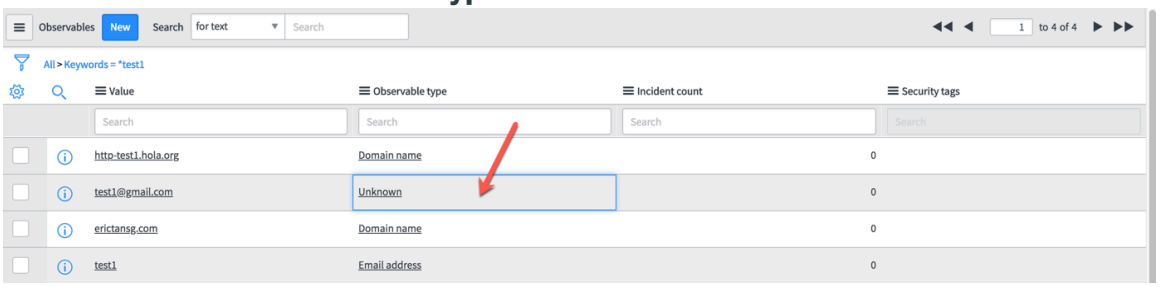
**6.** Bearbeiten Sie das Feld **Erkennbarer Typ**, um den Typ von **Unbekannt** in **E-Mail-Adresse** zu ändern, damit er Ihrem erkennbaren Element entspricht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie in der Spalte **„Erkennbarer Typ“ einmal** rechts neben dem Text **Unbekannt**, um ihn auszuwählen.

**Wählen Sie das Feld Erkennbarer Typ aus**

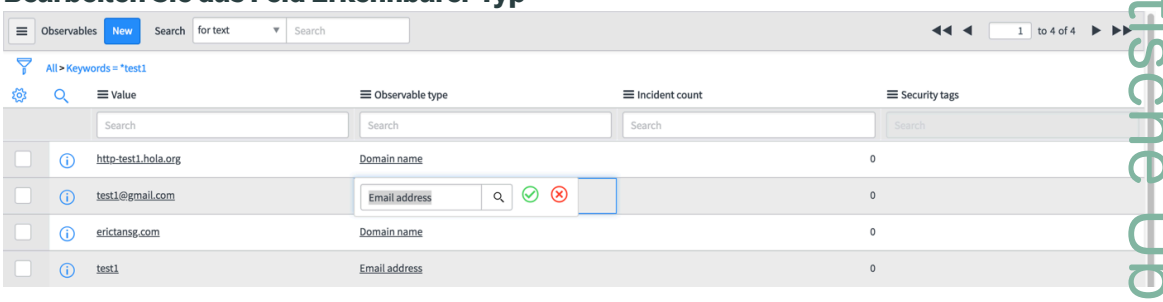



Das ausgewählte Feld wird blau umrandet.

**b.** Wenn das Feld blau umrandet ist, doppelklicken Sie auf eine beliebige Stelle im hervorgehobenen Feld, um den Editor zu öffnen.

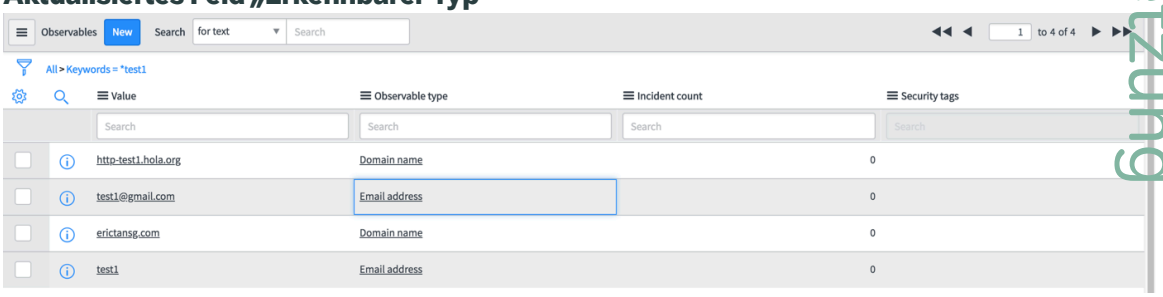
**c.** Geben Sie im angezeigten Feld den Typ des erkennbaren Elements (E-Mail-Adresse) ein, und klicken Sie auf das grüne Häkchen, um den Wert zu speichern.

**Bearbeiten Sie das Feld Erkennbarer Typ**




In der Spalte **Erkennbarer Typ** in der Liste wird E- Mail-Adresse für Ihr neues erkennbares Element angezeigt.

**Aktualisiertes Feld „Erkennbarer Typ“**




## Nächste Maßnahme

Wenn Sie ein erkennbares Element für die Suche erstellt und bearbeitet haben, führen Sie die Ergänzungssuche für erkennbare Elemente aus dem Datensatz „Erkennbares Element“ mit der API WHOISIQ aus.

### Überprüfen Sie die erwarteten Ergebnisse für manuelle WHOISIQ -Suchen

Führen Sie eine manuelle Suche für ein erkennbares Element aus, wenn es nicht automatisch einen Security Incident generiert. Für die Ergänzung erkennbarer Elemente mit der WHOISIQ -API für E-Mail-Adressen, Organisationsnamen, Telefonnummern oder Postadressen initiieren Sie die Suche manuell über die Tabelle „Erkennbare Elemente“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

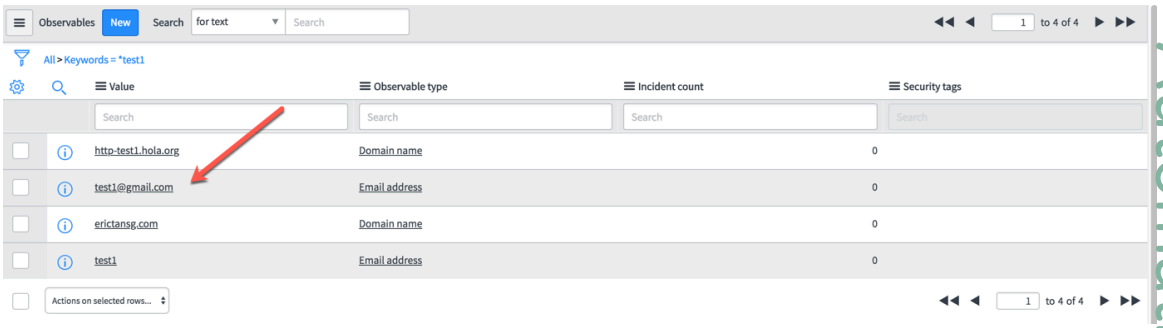
Erforderliche Rolle: sn_si.analyst

## Warum und wann dieser Vorgang ausgeführt wird

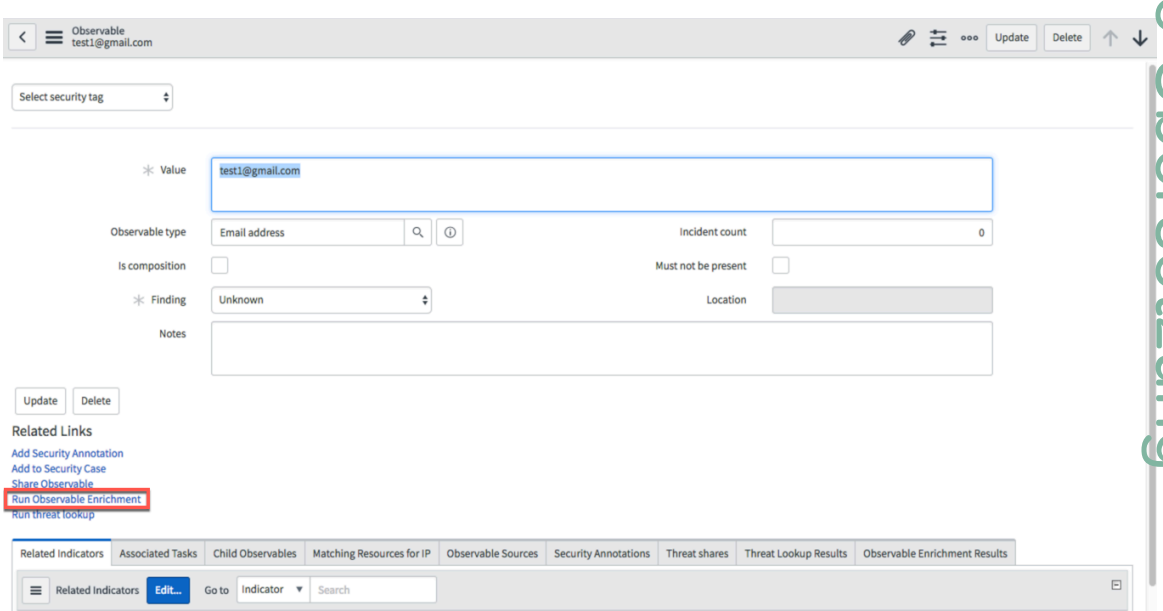
Erstellen Sie mithilfe der WHOISIQ -API ein erkennbares Element für eine manuelle Suche. Weitere Informationen zum Erstellen und Bearbeiten eines erkennbaren Elements finden Sie unter Erstellen Sie ein erkennbares Element für manuelle WHOISIQ Suchvorgänge.

## Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente** und suchen Sie das erkennbare Element in der Liste, mit der Sie arbeiten.
2. Klicken Sie in der Spalte **Wert** auf das erkennbare Element, um den Datensatz zu öffnen.



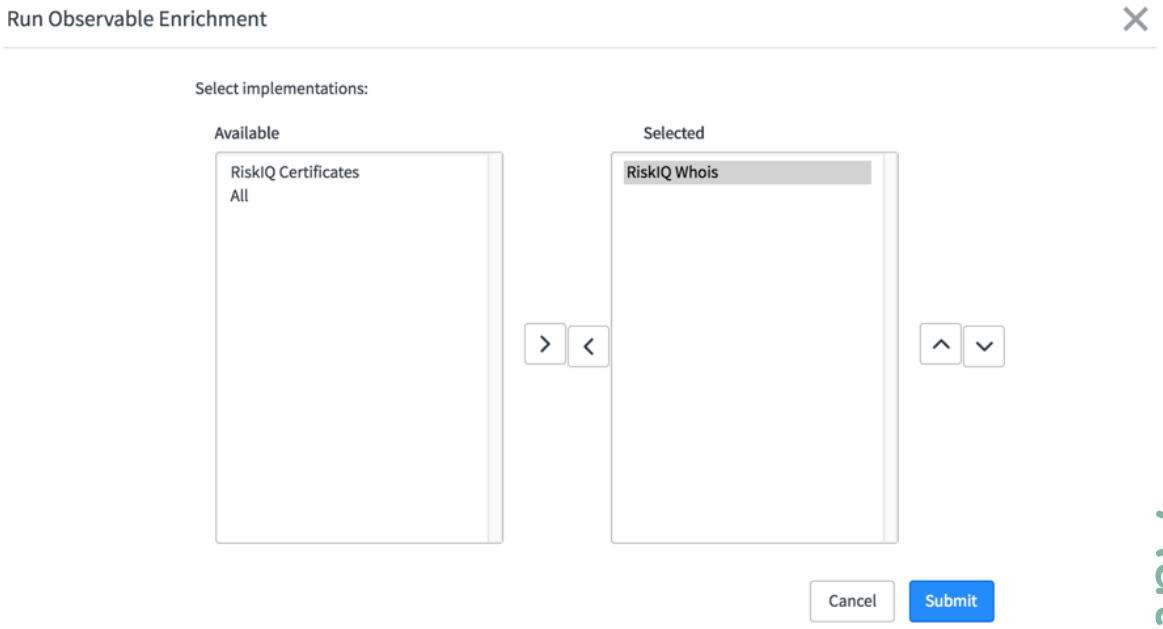

3. **Klicken** Sie auf den zugehörigen Link Ergänzung erkennbarer Elemente ausführen, um die Suche auszuführen.



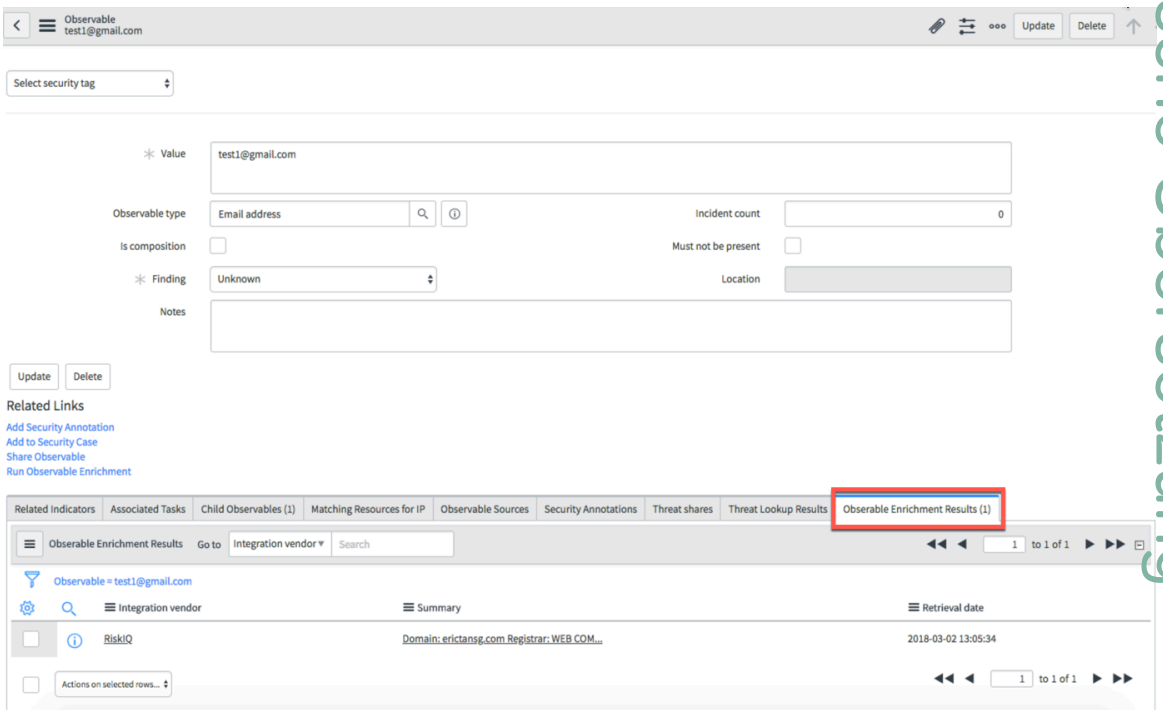

4. Verschieben Sie im Fenster „ **Anreicherungerkennbarer Elemente ausführen“ RiskIQ Whois** in die Liste Ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **Absenden**.
   Suchergebnisse werden auf der Registerkarte **„Anreicherung erkennbarer** Elemente“ im Datensatz „Erkennbares Element“ angezeigt.




### Trouble?

Wenn für das erkennbare Element keine Ergebnisse zurückgegeben werden, wird in der Spalte **Zusammenfassung** eine Meldung angezeigt. Wenn keine Ergebnisse angezeigt werden, stellen Sie sicher, dass das erkennbare Element von der API unterstützt wird.

### Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ und RISKIQ WHOISIQ

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Integration „Shodan“

Shodan ist eine Suchmaschine, die Service-Bannerinformationen von verbundenen Geräten rund um den Globus analysiert. Servicebanner enthalten Informationen zu einem Computersystem, z. B. Hostname, Gerätetyp, Betriebssystem, geografischer Standort und verbundener ISP. Bei Integration mit dem Produkt Now Platform Security Operations bieten diese Servicebannerinformationen Analysten zusätzliche Ergänzungsdaten und Einblicke für Security Incidents oder Untersuchungen.

Die Integration erfordert die Plugins Security Incident Response und Threat Intelligence.

Die Shodan -Integration führt eine Ergänzung der folgenden erkennbaren Elemente durch:

- IP-Adressen
- URLs
- Datei-Hashes

Die Anwendung sucht alle fünf Minuten nach neuen erkennbaren Elementen. Wenn die erkennbaren Elemente von einem Typ sind, der von der Shodan -Integration erkannt wird, werden die erkennbaren Elemente angereichert.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von Now Platform®kompatibel.

### Shodan installieren und konfigurieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit die Anwendung Shodan ordnungsgemäß in Now Platform Security Operationsintegriert wird.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Now Platform Rollen für Ihre Instanz zugewiesen haben. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Der Systemadministrator (admin) installiert die App und weist die Rolle Security Incident Administrator (sn_si.admin) zu.<br>• Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf das Modul Security Operations. |
| Rufen Sie den API-Schlüssel Shodan ab. | Erstellen Sie ein -Konto, und rufen Sie den API-Schlüssel von der Website Shodan ab: Shodan-Website . |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration | Für das Madrid-Release und spätere Familien-Releases ist das Plugin |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung für die Integration installieren. | Security Incident Response Dependency (com.snc.si_dep) erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Security Integration Framework<br>**3.** Security Support Common<br>**4.** Security Support Orchestration<br><br>Weitere Informationen zum Einrichten der Instanz Now Platform für die Integration finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

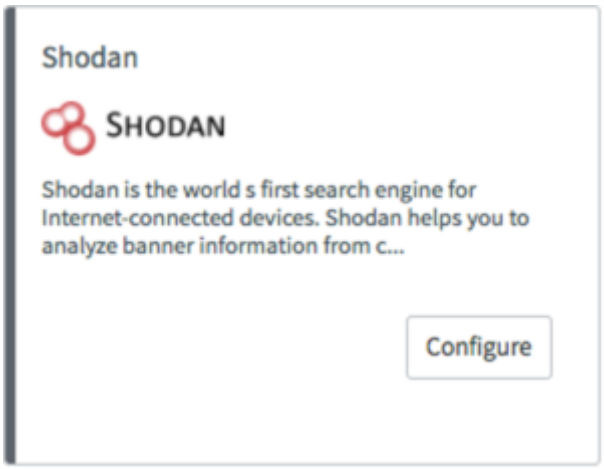
Erforderliche Rolle: admin

### Prozedur

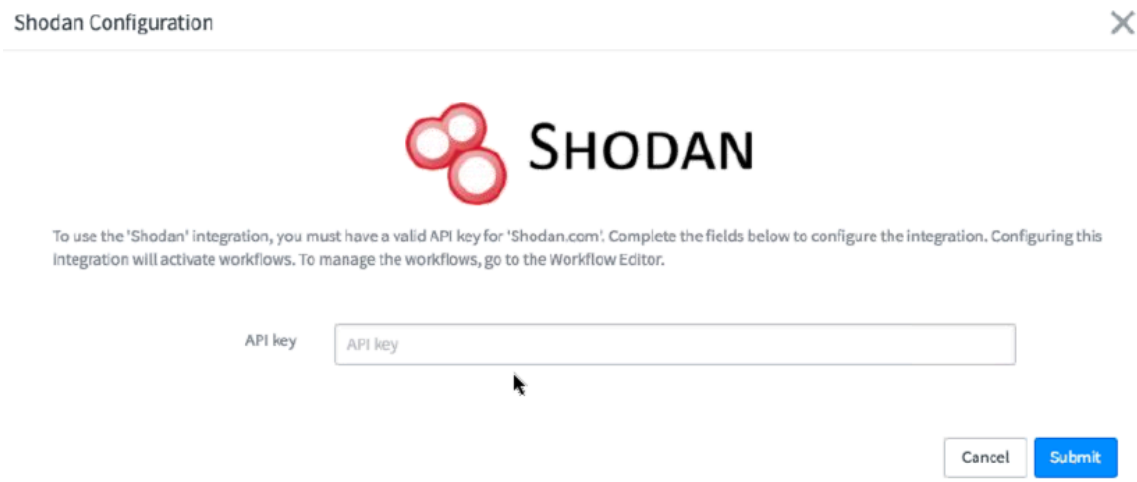
1. Wenn Sie die Anwendung für die Integration nicht installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte aus, um sie zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Shodan.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie auf **Konfigurieren**.
4. Geben Sie im Dialogfeld „ **Shodan-Konfiguration** “ den API-Schlüssel ein, den Sie von der Website Shodan erhalten haben, und klicken Sie auf **Absenden**.




5. Vergewissern Sie sich, dass die Konfiguration erfolgreich war.
   Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird.

   **Trouble?**

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, ist der API-Schlüssel Shodan möglicherweise ungültig.

### Überprüfen Sie die erwarteten Ergebnisse für Shodan

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Die Ergebnisse der Anreicherung werden auf den Registerkarten **„Anreicherung erkennbarer Elemente“** und **„Netzwerkbanner“** angezeigt.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

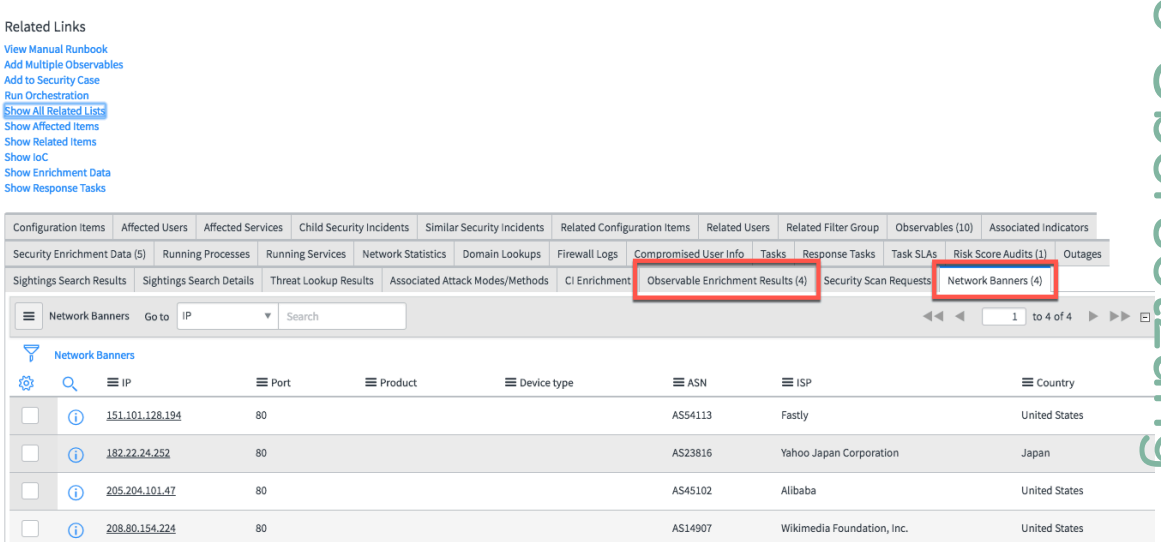
1. Öffnen Sie den Security Incident, an dem Sie arbeiten, und vergewissern Sie sich, dass die Suche erfolgreich ausgeführt wurde.

   Sobald die Anwendung konfiguriert ist, wird der Workflow automatisch bei der Incident-Erstellung gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident angezeigt.

2. Überprüfen Sie die Arbeitsnotizen auf weitere Informationen und Vorgehensweisen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident, und klicken Sie unter **Zugehörige Links** auf den Link **Alle zugehörigen Listen**anzeigen.

   **Hinweis:**
   Die Abbildungen in den folgenden Schritten werden mit der Einstellung **Formulare** mit Registerkarten in den Systemeinstellungen angezeigt. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der rechten oberen Ecke des Bannerframes auf das Zahnradsymbol für Einstellungen. Klicken Sie im angezeigten Dialogfeld „ **Systemeinstellungen** “ auf **Formulare**, und überprüfen Sie, ob **Formulare** mit Registerkarten und **Mit dem Formular** ausgewählt sind.




   Die Ergebnisse werden auf den Registerkarten **Anreicherung erkennbarer Elemente – Ergebnisse** und **Netzwerkbanner** am unteren Rand des Security Incident angezeigt.

4. Klicken Sie bei ausgewählter Registerkarte **Netzwerkbanner** auf das blaue Informationssymbol neben einem erkennbaren Element.

5. Klicken Sie im angezeigten Dialogfeld auf **Datensatz öffnen**, um Rohdaten und weitere Details anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Trouble?**
Wenn auf den Registerkarten „ **Anreicherung erkennbarer Elemente – Ergebnisse** “ und „ **Netzwerkbanner** “ keine Ergebnisse angezeigt werden, stellen Sie sicher, dass das erkennbare Element ein Typ ist, der für die Suche von der Integration unterstützt wird.

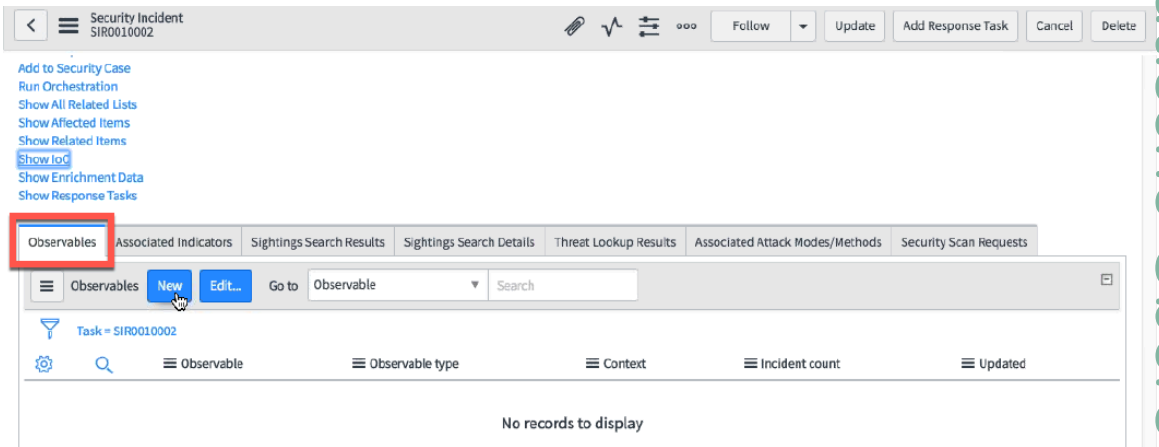
### (Optional) Hängen Sie ein erkennbares Element für manuell an Shodan

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie hängen erkennbare Elemente manuell an, wenn Sie eine Bedrohungssuche für erkennbare Elemente durchführen möchten, die beim ersten Event-Auslöser nicht an einen Security Incident angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Prozedur

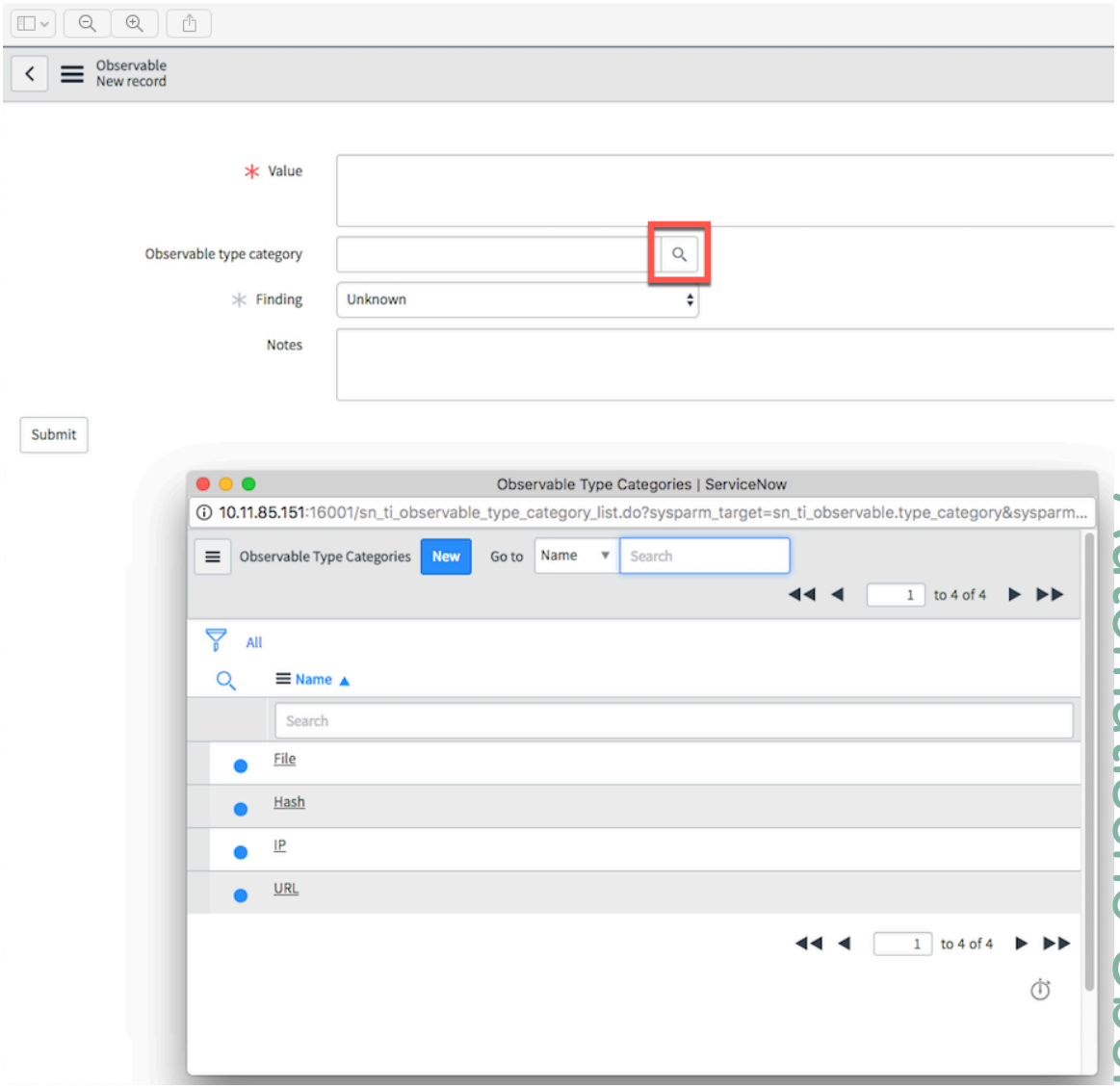
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie unten im Datensatz auf den Link **IoC**anzeigen in **Zugehörige Links**.




3. Klicken Sie auf der Registerkarte **Erkennbare** Elemente auf **Neu**.
   Das Formular „Erkennbares Element“ wird angezeigt.
4. Geben Sie im Feld **Wert** ein erkennbares Element ein (IP-Adresse, Datei-Hash oder URL).
5. Klicken Sie auf das **Suchsymbol**, und klicken Sie im Dialogfeld „Kategorien des erkennbaren Typs“ auf den gewünschten erkennbaren Typ in der Liste, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

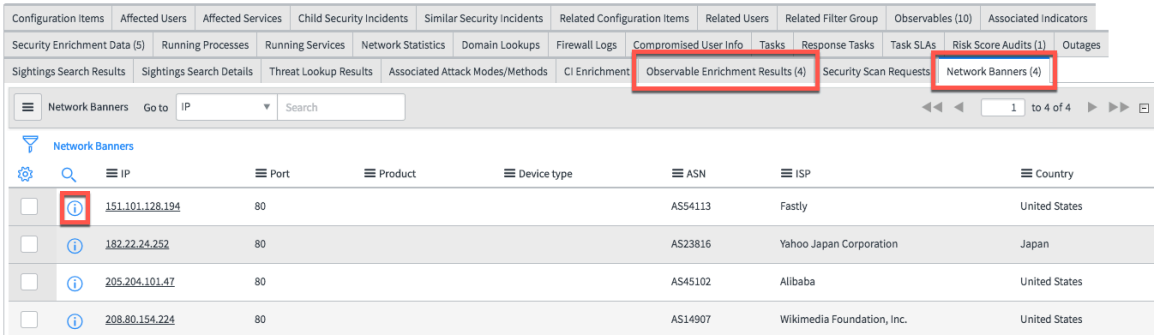





6. Klicken Sie auf **Absenden**.
   Der Workflow wird gestartet und sucht nach dem neuen erkennbaren Element. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ des Security Incident-Datensatzes angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.

8. Klicken Sie unten im Datensatz auf den zugehörigen Link **Alle zugehörigen Listen** anzeigen.
9. Klicken Sie auf die Registerkarten Ergebnisse der **Anreicherung erkennbarer Elemente** oder **Netzwerkbanner**, um Ergebnisse anzuzeigen, und klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element, um weitere Informationen zu einem bestimmten Element zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




10. Klicken Sie im angezeigten Dialogfeld auf **Datensatz öffnen**, um Rohdaten und weitere Details anzuzeigen.
11. **Wahlweise:** Klicken Sie auf das blaue Einstellungssymbol neben dem Suchsymbol, um die Spaltenausgabe und -reihenfolge zu personalisieren.
12. Wählen Sie in **Listenspalten personalisieren**die verfügbaren Einstellungen aus, verschieben Sie sie in die Spalte **Ausgewählt** und klicken Sie auf **OK**.

**Trouble?**
Überprüfen Sie die **Arbeitsnotizen** auf weitere Informationen und Vorgehensweisen, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

## Secureworks CTP Integration der Ticket-Erfassung

Mit der Secureworks Counter Threat Platform -Ticket-Erfassungsintegration können Sie Secureworks CTP -Tickets automatisch abrufen, in Security Incidents umwandeln und automatisierte Antwortaktionen durchführen.

Zu den wichtigsten Funktionen dieser Integration gehören:

- Automatische Erfassung ausgewählter Tickets (einschließlich Anhänge) basierend auf einem vordefinierten Zeitplan.
- Zuordnung von Ticket- und Event-Feldern zu Security Incident Response -Feldern.
- Vorschau der Security Incidents, die den Ticketfeldern zugeordnet sind
- Filtern und Zusammenfassung von Tickets.
- Bei Bedarf Abrufen von Ereignissen, die einem Ticket zugeordnet sind.
- Regelmäßige Nachverfolgung wichtiger Updates für Tickets.
- Automatisierung von Ticketaktualisierungen und -abschlüssen basierend auf dem SIR-Incident-Status
- Master-Ticket-Update.
- Synchronisierung von Secureworks-Arbeitsprotokollen mit Security Incident Response Arbeitsnotizen.

### Richten Sie Ihre Now Platform -Instanz für die Secureworks CTP -Integration der Ticket-Erfassung ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

| Setupaufgabe | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform und Security Incident Response zugewiesen haben. | Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform -Instanz erforderlich.<br>• Ein Benutzer mit der Now Platform -Administratorrolle (admin) installiert die Anwendung aus ServiceNow Store und weist die SIR -Administratorrolle (sn_si.admin) zu.<br>• Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform:<br>◦ Benennt, erstellt und bearbeitet Profile.<br>◦ Wählt die Ticketfelder Secureworks CTP aus und ordnet sie den Security Incident-Feldern zu.<br>◦ Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.<br>◦ Plant die laufende Ticket-Erfassung.<br>◦ Ermöglicht Ticket-Updates, wenn ein SIR-Incident SIR erstellt und geschlossen wird.<br>◦ Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.<br>◦ Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.<br>Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Managing roles |
| Vergewissern Sie sich, dass Sie die folgenden Versionen verwenden:<br>• Secureworks Ticket-API 4.0<br>• Secureworks Event-API 1.0<br>• Secureworks-Ergänzungs-API 1.0 | Wenn Sie Zugriff auf das Portal Secureworks CTP haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgabe | Beschreibung |
| --- | --- |
| Sie die Anwendung für die Integration installieren. | ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br><br>**1.** Security Incident Response<br>**2.** Event and Alert Ingestion for Security Operations (Erforderlich für SIEM-Integrationen): Diese Anwendung erfordert:<br>○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit<br>○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub-Aktionsschritt – REST<br><br>**Hinweis:**<br>Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Event and Alert Ingestion“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport.<br><br>Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store .. |

### Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration der Secureworks CTP-Ticketerfassung

Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform integriert wird.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Wenn Sie die Ticket-Anwendung [] nicht aus dem Secureworks CTPServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** und suchen Sie die Kachel Secureworks CTP Integration der Ticket-Erfassung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die Anwendung zu konfigurieren, klicken Sie auf **Neu**.
4. Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld die Felder aus.
6. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung und Übermittlung wird jede Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

### Ergebnisse

Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden. Klicken Sie rechts oben auf der Seite in der **Auswahlliste Konfigurationen** anzeigen auf **Ja**.

### Erstellen Sie ein Profil für die Integration der Secureworks CTP-Ticketerfassung

Erstellen Sie ein Profil in Ihrer Instanz Now Platform, und bestimmen Sie, welche Tickets erfasst werden müssen und welche Tickets zum Erstellen von Security Incidents verwendet werden. Bevor Security Incidents aus erfassten Tickets erstellt werden, werden die Feldwerte aus Tickets in einem Layout eines Now Platform -Security Incident angezeigt, sodass Sie eine Vorschau darauf erhalten, wie der tatsächliche Security Incident angezeigt wird.

Mit der Integration können Sie Tickets basierend auf den Profilen erfassen, die Sie in der Security Operations -Umgebung Ihrer Instanz konfigurieren. Alle Tickets werden anfänglich für einen konfigurierten Tickettyp in einem Profil erfasst. Erfasste Tickets können dann weiter gefiltert werden, um anzugeben, welche Tickets Security Incidents verursachen.

Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für Tickets erstellen, die als hohes Risiko identifiziert wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Tickets erstellt, werden einzelne Feldwerte in den Tickets den entsprechenden Feldern in einem Layout von Security Incidents für eine Vorschau zugeordnet.

### Identifizieren Sie die Quelle des Profils

Geben Sie den Namen und die Quelle des Profils an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

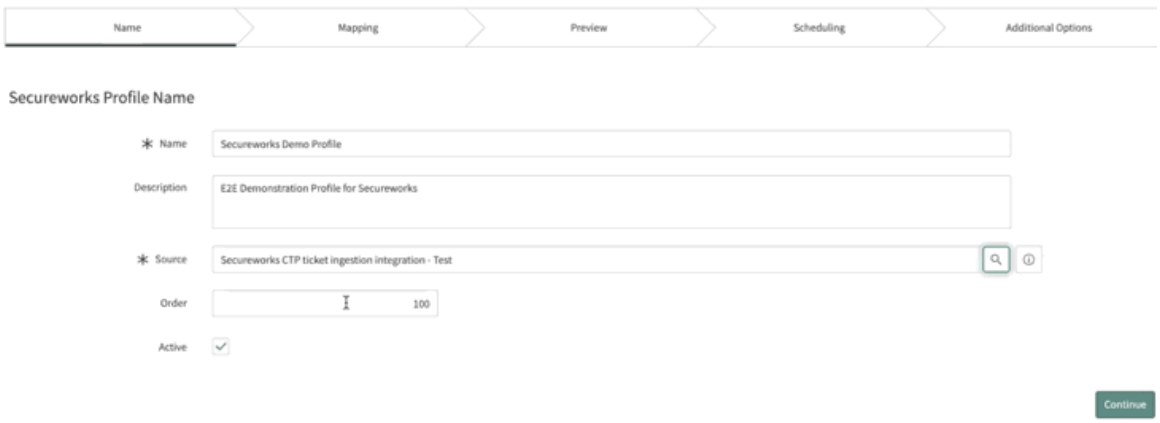
### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Prozedur

1. Um ein Profil für ein Ticket in Ihrer Instanz Now Platform zu erstellen, navigieren Sie zu **Integration der Secureworks-Ticketaufnahme** > **Secureworks-Profile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.




### Nächste Maßnahme
Ordnen Sie die Ticketfelder zu.

#### Zuordnung von Ticketfeldern für die SecureWorks CTP-Integration

Ordnen Sie die Ticket- und Event-Felder den Feldern im Security Incident-Formular zu.

Für den Zuordnungsschritt müssen Sie zuerst Beispieltickets erfassen und dann sicherstellen, dass alle relevanten Ticketfelder der entsprechenden Stelle im Formular Security Incident Response zugeordnet sind, und dann den Security Incident im Vorschaubereich visualisieren.

Die Zuordnung der Beispielticketfelder umfasst Folgendes:

- Beispieldaten abrufen und ausfüllen: Siehe Secureworks-Beispieltickets werden erfasst
- Ticketfelder dem Security Incident zuordnen: Siehe Secureworks-Ticketfelder werden Security Incident-Antwortfeldern zugeordnet

#### Secureworks-Beispieltickets werden erfasst

Wählen Sie die Beispieltickets aus, die erfasst werden sollen.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Sie können entweder die fünf letzten Beispieltickets abrufen oder die eindeutigen Ticket-IDs für die spezifischen Tickets angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   **Wählen** Sie in der Auswahlliste „Erfassungseinstellung“ eine der folgenden Optionen aus:
   - Letzte Tickets abrufen: Die 5 letzten Tickets werden abgerufen.
   - Tickets basierend auf Ticket-ID auswählen: Geben Sie die Ticket-ID für das abzurufende Ticket an. Sie können maximal 5 durch Kommas getrennte Ticket-IDs angeben.
3. Klicken Sie auf **Beispieldaten abrufen**, um die neuesten Beispielticketdaten vom Server Secureworks CTP abzurufen.
   Der Abruf für Beispieltickets kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt. Die abgerufenen Tickets werden als einzelne Registerkarten angezeigt. Klicken Sie auf eine Registerkarte, um die Ticketdaten anzuzeigen. Für jedes Ticket sehen Sie die Ticketfelder und ihre Werte sowie Details des beitragenden Ereignisses, das das Ticket ausgelöst hat.

**Hinweis:**
Details zu beitragenden Ereignissen werden nur angezeigt, wenn sie in den letzten 7 Tagen aufgetreten sind. Events, die älter als 7 Tage sind, werden nicht angezeigt.

### Nächste Maßnahme
Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie im nächsten Schritt die Ticketfelder dem Security Incident zu.

#### Secureworks-Ticketfelder werden Security Incident-Antwortfeldern zugeordnet

Ordnen Sie einzelne Ticket- oder Event-Felder Feldern in einem Now Platform SIR Security Incident zu.

### Ticket-Feldzuordnung

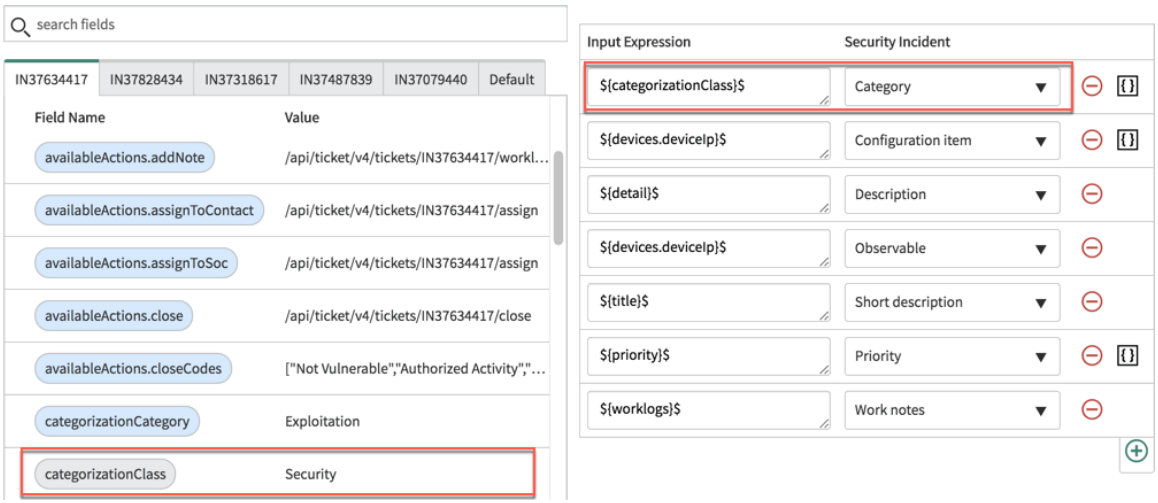
Verwenden Sie als Benutzer mit der Rolle „sn_si.admin“ die Felder aus dem Abschnitt „Beispieltickets“ auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte **SIR-Incident-Feldzuordnung** zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Ticket- oder Event-Felder von der linken Seite ziehen und sie im Abschnitt „SIR-Incident-Feldzuordnung“ auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Ticketfeld einem ausgehenden Security Incident-Feld zu.

1. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.
2. Sie können den Feldnamen manuell in die Spalte Eingabeausdruck eingeben oder den Feldnamen per Drag-and-Drop verschieben. Beispiel: Beschreibungund Ablegen in einem Feld in der Spalte **Eingabeausdruck** neben einem Feldnamen in der Spalte **Security Incident**.

   Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird categoryClass dem Feld Kategorie im Security Incident zugeordnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn Sie den Event-Feldnamen manuell im Abschnitt „ **Eingabeausdruck** “ eingeben, müssen Sie vor dem Namen des zugeordneten Felds das Präfix `${Event:eventfield}$` hinzufügen.

Um sicherzustellen, dass keine Ticket- oder Event-Felder im Zuordnungsprozess übersehen oder dupliziert werden, sind die Felder farbcodiert. Die Farbcodierung der Ticketfelder hilft Ihnen, die Ticketwerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Ticketinformationen nicht zugeordnet wurden.

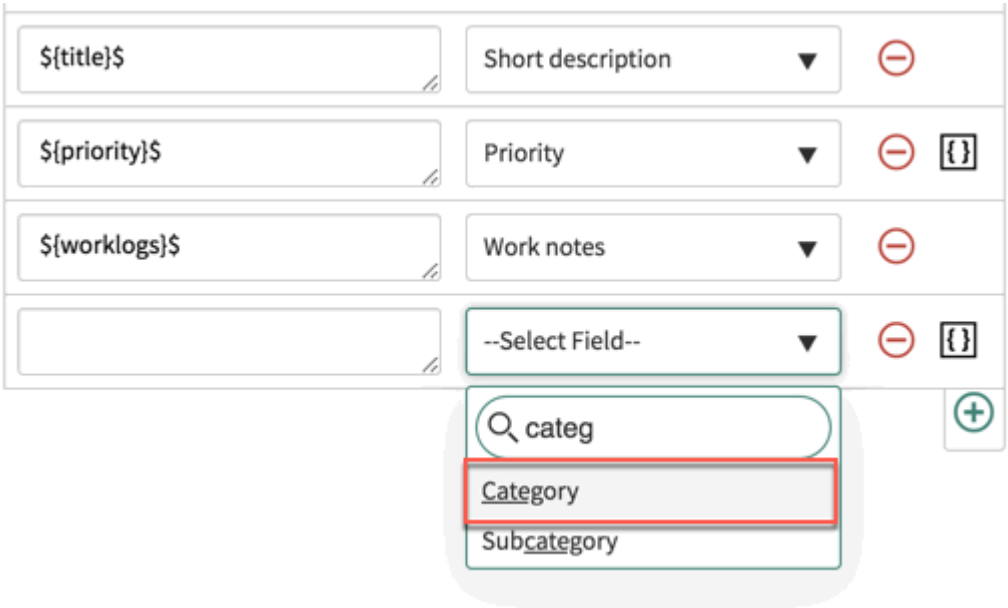
Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Ticketfeld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes Ticket- oder Event-Feld mehr als einem Feld in einem Security Incident zuordnen. Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:
   a. Klicken Sie rechts im Formular im Abschnitt SIR Incident-Feldzuordnung am unteren Rand des Rasters auf das Pluszeichen (+). Ein neues Feld wird angezeigt.
   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat die Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Ticketfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die bereits zugeordneten SIR Incident-Felder nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

**c.** Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

**d.** Wählen Sie auf der linken Seite des Formulars das Ticketfeld aus, und ziehen Sie es per Drag-and-Drop in ein entsprechendes Security Incident-Feld auf der rechten Seite.

4. Entfernen Sie Felder mithilfe des Symbols „-“ neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“.
5. Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder daraus entfernen.

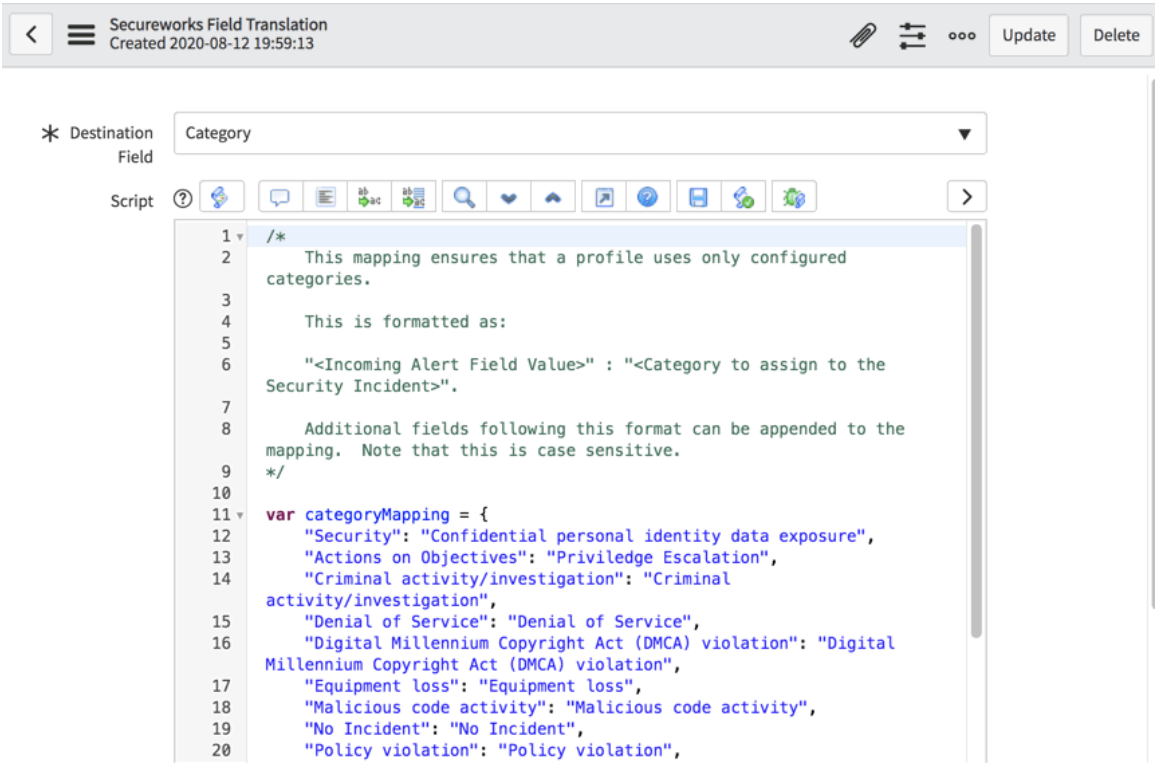
**Formatfeldübersetzung**

In bestimmten Fällen werden Ticketfelder möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Zum Beispiel kann mit dem Skript-Editor ein Kategoriewert von Malware-Warnung und Virusinfection unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mit in eine gemeinsame böswillige Codeaktivität im Feld Kategorie des Security Incident SIR übersetzt werden Funktion „Formatfeldübersetzung“.

Um den Skript-Editor zu verwenden, klicken Sie auf das Symbol {} neben dem Feld Kategorie. Der Skript-Editor wird



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




angezeigt.

Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern und zur Seite „Zuordnung“ zurückzukehren.

## Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um anzugeben, welche Tickets Security Incidents erstellen sollen und welche Tickets herausgefiltert werden sollen, z. B. Tickets mit niedriger Priorität. Sie können dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ticket erfüllen muss, um einen Security Incident zu erstellen. Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

1. Scrollen Sie im Formular zum Abschnitt „ **Bedingungen für Incident-Generierung** “, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern, um die Option zu aktivieren.

   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt **Beispiel für Ticket** -Erfassung für die erfassten Tickets angezeigt werden. Diese Felder sind dynamisch und ändern sich in Abhängigkeit von den Tickets, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des Tickets Secureworks CTP übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu Ihrer Secureworks CTP -Konsole zurück und überprüfen Ihre Tickets für die Stichwörter.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die Ticket-Felder „ `worklogs“`, „ `devices`“, „ `attaches`“, „ `watchers`“, „ `availableactions`“ und „`closeCodes“` können mehrere Werte haben (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie für diese Felder die Filterbedingung `Enthält` verwenden, um sicherzustellen, dass die Daten richtig gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**.
   - Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Diese Art der Filterung der Incident-Generierungsbedingung hilft Ihnen, die Tickets einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegenden Regeln oder Filter zu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden Security Incidents nur Tickets zugeordnet, die allen Kriterien entsprechen.

## Ticket-Zusammenfassungskriterien, um ähnliche Tickets zu behandeln und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Ticket-Zusammenfassungskriterien, die ein eingehendes Ticket zu einem vorhandenen SIR Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Ticketdaten in einem einzigen Security Incident platziert werden. Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen:

1. Scrollen Sie im Formular zum Abschnitt „ **Kriterien** für **Ticketzusammenfassung** “, und aktivieren Sie das Kontrollkästchen Zusammenfassungsbedingungen, um diese Option zu aktivieren.

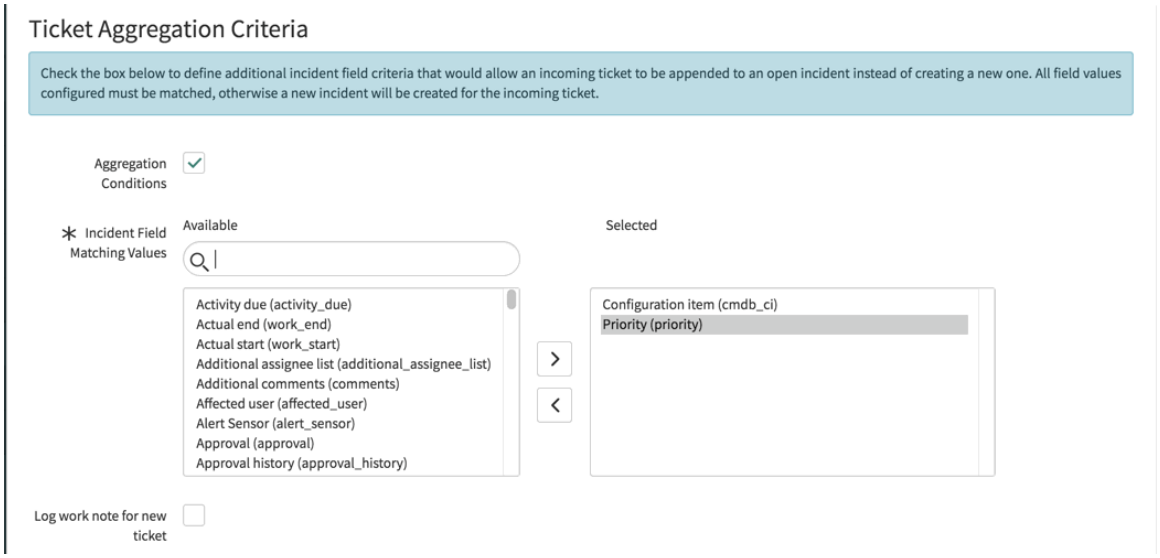
   Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.

2. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Ihrer NOW Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um dieses eingehende Ticket an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder wie erkennbare Elemente und Konfigurationselemente, denen mehrere Ticket-Feldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte abgeglichen wird, sind die Bedingungen für die Ticketzusammenfassung nicht erfüllt, und es wird ein neuer Security Incident erstellt. Im Screenshot unten sehen Sie die Zuordnung von Feldern mit mehreren Werten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn ein neues Ticket mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird das neue Ticket automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Tickets in einer zugehörigen Liste zu einem Security Incident anzeigen. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum diese Tickets zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte in einem Security Incident nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter **Zugehörige Links**, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.

**Hinweis:**
Die zugehörige Liste „Secureworks Aggregierte Tickets“ ist mit dem Basissystem nicht verfügbar. Sie müssen das Layout der zugehörigen Liste konfigurieren und es explizit in die anderen zugehörigen Listen einbeziehen.

3. (Optional) Um eine Arbeitsnotiz für ein neues Ticket zu protokollieren, das kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie diese Option. Die Arbeitsnotiz protokolliert, dass ein neues Ticket hinzugefügt wurde, zusammen mit einem Link zu den Ticketdetails und anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben Werte aus einem Ticket Secureworks CTP erfolgreich Feldern in einem Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung zu begrenzen. Sie haben auch Tickets an vorhandene Security Incidents angehängt, wenn Ticket-Feldwerte mit den konfigurierten Zusammenfassungskriterien übereinstimmen.

4. Klicken Sie auf **Fortfahren**, um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem SIR Security Incident zugeordnet haben

### Zeigen Sie eine Vorschau der zugeordneten Werte im Security Incident an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem SIR Security Incident zugeordnet haben. Mit diesem



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

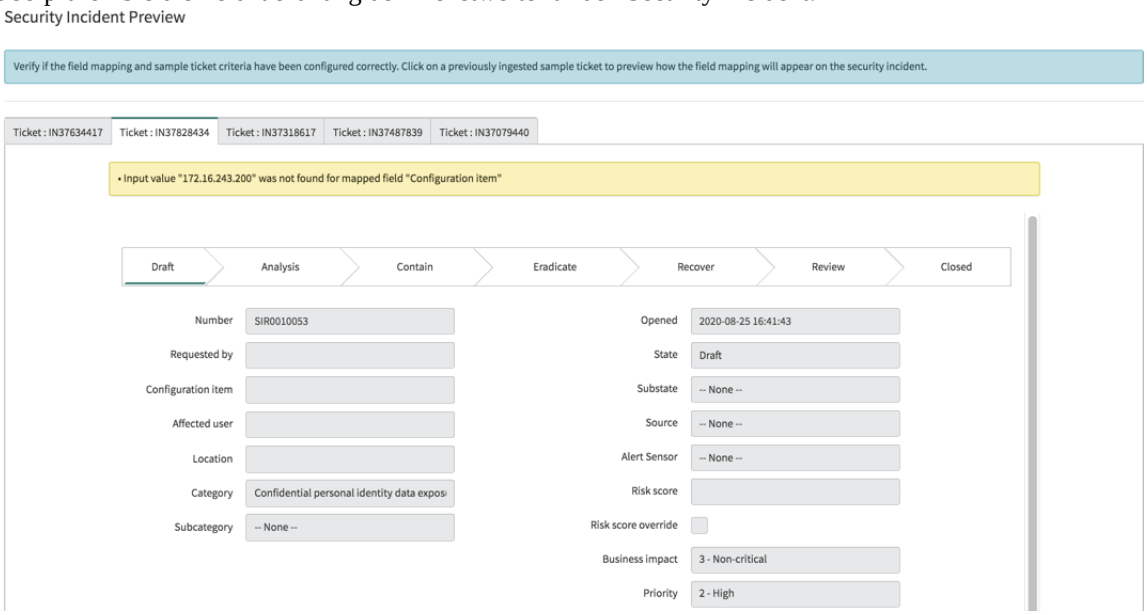
Vorschauschritt können Sie überprüfen, ob Sie alle Ticketfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie eine Vorschau eines Security Incident an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents im Security Incident Response-Produkt gespeichert.

### Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
   Die Tickets werden als Registerkarten angezeigt.
2. Klicken Sie auf eine Registerkarte, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Ticketwerte für den Security Incident.




   Die obige Abbildung zeigt ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

### Nächste Maßnahme
Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind. Definieren Sie den Zeitplan.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definieren Sie einen Zeitplan für die Secureworks CTP-Ticket-Erfassung

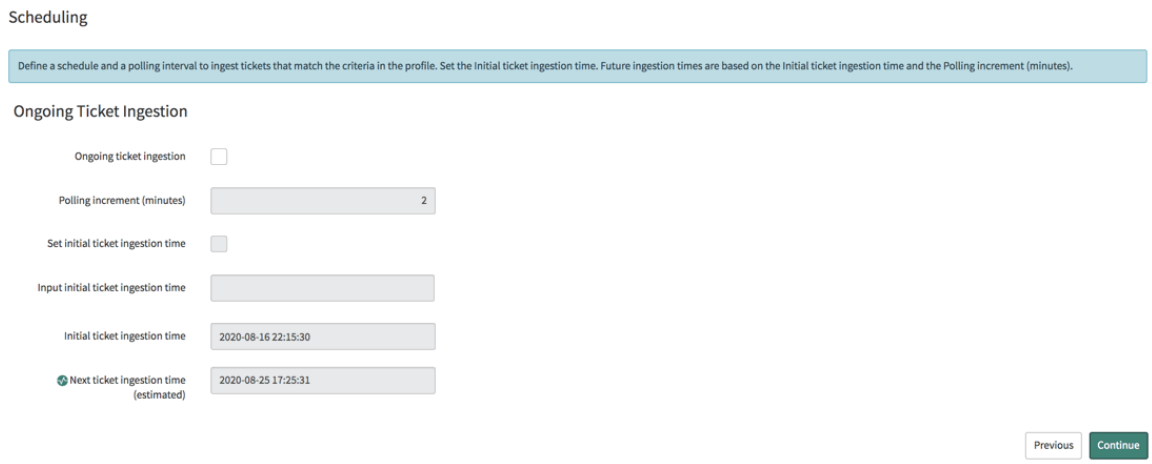
Überprüfen Sie die Standardeinstellungen für den Ticketabruf, oder ändern Sie die Planung nach Bedarf. Mit diesem Schritt können Sie Ihren Ticketabruf basierend auf einem Datumsbereich und einem Abfrageintervall filtern.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können auch auswählen, wie oft zukünftige Tickets abgefragt werden sollen, die der Ticketprofilkonfiguration entsprechen. Konfigurieren Sie diese Abfrageintervalle pro Profil. Bei der Planung möchten Sie möglicherweise die Systemlast mit der Dringlichkeit von Incidents in Einklang bringen. Für jedes Profil wird ein Standardwert von einer Minute festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des Incident und der erwarteten Auslastung Ihres Systems ändern.

#### Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie einen aus, um zu planen, wie und wann Tickets aus dem Secureworks CTP -Portal abgerufen werden.




3. Klicken Sie auf **Fortfahren**, um zur Seite „Zusätzliche Optionen“ zu navigieren.

### Automatisieren Sie die Aktualisierung und den Abschluss von Tickets basierend auf dem SIR-Incident-Status

Die Integration der Secureworks CTP Ticket-Erfassung verfügt über eine bidirektionale Schnittstelle, die die Erstellung von Security Incidents durch Tickets ermöglicht, sowie über die Möglichkeit, die Tickets zu aktualisieren, sobald der Security Incident mit relevanten Incident-Details wie der Security Incident-Nummer erstellt und/oder geschlossen wurde , Zuweisungsgruppe, Security Incident-URL usw.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Schließen Sie die Konfiguration für die Aktualisierung von Tickets ab, wenn der Security Incident erstellt wird.
3. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen und das Profil in den Status **Warten** zu verschieben.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Profil erfolgreich eingerichtet. Aktivieren Sie dieses Profil, um Tickets basierend auf Ihrer Planung aus dem Portal Secureworks CTP abzurufen.

#### Optional: Kopieren Sie ein Secureworks-CTP-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Profile zu kopieren, um Zeit zu sparen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Benutzer mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.

### Prozedur

1. Navigieren zu **Alle** > **Integration der Secureworks-Ticketaufnahme** > **Secureworks-Profil**.
2. Wählen Sie in der angezeigten Secureworks-Profilliste ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste **Aktionen für ausgewählte Zeilen** auf **Kopieren**.
   Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält (Kopie). Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass der Spaltenstatus **Aktiv** auf „false“ gesetzt ist, da das Profil aktiviert werden muss.

### Nächste Maßnahme

Nachdem Sie die Konfigurationsschritte abgeschlossen haben, werden Sie aufgefordert, das neue Profil zu aktivieren.

#### Das Security Incident Response-Formular ändert sich nach der Ticket-Erfassung

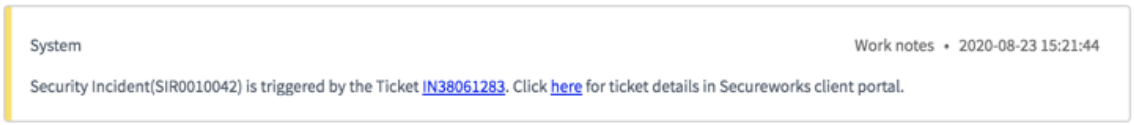
Nachdem ein Secureworks CTP -Ticket erfasst wurde, wird ein Security Incident erstellt und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

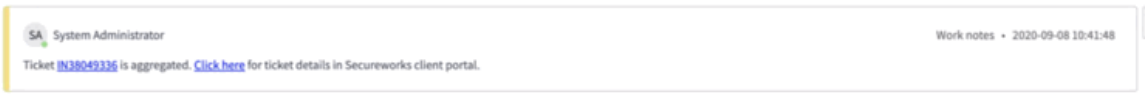
## Arbeitsnotiz

Eine Arbeitsnotiz mit Details zu dem Ticket, das den Security Incident ausgelöst hat, wird veröffentlicht.



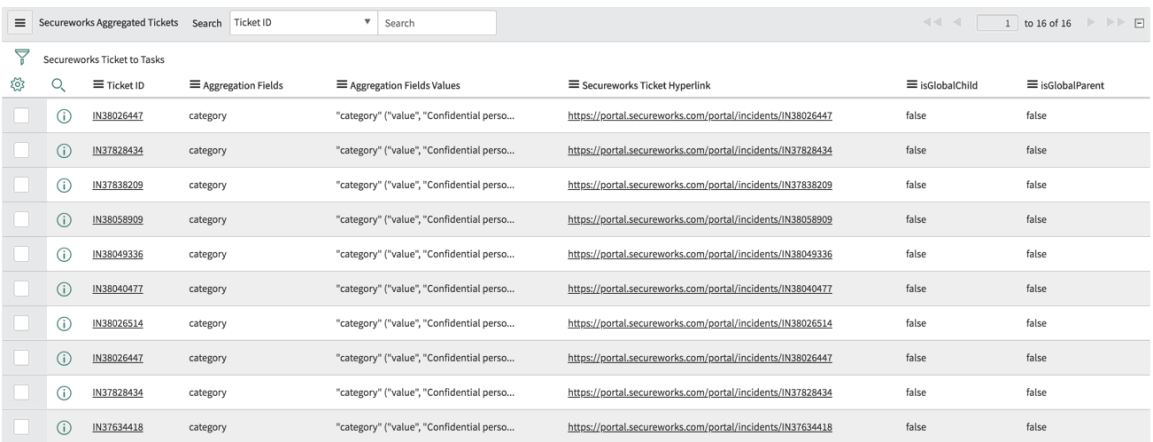

Klicken Sie auf den Ticket-Link, um zum internen Secureworks-Datensatz „Ticket zu Aufgabe“ zu navigieren. Der Hyperlink Hier **klicken** führt Sie zum Dashboard Secureworks CTP, in dem Sie die Ticketdetails anzeigen können.

Wenn Sie die Option **Arbeitsnotiz für neues Ticket** protokollieren in den Ticket-Zusammenfassungskriterien ausgewählt haben, wie auf der Seite „Profil erstellen: Zuordnung“ beschrieben, wird bei der Zusammenfassung des Tickets eine Arbeitsnotiz veröffentlicht.




## Zusammengefasste Tickets

Klicken **Zugehörige Listen** > **Zusammengefasste Secureworks-Tickets** , um das zum Security Incident zusammengefasste Ticket anzuzeigen. Klicken Sie auf den Ticket-Hyperlink, um das Ticket im Dashboard Secureworks CTP anzuzeigen.




| Ticket ID | Aggregation Fields | Aggregation Fields Values | Secureworks Ticket Hyperlink | isGlobalChild | isGlobalParent |
|---|---|---|---|---|---|
| IN38026447 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38026447 | false | false |
| IN37828434 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN37828434 | false | false |
| IN37838209 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN37838209 | false | false |
| IN38058909 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38058909 | false | false |
| IN38049336 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38049336 | false | false |
| IN38040477 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38040477 | false | false |
| IN38026514 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38026514 | false | false |
| IN38026447 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN38026447 | false | false |
| IN37828434 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN37828434 | false | false |
| IN37634418 | category | "category" ("value", "Confidential perso... | https://portal.secureworks.com/portal/incidents/IN37634418 | false | false |

Security Incident erstellen: Wählen Sie ein Ticket aus der Liste aus, klicken Sie auf das Menü **Aktionen**, und klicken Sie auf **Security Incident erstellen**. Mit dieser Option wird ein neuer Security Incident für das Ticket erstellt. Dieses Ticket wird aus dem übergeordneten Security Incident deaggregiert.

Ticketdatensatz löschen: Wählen Sie ein Ticket aus der Liste aus, klicken Sie auf das Menü **Aktionen** und dann auf **Löschen**. Mit dieser Option wird der Ticketdatensatz gelöscht.

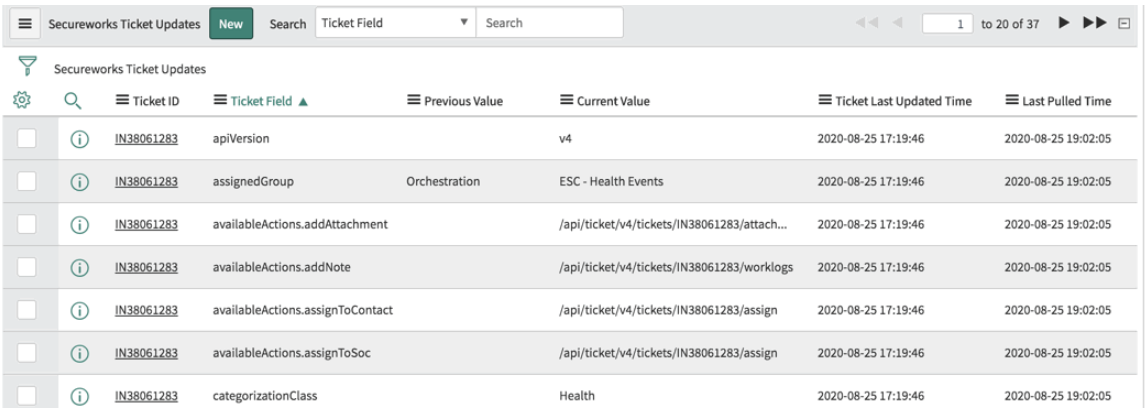
## Secureworks-Ticket-Updates

Dadurch werden die Standardticketfelder angezeigt und Änderungen an den Tickets während jedes Abfrageintervalls nachverfolgt. Das ist hilfreich, da Sie alle Ticket-Updates direkt anzeigen können, ohne zum Dashboard Secureworks CTP navigieren zu müssen. Alle



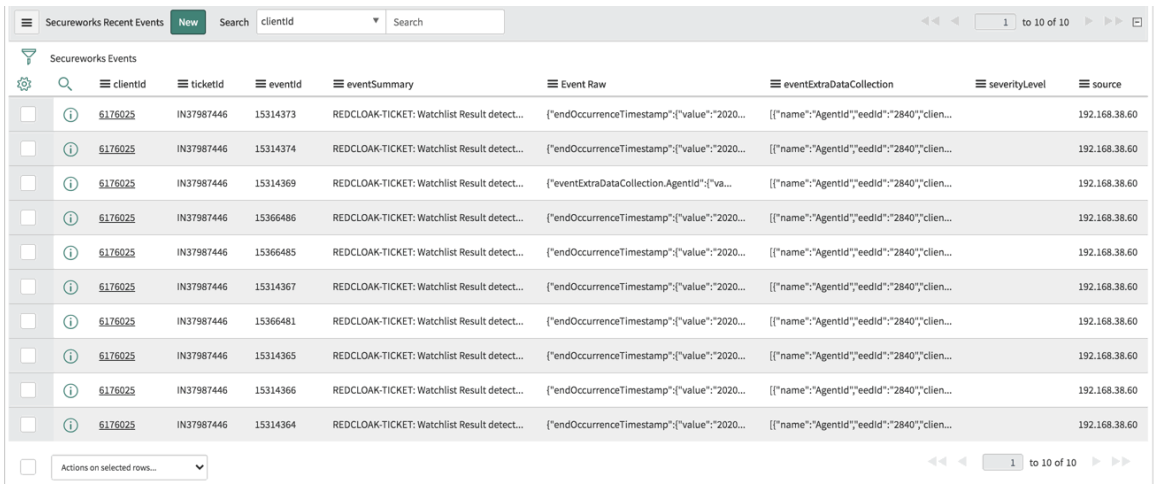
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Änderungen an den Werten werden in den Feldern Vorheriger Wert und Aktueller Wert angezeigt.




## Neueste Secureworks-Ereignisse

Klicken Sie unter den zugehörigen **Links** auf die Option **Letzte Secureworks-Ereignisse abrufen**, um die neuesten Secureworks-Ereignisse anzuzeigen.




Standardmäßig werden maximal 50 Events angezeigt. Sie können diese Standardeinstellung in den Secureworks-Integrationseinstellungen ändern.

### Zeigen Sie die Secureworks-Tickets und die entsprechenden Security Incidents an

Die importierten Secureworks CTP Tickets werden anfänglich in der Tabelle „Ticketimport“ gespeichert. Zeigen Sie alle Secureworks CTP Tickets an, die importiert wurden, bevor Filterbedingungen angewendet werden.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Prozedur**

1. Navigieren zu **Alle** > **Integration der Secureworks-Ticketaufnahme** > **Sicherer Ticketimport**.
2. Sie können alle Secureworks CTP Tickets anzeigen, die importiert wurden, bevor sie zusammengefasst oder Filterbedingungen angewendet werden.
3. Klicken Sie auf eine Ticket-ID, um die Ticket-Rohdaten anzuzeigen.
4. Navigieren zu **Secureworks-Ticket-Erfassung** > **Secureworks-Ticket zu Aufgabe**.
   Die Tickets Secureworks CTP werden mit den entsprechenden Security Incidents angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Secureworks CTP Master-Ticketabschlusshinweis

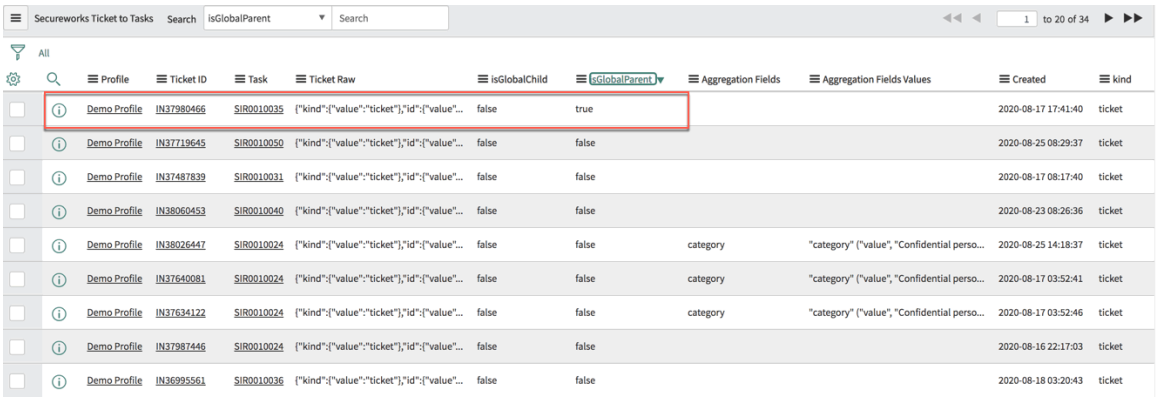
Bevor Sie einen Security Incident schließen, der von einem Master-Ticket Secureworks CTP erstellt wurde, müssen Sie überprüfen, ob alle dem Master-Ticket zugeordneten untergeordneten Tickets geschlossen sind.

## Vorbereitungen

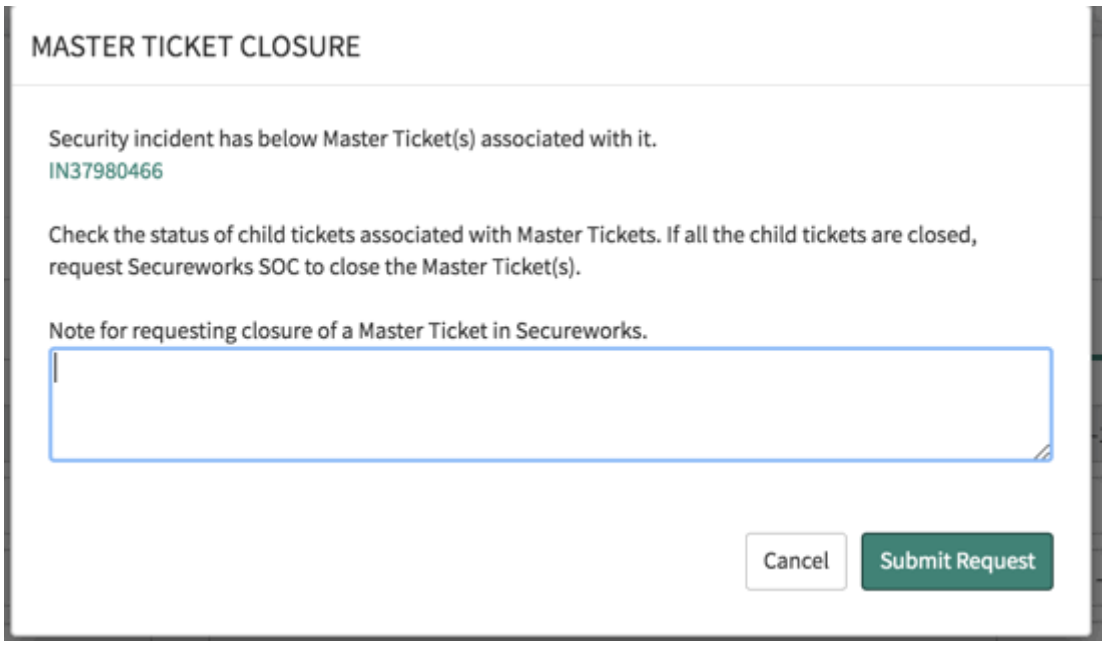
Erforderliche Rolle: sn_si.admin

## Prozedur

1. Navigieren zu **Alle** > **Secureworks-Ticket-Erfassung** > **Secureworks-Ticket zu Aufgabe**.
   Die Tickets Secureworks CTP werden mit den entsprechenden Security Incidents angezeigt.




2. Klicken Sie auf den Security Incident, wobei das Feld **isGlobalParent** auf **true gesetzt ist.**
3. Ändern Sie den Status des Security Incident in **Geschlossen**, geben Sie die Abschlusscodes an, und klicken Sie auf **Speichern**.
   Das folgende Dialogfeld wird angezeigt.




Dieser Security Incident ist einem Secureworks Master-Ticket zugeordnet. Einem Master-Ticket kann ein oder mehrere untergeordnete Tickets zugeordnet sein. Bevor das Master-Ticket geschlossen werden kann, müssen Sie zuerst überprüfen, ob alle diesem Master-Ticket zugeordneten untergeordneten Tickets geschlossen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

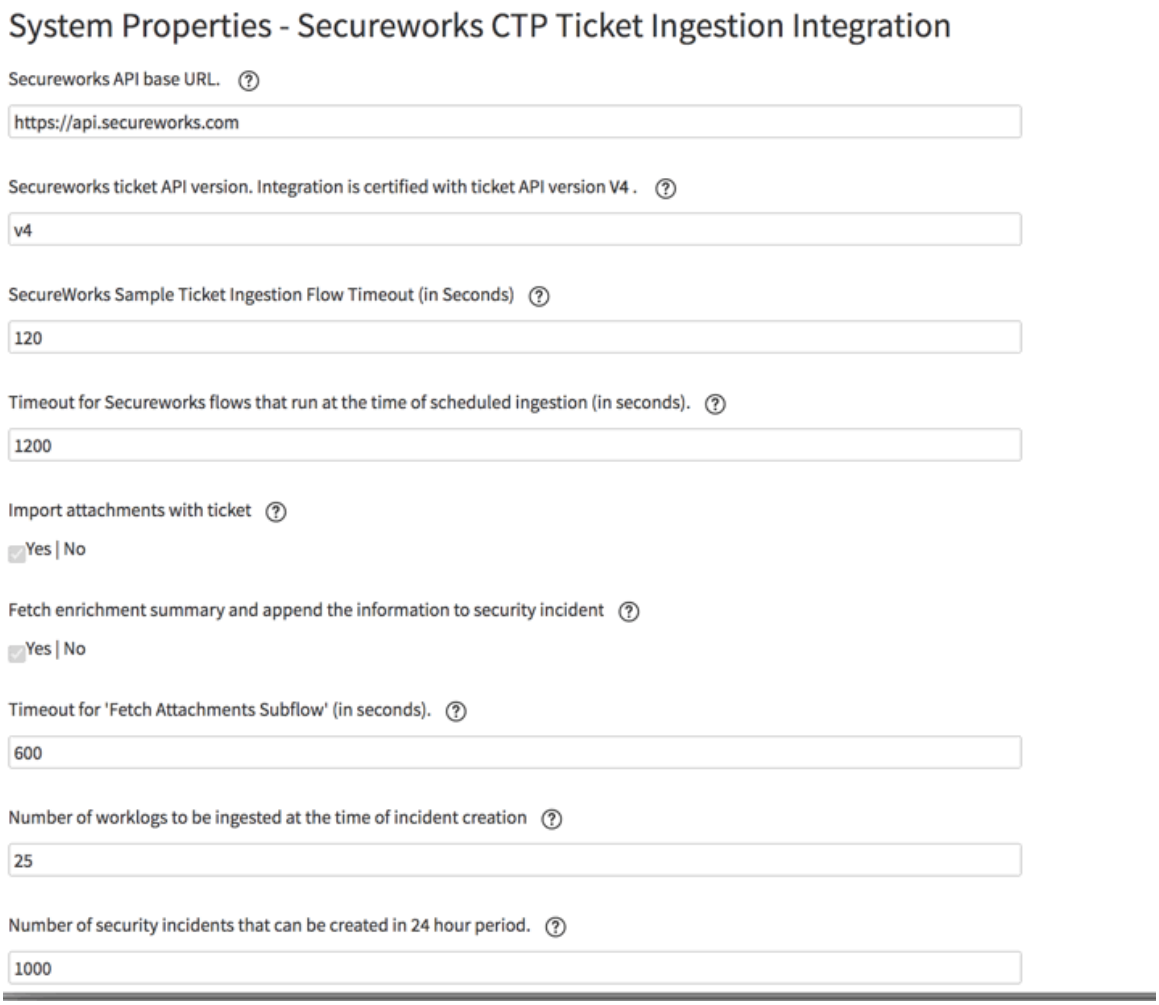
4. Fügen Sie in Secureworks eine Notiz hinzu, in der der Abschluss des Master-Tickets angefordert wird, und klicken Sie auf **Anforderung**senden.
   Das Master-Ticket wurde jetzt dem Secureworks SOC-Team zugewiesen.
5. Sobald die Anforderung übermittelt wurde, können Sie den Security Incident schließen.
6. Navigieren zu **Anwendung** > **Modul**.

### Konfigurationseinstellungen für die Secureworks CTP-Integration

Verwenden Sie diese Option, um die Standardsystemeigenschaften der Ticket-Erfassungsintegration Secureworks CTP zu ändern.

Um die Systemeigenschaften zu ändern, melden Sie sich als Benutzer mit der Rolle *sn_si.admin* an, und navigieren Sie zu **Integration der Secureworks-Ticketaufnahme** > **Secureworks-Integrationseinstellungen**.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.




Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

## Integration von Security Incident Response mit zScaler

Sie können das Produkt Integration von Security Incident Response mit zScaler verwenden, um die Protokolle Ihres Zscaler Internet Access Servers (ZIA) mit dem Now Platformzu verbinden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dieser Integration können Sie Dashboards anzeigen, benutzerdefinierte Warnungen erstellen und Security Incidents untersuchen.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Übersicht

Das Internet- und Web-Gateway-Produkt Zscaler wird über die Cloud bereitgestellt. Sie erhalten die wichtigsten Datenpunkte und Einblicke in die Sicherheitsumgebung Ihres Unternehmens. Integration von Security Incident Response mit zScaler verbindet das Produkt Zscaler Internet Access mit Ihrer Instanz Now Platform. Durch die Verwendung des Produkts [ Zscaler in Now Platformerhalten Sie mehr Einblicke in die Internetnutzung Ihrer Organisation.

## Schlüsselfunktionen der Integration

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Reputationssuche von erkennbaren Elementen in der globalen Bedrohungsbibliothek, die vom Produkt Zscaler verwaltet wird.

  **Hinweis:**
  Die globale Bedrohungsbibliothek Zscaler listet Bedrohungen nach Trends, Herkunftsland, Ziel, Volumen und verschiedenen Bedrohungskategorien auf. Mit dieser globalen Bedrohungsbibliothek können Sie Ihre erkennbaren Elemente im Hinblick auf die globale Bedrohungslandschaft untersuchen.

- Wartung von erkennbaren Elementen in einer Sperrliste oder Allow-Liste im Produkt Zscaler.
- Möglichkeit zum Abrufen und Überprüfen von Sandbox-Berichten aus dem Produkt Zscaler für einen MD5-Hash. Die Cloud Sandbox-Funktion im -Produkt Zscaler wird ausgeführt und analysiert Dateien in einer virtuellen Umgebung, um schädliches Verhalten zu erkennen.
- Sicherheitswarnungen von Patienten-0-Events, die im Produkt Zscaler generiert werden, wenn ein Benutzer eine unbekannte schädliche Datei herunterlädt.
- Mehrere URL-Kategorielisten, die als Sperrlisten oder Allow-Listen fungieren, wie im Produkt Zscaler definiert.
- Now Platform Security Incidents, die mit Tags versehen werden können, um die URL-Kategorie zu identifizieren, der die erkennbaren Elemente hinzugefügt werden.
- Ablaufzeiträume, die die Größe der Einträge der URL-Kategorieliste beibehalten, indem ältere Einträge automatisch ablaufen oder entfernt werden.
- Genehmigungsworkflow zum Hinzufügen und Entfernen von erkennbaren Elementen aus den URL-Kategorielisten.
- URL-Kategorieeinträge, die mit Datensätzen erkennbarer Elemente und Security Incidents verknüpft werden können, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| Zscaler Produktdokumentations-Website | ZScaler-Website mit Produktdokumentation |
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |

### Erste Schritte mit Integration von Security Incident Response mit zScaler

Aktivieren und richten Sie das Produkt Zscaler Internet Access als Schnittstelle mit Ihrer Instanz von Security Incident ResponseNow Platform und dem Produkt von [] ein.

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Weisen Sie die erforderlichen Rollen Now Platform und Security Incident Response zu, und überprüfen Sie sie. | Diese Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Die Administratorrolle installiert die Integration aus dem ServiceNow Store und weist die Rolle sn_si.admin zu.<br>• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:<br>  ○ Konfiguriert die Integration.<br>  ○ Erstellt, aktiviert und entfernt die URL-Kategorielisten.<br>  ○ Weist die Rolle sn_si.analyst zu.<br>• Die Rolle „sn_si.analyst“ erstellt Einträge und funktioniert mit Security Incidents. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow installiert und aktiviert sind, bevor Sie diese Integration konfigurieren. | Das Plugin ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] ist erforderlich.<br><br>Das Plugin Security Incident Response (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten für das Produkt Security Incident Response. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen für die Integration installieren und aktivieren.<br><br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn diese Anwendungen noch nicht installiert sind, installieren und aktivieren Sie die einzelnen Anwendungen nacheinander in der folgenden Reihenfolge: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
| --- | --- |
| | 1. Security Incident Response Abhängigkeit (com.snc.si_dep)<br>2. Security Integration Framework<br>3. Security Support Common<br>4. Security Support Orchestration<br>5. Threat Intelligence Support Common<br>6. Trusted Security Circles<br>7. Security Operations Setup-Assistent<br>8. Security Incident Response |
| Überprüfen Sie die Versionen Zscaler. | • Diese Integration wird ab Zscaler Internet Access Version 1.0 oder höher unterstützt.<br>• Diese Integration wird mit den folgenden Zscaler -Versionen getestet:<br>○ Zscaler Client Connector für Windows – 3.0<br>○ Zscaler Client Connector für macOS – 3.0<br>○ Zscaler-Client-Connector für Linux – Beta<br>○ Zscaler Cloud Connector – 6.1 |
| Vergewissern Sie sich, dass Sie über die erforderlichen Zscaler Berechtigungen verfügen und konfiguriert haben Zugriff auf Zscaler Internet Access APIs. | • Sie benötigen die Administratoranmeldeinformationen für Zscaler Internet Access.<br>• Sie benötigen ein gültiges Cloud Service API-Abonnement. Zscaler Der Support muss Ihren Schlüssel bereitstellen.<br>• Sie benötigen Zscaler Internet Access Administratoranmeldeinformationen (Benutzername und Passwort). Die API-Authentifizierung basiert auf einer Kombination aus API-Schlüssel und Zscaler Internet Access Administratoranmeldeinformationen.<br>**Hinweis:** Weitere Informationen zum Verwalten der Zscaler Internet Access -API-Schlüssel finden Sie in der Zscaler-Dokumentation . |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie den Zugriff auf Zscaler Internet Access APIs

Konfigurieren Sie den Zugriff auf den Server Zscaler Internet Access, um die sichere Verbindung zwischen der Instanz Now Platform und dem Server Zscaler ] zu authentifizieren.

#### Vorbereitungen
Erforderliche Rolle: Zscaler Internet Access admin

#### Warum und wann dieser Vorgang ausgeführt wird
Nachdem Zscaler Ihr API-Abonnement für den Cloud-Service Ihrer Organisation aktiviert hat, ist es auf der API-Schlüsselverwaltungsseite von Zscaler Internet Access mit der Basis-URL verfügbar. Ihre Organisation kann nur einen API-Schlüssel oder ein Token haben. Löschen Sie den vorhandenen Schlüssel oder das vorhandene Token, bevor Sie einen neuen hinzufügen.

Die Basis-URL für die API lautet `${Cloud_Name}/api/v1`. Überprüfen Sie den Cloud-Namen Zscaler, der für Ihre Organisation bereitgestellt wurde, und verwenden Sie ihn, um `{Cloud_Name}` im Basis-URI zu ersetzen. Beispiele für die Basis-URL:

- Beispiel.zscalerbeta.net
- Beispiel.zscalerone.net
- Beispiel.zscalertwo.net
- Beispiel.zscaler.net
- Beispiel.zscloud.net

**Hinweis:**
Weitere Informationen zum -Administrationsportal Zscaler Internet Access finden Sie in der Dokumentation zur Schlüsselverwaltung der Zscaler-API und in der Dokumentation zum Zscaler-Portal .

#### Prozedur

1. Melden Sie sich als Administrator beim Zscaler Internet Access -Administrationsportal an.
2. Navigieren zu **Administration** > **API-Schlüsselverwaltung**.
3. Klicken **Sie auf API-Schlüssel hinzufügen**.
   Wenn die Option **API-Schlüssel** hinzufügen nicht angezeigt wird, löschen Sie den vorhandenen Schlüssel. Der neue API-Schlüssel ist sofort gültig und wird auf der Registerkarte angezeigt.

#### Ergebnisse
Sie haben die Basis-URL und den API-Schlüssel abgerufen, um den Zugriff auf Zscaler über die Instanz Now Platform zu konfigurieren.

### Integration von Security Incident Response mit zScaler installieren und konfigurieren

Installieren und konfigurieren Sie das Internetzugriffsprodukt Integration von Security Incident Response mit zScaler aus dem [], um die Integration in Ihrer Instanz von Now PlatformServiceNow Store zu verwenden.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Laden Sie das Produkt Integration von Security Incident Response mit zScaler aus dem ServiceNow Store herunter, und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel Integration von Security Incident Response mit zScaler, und klicken Sie auf **Konfigurieren** > **Neue Konfiguration erstellen**.
4. Füllen Sie die Felder des Formulars aus.

**Zscaler Konfigurationsformular**

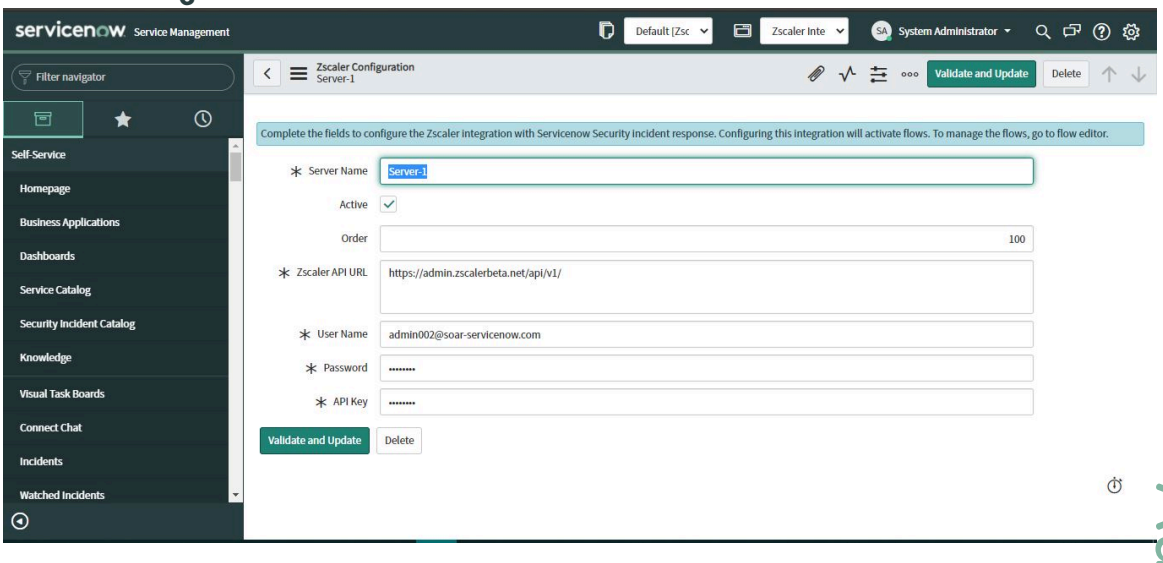
| Feld | Beschreibung |
|---|---|
| Servername | Zscaler Servername. Beispiel: ZSserver. |
| Aktiv | Indikator, der angibt, dass das Profil aktiv ist. |
| Reihenfolge | Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge der Workflows an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen.<br>Der Flow mit der niedrigsten Nummer hat die höchste Priorität.<br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300, 400.<br>Der Standardwert ist 100. |
| Zscaler API-URL | Basis-URL, die die Zscaler -API hostet. Beispiel: https://example.zscalerbeta.net |
| Benutzername | Benutzername für das Administratorkonto Zscaler Internet Access. |
| Passwort | Passwort für das Administratorkonto Zscaler Internet Access. |
| API-Schlüssel | API-Schlüssel, den Sie aus dem Zscaler Internet Access -Administrationsportal erhalten haben |

Das folgende Beispiel zeigt die Zscaler-Konfigurationsseite.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**ZScaler-Konfigurationsseite**




5. Klicken Sie **auf Validieren und aktualisieren**.

## Ergebnisse

Nachdem Sie diese Konfiguration validiert und gespeichert haben, kehren Sie zur Seite Zscaler „ Konfigurationen“ zurück.

### Fügen Sie Zscaler Internet Access URL-Kategorielisten hinzu

Fügen Sie die URL-Kategorien, die im Internetzugriffsprodukt Zscaler verfügbar sind, der Instanz Now Platform hinzu, um für jede URL eine Aktion anzugeben, sodass Sie einfachen Zugriff für granulare Filterung und Richtlinienerstellung haben.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

Integration von Security Incident Response mit zScaler bietet standardmäßige URL-Kategorielisten für Allow-Listen und Deny-Listen zum Filtern von Inhalten.

Die URL-Kategorien, die Sie in der Instanz Now Platform hinzufügen, sollten sich bereits in Ihrer Zscaler Internet Access -Umgebung befinden. Sie können Integration von Security Incident Response mit zScaler nicht zum Erstellen von URL-Kategorien auf Zscalerverwenden.

**Hinweis:**
Weitere Informationen zu URL-Kategorielisten im Produkt Zscaler finden Sie in der Zscaler-Dokumentation zu URL-Kategorien .

## Prozedur

1. Navigieren zu **Alle** > **ZScaler-Integration** > **ZScaler-URL-Kategorielisten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zscaler Formular „URL-Kategorielisten“

| Feld | Beschreibung |
|---|---|
| Quelle | Name des Servers. Sie können nur die zuvor konfigurierten Zscaler Internet Access Server aus der URL-Kategorieliste anzeigen. |
| Aktiv | Indikator, der angibt, dass die URL-Kategorieliste aktiv ist. |
| URL-Kategorie | Feld, das aktiviert wird, nachdem Sie die Quelle ausgewählt haben. Sie können die Liste der URL-Kategorien anzeigen, die in Zscalererstellt werden. |
| Ablaufzeitraum (in Tagen) | Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft.<br><br>Wenn Sie diesen Wert ändern, ist jedes erkennbare Element, das dieser URL-Kategorie hinzugefügt wurde, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben.<br><br>Wenn Sie beispielsweise die Ablauffrist auf 30 Tage festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt. |
| Tag anzeigen | Sicherheits-Tag, das im Security Incident SIR angezeigt wird<br><br>Wenn Sie die Option **Tag anzeigen** aktivieren, ist das Feld Zscaler Tag für erkennbare Elemente im Formular verfügbar. |
| Change-Anforderung erstellen | Change-Anforderung und Change-Aufgaben in Ihrer Now Platform -Instanz für die Datensätze, die an die URL-Kategorieliste angehängt sind.<br><br>Wenn Sie die Option **Change-Anforderungerstellen** aktivieren, ist das Feld Change-Anforderung im Formular verfügbar. |
| Genehmigung erforderlich | Liste der Genehmigergruppen. Nachdem Sie eine Anforderung gesendet haben, ist eine Genehmigung durch die Gruppe erforderlich, um die Anforderung abzuschließen.<br><br>Wenn Sie die Option **Genehmigung** erforderlich aktivieren, ist das Feld Genehmiger im **Formular** verfügbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beschreibung | Beschreibung der URL-Kategorieliste Zscaler. Verwenden Sie dieses Feld, um weitere Details zum URL-Kategoriedatensatz hinzuzufügen. |

4. Klicken Sie auf **Absenden**.
   Eine erfolgreiche Übermittlung löst eine E-Mail-Benachrichtigung an die Genehmigungsgruppe aus.

### Senden Sie erkennbare Elemente aus einem Security Incident-Datensatz an eine URL-Kategorieliste

Übermitteln Sie erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, mithilfe der Zulassungs- oder Blockierungsanforderung an eine konfigurierte URL-Kategorieliste. Durch das Hinzufügen von erkennbaren Elementen zur Allow- oder Sperrliste für Sicherheitsscans können Benutzer Inhalte von diesen URLs überprüfen und Zugriff auf vertrauenswürdige Inhalte erhalten.

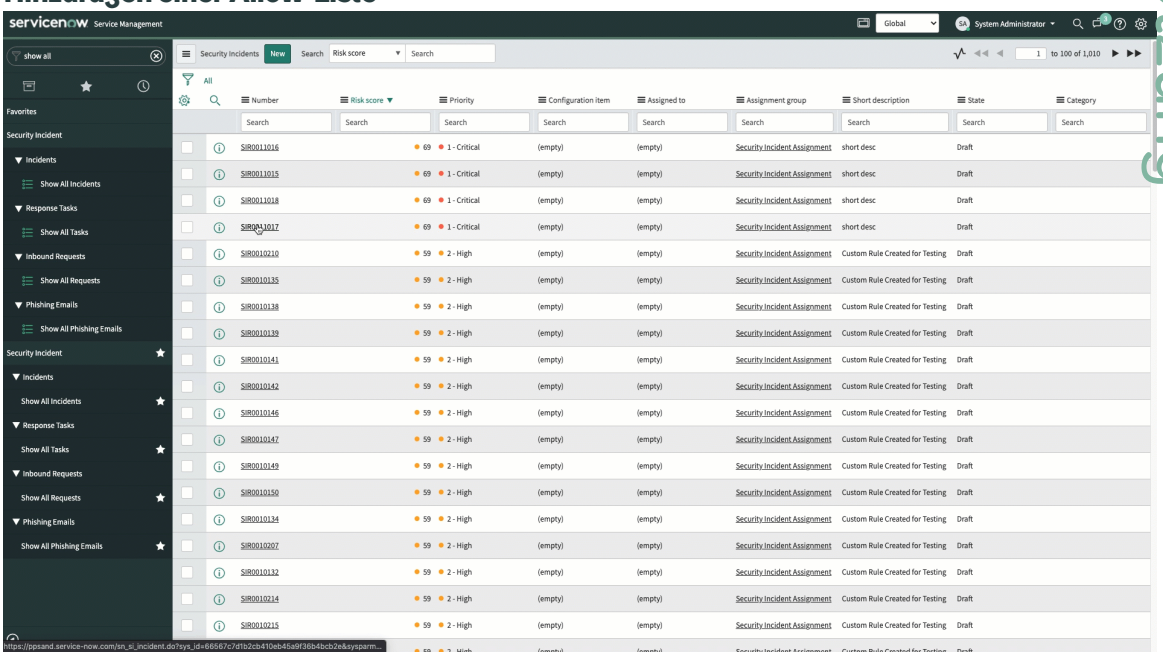
#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Sie übermitteln Einträge für erkennbare Elemente, indem Sie die Anforderungsaktion „Zulassen“ oder „Blockieren“ aus der zugehörigen Liste „Zugeordnete erkennbare Elemente“ verwenden. Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hinweisen. Verwenden Sie die Liste der zuvor konfigurierten URL-Kategorien, um das erkennbare Element auszuwählen, das Sie übermitteln möchten. Nachdem Sie die Anforderung gesendet haben, wird eine Genehmigungsanforderung an Ihre Genehmigungsgruppe gesendet.

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
   In diesem Beispiel sehen Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen und eine Allow-Liste hinzufügen.

**Hinzufügen einer Allow-Liste**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie den Security Incident aus, den Sie der Zscaler -Zulassungs- oder Blockierungsanforderung zuordnen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.
   Wenn Sie keine erkennbaren Elemente finden, klicken Sie auf **Neu**.
4. Wählen Sie ein erkennbares Element aus, und klicken Sie dann im Menü „Aktionen“ auf **Anforderung zulassen/blockieren**.
5. Wählen Sie im Dialogfeld „Allow/Block-Anforderung“ aus, ob die Allow- oder Block-Anforderung für das erkennbare Element ausgeführt werden soll.
6. Klicken Sie auf **Absenden**.
7. Zeigen Sie die Arbeitsnotizen an, um den Status Ihrer Übermittlung und die Sicherheits-Tags anzuzeigen. Klicken Sie auf die Links in den Arbeitsnotizen, um weitere Informationen zum Status zu erhalten oder die Details im Flow Designerzu analysieren. Sicherheits-Tags sind Metadaten im antwortenden Datensatz und definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll.
8. Um den Status des ausgewählten erkennbaren Elements anzuzeigen, navigieren Sie zu **Zscaler-Integration** > **Zscaler-URL-Kategorielisteneinträge**.
9. Klicken Sie auf der Seite Zscaler-URL-Kategorielisteneinträge auf das erkennbare Element, um den Datensatz anzuzeigen.

### Erkennbare Elemente für URL-Kategorielisten genehmigen

Genehmigen Sie erkennbare Elemente, die einer URL-Kategorieliste hinzugefügt werden, sodass sich die Einträge für erkennbare Elemente in den entsprechenden Allow- oder Deny-Listen befinden.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Zscaler-Genehmigungen**.
2. Wählen Sie den zu genehmigenden Datensatz aus.
3. Klicken Sie auf **Genehmigen**.
   Die Genehmigergruppe erhält eine E-Mail-Benachrichtigung für die Genehmigungsanforderung. Nachdem die Genehmiger in der E-Mail auf den Link **Genehmigen/Ablehnen geklickt** haben, ändert sich der Status in „Genehmigt“.

### Senden Sie den Security Incident an die URL-Kategorieliste Zscaler .

Übermitteln Sie Einträge direkt für erkennbare Elemente, die nicht mit einem bestimmten Now Platform Security Incident-Datensatz verknüpft sind, sodass sich die Einträge für erkennbare Elemente in den entsprechenden Allow- oder Deny-Listen befinden.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können der URL-Kategorieliste auch direkt aus dem Datensatz „Erkennbares Element“ erkennbare Elemente hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Zscaler-URL-Kategorielisteneinträge**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Zscaler Formular „URL-Kategorielisteneinträge“.**

| Feld | Beschreibung |
|---|---|
| Eingabewert | Name des erkennbaren Elements<br><br>Wenn ein übereinstimmendes erkennbares Element gefunden wird, wird der Rest des Formulars automatisch ausgefüllt.<br><br>Wenn kein passendes erkennbares Element gefunden wird, müssen Sie die restlichen Informationen manuell eingeben. |
| Erkennbares Element | Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. |
| Erkennbarer Typ | Klassifizierung erkennbarer Elemente, z. B. eine IP-Adresse oder ein Datei-Hash. |
| URL-Kategorieliste | URL-Kategorie. Wenn eine Organisation beispielsweise „example.com“ für Office 365-Services verwendet, kategorisiert Zscaler „ example.com“ als „Professional Services“ und „Office 365“. |
| Quelle | Name des Servers. Sie können nur die zuvor konfigurierten Zscaler Server aus der URL-Kategorieliste anzeigen. |
| Incident-Anzahl | Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow zu einem anderen Incident hinzugefügt wird. |
| Aktiv | Indikator, der angibt, dass die URL-Kategorieliste aktiv ist. |
| Status | Status, ob das erkennbare Element genehmigt oder abgelehnt wurde. |
| Ablaufzeitraum (in Tagen) | Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft.<br><br>Wenn Sie diesen Wert ändern, ist jedes erkennbare Element, das Sie dieser URL-Kategorie hinzufügen, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Wenn Sie beispielsweise die Ablauffrist auf 30 Tage festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt.<br><br>**Hinweis:**<br>Wenn Sie den standardmäßigen Ablaufzeitraum des URL-Kategorielisteneintrags ändern, wird eine Warnung angezeigt, dass sich der Zeitraum von dem Zeitraum unterscheidet, der in der ausgewählten URL-Kategorieliste konfiguriert ist. |
| Zusätzliche Information | Feld, in dem Sie weitere Details zum erkennbaren Element hinzufügen können. |

4. Klicken Sie auf **Absenden**.

### Führen Sie eine Bedrohungssuche mithilfe der globalen Bedrohungsbibliothek Zscaler aus

Führen Sie eine Bedrohungssuche für ein erkennbares Element aus, indem Sie die globale Bedrohungsbibliothek des Produkts Zscaler Internet Access verwenden. Zscaler unterstützt Suchvorgänge für erkennbare Elemente vom Typ IPs, URLs und Domänen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Wenn ein erkennbares Element zum ersten Mal einem Security Incident zugeordnet wird, führen alle aktiven Implementierungen der Bedrohungssuche in Now Platform eine automatische Bedrohungssuche durch. Sie können die Ergebnisse in der zugehörigen Liste „Ergebnisse der Bedrohungssuche“ anzeigen.

Standardmäßig wird die Konfiguration mit der geringsten Reihenfolge ausgewählt, um die Bedrohungssuche für die globale Bedrohungsbibliothek des Produkts Zscaler Internet Access durchzuführen. Sie können die Bedrohungssuche auch manuell durchführen.

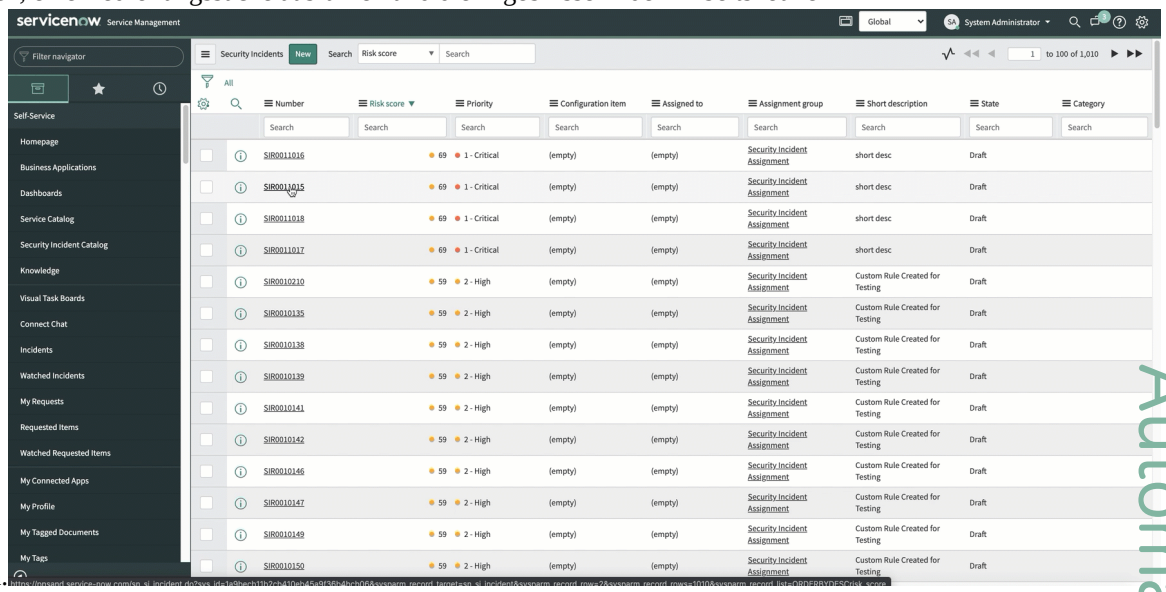
#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die Bedrohungssuche ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen“ auf **Bedrohungssuche ausführen**.
   In diesem Beispiel sehen Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen, eine Bedrohungssuche ausführen und die Ergebnisse in den Arbeitsnotizen anzeigen.




## Ergebnisse

Nachdem Sie die Bedrohungssuche initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen.

### An Zscaler Sandbox-Analyse senden

Verwenden Sie den Sandbox-Service Zscaler Internet Access für Produkte, um Dateien in einer virtuellen Umgebung zu analysieren und schädliches Verhalten zu erkennen.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Zscaler -Konfiguration erstellen, wird im Modul „Zscaler-Sandbox-Konfiguration“ standardmäßig eine Zscaler -Sandbox-Übermittlung erstellt.

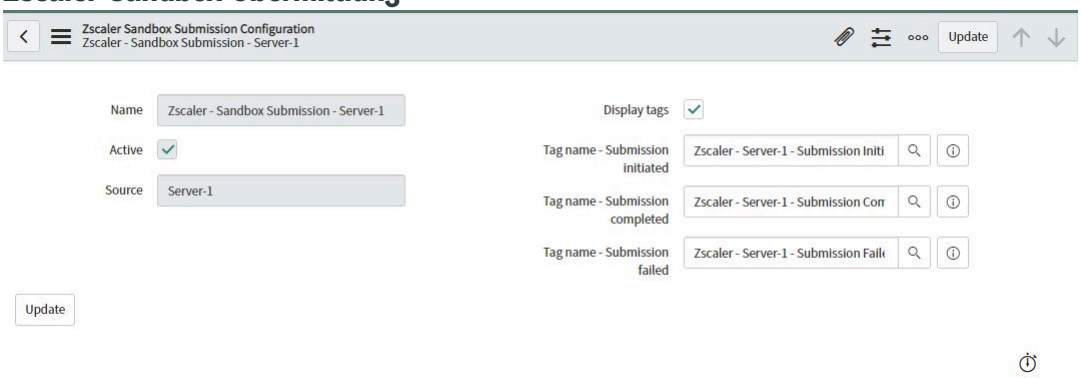
Die Felder „Name“ und „Quelle“ werden automatisch ausgefüllt, und die Konfiguration ist standardmäßig aktiviert. Sie können nur das Anzeige-Tag und die aktiven Optionen bearbeiten. Mit dem Produkt Zscaler Internet Access können Sie nur den Sandbox-Bericht für erkennbare Elemente des MD5-Hash-Typs abrufen.

Die Analyse für die Datei, die dem MD5-Hash zugeordnet ist, sollte abgeschlossen sein, und der entsprechende Bericht sollte sich in der Sandbox Zscaler befinden. Wenn der von Ihnen gesendete MD5-Hash keinen Bericht in Zscalerenthält, erhalten Sie eine Fehlermeldung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zscaler-Sandbox-Übermittlung




## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, für den Sie die Sandbox-Analyse ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.
4. Wählen Sie ein erkennbares Element vom Typ MD5-Hash aus, und wählen Sie dann im Menü Aktionen die **Option An Sandbox senden aus**.
   Erstellen Sie ein erkennbares Element vom Typ MD5-Hash, wenn Sie kein vorhandenes erkennbares Element vom Typ MD5-Hash finden.
5. Wählen Sie im Dialogfeld „Dateiübermittlung“ in der Übermittlungskonfiguration die Option **Zscaler - Sandbox-Übermittlung - Server** aus, und klicken Sie **auf An Sandbox senden**.
   Nachdem Sie die Sandbox-Übermittlung initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen. An den Security Incident wird auch ein Tag angehängt.
6. Klicken Sie in den Arbeitsnotizen auf den Link im Beitrag Sandbox-Übermittlungsergebnis.

## Ergebnisse

Sie können die Ergebnisse auch über die Registerkarte Alle zugehörigen Listen anzeigen und Sandbox-Übermittlungsergebnisse anzeigen.

### Richten Sie E-Mail-Benachrichtigungen für Patienten-0-Ereignisse ein

Konfigurieren Sie das Produkt Zscaler Internet Access, um unbekannte, potenziell schädliche Dateien zu identifizieren und nach ihnen zu scannen, z. B. Patienten-0-Ereignisse, damit Sie Ihr Netzwerk vor schädlichen Dateien schützen können.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin, Zscaler Internet Access admin

## Warum und wann dieser Vorgang ausgeführt wird

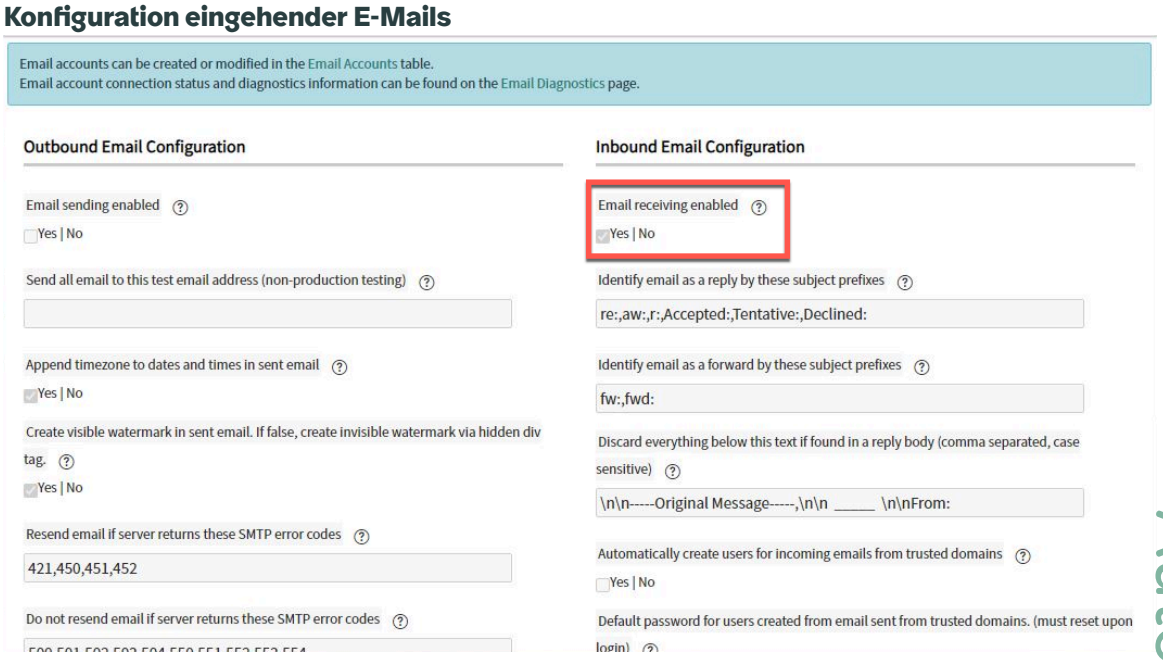
Patient O ist eine Warnungsklasse, die eine unbekannte Datei enthält, deren Download genehmigt wurde, die jedoch als böswillig befunden wurde. Das Ereignis „Patient 0“ wird als kritisch eingestuft. Sie können Now Platform so einrichten, dass er in regelmäßigen Abständen E-Mail-Benachrichtigungen für Patienten-0-Ereignisse erhält.

## Prozedur

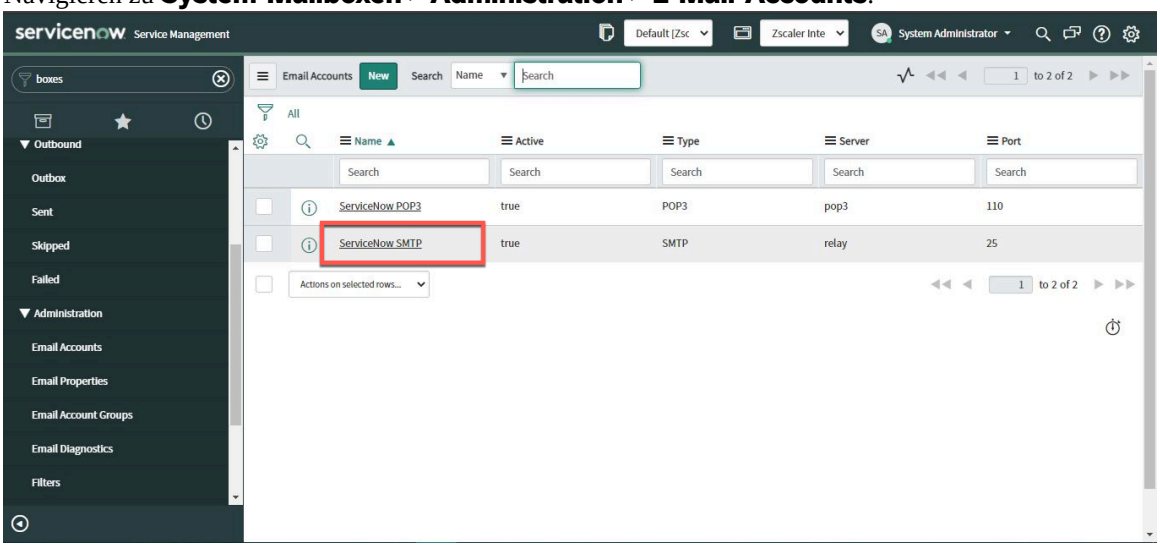
1. Navigieren zu **Alle** > **System-Mailboxen** > **Administration** > **E-Mail-Eigenschaften**.
2. Wählen Sie im Abschnitt „Konfiguration eingehender E-Mails“ die Option E- **Mail-Empfang aktiviert** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie auf **Speichern**.
4. Navigieren zu **System-Mailboxen** > **Administration** > **E-Mail-Accounts**.

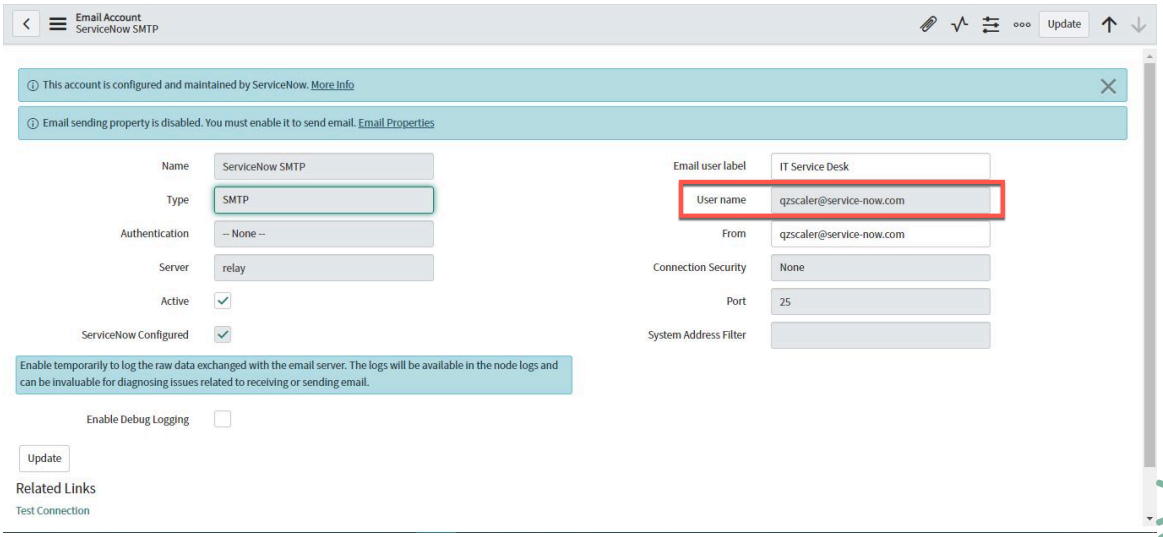



5. Wählen Sie das **SMTP-E-Mail-Konto von ServiceNow aus**.
   Notieren Sie sich den Benutzernamen. Der hier identifizierte Benutzername ist die E-Mail-Adresse Now Platform, die Sie zur Konfiguration in Zscaler für Warnungen zu Patient 0 verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Benutzername für den Now Platform-SMTP-Account**




6. Melden Sie sich beim Zscaler Internet Access -Administrationsportal an.

> **Hinweis:**
> Weitere Informationen zum Zscaler Internet Access -Administrationsportal finden Sie in der Zscaler-Dokumentation .

7. Navigieren zu **Administration** > **Warnungen** > **Veröffentlichen von Warnungen**.
8. Klicken **Sie auf Warnungsabonnement hinzufügen**.
9. Füllen Sie die Felder des Formulars aus.

**Formular „Warnungsabonnement hinzufügen“**

| Feld | Beschreibung |
|---|---|
| E-Mail | Now Platform E-Mail-Adresse des SMTP-Accounts. |
| Beschreibung | Feld zum Hinzufügen weiterer Details zu den Patientenwarnungen 0. |

10. Klicken Sie auf **Speichern**.

## ServiceNow Security Operations -Add-on für die Splunk-Übersicht

Mit dem Add-on [ ServiceNow Security Operations für Splunk kann ein Splunk -Softwareadministrator Daten sammeln und Incidents und Events in Now Platformerstellen.

Das Add-on wird von Splunkbase installiert.

> **Wichtig:**
> Splunk wird auch für die MSP-Umgebung (Managed Service Provider) unterstützt.

### Setup der Splunk-Integration

Zu den Setup-Verfahren für das Add-on ServiceNow Security Operations für Splunk gehören das Herunterladen der Add-on-Datei in Splunk, die Installation des Add-on und das Einrichten der Instanz ServiceNow, in der Security Incidents und Events erstellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erforderliche Rolle

Bevor Sie Setup-Verfahren für die Splunk-Integration durchführen, müssen Sie einen Integrationsbenutzer mit den Rollen sn_si.integration_user und sn_si.analyst in Ihrer ServiceNow-Instanz definieren. Darüber hinaus benötigen Sie zum Ausführen von Importen die Rolle import_transformer, um Lese- und Schreibberechtigungen für die Sicherheitstabellen zu erhalten. Die Rolle sn_si.integration_user muss mit dem Teil import_transformer der Rolle definiert werden.

### Laden Sie die Anwendung ServiceNow Security Operations herunter

Der erste Schritt beim Einrichten der ServiceNow-to-Splunk-Integration besteht darin, die Anwendung ServiceNow Security Operations aus Splunkbase herunterzuladen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Öffnen Sie Splunkbase.
2. Suchen Sie nach ServiceNow Security Operations Integration .
3. Laden Sie die Anwendung herunter.

### Installieren Sie das Add-on „ServiceNow Security Operations“ für Splunk

Installieren Sie das **Add-on „ServiceNow Security Operations“ für Splunk**, um Splunk mit ServiceNowzu verknüpfen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Öffnen Sie Splunk.
2. Klicken Sie entweder auf das Zahnradsymbol für **Apps** oder auf das Kontextmenüelement **Apps verwalten**.
3. Klicken **Sie auf App aus Datei installieren**.
4. Klicken Sie auf **Datei**auswählen, wählen Sie sn_sec_ops.spl aus, und klicken Sie auf **Hochladen**.
5. Wenn Sie dazu aufgefordert werden, starten Sie Splunkneu.
   Das Add-on ServiceNow Security Operations für Splunk ist installiert und kann eingerichtet werden.

### Richten Sie die Instanz ein, in der Incidents oder Events erstellt werden, oder ändern Sie sie

Um die Instanz ServiceNow einzurichten oder zu ändern, in der neue Security Incidents und Sicherheits-Ereignisse erstellt werden, verwenden Sie die Aktion Setup in der Anwendungsliste.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

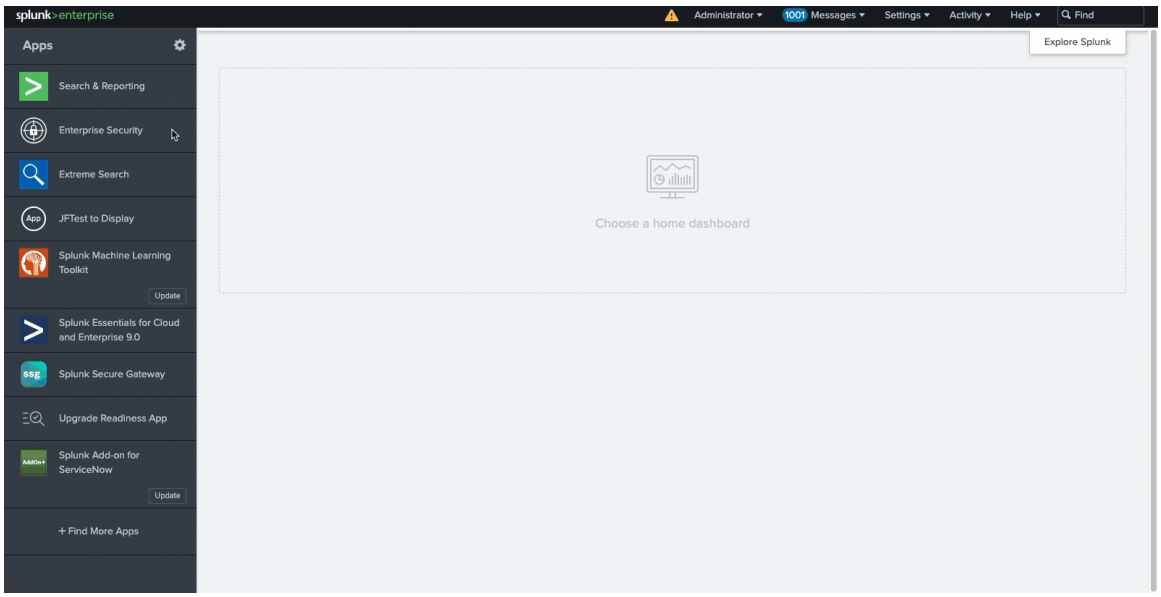
**Prozedur**

1. Öffnen **Sie Splunk**.
2. Klicken Sie entweder auf das Zahnradsymbol für **Apps** oder auf das Kontextmenüelement **Apps verwalten**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Suchen Sie in der Liste der Anwendungen mithilfe des Filters nach **ServiceNow** -Apps.
4. Suchen Sie nach der **ServiceNow Security Operations-Integration**und klicken Sie auf die entsprechende Aktion **Einrichten**.
5. Füllen Sie die Felder des Formulars aus.



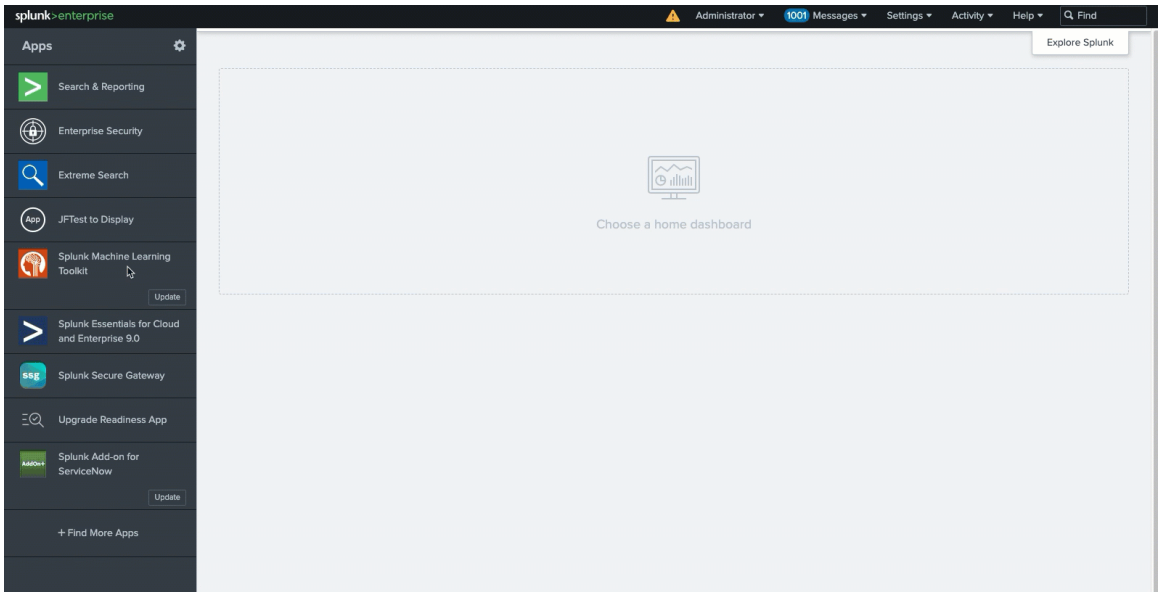

6. Klicken Sie auf **Speichern**.
7. Alternativ können Sie nach der **ServiceNow Event Ingestion Integration**suchen und auf die entsprechende Aktion „ **Einrichten** “ klicken.

   Die ServiceNow Event Ingestion Integration ist auf drei verschiedenen Registerkarten konfiguriert.

   - **Splunk Primär**: Die standardmäßige oder primäre Splunk-Konfiguration.
   - **Splunk sekundär**: (Optional) Die Sicherungs- oder zweite Splunk-Konfiguration.
   - **Protokollierungsebene**: Die Ebene der von der Integration generierten Berichtsprotokolle, d. h. der Name des Informationstyps.
8. Wählen Sie die Registerkarte **Splunk Primär aus**.
9. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




10. **Wahlweise:** Wählen Sie die Registerkarte **Splunk sekundär aus**.
11. **Wahlweise:** Füllen Sie die Felder des Formulars aus.
12. Wählen Sie die Registerkarte **Protokollebene** aus.
13. Füllen Sie die Felder des Formulars aus.
14. Klicken Sie auf **Speichern**.
    Nach erfolgreicher Validierung wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Aktualisieren** und **Löschen** angezeigt (siehe folgende Abbildung).

**Hinweis:**
Sie müssen entweder die Standardauthentifizierung oder nur die OAuth 2.0-Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beides aktivieren, wird ein Fehler angezeigt.

Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Event-Erfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Liste „Konfigurationen anzeigen“ auf **Ja**.

### Konfigurieren Sie die Anwendungsregistrierung in der ServiceNow-Instanz

Registrieren Sie die Anwendung bei der Instanz, um die OAuth-Autorisierung zu verwenden.

#### Vorbereitungen
Erforderliche Rolle: admin

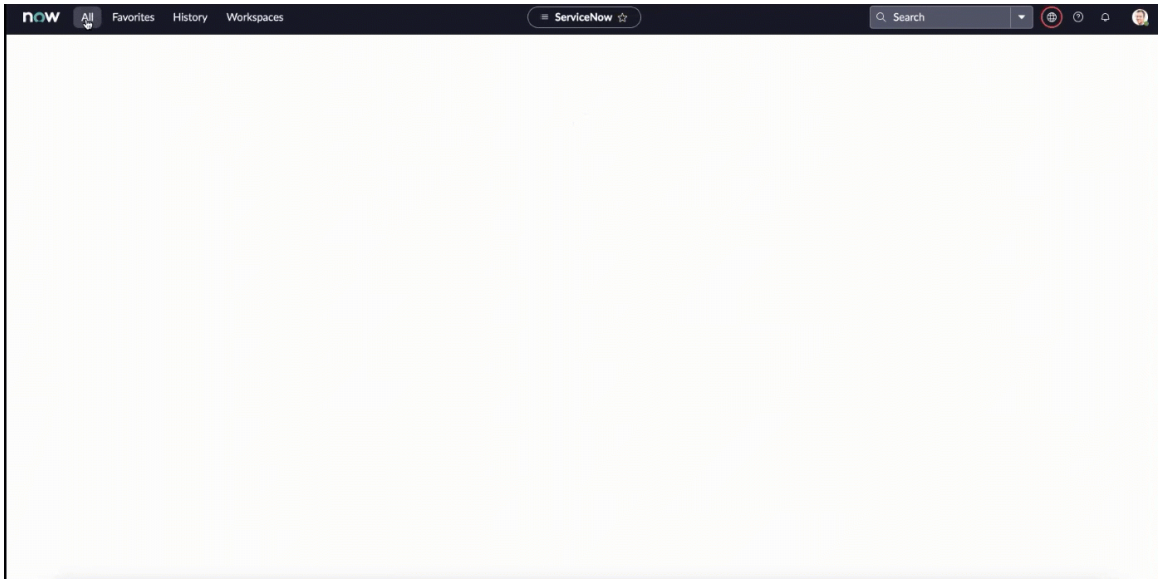
#### Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken **Sie auf Einen OAuth-API-Endpunkt für externe Clients erstellen**.
4. Füllen Sie die Felder des Formulars aus.




5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
6. Klicken Sie auf **Absenden**.

### Manuelle Suchbefehle

Manuelle Suchbefehle werden in einem beliebigen Suchfenster eingegeben. Sie können einen Security Incident oder ein Event erstellen. Nach dem Befehl gibt es Paare von Feldnamen und Werten, die zum Erstellen des gewünschten Datensatzes verwendet werden.

### Sicherheitsereignis

Der Sicherheitsereignisbefehl **snsecevent**erstellt ein Ereignis in ServiceNow mit der Klassifizierung Security.

Diese Events können einzeln überprüft werden, oder Warnungsregeln in ServiceNow oder manuelle Aktionen können ein Event oder eine Sammlung von Events in einen Security Incident umwandeln.

Wenn das Event zu einem Security Incident wird und jeder Parameter an das Event gesendet wird, werden diese Daten verwendet, um den Security Incident wie folgt auszufüllen:

#### Sicherheitsereignis

| Parametername | Erforderlich | Verwenden | Wird in Security Incident verwendet |
|---|---|---|---|
| Knoten | Ja | Der Knoten stellt den Server oder das Konfigurationselement für das Event dar. Idealerweise ist dieser Knoten einem | Wird in Security Incident verwendet |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Sicherheitsereignis (Fortsetzung)

| Parametername | Erforderlich | Verwenden | Wird in Security Incident verwendet |
|---|---|---|---|
| | | vorhandenen CI in ServiceNowzugeordnet. | |
| type | Ja | Kategorie des Events. | Kurzbeschreibung |
| Ressource | Ja | Das Konfigurationselement. | Kurzbeschreibung |
| Quelle | Nein | Der Ursprung dieser Daten. Standardmäßig generiert der Splunk-Server die Daten. | Aktivitätsprotokoll |
| external_url | Nein | Die in ServiceNow zu verwendende Drilldown-URL, um zu den Splunk-Daten zu diesem Event zurückzukehren. Standardmäßig enthält diese URL den Ergebnislink für eine Warnung oder einen Link zur standardmäßigen Splunk-Suchseite. | Externe URL, auf die über die Schaltfläche **Drilldown** im Security Incident-Formular zugegriffen wird |
| time_of_event | Nein | Die Zeit, zu der das Event in Splunk protokolliert wurde. | N/V |
| Alle anderen Werte (Kategorie, Unterkategorie im Beispiel) | Nein | Jedes Feld, das nicht Teil des Informationsfelds im Event ist. Wenn ein Security Incident erstellt wird, wird er verwendet. | Wenn das Feld vorhanden und nicht ausgefüllt ist, verwendet der Security Incident diesen Wert. Beispielsweise wird die durch das Event übergebene Kategorie zur Kategorie des neuen Security Incidents. Wenn ein Feld mit diesem Namen nicht vorhanden ist, wird der Wert im Aktivitätsprotokoll gespeichert. |

### Sicherheitsvorfall

Der Security Incident-Befehl **snsecincident**erstellt einen Security Incident in Ihrer Instanz ServiceNow.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Sicherheitsvorfall**

| Parameter | Erforderlich | Verwenden |
|---|---|---|
| short_description | Ja | Eine kurze, einzeilige Beschreibung des Incidents. |
| Kategorie | Nein | Die Kategorie des Security Incident. Wenn diese Kategorie nicht vorhanden ist, wird sie erstellt. |
| Unterkategorie | Nein | Die Unterkategorie. Wenn diese Unterkategorie nicht vorhanden ist, wird sie erstellt. |
| cmdb_ci | Nein | Das Konfigurationselement für den Security Incident Idealerweise wird dieses Element einem vorhandenen CI in ServiceNowzugeordnet. |
| Beschreibung | Nein | Die längere, detaillierte Beschreibung des Incident. |

Es gibt viele mögliche nützliche Spalten – alles in der Security Incident-Transformationszuordnung kann verwendet werden. Wenn dem Security Incident neue Spalten hinzugefügt werden, werden sie ebenfalls verwendet, solange sie sich in der Transformationszuordnung befinden. Einige nützliche Spalten: „location“, „priority“, „assignment_group“, „assigned_to“, „affid_user“, „attach_vector“ und „watch_list“.

### Splunk-Ereignisaktionen

Wenn Sie Splunk-Protokolle überprüfen, können Sie mit den Event-Aktionen schnell Sicherheits-Events und Security Incidents aus jedem Element im Protokoll erstellen.

Wenn Sie auf eine dieser Aktionen klicken, wird ein manueller Suchbefehl erstellt, der mit den Daten im Protokolleintrag gefüllt wird, und ausgeführt, um den neuen Datensatz zu generieren.

Diese Aktionen lassen sich einfach konfigurieren, um Felder in Ihren normalisierten Daten hinzuzufügen. Innerhalb von Splunk mit **Einstellungen** > **Felder** > **Workflow-Aktionen**, können Sie eine dieser Aktionen mithilfe der manuellen Suchfelder auswählen und bearbeiten.

Sie können auswählen, wo die Aktion für welche Felder angezeigt wird, und die Suchzeichenfolge ändern, die einen Suchbefehl enthält, um Ihren Datensatz zu erstellen.

### Splunk-Warnungen für einzelnen Datensatz

Innerhalb jeder Warnung können Sie Sicherheits-Events oder Security Incidents angeben, die erstellt werden sollen, wenn die Warnung ausgelöst wird.

Öffnen oder erstellen Sie eine Warnung, und wählen Sie beim Bearbeiten von Aktionen den gewünschten Datensatztyp aus, und füllen Sie das Warnungsdialogfeld aus.

### Splunk-Warnungen für benutzerdefiniertes Feld mit mehreren Datensätzen

Warnungen mit mehreren Datensätzen (definiert mit den Auslöseraktionen Mehrere ServiceNow- **Sicherheitsvorfälleerstellen und Mehrere ServiceNow-Sicherheitsereignisse erstellen** ) können automatisch Datensätze mit einem beliebigen Satz unterstützter Felder erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese verhalten sich anders als die anderen Warnungsaktionen, für die Standardwerte bereitgestellt werden. Die meisten Daten stammen jedoch aus dem Suchergebnis für diese Warnung.

**Hinweis:**
In früheren Versionen des Add-on und dieser Dokumentation wurden geskriptete Warnungen unterstützt. Diese Funktion ist veraltet und wurde durch diese Anweisungen ersetzt.

### Erstellen Sie eine Splunk-Warnung für ein benutzerdefiniertes Feld mit mehreren Datensätzen

Um eine Splunk-Warnung mit mehreren Datensätzen und benutzerdefinierten Feldern zu erstellen, müssen Sie eine Suche erstellen, die den ServiceNow-Spalten entspricht, die Sie ausfüllen möchten.

**Vorbereitungen**
Erforderliche Rolle: sn_si.admin

**Prozedur**

1. Navigieren Sie zu **Suche**.
2. Erstellen Sie im Feld **Suche** eine Suche, die Ihre Datensatzdaten generiert.
   Siehe Beispiele für empfohlene Suchkriterien.
3. Klicken Sie auf **Speichern unter**, und wählen Sie **Warnung**aus.
4. Legen Sie den Namen, die Berechtigungen und den Zeitplan nach Bedarf fest.
5. Klicken **Sie auf Aktionen hinzufügen**.
6. Treffen Sie eine der folgenden Auswahlmöglichkeiten.
   - Um ein Ereignis pro Suchergebnis zu **erstellen, wählen Sie Mehrere ServiceNow-Sicherheitsereignisse erstellen**aus.
   - Um einen Incident pro Suchergebnis zu **erstellen, wählen Sie Mehrere ServiceNow-Security Incidents erstellen**aus.
7. Legen Sie nach Bedarf Standardwerte fest.
   Wenn das Feld im Suchergebnis leer oder nicht vorhanden ist, werden die Standardwerte verwendet. Wenn das Ergebnis einen Wert enthält, werden die Standardwerte überschrieben.

### Beispiele für Splunk-Warnungen in benutzerdefinierten Feldern mit mehreren Datensätzen

Wenn Sie Splunk-Warnungen mit mehreren Datensätzen mit benutzerdefinierten Feldern erstellen, müssen Sie Suchkriterien für die Generierung von Warnungsdaten definieren. Beispiele für Suchkriterien für Security Incidents und Security Events werden angezeigt.

## Security Incident-Suche

Für einen Security Incident erstellen diese Kriterien eine Suche, um Spalten in der Security Incident-Tabelle auszufüllen.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Suche nach Sicherheitsereignissen

Für ein Sicherheits-Event ist dies dieselbe Suche, aber es werden stattdessen Event-Felder ausgefüllt. Wenn dieses Event in einen Security Incident umgewandelt wird und alle Felder, die im Event nicht vorhanden sind, ausgefüllt werden, werden sie in den Security Incident übertragen. Andernfalls verbleiben sie im Feld mit zusätzlichen Informationen des Events und der Warnung.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

**Hinweis:**
Die von Ihnen verwendeten Suchkriterien fügen so viele Datensätze hinzu, wie in der Suche gefunden werden. Es können 5 oder 10.000.000.000 Datensätze hinzugefügt werden. Daher ist dies KEINE empfohlene Methode für die Massenübertragung von Daten. Diese Methode dient dazu, der ServiceNow-Instanz einen Datensatz pro REST-Aufruf hinzuzufügen.

#### Splunk-Fehlerberichterstellung

Immer wenn ein Konnektivitätsproblem mit Ihrer ServiceNow-Instanz auftritt, wird in Splunk ein Fehler mit Informationen zur Beschreibung des Problems protokolliert.

Fehlermeldungen werden in einem neuen Index namens **servicenow** mit Quelltyp **servicenow gespeichert**.

Um nach Fehlerprotokollen zu suchen, stellen Sie sicher, dass Sie den **ServiceNow-** Index in Ihrer Suche angeben. Alternativ dazu erfahren Sie in der aktuellen Splunk-Dokumentation, wie Sie den neuen **servicenow-** Index zu den Standardsuchindizes hinzufügen.

## Splunk Enterprise Event Ingestion Integration für Security Operations nach ServiceNow

Die Integration von Splunk Enterprise Event- und Warnungsdaten mit dem Produkt Security Incident Response (SIR) ermöglicht Security Incident-Analysten die Erfassung und Verarbeitung von Sicherheitsprotokollen und zugehörigen Event-Daten.

## Übersicht

Daten werden in Echtzeit erfasst und von Analysten verwendet, um potenzielle Cyberbedrohungen zu identifizieren und Berichte darüber zu erstellen. Die erfassten Sicherheits-Events können in ausgelöste Warnungen verarbeitet werden, die mit dieser Integration automatisch erfasst werden. Außerdem können einzelne Sicherheits-Events bei Bedarf manuell von der Such- und Berichtsschnittstelle von Splunk Enterprise ] an das Produkt Security Incident Response von Now Platform weitergeleitet werden, um Security Incidents zu erstellen. Mit der Konfiguration des Suchkopf-Clusters können Sie wichtige Events aus der Suche Splunk Enterprise abrufen. Sie können dies erreichen, indem Sie die URL und den API-Port eines beliebigen Suchkopfs verwenden, der Teil des Clusters ist.

Diese Integration bietet einem SOC-Analysten (Security Operations Center) Einblick in Events und zugehörige Warnungsdaten. Diese Daten können zur weiteren Untersuchung und Korrektur in Now Platform Security Incident Response (SIR) Security Incidents integriert werden. Profile für Splunk laufende erfasste Warnungen und weitergeleitete Events



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden in Ihrer Instanz Now Platform erstellt. Diese Profile passen an, wie verschiedene Splunk Warnungs- und Event-Felder in SIR Security Incidents angezeigt werden. Eine Standardzuordnung von Warnungsfeldern wird bereitgestellt, die bearbeitet und erweitert werden kann, um kundenspezifische Anforderungen zu erfüllen.

## Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere Warnungserfassungsprofile, um SIR-Security Incidents für bestimmte Arten von Bedrohungen wie Phishing und Malware zu erstellen.
- Erstellen Sie mehrere Event-Profile für die On-Demand-Event-Weiterleitung über Ihre Splunk -Konsole, um SIR-Security Incidents zu erstellen.
- Drag-and-Drop-Zuordnung von Splunk Warnungs- und Event-Feldwerten zu zugehörigen SIR-Security Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf Beispielwarnungen oder -events zur Validierung der Profilkonfiguration.
- Erfassen Sie historische Warnungen sowie laufende, zukünftige Warnungen in konfigurierbaren Intervallen.
- Fassen Sie Events oder Warnungen zu vorhandenen SIR Security Incidents basierend auf übereinstimmenden Feldwerten zusammen, um doppelte Security Incidents zu vermeiden.

## Unterstützte Versionen Now Platform .

Das Plugin „com.snc.si_dep“ ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations Anwendungen müssen über den ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store ..

## ServiceNow Add-ons

Das Add-on ServiceNow Security Operations Event Ingestion für Splunk Enterprise ist nur erforderlich, wenn Sie Events manuell von Ihrer Splunk Enterprise -Konsole an Ihre Now Platform -Instanz weiterleiten möchten. Dieses Add-on ServiceNow ist in splunkbase verfügbar.

Diese Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise in splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Splunk Unterstützte Versionen

Diese Integration unterstützt Version 6.0 oder höher von Splunk Enterprise. Die Integration unterstützt auch den Enterprise Cloud-Service Splunk.

## MID-Server

Für diese Integration muss ein installierter und konfigurierter MID Server in Ihrer Now Platform® -Instanz eine Verbindung zum Splunk -Service herstellen, wenn der Splunk -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Wenn Sie den Service Splunk Cloud verwenden, ist kein MID Server erforderlich. Weitere Informationen zu MID Servern finden Sie unter MID Server .

## Integrationsarchitektur und Systemverbindung

Weitere Informationen zur Architektur der Integration, einschließlich wichtiger Begriffe und Details zur Verbindung externer Systeme, finden Sie unter Integrationsarchitektur und externe Systemverbindung für die Splunk Enterprise Event Ingestion -Integration.

## Prüfliste

Eine Prüfliste mit diesen Themen zum Ausdrucken finden Sie unter Prüfliste für die Integration von Splunk Enterprise Security Notable Event Ingestion. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Durcharbeitung der Aufgaben der Integration zu überwachen.

Die in den folgenden Themen verwendeten Images wurden für das Kingston-Release von Now Platformgeneriert. Weitere Informationen zur Benutzeroberfläche von San Diego finden Sie unter Sicherheitsbedrohungen mit Security Analyst Workspace verwalten.

Die folgenden Themen sind nummeriert. Befolgen Sie die unten aufgeführten Themen in der Reihenfolge, in der sie für eine reibungslose Installation und Konfiguration der Anwendung angezeigt werden.

### Richten Sie Ihre Now Platform® -Instanz für die Splunk Enterprise Event Ingestion -Integration ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

#### Prozedur

1. Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.

   Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform® -Instanz erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus dem ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.
- Wenn Sie Events für diese Integration manuell von Splunk Enterprise weiterleiten möchten, weist ein Benutzer mit der Administratorrolle Now Platform® einem Benutzer mit der Rolle (sn_sec_splunk_v2.api_account_access) in Now Platform®zu. Diese Rolle ermöglicht einem Benutzer mit der Administratorrolle Splunk Enterprise den Zugriff auf die API in Now Platform®, die für die manuelle Event-Weiterleitung für diese Integration erforderlich ist.

  Die Rolle (sn_sec_splunk_v2.api_account_access) ist für die Integration nicht erforderlich, wenn Sie Warnungen automatisch aus Splunk Enterprise in Ihre Instanz von [ Now Platform® erfassen.

- Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform®:
  - Benennt, erstellt und bearbeitet Warnungs- und Event-Profile.
  - Wählt Werte aus Warnungen und Events aus und ordnet sie Now Platform® Security Incidents zu.
  - Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.
  - Plant die laufende Warnungserfassung.
  - Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.
  - Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.

Weitere Informationen zu Rollen und zum Zuweisen von Rollen zu Benutzern finden Sie unter Managing roles .

2. Vergewissern Sie sich, dass Sie Version 6.0 oder höher der Splunk -API verwenden.

   Wenn Sie Zugriff auf die Konsole Splunk Enterprise haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.

3. Vergewissern Sie sich, dass Sie einen MID Server installiert und konfiguriert haben.

   Ein MID Server in Ihrer Now Platform® -Instanz ist erforderlich, um eine Verbindung zum Splunk -Service herzustellen, wenn der Splunk -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Weitere Informationen zu MID Servern finden Sie unter MID Server

   Wenn Sie den Service Splunk Cloud verwenden, ist kein MID Server erforderlich.

4. Vergewissern Sie sich, dass die zur Unterstützung der Integration erforderlichen ServiceNow Kernanwendungen installiert und aktiviert sind.

   Das Plugin Security Incident Response Dependency (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.

   Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

**a.** Security Incident Response

**b.** Security Integration Framework

**c.** Security Support Common

**d.** Security Support Orchestration

Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store ..

### Nächste Maßnahme

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht darin, die Anwendung Splunk Enterprise Event Ingestion aus dem ServiceNow Store für die Integration zu installieren. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Event Ingestion ..

Wenn Sie keine Suchen in Ihrer Splunk Enterprise -Konsole für die Erfassung gespeichert haben oder wenn Sie das erste Setup für diese Integration in Ihrer Splunk Enterprise -Konsole und im Security Operations -Produkt Ihrer Now Platform® -Instanz gleichzeitig durchführen, finden Sie weitere Informationen unter Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

Wenn Sie Events manuell und bei Bedarf aus Ihrer Splunk Enterprise -Konsole für die Integration exportieren möchten, finden Sie weitere Informationen unter Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Splunk Enterprise -Integration der Event-Erfassung ein.

## Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Event Ingestion .

Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform® ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform® integriert wird.

### Vorbereitungen

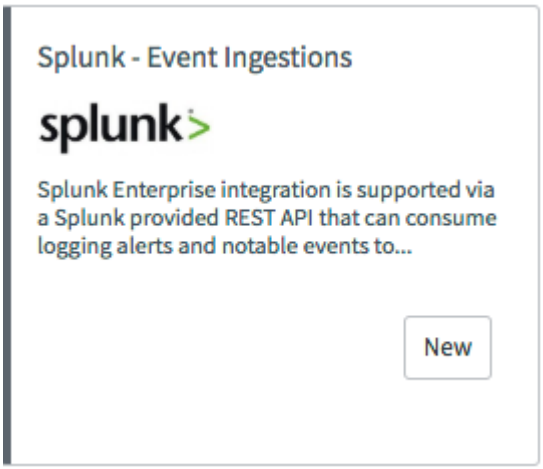
Erforderliche Rolle: admin

### Prozedur

1. Wenn Sie die Anwendung Splunk Enterprise Event Ingestion nicht aus dem ServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die Kachel Splunk „ Event Ingestions“.
3. Um die Anwendung zu konfigurieren, klicken Sie auf **Neu**.

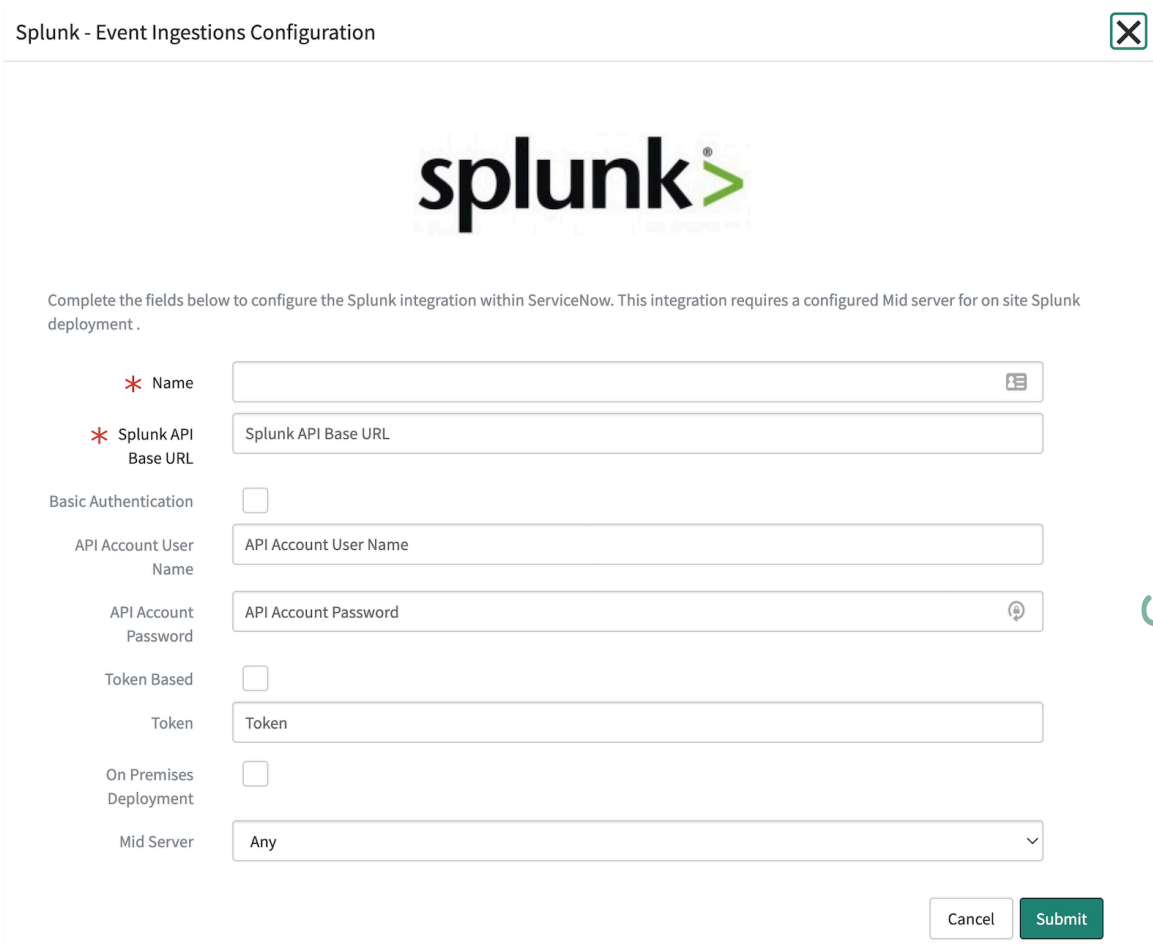


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld „Konfiguration der Event-Erfassung“ die Felder aus.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für die Konfiguration einer lokalen Version von Splunk Enterprise mit einem MID Server.




Jede Splunk Enterprise -Warnung, die Sie über Ihre Splunk Enterprise -Konsole erfassen, erfordert ein eindeutiges Event-Profil in Ihrer Now Platform® -Instanz. Die Quelle, die Sie

Automatische Übersetzung

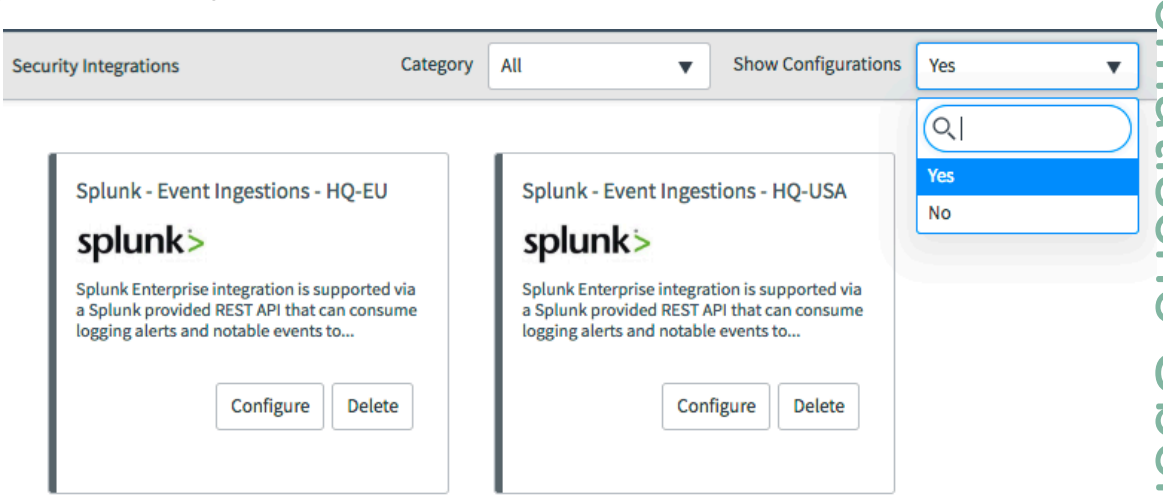
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im Formular Event-Erfassungskonfiguration konfigurieren, kann jedoch für mehrere Now Platform® Profile wiederverwendet werden, solange jedes Profil eindeutige Splunk ausgelöste Warnungen erfasst.

6. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Konfigurieren** und **Löschen** angezeigt (siehe folgende Abbildung).

   **Hinweis:**
   Sie müssen entweder die Standardauthentifizierung oder die tokenbasierte Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beides aktivieren, wird ein Fehler angezeigt.

   Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Event-Erfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.




**Trouble?**

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie auf Absenden **geklickt**haben, geben Sie Ihre Informationen erneut ein, und klicken Sie auf **Absenden**.

## Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Event-Profil zu erstellen.

### Konfigurieren Sie die Einstellungen für die Splunk Enterprise-Event-Erfassung

Verwenden Sie die Einstellungen für die Splunk Enterprise-Event-Erfassung, um die voreingestellten Konfigurationen und ihre Werte gemäß Ihren Anforderungen zu ändern.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Integrationseinstellungen**.
2. Füllen Sie die Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Splunk-Integrationseinstellungen

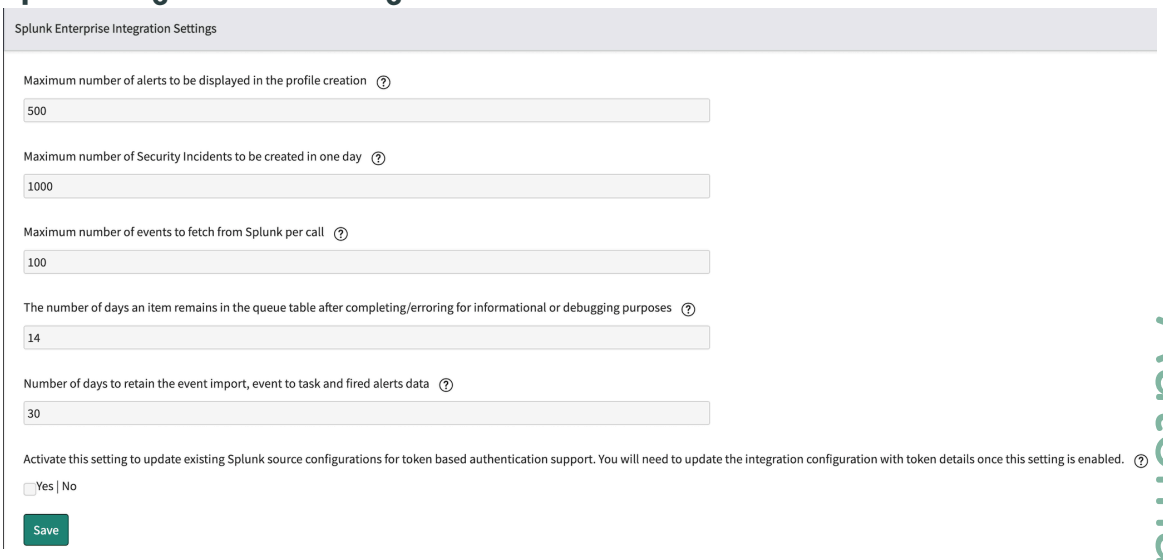
| Feld | Beschreibung |
|---|---|
| Maximale Anzahl von Warnungen, die in der Profilerstellung angezeigt werden sollen | Option zum Definieren der maximalen Anzahl von Warnungen, die beim Erstellen eines Event-Profils angezeigt werden sollen.<br><br>Standardmäßig ist der Wert auf 500 festgelegt. |
| Maximale Anzahl von Security Incidents, die an einem Tag erstellt werden sollen | Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können.<br><br>Standardmäßig ist der Wert auf 1000 festgelegt. |
| Maximale Anzahl von Events, die pro Aufruf aus Splunk abgerufen werden sollen | Option zum Definieren der maximalen Anzahl von Events, die für jeden Anruf aus Splunk abgerufen werden sollen.<br><br>Standardmäßig ist der Wert auf 100 festgelegt. |
| Die Anzahl der Tage, die ein Element in der Warteschlangentabelle verbleibt, nachdem es zu Informations- oder Debugging-Zwecken abgeschlossen oder fehlerhaft war | Option zum Definieren der Anzahl von Tagen, für die ein Element nach Abschluss oder Auftreten eines Fehlers aufgrund von Informations- oder Debugging-Zwecken in der Warteschlangentabelle verbleibt.<br><br>Standardmäßig ist der Wert auf 14 festgelegt. |
| Anzahl der Tage, für die die Daten für Event-Import, Event zu Aufgabe und ausgelöste Warnungen aufbewahrt werden sollen | Option, um die Anzahl der Tage zu bestimmen, für die Sie die Daten für Event-Import, Event zu Aufgabe und ausgelöste Warnungen aufbewahren möchten.<br><br>Standardmäßig ist der Wert auf 30 festgelegt. |
| Aktivieren Sie diese Einstellung, um vorhandene Splunk-Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung zu aktualisieren. Sie müssen die Integrationskonfiguration mit Tokendetails aktualisieren, sobald diese Einstellung aktiviert ist. | Option zum Aktualisieren der vorhandenen Splunk-Quellkonfiguration auf die Unterstützung der tokenbasierten Authentifizierung von einer vorhandenen Version.<br><br>**Hinweis:**<br>Nach dem Upgrade auf die neue Version ist das Tokenfeld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung zu erhalten. Anschließend müssen Sie die Integrationskonfiguration mit Tokendetails aktualisieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Standardmäßig ist der Wert auf Nein festgelegt. |

**Splunk-Integrationseinstellungen**




3. Klicken Sie auf **Speichern**.

## Erstellen und benennen Sie ein Event-Profil für die Splunk Enterprise Event Ingestion -Integration

Erstellen Sie ein Event-Profil in Ihrer Now Platform -Instanz, und bestimmen Sie, welche Splunk -Warnungen Security Incidents verursachen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Bevor Now Platform Security Incident Response (SIR) Security Incidents aus erfassten Warnungen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform Security Incident angezeigt, sodass Sie eine Vorschau des tatsächlichen Security Incident anzeigen können.

Aus Perspektive der Integration mit verfügbaren APIs werden Splunk -Events einzeln und manuell als diskrete Events weitergeleitet, oder sie werden zu ausgelösten Warnungen kombiniert, die automatisch in die Security Operations -Umgebung Ihrer Now Platform -Instanz erfasst werden. Die Integrations-Workflows erfassen verschiedene Arten von Warnungen, z. B. nicht autorisierte Zugriffsversuche und Malware.

Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in der Security Operations -Umgebung Ihrer Instanz konfigurieren. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents verursachen. Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hohes Risiko identifiziert wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen den entsprechenden Feldern in einem Layout von Security Incidents für eine Vorschau zugeordnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsnamen für Event-Profile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Event-Profil zugeordnet werden. Dies sind die Namen der ausgelösten Warnungen, die Sie in Ihrem Splunk -Service als Teil des Setups für die -Integration konfiguriert haben. Weitere Informationen zum Konfigurieren von Warnungen in Ihrer Umgebung Splunk Enterprise finden Sie unter Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

Now Platform erfasst bestimmte Warnungen mithilfe der Workflows der Integration. Alle Warnungen, die die Auswahlkriterien in Ihrer Splunk Enterprise-Konsole erfüllen, werden anfänglich in Ihrer Now Platform -Instanz erfasst.

Ein Profil in Now Platform ist eine Kapselung einer Splunk -Warnung in Ihrer Splunk Enterprise-Konsole. Zwischen Warnungen, die mit einem Profil erfasst werden, und Verbindungen zu Ihrer Splunk Enterprise-Konsole besteht eine 1:1-Beziehung: eine Warnung für eine Verbindung. In Ihrer Splunk Enterprise -Konsole besteht eine einzelne https-Verbindung zu einem Suchkopf. Mehrere Warnungen können aus einem einzelnen Suchkopf stammen. Wenn Sie eine Verbindung zu mehreren Suchköpfen in Ihrer Splunk Enterprise -Konsole herstellen, müssen Sie mehrere Profile in Ihrer Instanz von Now Platform erstellen, um diese Warnungen zu erfassen.

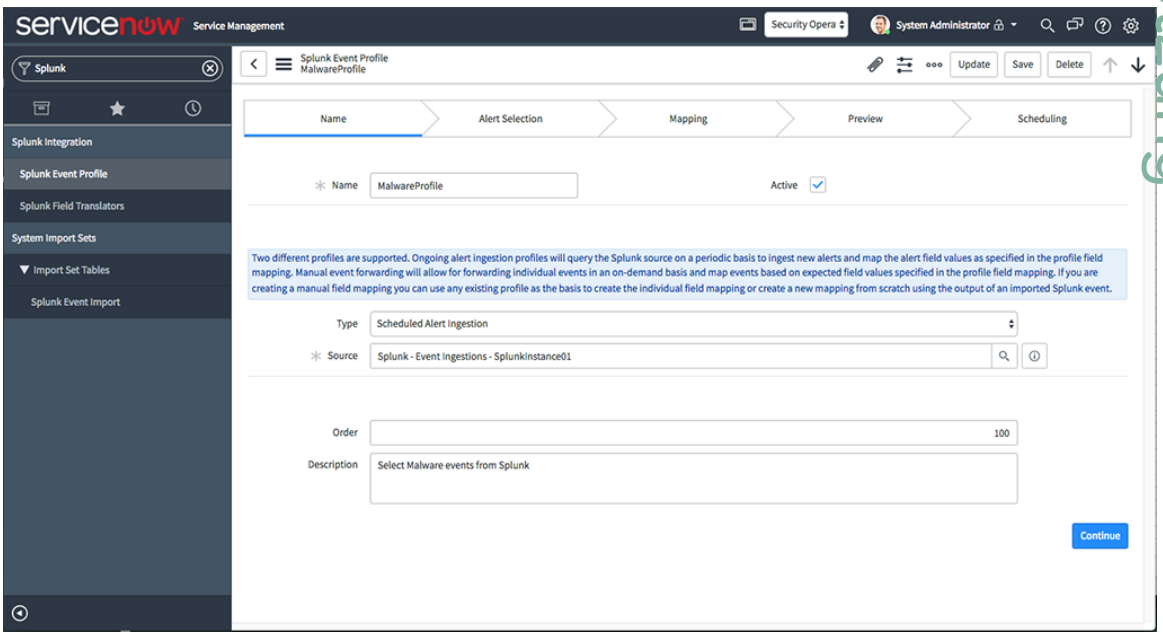
Schritte zum Erstellen von Profilen für die geplante Warnungserfassung

### Prozedur

1. Um ein Event-Profil für eine Warnung zu erstellen, navigieren Sie in Ihrer Instanz Now Platform zu **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wenn das Formular Splunk Event-Profil nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Name**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für eine geplante Warnung.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

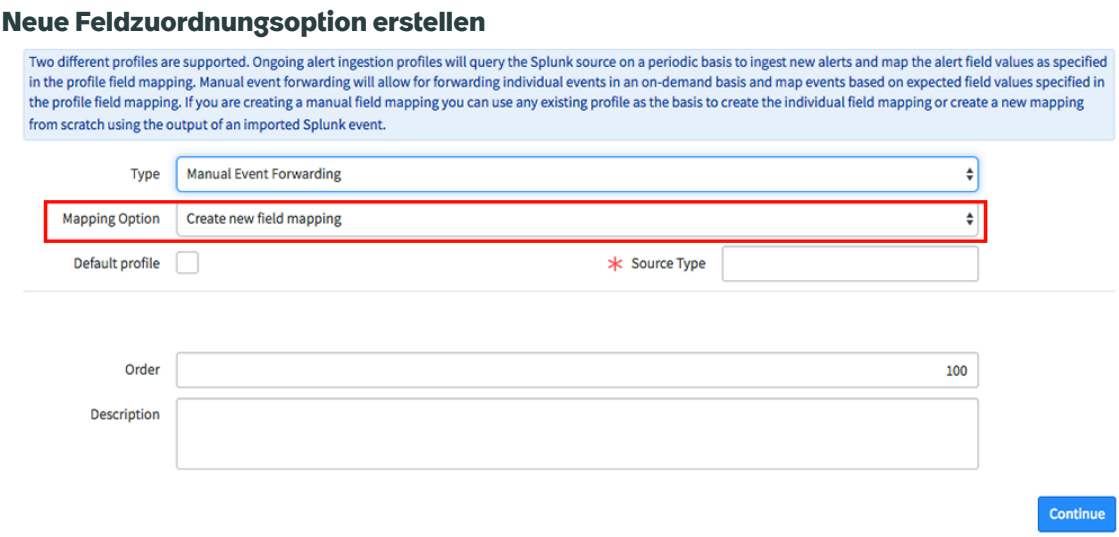
5. Wählen Sie für ein Profil mit einer geplanten Warnung eine Option aus, um mit der Profilkonfiguration fortzufahren.
   Schritte zum Erstellen von Profilen für die manuelle Event-Weiterleitung
6. Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Event-Weiterleitung unterstützt.

   Für Events, die Sie bei Bedarf von Ihrer Splunk Enterprise-Konsole aus weiterleiten, können Sie die einzelne Feldzuordnung auf ein vorhandenes Profil stützen. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangdaten erstellen. Events, die Sie manuell weiterleiten, werden nicht im Event-Profil geplant.

   a. Wenn dies noch nicht geschehen ist, wählen Sie in der Auswahlliste für das Feld Typ die Option **Manuelle Event-Weiterleitung**aus.

   b. Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

      In den folgenden Abbildungen und Tabellen finden Sie weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen.




**Neue Feldzuordnungsoption erstellen**

| Option oder Feld | Beschreibung |
|---|---|
| Neue Feldzuordnungsoption erstellen | Neue Feldzuordnung für Ihr Event.<br><br>Wenn keine Feldzuordnung vorhanden ist, die dem von Ihnen erstellten Profil ähnelt, wählen Sie diese Option aus, um eine neue Zuordnung zu erstellen. |
| Standardprofil | Standardmäßiges Event-Weiterleitungsprofil für alle Splunk -Events. Der Standardwert ist deaktiviert. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
|---|---|
| | Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Event-Weiterleitung. Dieses Profil ist das einzige Profil, das aktiv ist und für jede Splunk Event-Feldzuordnung zu einem SIR Security Incident verwendet wird. Ein Profil passt zu allen weitergeleiteten Events.<br><br>Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. |
| Quelltyp | Splunk -Server.<br><br>Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.<br><br>Wenn verfügbar, ermöglicht die Option Quelltyp die eindeutige Zuordnung von Event-Feldern zu Security Incident-Feldern basierend auf dem Splunk Quelltyp .<br><br>Wenn Sie Firewall-Protokoll-Events anders verwalten möchten als Endpunkt-Erkennungs-Events, und sie unterschiedliche Splunk Quelltypen haben, können Sie verschiedene Event-Profile basierend auf Quelltypen erstellen, um diese Anforderung zu erfüllen. |
| Reihenfolge | Der Standardwert ist 100. Belassen Sie diese Einstellung auf der Standardeinstellung.<br><br>Wenn Sie eine große Anzahl von Profilen erstellt haben, gibt dieser Wert eine Ausführungszeitpriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität. |
| (Optional) Beschreibung | Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

Vergewissern Sie sich bei einem Profil mit einer neuen Feldzuordnung, dass Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fortsetzen**, um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Für ein Profil mit einer vorhandenen Feldzuordnung finden Sie weitere Informationen in der folgenden Abbildung und Tabelle.

**Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

| Option oder Feld | Beschreibung |
|---|---|
| Wählen Sie ein vorhandenes Profil für die Feldzuordnung aus | Eine vorhandene Feldzuordnung für Ihr Event.<br><br>Das Feld Aus Profil kopieren wird angezeigt.<br><br>Befolgen Sie diese Schritte, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren.<br><br>i. Klicken Sie links neben dem angezeigten Feld Aus Profil kopieren auf das Suchsymbol.<br>ii. Klicken Sie in der angezeigten Liste Splunk Event-Profile auf den Profilnamen mit der zu kopierenden Karte.<br><br>Der Profilname wird im Feld Aus Profil kopieren angezeigt. |
| Standardprofil | Standardmäßiges Event-Weiterleitungsprofil für alle Splunk -Events. Der Standardwert ist deaktiviert.<br><br>Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Event-Weiterleitung. Dieses Profil ist das einzige Profil, das aktiv ist. Sie wird für jedes Splunk Event-Feld verwendet, das einem SIR Security Incident zugeordnet ist. Ein Profil passt zu allen weitergeleiteten Events.<br><br>Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. |
| Quelltyp | Splunk -Server.<br><br>Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption ausgewählt ist.<br><br>Wenn verfügbar, ermöglicht die Option Quelltyp die eindeutige Zuordnung von Event-Feldern zu Security Incident-Feldern basierend auf dem Splunk Quelltyp .<br><br>Wenn Sie Firewall-Protokoll-Events anders verwalten möchten als Endpunkt-Erkennungs-Events, und sie unterschiedliche Splunk Quelltypen haben, können Sie verschiedene Event-Profile |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
|---|---|
| | basierend auf Quelltypen erstellen, um diese Anforderung zu erfüllen. |
| Reihenfolge | Der Standardwert ist 100. Belassen Sie diese Einstellung auf der Standardeinstellung.<br><br>Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Ausführungszeitpriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität. |
| (Optional) Beschreibung | Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

**Klicken** Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil auf Fertigstellen, um die Profilkonfiguration abzuschließen.

### Nächste Maßnahme

Sie haben die Schritte zum Erstellen von Profilen für geplante Warnungen und die manuelle Event-Weiterleitung erfolgreich abgeschlossen. Für Profile für die manuelle Event-Weiterleitung haben Sie die Profilkonfiguration abgeschlossen. Der nächste Schritt besteht darin, Anhangdaten im Zuordnungsschritt zu laden.

Bei Profilen für geplante Warnungen besteht der nächste Schritt darin, Warnungen für die automatische Erfassung auszuwählen.

## Wählen Sie geplante Warnungen für die Splunk Enterprise Event Ingestion -Integration aus

Nachdem Sie ein Profil für eine geplante Warnung erstellt haben, wählen Sie eine Splunk Warnung für dieses Profil aus, die Sie einem Now Platform Security Incident Response Security Incident zuordnen möchten.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Warnungen in Ihrer Instanz Now Platform an, damit Sie wissen, welche Feldwerte für die Zuordnung verfügbar sind. Wählen Sie eine Warnung aus, um sicherzustellen, dass Sie die erwarteten Ergebnisse im Basisformularlayout erhalten, bevor Sie die Werte Feldern in SIR Security Incidents zuordnen. Sie können in diesem Formular nur eine Warnung aus der Liste auswählen.

### Prozedur

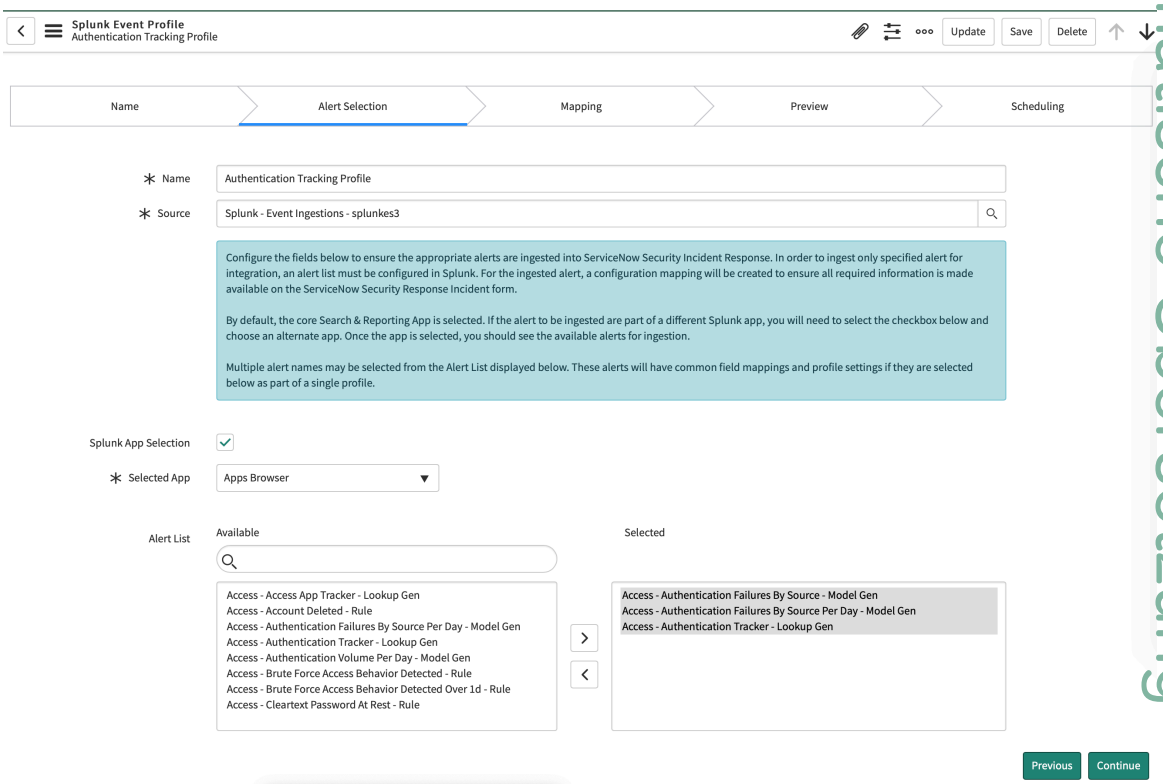
1. Wenn die Seite „Warnungsauswahl“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
   Standardmäßig ist die Core Search & Reporting-App ausgewählt.
2. Wenn die zu erfassende Warnung Teil einer anderen App Splunk ist, wählen **Sie Splunk-App-Auswahl** und dann Ihre App Splunk aus der Liste **Ausgewählte App** aus.
3. **Wählen**Sie in der Warnungsliste eine Warnung aus, und verschieben Sie sie aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
   Sie können auch mehrere Warnungen auswählen. Wenn die Warnungen als Teil eines einzelnen Profils ausgewählt werden, weisen die Warnungen gemeinsame Feldzuordnungen und Profileinstellungen auf.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste der Warnungen in diesem Formular stimmt mit der Liste der Warnungen in Ihrer Splunk -Konsole überein. In diesem Formular werden bis zu 500 Warnungen angezeigt. Wenn in Ihrer Splunk-Konsole auf der Seite „Warnungen“ mehr als 500 Warnungen aufgelistet sind, werden in diesem Formular in Ihrer Now Platform -Instanz nur die ersten 500 Warnungen angezeigt.

| Option | Beschreibung |
|---|---|
| Geben Sie im Suchfeld der Warnungsliste Text ein. | Die Spalte unter dem Suchfeld wird basierend auf dem von Ihnen eingegebenen Text mit verfügbaren Optionen gefiltert. Wählen Sie eine Warnung aus, und verschieben Sie den ausgewählten Alarm mit den Pfeiltasten von **Verfügbar** zu **Ausgewählt**. |
| Doppelklicken Sie in der Warnungsliste auf eine Warnung. | Die Spalte **Ausgewählt** wird mit Ihrer Auswahl ausgefüllt. |
| Klicken Sie in der Warnungsliste einmal auf eine Warnungsregel. | Der Alarm ist ausgewählt. Verschieben Sie die ausgewählte Warnung mit den Pfeiltasten von **Verfügbar** zu **Ausgewählt**. |




4. Wählen Sie eine Option aus, um fortzufahren.

## Nächste Maßnahme

Sie haben erfolgreich eine Warnung für ein geplantes Warnungsprofil ausgewählt. Der nächste Schritt besteht darin, Warnungswerte Feldern in einem Security Incident zuzuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zuordnung von Warnungen und Events für die Splunk Enterprise Event Ingestion -Integration

Nachdem Sie die Quellen für die geplante Warnungserfassung oder die manuelle Event-Weiterleitung identifiziert haben, besteht der nächste Schritt darin, einzelne Event-Felder den Feldern in einem Now Platform Security Incident Response (SIR) Security Incident zuzuordnen.

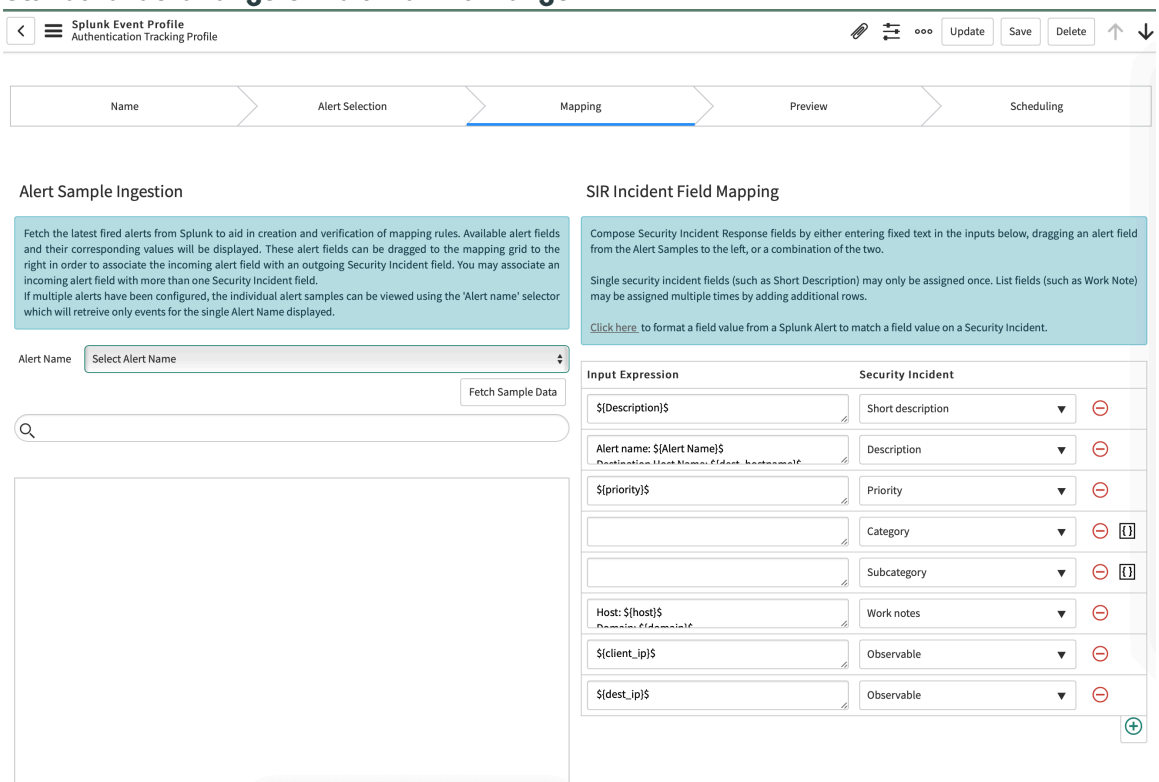
## Übersicht

Für den Zuordnungsschritt erfassen Sie als Benutzer mit der Rolle „sn_si.admin“ Beispielwarnungen aus Ihrer Splunk Enterprise -Konsole, oder exportieren Event-Daten für ein Splunk Enterprise -Event.

Die folgenden Abbildungen sind Beispiele für die standardmäßigen Zuordnungsraster, die für jeden Typ von Event-Profil bereitgestellt werden. Diese Standardzuordnung kann bearbeitet werden. Mit dieser Änderung können Sie die Felder anpassen, die den Security Incident ausfüllen. Mit dem Zuordnungsschritt können Sie visualisieren, wie sich das Hinzufügen oder Entfernen von Event-Feldern auf die Feldwerte des SIR Security Incident auswirkt.

Wählen Sie den **Warnungsnamen**aus. Nachdem Sie auf **Beispieldaten abrufen geklickt**haben, werden die Feldwerte der Warnung Splunk auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Warnungsfelder von Splunk, die Sie den Security Incident-Feldern von SIR zuordnen.

### Standardzuordnungsformular für Warnungen

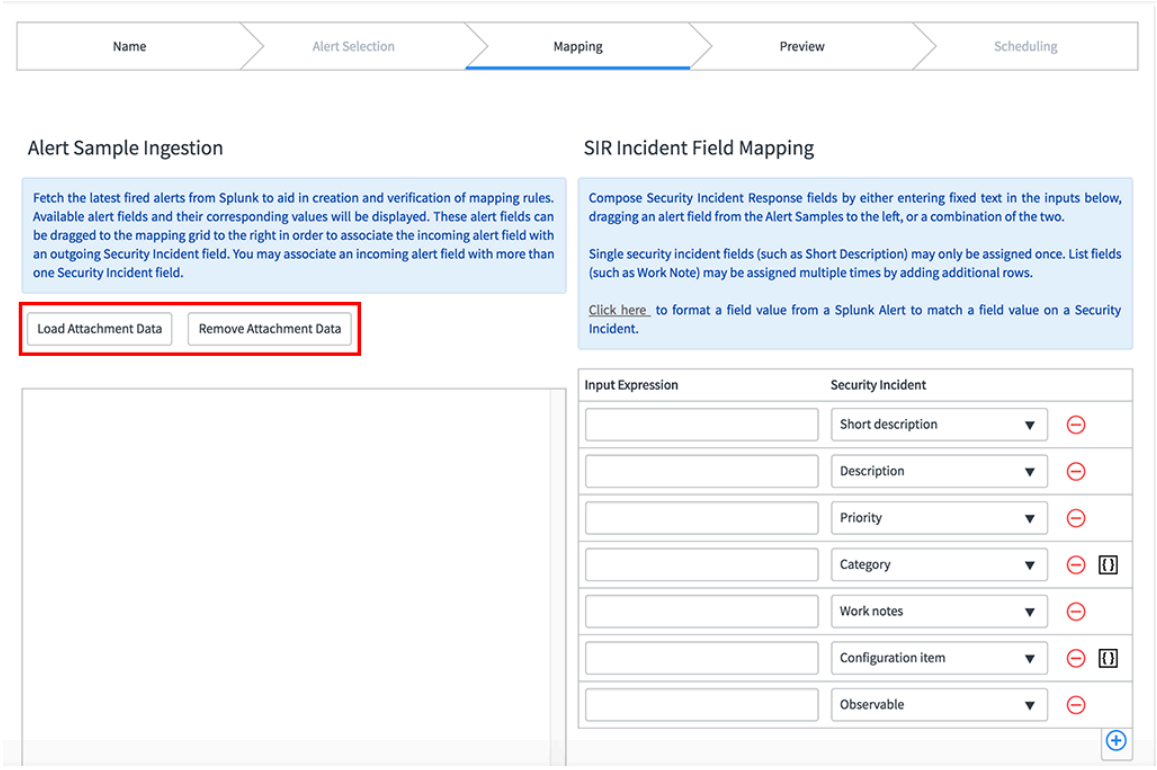



Nachdem Sie auf „Anhangdaten für weitergeleitete Events laden“ geklickt haben, werden die Event-Felder Splunk auf der linken Seite des Formulars ausgefüllt. Dies sind die Datenfelder Splunk ], die den Security Incident-Feldern SIR zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Standardzuordnungsformular für weitergeleitete Events**




Möglicherweise ziehen Sie es vor, einige Beispielwarnungen in Ihrer Splunk -Konsole zu überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird in der Fortschrittsleiste mit **Zuordnung** gekennzeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.

Das Zuordnen von Warnungen und das Exportieren von Events bei Bedarf aus Ihrer Splunk Enterprise-Konsole umfasst die folgenden Konzepte und Aufgaben:

- Rufen Sie Beispieldaten für automatisch erfasste Warnungsprofile ab. Nachdem Daten aus einer ausgelösten Warnung in der Konsole Splunk Enterprise abgerufen (abgerufen) wurden, werden verfügbare Warnungsfelder und ihre entsprechenden Werte in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt. Registerkarten werden angezeigt, um die Werte für eine von Ihnen abgerufene Warnungs-ID anzuzeigen. Vergewissern Sie sich, dass alle kritischen Felder aus dem Abschnitt „Warnungsbeispielerfassung“ auf der linken Seite des Formulars dem Raster auf der rechten Seite des Formulars zugeordnet sind.
- Laden Sie bei Bedarf Event-Beispieldaten für manuell weitergeleitete Event-Profile. Beispieldaten für diese Events werden in eine XML -Datei aus der Konsole Splunk Enterprise exportiert und in Ihre Instanz Now Platform® ] geladen. Die importierten Daten werden im Abschnitt „Warnungsbeispielerfassung“ auf der linken Seite des Formulars angezeigt.
- Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungen von der linken Seite ziehen und im Zuordnungsraster auf der rechten Seite ablegen. Das Zuordnungsraster auf der rechten Seite ordnet das eingehende Warnungsfeld einem ausgehenden Security Incident-Feld zu.
- Passen Sie das Zuordnungsraster an, indem Sie Felder hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder anhand der bereitgestellten Farbcodierung nach.
- Legen Sie Filterbedingungen fest, damit Sie angeben können, welche Warnungen in der Anwendung SIR erfasst und welche herausgefiltert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definieren Sie zusätzliche Incident-Feldkriterien, die eine eingehende Warnung zu einem vorhandenen SIR Security Incident zusammenfassen, um doppelte Incidents zu verhindern. Durch diese zusätzliche Filterung kann die Anzahl der aktiven, sich überschneidenden Security Incidents reduziert werden, indem alle zugehörigen Sicherheitsereignisdaten in einem einzigen Security Incident platziert werden.
- In bestimmten Fällen werden Event-Feldwerte in der Splunk Enterprise-Konsole möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Mit dem Skript-Editor werden beispielsweise die Feldwerte Malware-Warnung und Virusinfection in der Konsole Splunk beide in Böswillige Codeaktivität im Feld Kategorie des Security Incident SIR übersetzt.

## Geplante Warnungsprofile

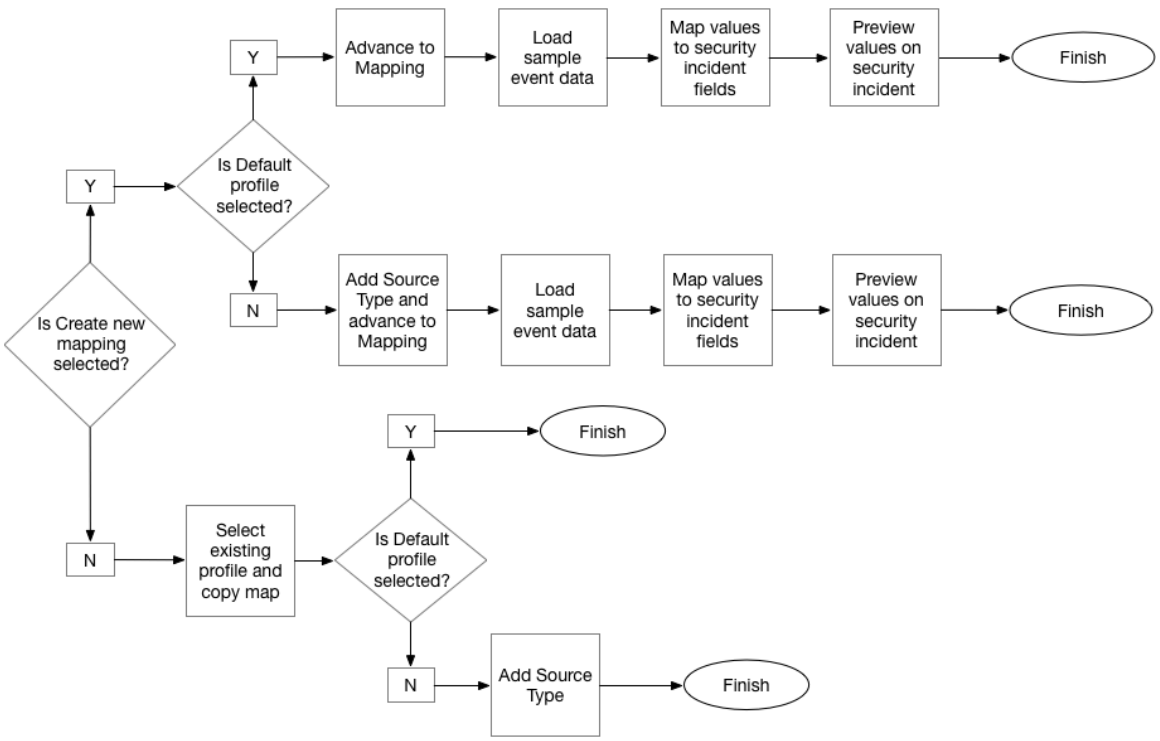
Nach dem Erstellen eines geplanten Warnungsprofils wird der Prozessablauf für die Konfiguration in der folgenden Abbildung dargestellt.

**Prozess-Flow für geplante Warnungsprofile**

## Manuelle Event-Weiterleitungsprofile

Nach dem Erstellen eines Profils für ein Event wird der Prozessablauf für die Konfiguration in der folgenden Abbildung dargestellt.

**Prozess-Flow für Event-Profile**




Der nächste Schritt besteht darin, ausgelöste Warnungen zu erfassen oder Daten zu exportieren und Werte den SIR Security Incident-Feldern zuzuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ordnen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration zu

Während des Schritts der Event-Feldzuordnung ordnen Sie einzelne Event-Felder aus ausgelösten Warnungen oder importierten Event-Daten Feldern in einem Now Platform Security Incident Response (SIR) Security Incident zu.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Das vorkonfigurierte Zuordnungsraster der standardmäßigen Security Incident-Felder kann bearbeitet werden. Die Farbcodierung der Event-Felder hilft Ihnen, die Feldwerte zu überwachen, die Sie bereits zugeordnet haben. Dieser Schritt hilft Ihnen zu visualisieren, wie sich Ihre Änderungen auf die Felder des Security Incident auswirken.

Ordnen Sie bis zu fünf Warnungen aus der Spalte „Erfassung von Warnungsbeispiel“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk Felder zuordnen, die nicht im Standardzuordnungsraster des Security Incident SIR angezeigt werden.

#### Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Wählen Sie für ein Profil mit einer geplanten Warnung unter „Erfassung von **Alarmbeispielen** “ die Warnung im Warnungsnamen aus, und klicken Sie auf **Beispieldaten abrufen**, um die letzte Instanz einer ausgelösten Warnung aus der Konsole Splunk Enterprise abzurufen.

   Die Warnungen werden als Registerkarten angezeigt. Sie können bis zu fünf der letzten Warnungen erfassen.

   Der Abruf für Beispiel-Events kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

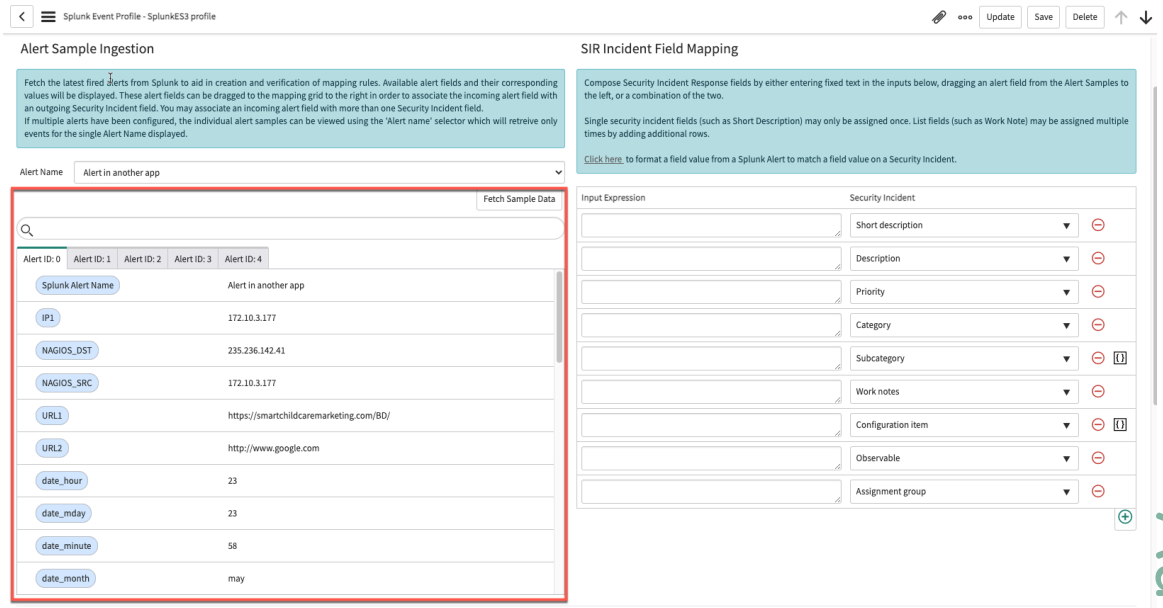
   **Hinweis:**
   Das zusätzliche Zuordnungsfeld **Splunk**-Warnungsname wird durch die Integration hinzugefügt, um die Nachverfolgung eines Events zur Quellwarnungsregel in Splunkzu ermöglichen. Dies kann in Szenarien hilfreich sein, in denen mehrere Splunk Warnungen in einem einzigen Profil kombiniert werden.

   Wenn ein einzelnes Feld mehrere Werte enthält, werden diese Werte analysiert und einzelnen Feldeinträgen im Abschnitt „SIR-Incident-Feldzuordnung“ zugeordnet. Beispielsweise können die Quell-IP-Adressen, Asset-Namen oder URLs mehrere erkennbare Feldeinträge oder mehrere CIs aufweisen, die analysiert und einzelnen Feldeinträgen im Abschnitt „SIR-Incident-Feldzuordnung“ zugeordnet werden.

   In der folgenden Abbildung werden die Feldname-Wert-Paare für die erfasste Warnung oder das importierte Beispiel-Event nach Abschluss des Abrufs auf der linken Seite dieses Formulars angezeigt. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Fahren Sie für geplante Warnungsprofile mit Schritt 5 fort, um die Werte zuzuordnen.
4. Alternativ führen Sie für ein Profil für einen Event-Typ, den Sie aus Ihrer Splunk Enterprise -Konsole exportieren möchten, diese Schritte aus, um Anhangdaten in Ihre Now Platform® -Instanz hochzuladen.

   a. Wenn Sie noch nicht angemeldet sind, melden Sie sich bei Ihrer Splunk Enterprise -Konsole an.

   b. Navigieren Sie zur Registerkarte Suche, und geben Sie einen Namen für eine Suche ein, die die Event-Daten enthält, die Sie exportieren möchten.

      Zum Beispiel ist Malware ein Suchbegriff, der für alle Malware-Ereignisse verwendet wird, die Sie mit dem Workflow dieser Integration weiterleiten können.

   c. Erweitern Sie das Event, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

      Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Seite „Zuordnung“ in Ihrer Instanz Now Platform® angezeigt werden.

   d. Klicken Sie in der Konsole Splunk Enterprise oben rechts auf der Suchseite auf das Symbol **Exportieren**.

   e. Klicken Sie in der Liste für das Feld Format im angezeigten Dialogfeld auf **XML-Format**.

   f. **Wahlweise:** Geben Sie einen neuen Dateinamen ein.

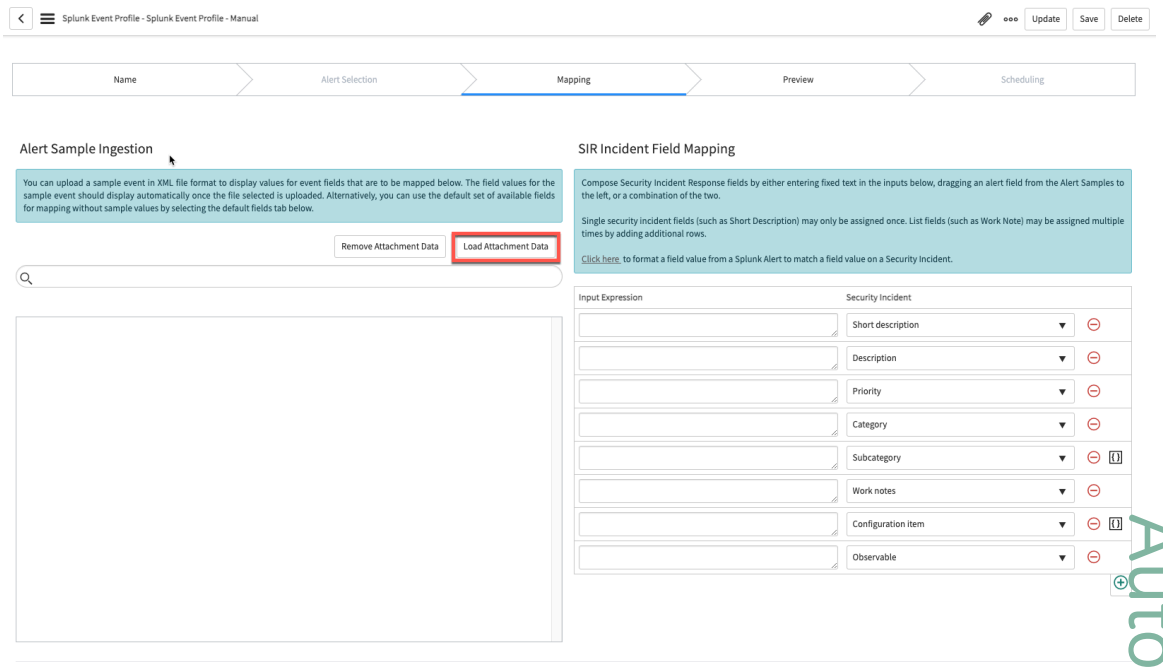
   g. Klicken Sie auf **Exportieren**.
   Die Datei wird in Ihre Instanz Now Platform® heruntergeladen.

   h. Wenn die Zuordnungsseite in Ihrer Instanz Now Platform® noch nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.

   i. Klicken Sie in der Spalte „Erfassung von Warnungsbeispiel“ auf **Anhangdaten laden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**j.** Klicken Sie im angezeigten Dialogfeld auf **Dateien** auswählen, navigieren Sie zur XML -Datei, die Sie exportiert haben, und klicken Sie auf **Öffnen**.
Die Wertepaare für die Felder, die Sie für das Event exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

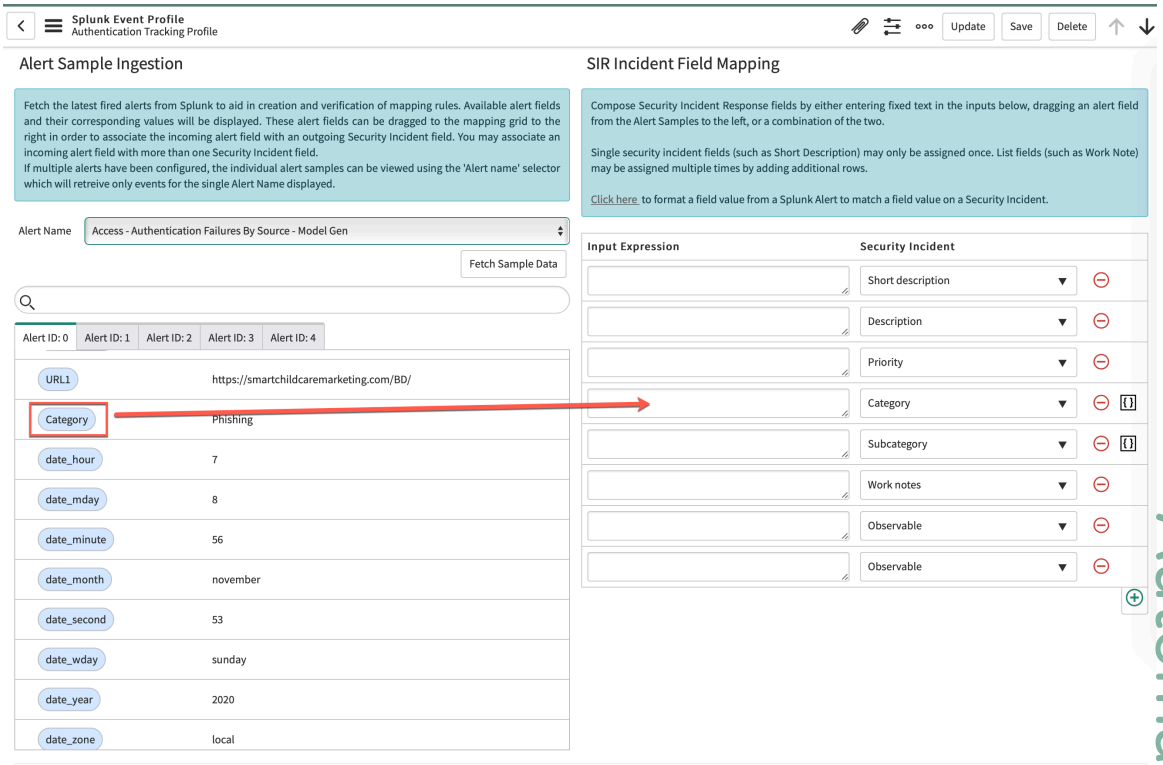
In der folgenden Abbildung werden die Datenpaare für eine erfasste geplante Warnung auf der linken Seite dieses Formulars angezeigt. Wertepaare für importierte Events werden auch auf dieser Seite des Formulars angezeigt. Diese Werte sind die Feldwerte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

**5.** Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.

**6.** Ziehen Sie den Feldnamen, z. B. Kategorie, in ein Feld in der Spalte Eingabeausdruck neben einem Feldnamen in der Spalte Security Incident.

Automatische Übersetzung

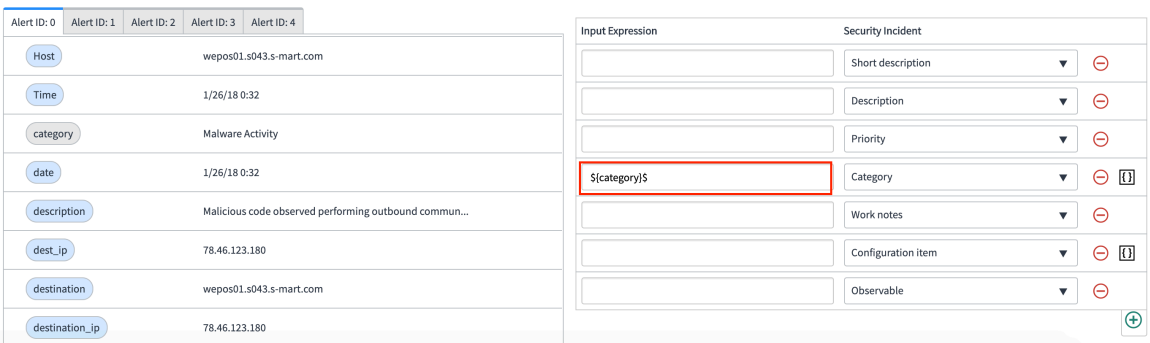
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird die Kategorie dem Kategoriefeld im Security Incident zugeordnet. Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert während des Vorschauschritts dem Security Incident korrekt zugeordnet wurde.

Um sicherzustellen, dass keine Events im Zuordnungsprozess übersehen oder dupliziert werden, sind die Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Feld ausgewählt und dem Security Incident zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes Warnungsfeld mehr als einem Feld in einem Security Incident zuordnen.

Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen, da Warnungsereignisfelder in bestimmten Fällen nur einmal zugewiesen werden können. Beispielsweise können Sie Feldern wie Kurzbeschreibung nur einmal Werte zuweisen. Sie können Listenfelder wie Arbeitsnotiz jedoch mehrmals zuweisen, indem Sie dem Zuordnungsraster zusätzliche Zeilen hinzufügen.

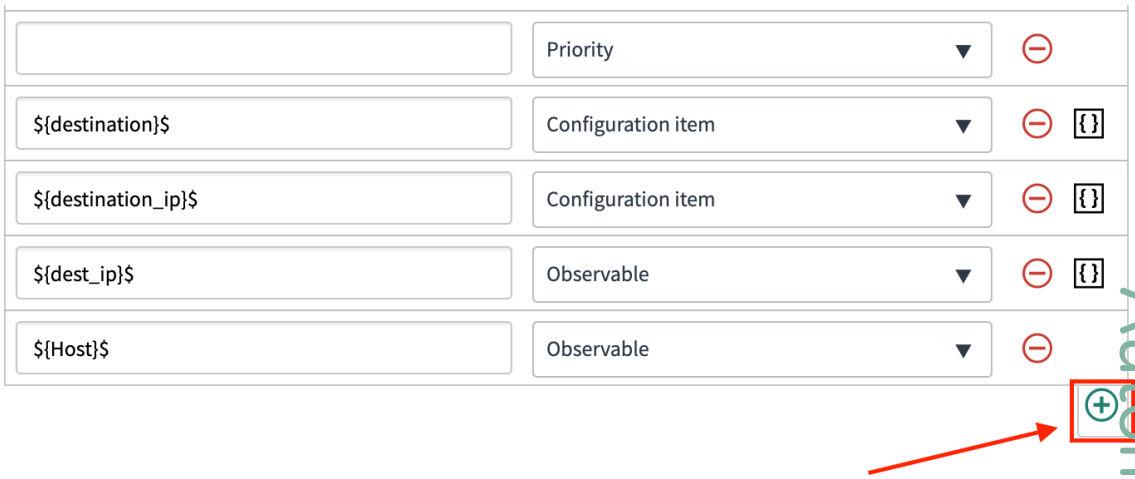



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Führen Sie die folgenden Schritte aus, um der Standardzuordnung des Security Incident auf der rechten Seite des Formulars Felder hinzuzufügen.

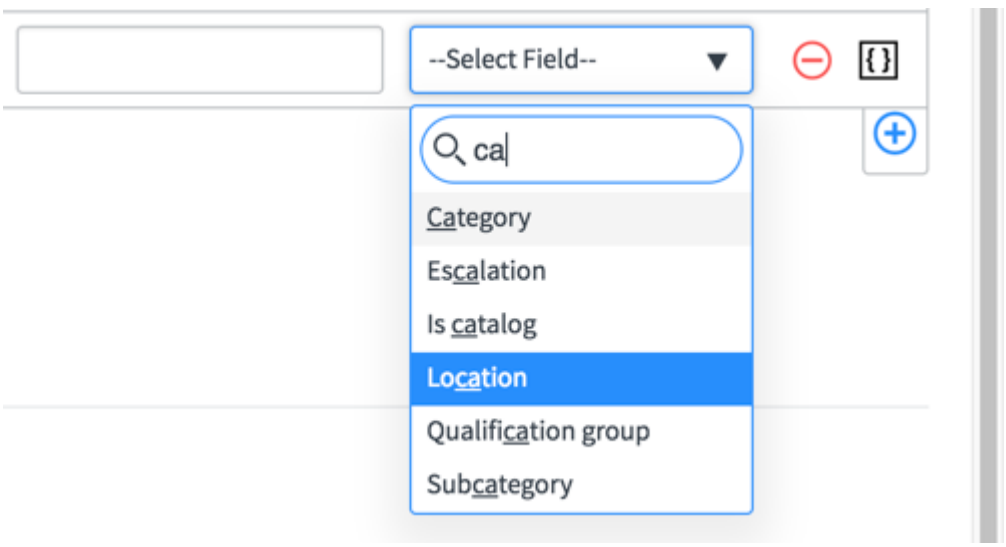
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ am unteren Rand des Rasters auf das Plus-Symbol.




   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

   In der erweiterten Liste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat die Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für Warnungsfelder auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die Zuordnung nachzuverfolgen.




Automatische Übersetzung

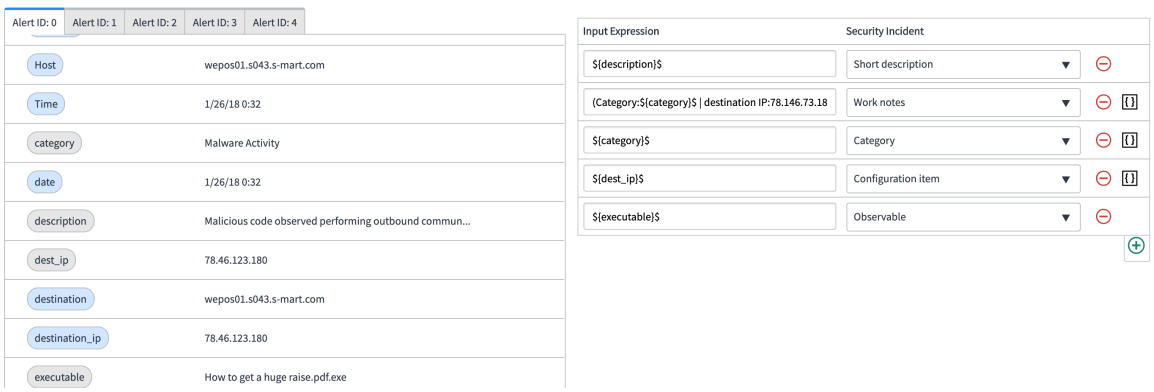
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident eine Liste enthält, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

**c.** Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

**d.** Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte **Warnungs-ID** im Feld Eingabeausdruck auszuwählen.
Ordnen Sie es mit der Drag-Funktion neben Ihrem neuen Feld zu.

**8.** Setzen Sie die Zuordnung fort, indem Sie Felder hinzufügen oder entfernen und der Zuordnung Werte hinzufügen.
Die folgende Abbildung zeigt ein Beispiel für ein bearbeitetes Zuordnungsraster. Im unteren Feld auf der rechten Seite wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Die Werte werden durch Leerzeichen und Satzzeichen getrennt (Kategorie:${category} | Ziel-IP:78.146.73.180).




In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Raster hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die Leerzeichen und Satzzeichen, die Sie in das Feld eingegeben haben, im Abschnitt „Zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

Die folgende Abbildung zeigt ein Beispiel dafür, wie die Werte in der vorherigen Abbildung im Security Incident angezeigt werden.

Filterbedingungen für die Incident-Generierung

**9. Wahlweise:** Nachdem Sie die vorherigen Schritte der Zuordnung auf Feldebene abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Filterbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen SIR Security Incident zu erstellen.



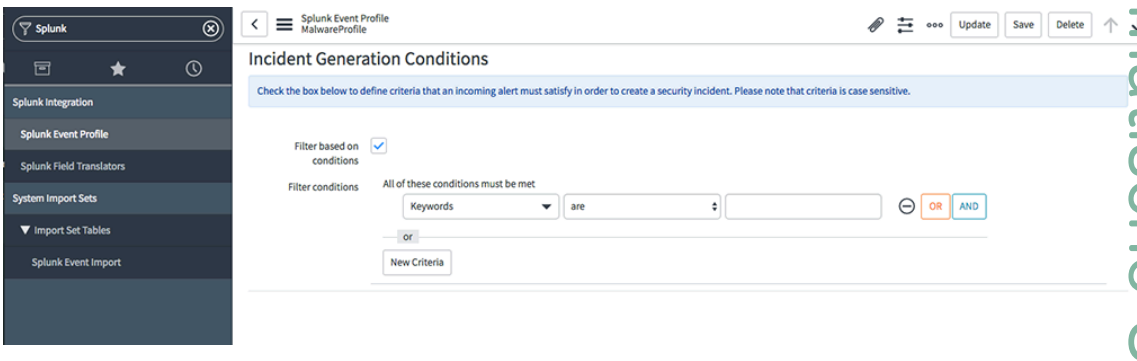
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die folgenden Schritte aus, um Filterbedingungen festzulegen.

**a.** Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern, um die Option zu aktivieren.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.

Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Warnungsbeispielerfassung“ für die erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich abhängig von der Warnung Splunk, die Sie erfassen, oder dem Event, das Sie manuell weiterleiten. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten der Warnung oder des Ereignisses Splunk Enterprise übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu Ihrer Splunk Enterprise -Konsole zurück und überprüfen Ihre Warnungen und Events auf die Stichwörter.

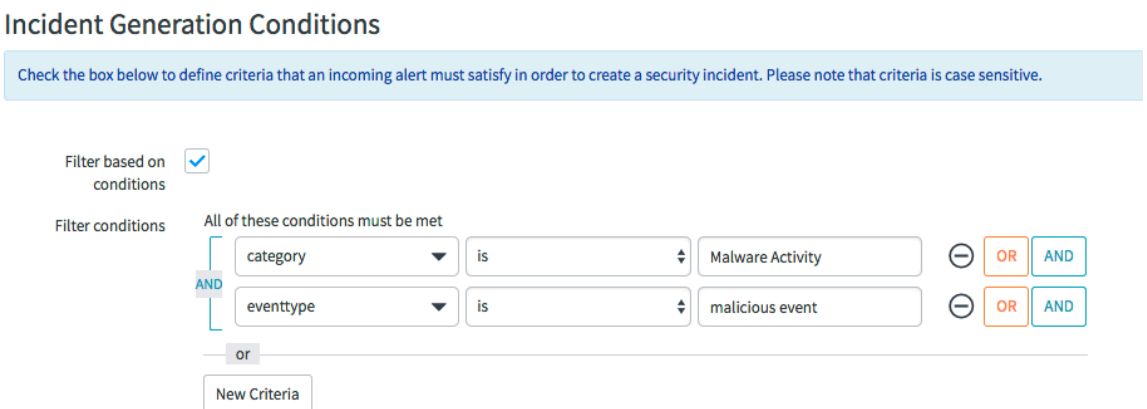



**b.** Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

**c.** Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**. Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.

**d.** **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

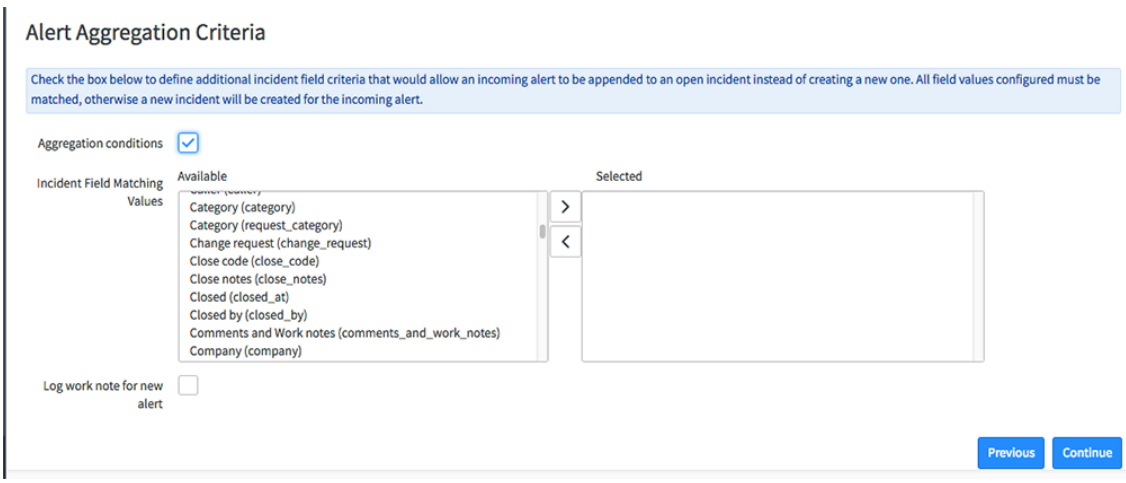
Diese Art der Filterung hilft Ihnen, Sicherheits-Events zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn zusätzliche Filterkriterien festgelegt werden, werden nur erforderliche Warnungen erfasst, ohne dass die Abfrage Splunk oder die Konfiguration der ausgelösten Warnung geändert werden muss.

Zusammenfassung von Warnungen zur Verhinderung doppelter Incidents

10. **Wahlweise:** Um zu vermeiden, dass potenziell doppelte Security Incidents erstellt werden, definieren Sie zusätzliche Incident-Feldkriterien, damit eingehende Warnungen zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um diese Kriterien festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt „Warnungszusammenfassungskriterien“, und aktivieren Sie das Kontrollkästchen Bedingungen zusammenfassen, um diese Option zu aktivieren.

   (Optional) Die Spalten „Übereinstimmungswerte für Incident-Feld“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.




   b. Wählen Sie in der Liste Verfügbar die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Now Platform abgleichen möchten, und verschieben Sie sie in die Liste Ausgewählt.

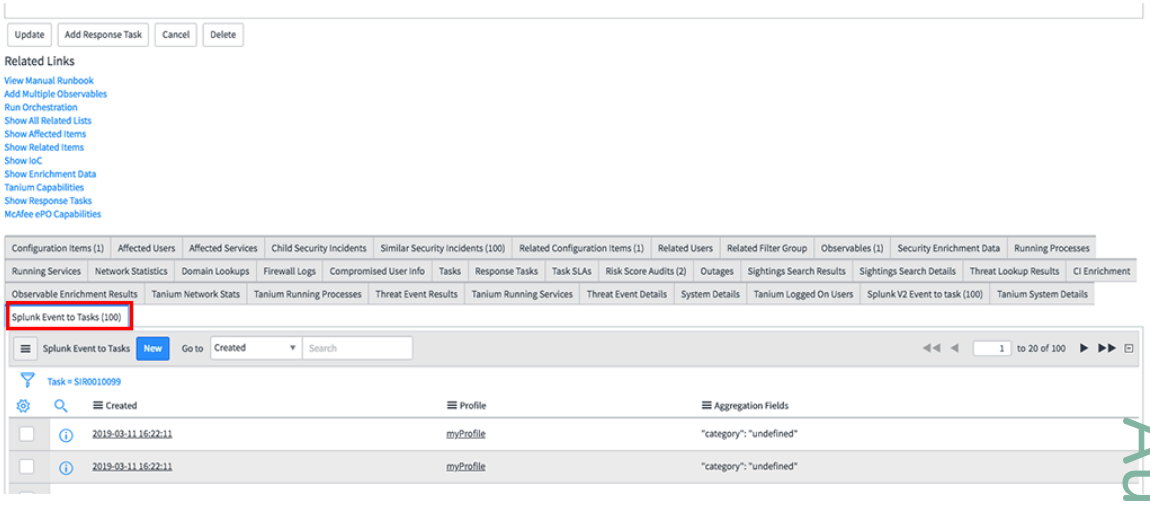
   (Optional) Alle von Ihnen ausgewählten Feldwerte müssen übereinstimmen, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Wenn Sie Feldwerte für Security Incidents überprüfen möchten, um sie für diese Kriterien zu verwenden, navigieren Sie zu **Incidents** > **Alle Incidents anzeigen**.

   Wenn eine neue Warnung mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Warnungen zu einem Security Incident werden in der zugehörigen Liste Splunk Event zu Aufgaben angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen zu vorhandenen Security Incidents hinzugefügt werden. Wenn diese

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter Zugehörige Links, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.




c. **Wahlweise:** Um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie diese Option.
Die Arbeitsnotiz protokolliert, dass eine neue Warnung hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails.

Sie haben Werte aus einer Splunk -Warnung oder einem []-Ereignis erfolgreich Feldern in einem SIR -Security Incident zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien zu begrenzen. Sie haben auch Warnungen oder Events an vorhandene SIR Security Incidents angehängt.

11. **Wahlweise:** Öffnen Sie den Skript-Editor, und setzen Sie die Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor, um Warnungswerte für die Splunk Enterprise Event Ingestion -Integration zu formatieren.

12. Wählen Sie eines aus, um mit der Profilkonfiguration fortzufahren.

### Nächste Maßnahme
Der nächste Schritt besteht darin, eine Vorschau der Werte anzuzeigen, die Sie dem Security Incident zugeordnet haben.

## Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Event Ingestion -Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Now Platform® Security Incident Response (SIR)-Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

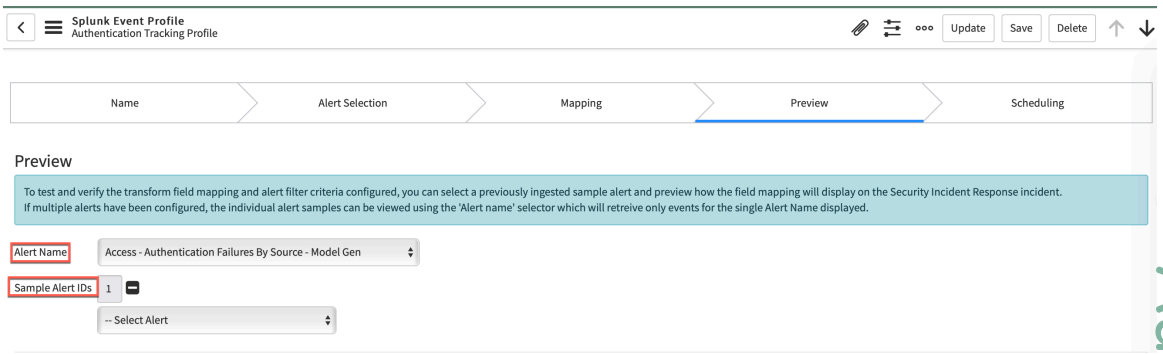
### Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie eine Vorschau eines Security Incident an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents im Produkt SIR gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

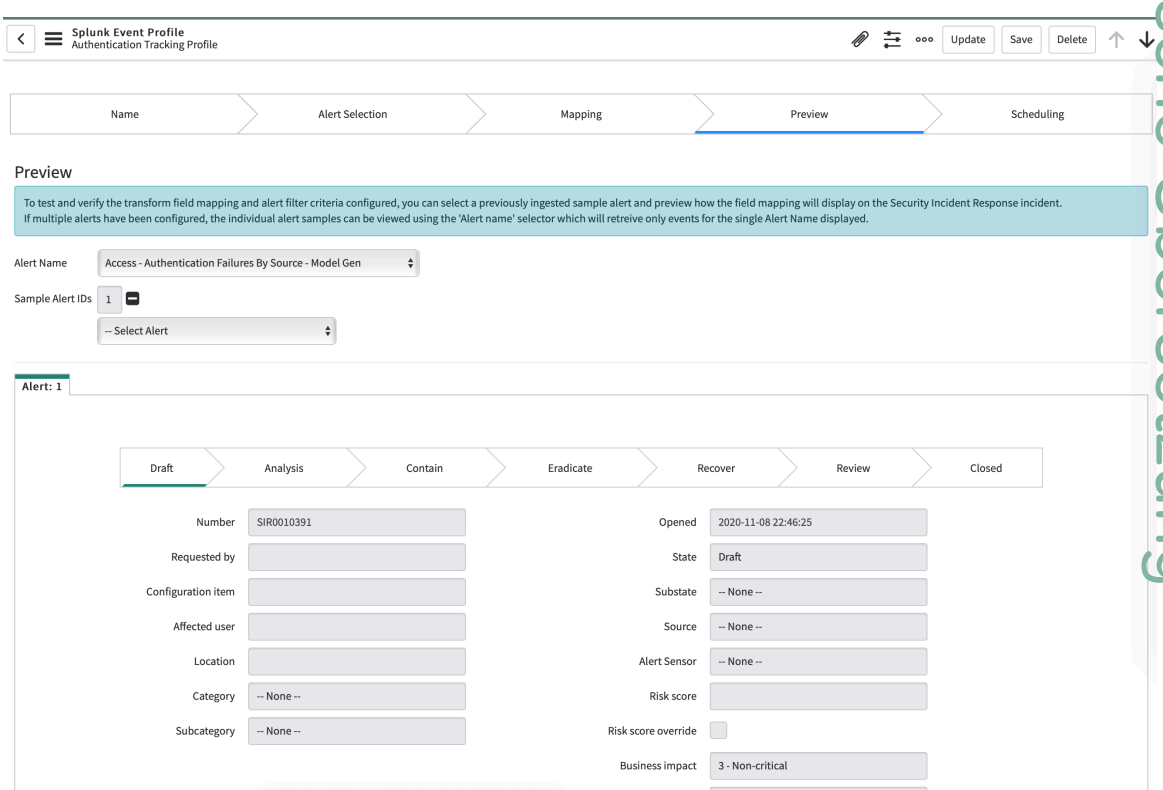
## Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
2. Wählen Sie den **Warnungsnamen** aus, und wählen Sie dann ein Element aus der Liste **Beispielwarnungs-IDs** aus.




Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.

3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.




Die vorherige Abbildung zeigt eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel ist ein Feld im Security Incident für einen Wert nicht vorhanden, oder das Feld unterstützt den von Ihnen zugeordneten Wert nicht. Eine Fehlermeldung wird angezeigt, die angibt, dass für das Feld Konfigurationselement kein Eingabewert gefunden wurde.

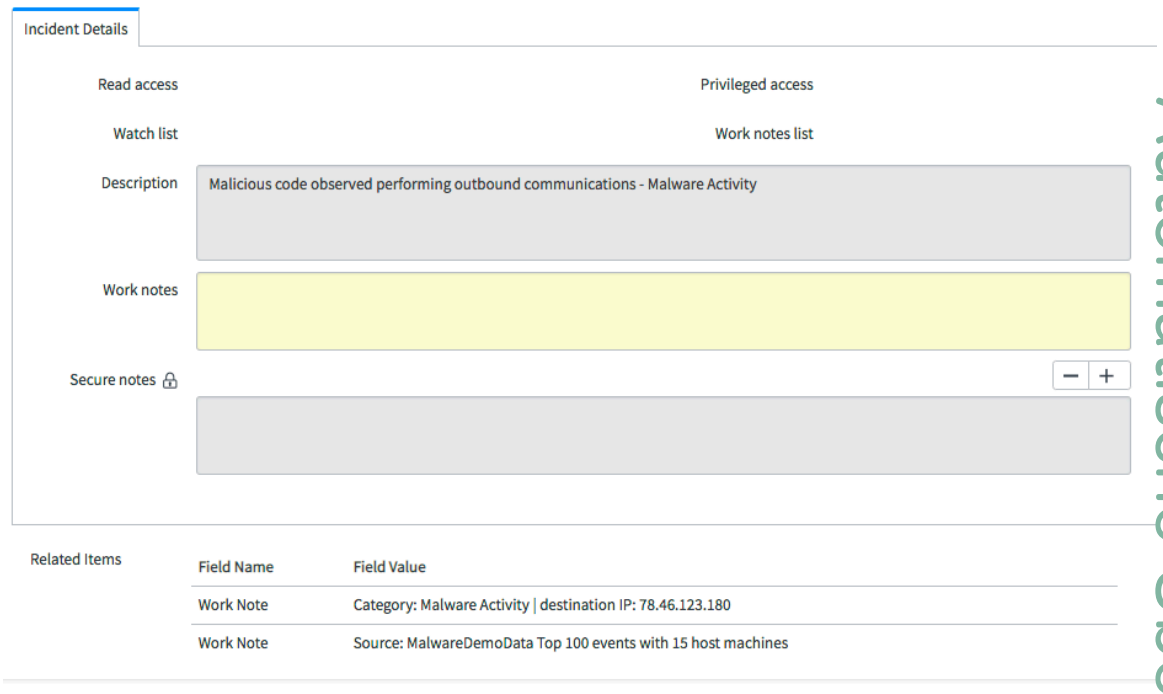
4. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Incident-Details“ in der unteren Hälfte eines SIR Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertepaaren ausgefüllt, die aus der Konsole Splunk Enterprise abgerufen wurden. Das erste Feld „Arbeitsnotizen“ hat keinen Wert. Dieses Feld wurde während des Zuordnungsschritts im Zuordnungsraster leer gelassen. Die zusätzlichen Arbeitsnotizfelder mit Werten wurden dem Zuordnungsraster während des Zuordnungsschritts hinzugefügt.




7. Nachdem Sie alle Fehler behoben und überprüft haben, ob die Felder Ihren Vorstellungen entsprechen, wählen Sie eine Option aus, um fortzufahren.

### Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, führen Sie den nächsten Schritt zu Planen und rufen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration ab.

## Planen und rufen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration ab

Für automatisierte Warnungserfassungsprofile ist dieser Schritt der letzte Schritt der Event-Profilkonfiguration. Während dieses Schritts können Sie die Standardeinstellungen für den Warnungsabruf überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie Ihren Warnungsabruf basierend auf einem Datumsbereich filtern.

### Vorbereitungen

Erforderliche Rolle: Rolle sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie alle Schritte im Fortschrittsbalken für die Profilkonfiguration abgeschlossen haben (siehe folgende Abbildung), haben Sie die Konfiguration für Profile für die manuelle Event-Weiterleitung abgeschlossen. Für Events, die manuell über die Konsole Splunk

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enterprise weitergeleitet werden, ist keine Zeitplanung verfügbar. Bei Profilen für die automatisierte Warnungserfassung wählen Sie während des Schritts „Zeitplanung“ aus, ob Sie historische Warnungen erfassen möchten. Sie können auch auswählen, wie oft zukünftige Warnungen abgefragt werden sollen, die der Konfiguration des Warnungsprofils entsprechen.

**Fortschrittsbalken**

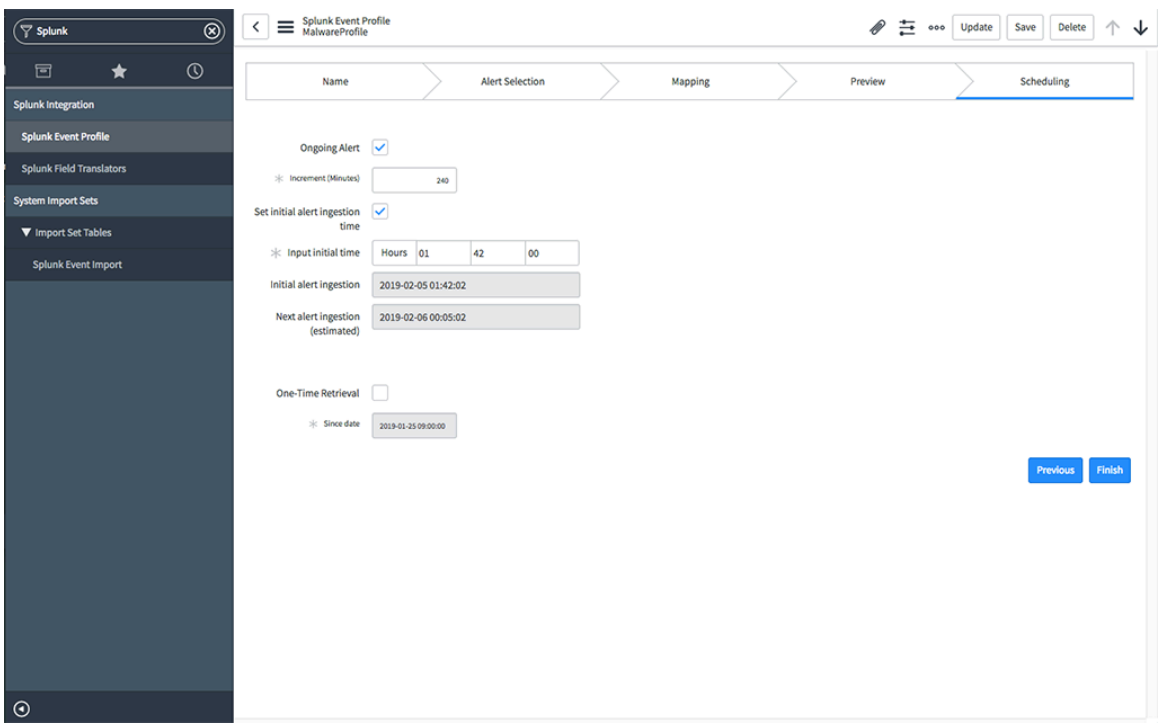
Bei Profilen für die automatisierte Warnungserfassung überprüfen und ändern Sie die Zeitplanung und den Warnungsabruf, bevor das Profil aktiviert wird. Dieser Schritt ist der letzte Schritt des Event-Profilkonfigurationsprozesses für geplante Warnungsprofile.

Konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung der Splunk -Integration der Event-Erfassung wird durch die unterschiedlichen Abfrageintervalle beeinflusst. Bei der Planung möchten Sie möglicherweise die Systemlast mit der Dringlichkeit von Incidents in Einklang bringen. Für jedes Profil wird ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch je nach Dringlichkeit des Incident und der erwarteten Auslastung Ihres Systems ändern.

In der Konsole Splunk Enterprise legen Sie eine Warnung so fest, dass sie basierend auf Inkrementen oder zu einem bestimmten Zeitpunkt ausgelöst wird. Verwenden Sie diese Einstellung, um die Zeitplanung in Ihrer Now Platform -Instanz so zu konfigurieren, dass die Zeitschritte in Ihrer Splunk Enterprise -Konsole mit der Zeitplanung synchronisiert werden, die Sie in Ihrer Now Platform -Instanz eingerichtet haben.

## Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie einen aus, um zu planen, wie und wann Warnungen aus der Konsole Splunk Enterprise abgerufen werden.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie beispielsweise eine tägliche Splunk -Warnung haben, die einmal täglich um 4:05 Uhr Ortszeit ausgeführt wird, können Sie das entsprechende Warnungsprofil in Ihrer Now Platform -Instanz so einrichten, dass es um 4:05 Uhr Ortszeit ausgeführt wird, um die zu erfassen sofort eine Warnung ausführen und einen Security Incident erstellen. Geben Sie `04 05 00` in das Feld **Anfängliche Warnungserfassung** ein. Geben Sie im Feld **Increment (Minutes) (Schrittweite (Minuten))**`1440` (24 Stunden) ein, um die nächste Warnungserfassung für 24 Stunden nach der ersten Warnungserfassung zu planen. Sowohl die anfängliche als auch die nächste Warnungserfassungszeit werden in den Feldern angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie bei angezeigter Seite „Zeitplanung“ das Kontrollkästchen **Ongoing alert** (Laufende Warnung), um diese Option zu aktivieren.

   b. **Geben Sie im Feld Schritt (Minuten)** den Wert `1440` (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Anfängliche Warnungserfassung auswählen**, um die Bearbeitung der Felder Anfängliche Warnungserfassung und Nächste Warnungserfassung zu aktivieren.

   d. Geben Sie im Feld Anfängliche Warnungserfassung `04 05 00`ein.
   Im Feld **Nächste Warnungserfassung (geschätzt)** wird die Zeit der nächsten Warnungserfassung angezeigt.

4. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Dieses Profil ist aktiviert und ruft basierend auf Ihrer Planung Warnungen aus der Konsole Splunk Enterprise ab. Es gibt ein Limit von 1.000 Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Bis zu 100 Events pro ausgelöster Warnung. Nachfolgende Events werden ignoriert, nachdem die Grenzwerte erreicht sind.

### Integrationsarchitektur und externe Systemverbindung für die Splunk Enterprise Event Ingestion -Integration

Im folgenden Thema wird die Integrationsarchitektur beschrieben, die zur Unterstützung der Erfassung ausgelöster Warnungen über die Konsole Splunk Enterprise entwickelt wurde. Diese Informationen verdeutlichen auf einer hohen Ebene die konzeptionelle Funktionsweise der Integration. Außerdem wird erläutert, warum vor der Installation der Anwendung aus dem ServiceNow StoreSetupschritte erforderlich sind.

## Wichtige Begriffe, die für diese Integration verwendet werden

Die folgenden wichtigen Begriffe werden während der Installation und Konfiguration verwendet. Weitere Informationen zu diesen Begriffen finden Sie auf der ServiceNow-Website mit Produktdokumentation , der Splunk-Website und den Ressourcen auf der Seite „Splunk-Ressourcen “.

**Now Platform**

Ein Unternehmensprodukt ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere Produkte basieren.

**ServiceNow Splunkbase-Add-on**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine ServiceNow -Anwendung, die auf Ihrer Splunk Enterprise -Konsole installiert ist und die Option zur manuellen Event-Weiterleitung der Integration unterstützt. Die manuelle Event-Weiterleitung ist eine optionale Funktion der Integration. Dieses ServiceNow Splunkbase-Add-on ist für die automatisierte Warnungserfassung, die von der -Integration bereitgestellt wird, nicht erforderlich.

**Security Incident Response (SIR)**

Eine Now Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und dem Abschluss nach Incidents nachverfolgt.

**Splunk Enterprise**

Ein automatisiertes SIEM-Produkt (Security Incident Event Management) oder ein Cloud-Service, das Daten erfasst, die für die Analyse und Verwaltung von Incidents verwendet werden. Dieser Service befindet sich auf einem Host, der in diesem Leitfaden manchmal auch als Splunk -Konsole bezeichnet wird.

**Splunk Warnung**

Eine Suche, die Sie konfigurieren und in Splunk speichern, um basierend auf den Parametern, die Sie im Service Splunk Enterprise eingerichtet haben, nach bestimmten Daten zu suchen. Wenn Sie Warnungen aus Splunkabrufen, rufen Sie auch alle mit dieser Warnung verknüpften Events ab.

**Splunk hat Warnung ausgelöst**

Eine konfigurierte Suche in der Konsole Splunk Enterprise, die Ergebnisse zurückgibt und diese Ergebnisse als ausgelöste Warnungen kennzeichnet. Die ausgelösten Warnungen werden für diese Integration von der Konsole Splunk in Ihre Instanz Now Platform erfasst. Ausgelöste Warnungen haben ein oder mehrere Splunk Events.

**Splunk Termin**

Ein oder mehrere Datenelemente, die zu den ausgelösten Warnungen des Service Splunk führen. In Ihrer Now Platform -Instanz können Sie nachschlagen, welche Splunk -Ereignisse Now Platform Security Incidents ausgelöst haben.

**MID-Server**

Diese Anwendung erleichtert die Kommunikation und Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Diese Anwendung ist in der Regel für die Integration mit lokalen Technologien erforderlich, und für diese Splunk Enterprise Event Ingestion -Integration erleichtert der MID Server die Kommunikation zwischen Now Platform und der lokalen Instanz von Splunk Enterprise. Ein MID Server ist nicht erforderlich, wenn Sie Ihre Now Platform -Instanz mit einer Splunk Cloud -Instanz integrieren.

**Security Incident-Administrator (sn_si.admin)**

Benutzer mit dieser Rolle überwachen die Konfiguration der Integration mit dem Produkt SIR in Ihrer Instanz Now Platform.

**Security Incident-Analyst (sn_si.analyst)**

Benutzer mit dieser Rolle interagieren mit und analysieren Security Incidents im Produkt ServiceNow Security Incident Response.

## Verbindung mit externen Systemen

Ein Event-Profil ist ein Container, den Sie für eine einzelne Verbindung erstellen, benennen und konfigurieren und den Service Splunk aufrufen, um die aktuellsten ausgelösten Warnungen abzurufen, die bestimmten Kriterien entsprechen. Nachdem ausgelöste Warnungen, die Ihrem Profil entsprechen, aus Splunkabgerufen wurden, wählen Sie aus, welche dieser Warnungen als Now Platform Security Incident Response SIR Security Incident angezeigt werden sollen. Eine Standardansicht der Splunk Enterprise -Warnungsfelder ist



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verfügbar, und Sie bearbeiten diese Zuordnung von Warnungsfeldern zu den Feldern in einem SIR -Security Incident entsprechend Ihren Anforderungen. Sie zeigen eine Vorschau Ihrer Zuordnung an, um sicherzustellen, dass Sie alle erforderlichen Warnungsfeldwerte für den Security Incident SIR ausgefüllt haben. Um die Konfiguration des Warnungsprofils abzuschließen, planen Sie den Abruf von Warnungen und aktivieren dann das Profil. Nachdem Sie das Profil in Now Platformaktiviert haben, können Sie historische und laufende Splunk Warnungen automatisch erfassen.

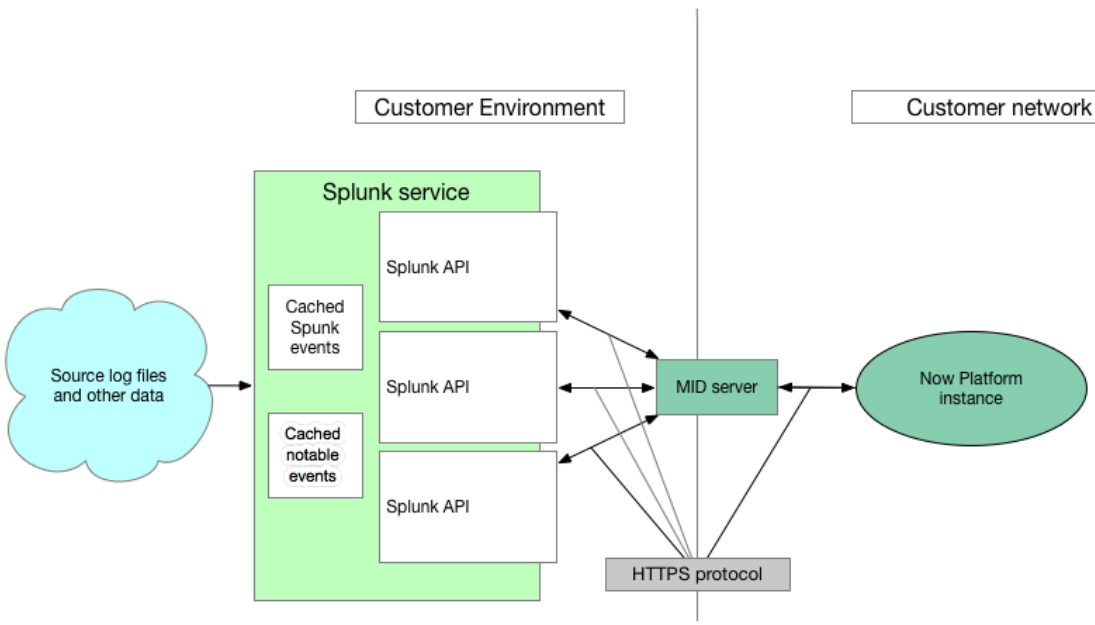
Wenn Sie als Benutzer mit der Rolle „sn_si.admin“ feststellen, dass eine neu ausgelöste Warnung zuvor erfassten Warnungen ähnelt, können Sie neu ausgelöste Warnungen zu vorhandenen SIR Security Incidents zusammenfassen. Sie legen Kriterien fest, um übereinstimmende Zielfeldwerte im Warnungsprofil Splunk Enterprise anzugeben, die definieren, wann ein vorhandener Security Incident aktualisiert und wann ein neuer Security Incident erstellt wird. Wenn die Zusammenfassungsfunktion in Ihrem Event-Profil aktiviert ist, sucht Ihre Now Platform -Instanz bei der Transformation des Importsatzes nach einem vorhandenen Datensatz in der Zieltabelle, der denselben Wert in den Ziel- und Quellfeldern aufweist. Wenn ein vorhandener Datensatz mit einem übereinstimmenden Wert in der Zieltabelle gefunden wird, wird dieser Datensatz aktualisiert. Wenn kein passender Datensatz gefunden wird, wird ein neuer Datensatz in der Zieltabelle erstellt. Wenn diese Option aktiviert ist, aktualisiert die Zusammenfassungsoption vorhandene Security Incidents mit neuen ausgelösten Warnungen, und Sie vermeiden die Erstellung mehrerer Security Incidents. Weitere Informationen zum Aktualisieren von Datensätzen mithilfe von Zusammenfassungsoptionen finden Sie unter Datensätze durch Zusammenfügen aktualisieren.

Diese Anwendung verwendet den API-Service Splunk, um Informationen aus dem Service Splunk abzurufen. Eine ausgehende HTTPS-Verbindung vom MID-Server zu dieser Umgebung ist erforderlich, damit die Integration ordnungsgemäß funktioniert.

Nach der Verbindung mit dem Service Splunk unterstützt die Integration das Abrufen und Erfassen von ausgelösten Warnungen und Events, die Security Incidents auslösen.

Der grundlegende Datenfluss wird in den folgenden Abbildungen veranschaulicht. In jeder Abbildung ruft (erfasst) Ihr Now Platform Daten ab. Splunk übermittelt keine Daten für geplante Warnungen.

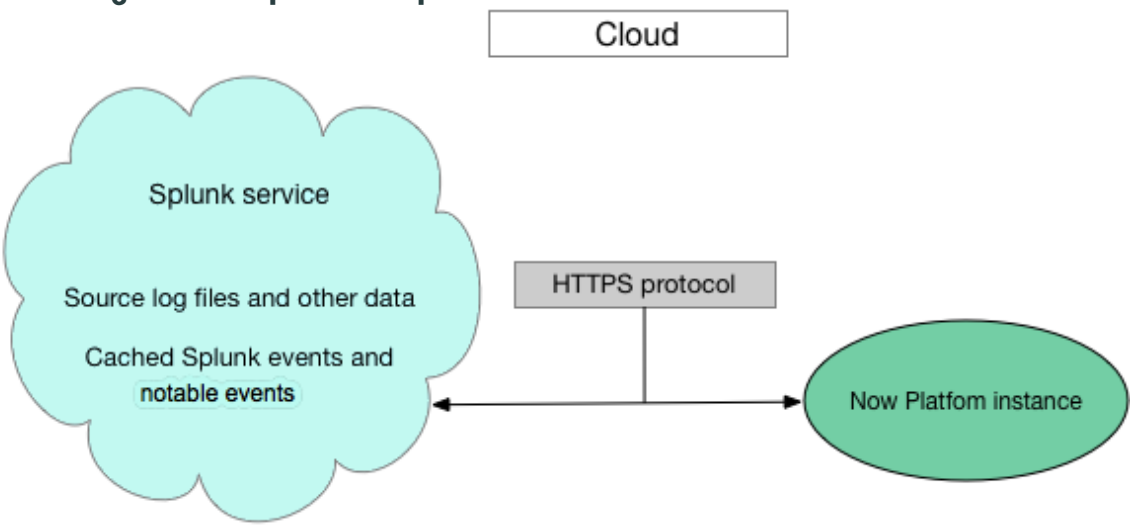
**Verbindung mit lokalem [ Splunk Unternehmensservice mit einzelnen MID-Servern**



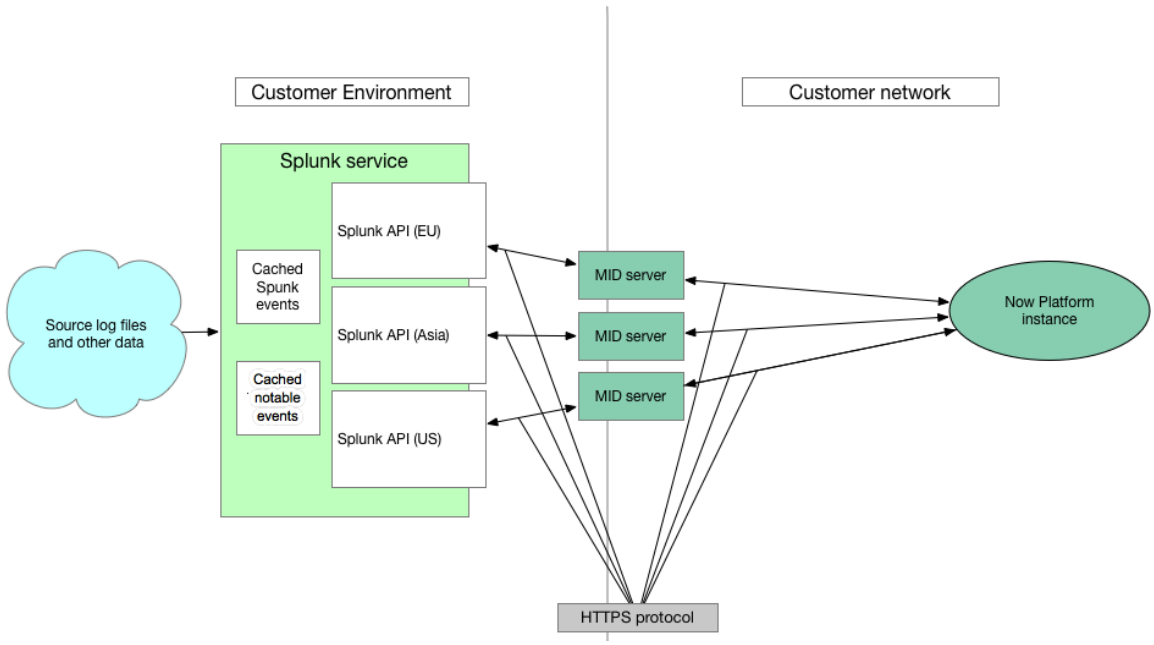



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Verbindung mit einer Splunk Enterprise-Cloud-Instanz**




**Mehrere Verbindungen mit dem Unternehmensservice Splunk über mehrere MID-Server**






## Kopieren Sie Splunk Enterprise Event Ingestion Profile mithilfe der Export-/Importfunktion von einer Instanz in eine andere

Sie können Splunk Enterprise Event Ingestion -Profileinstellungen aus einer Now Platform -Instanz in eine andere Now Platform -Instanz exportieren und importieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

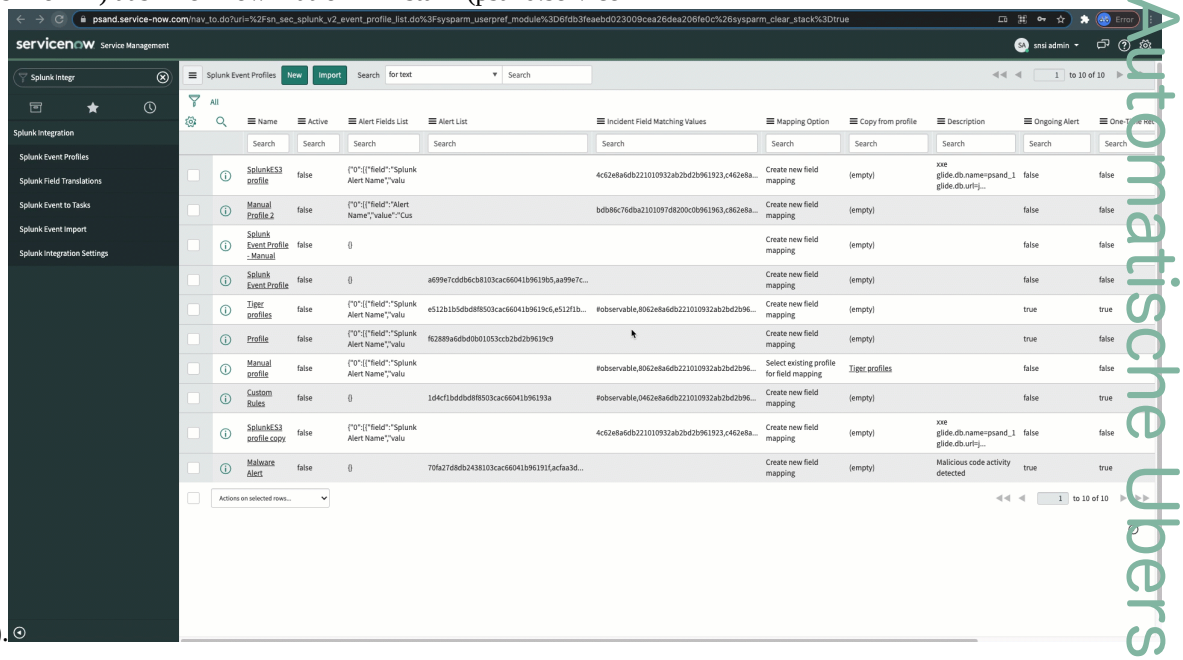
Mit dieser Funktionalität kann der Sicherheitsadministrator Profile, die in einer Now Platform -Instanz getestet und verifiziert wurden, z. B. außerhalb der Produktion, in eine andere Now Platform -Instanz kopieren, z. B. in der Produktion, ohne alle Konfigurationseinstellungen wiederholen zu müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn Sie einen manuellen Event-Weiterleitungsprofiltyp exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangdaten kopiert, die Anhangdatei selbst wird jedoch nicht exportiert.

## Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofile**.
2. Wählen Sie ein Profil aus, das Sie in eine andere Now Platform -Instanz exportieren möchten. Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren**.
4. Sobald die Meldung „Export abgeschlossen“ angezeigt wird, klicken Sie auf **Herunterladen**. Die folgende Abbildung zeigt das Exportieren eines Splunk -Profils (manuelles Profil 2) aus Ihrer Now Platform -Instanz (psand.service-now.com).



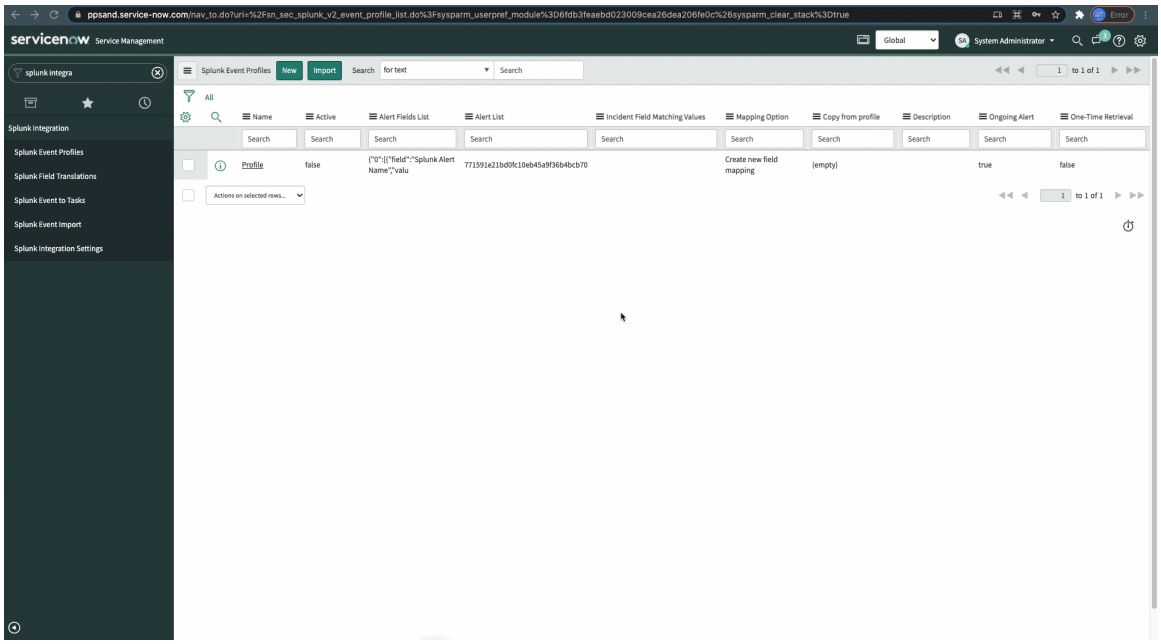

Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben payload.xml-Datei angezeigt.

Sie können jetzt das Profil in eine andere Now Platform -Instanz importieren.

5. Navigieren zu **Splunk-Integration** > **Splunk-Ereignisprofile**.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie auf **Datei** auswählen, und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie **auf Profile schließen und neu laden**.
   Die folgende Abbildung zeigt den Import eines Splunk -Profils (manuelles Profil 2) aus der Now Platform -Instanz (psand.service-now.com) in eine andere Now Platform -Instanz (ppsand.service-now.com).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie haben das Profil erfolgreich aus einer anderen Now Platform -Instanz importiert.

Vergewissern Sie sich, dass die exportierte Quelle (Splunk API-Konto und Splunk Server-URL) und die MID Server-Konfigurationseinstellungen gültig und in der importierten Now Platform -Instanz verfügbar sind. Aktualisieren Sie bei Bedarf Ihre Splunk Enterprise Event Ingestion -Konfiguration.

10. **Wahlweise:** Überprüfen Sie die MID Server-Einstellungen, nachdem Sie ein Profil importiert haben.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**.
12. **Wahlweise:** Wählen Sie die Konfigurationskachel Splunk Enterprise Event Ingestion aus, und klicken Sie auf **Aktualisieren**.
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Quell- und MID Server-Details nach Bedarf.

### Kopieren Sie ein Event-Profil für die Splunk Enterprise Event Ingestion -Integration

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Alarmprofile zu kopieren, um Zeit zu sparen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Das Kopieren eines vorhandenen Profils und der zugehörigen Einstellungen ist optional.

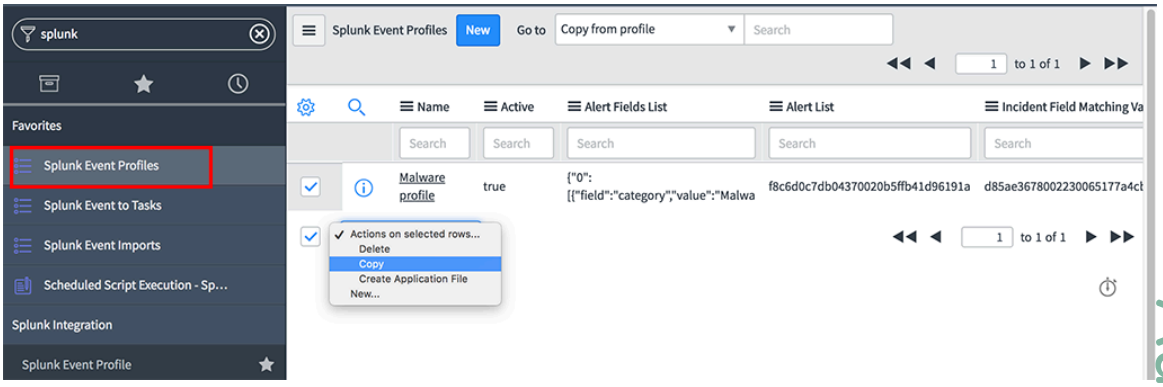
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.



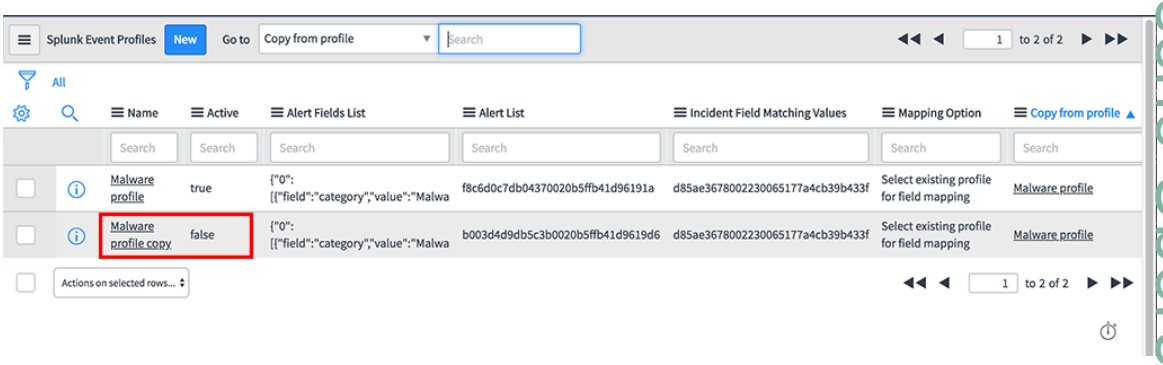
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wählen Sie in der angezeigten Liste Splunk Ereignisprofile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.




Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.




Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

### Nächste Maßnahme

Nachdem Sie die Konfigurationsschritte abgeschlossen haben, werden Sie aufgefordert, das neue Profil zu aktivieren.

## Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Splunk Enterprise -Integration der Event-Erfassung ein

Wenn Sie Events manuell und bei Bedarf aus Ihrer Splunk Enterprise -Konsole für diese Integration exportieren möchten, installieren und richten Sie die Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise in Ihrer Splunk Enterprise-Konsole oder Splunk-Cloud-Instanz ein.

### Vorbereitungen

Vergewissern Sie sich, dass Sie die Anwendung für diese Integration aus dem ServiceNow Store installiert haben, bevor Sie das Add-on-Plugin von splunkbase installieren, das für die manuelle Event-Erfassung erforderlich ist. Wenn Sie die Anwendung für die Integration von ServiceNow Storenicht installiert haben, lesen Sie Installieren und konfigurieren Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Anwendung ServiceNow für die Integration von Splunk Enterprise Event Ingestion ., und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: Now Platform Administrator (admin)

### Warum und wann dieser Vorgang ausgeführt wird

Die Installation und Einrichtung des Add-ons ServiceNow „ Security Operations Event Ingestion“ ist optional.

Wenn Sie Events manuell und bei Bedarf aus Ihrer Splunk Enterprise -Konsole für die -Integration exportieren möchten, laden Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise aus splunkbase in Ihrer Splunk Enterprise -Konsole herunter, installieren Sie es und richten Sie es ein.

Dieses Erweiterungs-Add-on ServiceNow ist erforderlich, damit Security Incidents aus manuell exportierten Events in Ihrer Now Platform -Instanz erstellt werden können. Diese Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise ist auf splunkbase verfügbar.

Für die manuelle Event-Weiterleitung können Sie bis zu zwei verschiedene Now Platform -Endpunkte (Instanzen) in Ihrer Splunk Enterprise -Konsole identifizieren. Sie leiten die Events manuell an den Endpunkt oder die Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise sowohl eine Staging-Instanz (Entwicklungsinstanz) als auch eine Produktionsinstanz angeben. Indem Sie separate Instanzen angeben und primäre und sekundäre Workflows für jede Instanz benennen, können Sie auswählen, wohin Sie verschiedene Events weiterleiten möchten.

### Prozedur

1. Wenn Sie das Add-on „ ServiceNow Security Operations Event Ingestion“ für Splunk Enterprisenoch nicht installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu splunkbase .

   b. Suchen Sie nach dem Add-on „ ServiceNow Security Operations Security Operations Event Ingestion“ für Splunk Enterprise.

   **Hinweis:**
   Stellen Sie sicher, dass Sie ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterpriseausgewählt haben. Es gibt zusätzliche ServiceNow Add-ons, die in dieser Liste angezeigt werden. Diese Add-ons sind für verschiedene ServiceNow Splunk -Integrationen vorgesehen und für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihr Konto Splunk Enterprise.

   e. Klicken Sie auf der Seite „Apps“ in der Dropdown-Liste des Menüs auf das Zahnradsymbol oder die Verknüpfung **Apps verwalten**.

   f. Klicken Sie oben links auf der angezeigten Seite „Apps“ auf **App aus Datei installieren**.

   g. Klicken Sie auf **Datei**auswählen, wählen Sie ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterpriseaus, und klicken Sie auf **Hochladen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**h.** Wenn Sie dazu aufgefordert werden, starten Sie Splunk Enterpriseneu.
Das Add-on ServiceNow Security Operations Event Ingestion für Splunk Enterprise wird in Ihrer Splunk Enterprise Enterprise-Konsole installiert. Der nächste Schritt zum Einrichten des Add-ons.

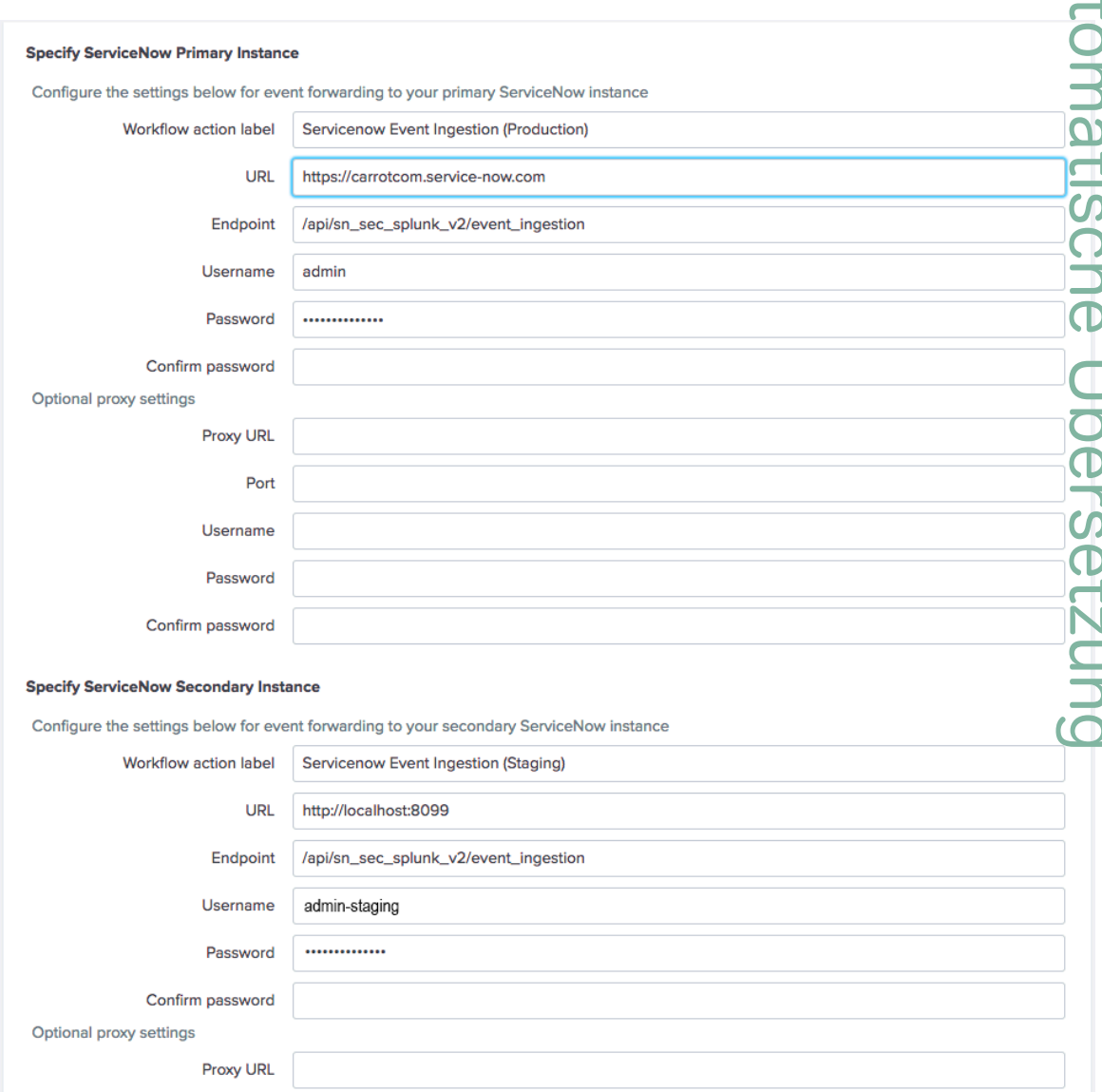
**2.** Führen Sie die folgenden Schritte aus, um das Add-on einzurichten.

**a.** Klicken Sie in Splunk Enterpriseauf das Zahnradsymbol für **Apps** oder auf **Apps verwalten** in der Dropdown-Liste des Menüs.

**b.** Klicken Sie in der Liste der angezeigten Anwendungen in der Spalte **Aktionen** auf **Setup** für ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise.

**c.** Füllen Sie das Formular aus.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular in der Konsole Splunk Enterprise.

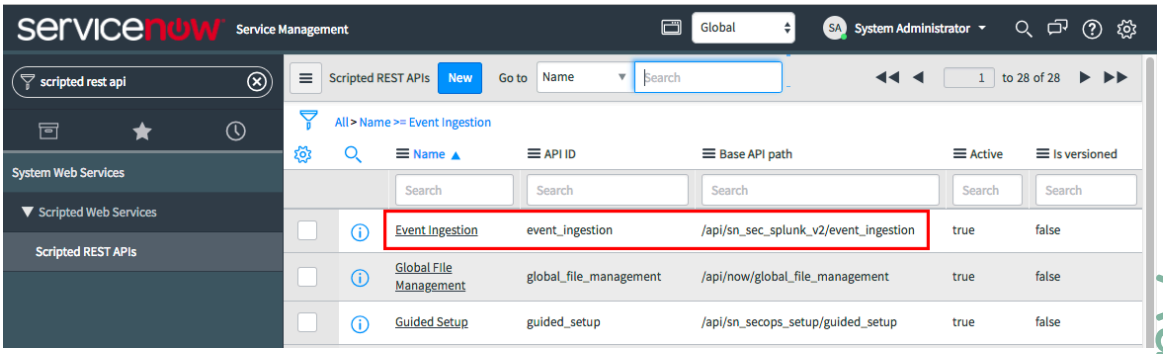



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für die Liste der Scripted REST APIs in Now Platform. In der Liste wird die Position des Endpunktwerts einer Now Platform -Instanz angezeigt, die Sie im Formular als Teil des Setups für die Erweiterung ServiceNow „ Security Operations Event Ingestion Add-on for Splunk Enterprise “ in Ihrer Splunk Enterprise -Konsole eingegeben haben.

**Liste der Scripted REST APIs in Now Platform**




3. Klicken Sie im Setup-Formular in der Konsole Splunk Enterprise auf **Speichern**, um Ihre Änderungen zu speichern.

   Nach einigen Minuten wird oben links im Formular in Ihrer Splunk Enterprise -Konsole eine Meldung angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, sind die Namen (Workflow-Aktionsbezeichnungen) für Ihre Now Platform Instanzen, die Sie im Formular erstellt haben, in der Auswahlliste Ereignisaktionen für ein ausgewähltes Event einer Suche in Ihrer Splunk Enterprise -Konsole verfügbar.

## Nächste Maßnahme

Wenn Sie Suchen noch nicht in Ihrer Splunk Enterprise -Konsole gespeichert haben, besteht der nächste Schritt darin, Suchen als Warnungen in Ihrer Splunk Enterprise -Konsole zu speichern.

### Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration

Die folgenden Schritte zum Speichern von Suchen in Ihrer Splunk Enterprise -Konsole werden für einen Benutzer mit der Splunk Enterprise ]-Administratorrolle bereitgestellt.

## Vorbereitungen

Wenn Sie bereits gespeicherte Suchen und ausgelöste Warnungen in Ihrer Konsole Splunk Enterprise haben, müssen Sie diese Suchen für diese Integration nicht ändern.

Durch die Integration des Produkts Now Platform® Security Operations mit dem Event-Benachrichtigungsservice Splunk werden Event- und Warnungsinformationen aus Splunkabgerufen .

Konfigurieren Sie vor der Erfassung von Warnungen in Ihrer Security Operations -Umgebung Suchen in Ihrer Splunk Enterprise -Konsole, damit Sie automatisch die relevanten Sicherheits-Events in Splunk Enterprise abrufen, die Sie als Warnungen speichern möchten.

Wenn Sie keine gespeicherten Suchen und keine ausgelösten Warnungen für die Benachrichtigung eingerichtet haben, wenn in Ihrer Konsole Splunk Enterprise wichtige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheits-Ereignisse auftreten, führen Sie die folgenden Schritte aus, um Suchen zu speichern.

Erforderliche Rolle: Splunk Enterprise Administrator

### Prozedur

1. Melden Sie sich bei Ihrem Splunk Enterprise-Konto an.
2. Klicken Sie auf die Registerkarte **Suche**.
3. Geben Sie im angezeigten Feld Neue Suche einen Wert für die Warnung ein, z. B. Malware.
4. Um die Events anzuzeigen, die sich auf Ihre Suche beziehen, klicken Sie rechts neben dem Feld Neue Suche auf das Suchsymbol, oder drücken Sie die Eingabetaste.
   Die Suchergebnisse mit Events werden angezeigt.
5. Um die Suche als Warnung zu speichern, erweitern Sie oben rechts auf der Seite die Auswahlliste Speichern unter, und wählen Sie **Warnung**aus.
6. Füllen Sie die Felder im angezeigten Formular aus.
7. Klicken Sie auf **Speichern**.
   Ihre Warnung wird gespeichert und auf der Suchseite auf der Registerkarte Warnungen angezeigt.
   Der Service Splunk ruft die Events ab, indem er die Kriterien abgleicht, die Sie in der Warnung konfiguriert haben. Die Events werden zwischengespeichert, und Sie fordern diese Events dann von Ihren Profilen an, die Sie in Ihrer Now Platform -Instanz eingerichtet haben. Da der Erfassungsabruf von Events aus einem Cache im Splunk -Service erfolgt, wirkt sich diese Erfassung aus Ihrem Now Platform nicht auf die Leistung auf Ihrer Splunk -Plattform aus.

### Nächste Maßnahme

Sie haben das erforderliche Setup für die -Integration in Ihrer Splunk Enterprise -Konsole erfolgreich abgeschlossen. Wenn Sie die Anwendung für die Integration von ServiceNow Storenoch nicht installiert haben, besteht der nächste Schritt darin, die Anwendung für die Integration zu installieren und zu konfigurieren.

## Verwenden Sie den Skript-Editor, um Warnungswerte für die Splunk Enterprise Event Ingestion -Integration zu formatieren

Verwenden Sie den Skript-Editor, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren.

### Vorbereitungen

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Warnungswerten und den manuell eingegebenen Warnungswerten können Sie optional den Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Der Skript-Editor ändert die Werte einer Splunk -Warnung, sodass Werte, die vom Now Platform® Security Incident Response -Security Incident unterstützt werden, den Feldern „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ zugeordnet werden.

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen werden die Warnungswerte Splunk Enterprise den Feldern „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ im Incident SIR zugeordnet und nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie

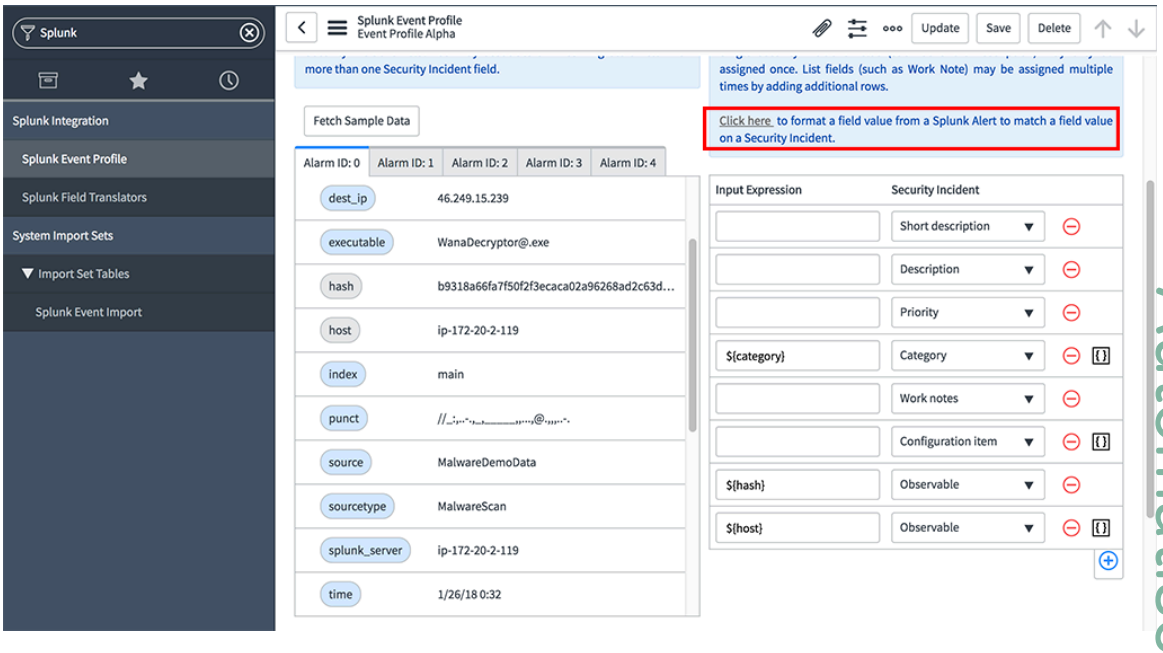


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Wert einer Warnung Splunk Enterprise in einen Wert übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.

### Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.

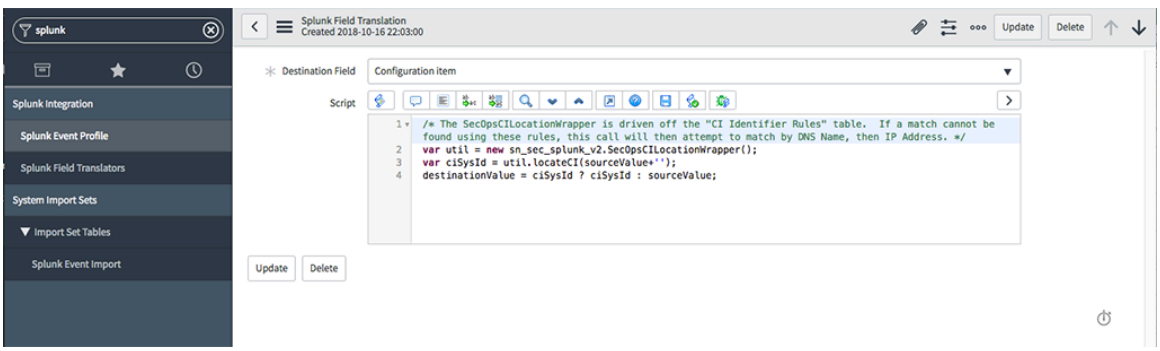



2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Configuration Item geeignet sein. Bei einer Warnung stimmt beispielsweise ein Wert für das Konfigurationselement möglicherweise nicht überein.

   Wie in der folgenden Abbildung dargestellt, können Sie, wenn im Now Platform® CMBD für das Feld „Konfigurationselement“ keine Übereinstimmung mit einem Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld „Konfigurationselement“ ausgefüllt wird, wenn eine IP-Adresse gefunden wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null gesetzt.

   Der Editor wird geöffnet, und das Feld wird in Zielfeld angezeigt. Die folgende Abbildung zeigt den Editor mit dem Feld Configuration Item als Zielfeld.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle Splunk „ Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Formular „Zuordnung“ zurückzukehren.

### Prüfliste für die Splunk Enterprise Event Ingestion -Integration

Verwenden Sie diese Prüfliste, um alle Aufgaben der Integration zu durchlaufen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration mit der folgenden Tabelle nach. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. In jeder Zeile der Tabelle werden Aufgaben aufgelistet und die Rollen angegeben, die zum Ausführen der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

Erforderliche Rollen: Rollen werden für jeden Schritt unten aufgelistet.

#### Prozedur

1. Richten Sie als Benutzer mit der Administratorrolle Now Platform ] Ihre Now Platform -Instanz ein.
   - Weisen Sie Benutzer mit den Rollen sn_si.admin und sn_si.analyst nach Bedarf zu.
   - Installieren und konfigurieren Sie einen MID Server, wenn der Server Splunk in Ihrem Unternehmensnetzwerk bereitgestellt wird.
   - Vergewissern Sie sich, dass die Plugins ServiceNow Security Incident Response für Ihr Release von Now Platformaktiviert sind.
   - Wenn Sie Events manuell von Ihrer Splunk Enterprise -Konsole an Ihre Now Platform -Instanz weiterleiten möchten, vergewissern Sie sich, dass Sie die Rolle (sn_sec_splunk_v2.api_account_access) einem Benutzer mit der Splunk Enterprise -Unternehmensadministratorberechtigung zugewiesen haben.

   Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die Splunk Enterprise Event Ingestion -Integration ein.

   Sie haben die Setup-Schritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration überprüft.
2. Installieren und konfigurieren Sie als Benutzer mit der Administratorrolle Now PlatformSplunk Enterprise Event Ingestion die Anwendung [] aus dem ServiceNow Store.
   a. Laden Sie die Anwendung herunter, und installieren Sie sie in Ihrer Instanz Now Platform.
   b. Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung zu Ihrer Splunk Enterprise -Konsole her.

   Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Event Ingestion ..
3. **Wahlweise:** Wenn Sie Events manuell aus Ihrer Splunk Enterprise -Konsole in Ihre Now Platform -Instanz exportieren möchten, führen Sie die folgenden Aufgaben aus:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Installieren, richten Sie als Splunk Enterprise ]-Administrator das Add-on „ ServiceNow Security Operations Event Ingestion“ für Splunk Enterprise aus splunkbase in Ihrer Splunk Enterprise -Konsole ein, richten Sie es ein und aktivieren Sie es.

b. Speichern Sie als Splunk Enterprise -Administrator, falls noch nicht konfiguriert, Suchen als Warnungen in Ihrer Splunk Enterprise -Konsole.

(Optional) Weitere Informationen finden Sie unter Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Splunk Enterprise -Integration der Event-Erfassung ein und Speichern Sie Suchen in Ihrer Splunk Enterprise -Konsole für die Splunk Enterprise Event Ingestion -Integration.

4. Erstellen und benennen Sie als Benutzer mit der Rolle Now Platform sn_si.admin ein Event-Profil.

Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Event-Profil, mit dem Sie Anhangdaten manuell aus Ihrer Splunk Enterprise -Konsole exportieren können.

- Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus.
- Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Zuordnung, oder kopieren Sie eine vorhandene Zuordnung.

Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Event-Profil für die Splunk Enterprise Event Ingestion -Integration.

5. Ordnen Sie als Benutzer mit der Rolle Now Platform sn_si.admin erfasste Werte oder Anhangdaten, die aus Splunk Enterprise exportiert werden, zu Now Platform Security Incidents zu.

a. Rufen Sie Beispieldaten für eine geplante Warnung ab.

b. Exportieren Sie Anhangdaten manuell aus Splunk Enterprise für ein Event.

c. Bearbeiten Sie die Standardzuordnungskonfiguration.

d. Fügen Sie optional Filterkriterien hinzu, hängen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skript-Editor.

Weitere Informationen finden Sie unterZuordnung von Warnungen und Events für die Splunk Enterprise Event Ingestion -Integration und Ordnen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration zu.

6. Zeigen Sie als Benutzer mit der Rolle Now Platform sn_si.admin eine Vorschau der Daten aus Splunk Enterprise an, die für einen Now Platform Security Incident angezeigt werden.

Beheben Sie alle Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden.

Weitere Informationen finden Sie unter Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Event Ingestion -Integration an.

7. Planen Sie als Benutzer mit der Rolle Now Platform sn_si.admin den Warnungsabruf für ein Profil mit einer geplanten Warnung.

Weitere Informationen finden Sie unter Planen und rufen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration ab.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Splunk Enterprise Security Event-Erfassungsintegration für Security Operations von ServiceNow

Die Integration von Splunk Enterprise Security Notable Event Ingestion mit dem Produkt Security Incident Response (SIR) ermöglicht Security Incident-Analysten die Erfassung und Verarbeitung von Daten zu wichtigen Events (sogenannte Notables).

### Übersicht

Daten werden kontinuierlich basierend auf einem konfigurierten Abfragezeitplan erfasst und von Analysten verwendet, um potenzielle Cyberbedrohungen zu erkennen und darauf zu reagieren. Erfasste Sicherheits-Events können mit wichtigen Events in Splunk Enterprise Security korreliert und dann mit dieser Integration automatisch erfasst werden. Außerdem können einzelne wichtige Ereignisse bei Bedarf manuell von der Incident-Überprüfungskonsole und der Berichterstellungsschnittstelle von Splunk Enterprise Security ] an das Produkt Security Incident Response von Now Platform weitergeleitet werden, um Security Incidents zu erstellen.

Diese Integration bietet einem Security Operations Center (SOC)-Analysten Einblick in wichtige Events und zugehörige beitragende Event-Daten. Diese Daten können zur weiteren Untersuchung und Korrektur in Now Platform Security Incident Response (SIR) Security Incidents integriert werden. Profile werden in Ihrer Instanz Now Platform erstellt, um verschiedene wichtige Event-Typen zu verarbeiten, die über Korrelationssuchen in Splunk Enterprise Securityerstellt werden. Diese Profile passen an, wie verschiedene Splunk Event-Felder in SIR Security Incidents angezeigt werden.

### Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere wichtige Event-Erfassungsprofile, um SIR-Security Incidents für bestimmte Arten von Bedrohungen zu erstellen, z. B. Phishing, Malware und nicht autorisierte Zugriffsversuche.
- Erstellen Sie mehrere Event-Profile für die On-Demand-Event-Weiterleitung über Ihre Splunk ES Incident-Überprüfungskonsole, um SIR-Security Incidents zu erstellen.
- Drag-and-Drop-Zuordnung von Splunk Feldwerten für wichtige Ereignisse zu zugehörigen SIR-Security Incident-Feldern.
- Eine Vorschau des SIR Security Incident-Layouts basierend auf wichtigen Beispiel-Events zur Validierung der Event-Zuordnungsdetails.
- Erfassen Sie historische wichtige Ereignisse sowie laufende, neue und aktualisierte wichtige Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie wichtige Events heraus, die die SIR-Kriterien für die Incident-Generierung nicht erfüllen, z. B. Events mit niedriger Priorität, Events, die einen bestimmten Status noch nicht erreicht haben usw.
- Fassen Sie Events oder Warnungen zu vorhandenen SIR Security Incidents basierend auf übereinstimmenden Feldwerten zusammen, um doppelte Security Incidents zu vermeiden.
- Aktualisieren Sie wichtige Ereignisse basierend auf SIR-Incident-Erstellungs- und/oder -Abschlussbedingungen über eine bidirektionale Schnittstelle, um Splunk ES wichtige Ereignisaktualisierungen mit dem ServiceNow SIR-Incident-Status synchron zu halten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Unterstützte Versionen Now Platform .

Das Plugin „com.snc.si_dep“ ist für diese Integration erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen Security Operations -Anwendungen installieren und aktivieren.

Die folgenden Security Operations Anwendungen müssen über den ServiceNow Storeinstalliert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response

Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store ..

## ServiceNow Add-ons

Das Add-on ServiceNow Security Operations Event Ingestion für Splunk ES ist nur erforderlich, wenn Sie Events manuell aus Ihrer Splunk Enterprise Security Incident Review-Konsole an Ihre Now Platform -Instanz weiterleiten möchten. Dieses Add-on ServiceNow ist in splunkbase verfügbar.

Diese Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise in splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.

## Splunk Unterstützte Versionen

Diese Integration wurde mit Splunk Enterprise Version 8.0.1 und mit Splunk Enterprise Security Anwendungsversion 6.2.1 getestet.

## MID-Server

Für diese Integration muss ein installierter und konfigurierter MID Server in Ihrer Now Platform® -Instanz eine Verbindung zum Splunk -Service herstellen, wenn der Splunk -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Wenn Sie den Service Splunk Cloud verwenden, ist kein MID Server erforderlich. Weitere Informationen zu MID Servern finden Sie unter MID Server .

## Referenzen

| Referenz | Dokumentbezeichner | Dokumententitel |
|---|---|---|
| 1 | Splunk -Produktwebsite | Produktwebsite von Splunk Enterprise Security . |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prüfliste

Eine Prüfliste mit diesen Themen zum Ausdrucken finden Sie unter Prüfliste für die Integration von Splunk Enterprise Security Notable Event Ingestion. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Durcharbeitung der Aufgaben der Integration zu überwachen.

### In dieser Integration verwendete Schlüsselbegriffe

In diesem Abschnitt werden einige der wichtigsten Begriffe beschrieben, die in dieser Integration verwendet werden.

Die folgenden wichtigen Begriffe werden während der Installation und Konfiguration verwendet. Weitere Informationen zu diesen Begriffen finden Sie auf der ServiceNow-Website mit Produktdokumentation , der Splunk-Website und den Ressourcen auf der Seite „Splunk-Ressourcen “.

**Now Platform**

Ein Unternehmensprodukt ServiceNow. Now Platform ist die Basis, auf der einzelne Komponenten wie Security Incident Response (SIR), IT Service Management (ITSM) und andere Produkte basieren.

**ServiceNow Splunkbase-Add-on**

Eine ServiceNow -Anwendung, die auf Ihrer Splunk Enterprise Security -Konsole installiert ist und die Option zur manuellen Event-Weiterleitung der Integration unterstützt. Die manuelle Event-Weiterleitung ist eine optionale Funktion der Integration. Dieses ServiceNow Splunkbase-Add-on ist nicht für die automatisierte Erfassung wichtiger Ereignisse erforderlich, die von der Integration bereitgestellt wird, die Ereignisse aus Splunk] abruft.

**Security Incident Response (SIR)**

Eine Now Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und der ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und dem Abschluss nach Incidents nachverfolgt.

**Splunk Enterprise Security**

Splunk Enterprise Security hilft Teams, unternehmensweite Transparenz und Sicherheitsinformationen für kontinuierliche Überwachung, Reaktion auf Incidents, SOC-Vorgänge zu erhalten und Führungskräften Einblicke in Geschäftsrisiken zu gewähren. Splunk Enterprise Security ist eine Premium-Sicherheitslösung, die eine kostenpflichtige Lizenz erfordert. Dieser Service befindet sich auf einem Host oder einem Splunk-Cloud-Angebot, das in diesem Leitfaden als Splunk -Konsole bezeichnet wird.

**Splunk Enterprise Security Bemerkenswertes Ereignis**

Wenn eine Korrelationssuche ein Event oder ein Muster von Events identifiziert, wird ein wichtiges Event erstellt. Korrelationssuchen filtern die Sicherheitsdaten und korrelieren über Ereignisse hinweg, um einen bestimmten Typ von Incident (oder Muster von Ereignissen) zu identifizieren und dann wichtige Ereignisse zu erstellen.

**Splunk Termin**

Ein oder mehrere Datenelemente, die zu den wichtigen Ereignissen des Service Splunk führen. In Ihrer Now Platform -Instanz können Sie nachschlagen, welche Splunk -Ereignisse Now Platform Security Incidents ausgelöst haben.

**MID-Server**

Diese Anwendung erleichtert die Kommunikation und Bewegung von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Diese Anwendung ist in der Regel für die Integration mit lokalen Technologien erforderlich, und für diese Splunk Enterprise Security Event-Erfassungsintegration erleichtert der MID Server die Kommunikation zwischen Now Platform und der lokalen Instanz von Splunk Enterprise Security. Ein MID Server ist nicht erforderlich, wenn Sie Ihre Now Platform -Instanz mit einer Splunk Cloud -Instanz integrieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident-Administrator (sn_si.admin)**

Benutzer mit dieser Rolle überwachen die Konfiguration der Integration mit dem Produkt SIR in Ihrer Instanz Now Platform.

**Security Incident-Analyst (sn_si.analyst)**

Benutzer mit dieser Rolle interagieren mit und analysieren Security Incidents im Produkt ServiceNow Security Incident Response.

### Richten Sie Ihre Now Platform® -Instanz für die Splunk Enterprise Security -Integration ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die Sie in Ihrer Instanz Now Platform® ausführen müssen, bevor Sie die Anwendung aus dem ServiceNow Storeinstallieren.

Erforderliche Rolle: admin.

Überprüfen Sie in der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

1. Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform® und Security Incident Response (SIR) zugewiesen haben.

   Die folgenden Rollen sind für die Installation, Einrichtung und Verwendung der -Integration in Ihrer Now Platform® -Instanz erforderlich.

   - Ein Benutzer mit der Administratorrolle Now Platform® (admin) installiert die Anwendung aus dem ServiceNow Store und weist die Rolle „Security Incident-Administrator“ (sn_si.admin) zu.
   - Wenn Sie für diese Integration wichtige Events manuell aus Splunk Enterprise Security weiterleiten möchten, weist ein Benutzer mit der Administratorrolle Now Platform® einem Benutzer mit der Rolle (sn_sec_splunkes.api_account_access) in Now Platform®zu. Diese Rolle ermöglicht einem Benutzer mit der Administratorrolle Splunk Enterprise Security den Zugriff auf die API in Now Platform®, die für die manuelle Event-Weiterleitung für diese Integration erforderlich ist.

     Die Rolle (sn_sec_splunkes.api_account_access) ist für die Integration nicht erforderlich, wenn Sie wichtige Ereignisse automatisch aus Splunk Enterprise Security in Ihre Instanz von [ Now Platform® erfassen.

   - Ein Benutzer mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in Now Platform®: Benennt
     - , erstellt und bearbeitet Event-Profile.
     - Wählt Werte aus Splunk Enterprise Security bis Now Platform® Security Incidents aus und ordnet sie zu.
     - Zeigt eine Vorschau der Details zu Security Incidents auf Richtigkeit an, bevor die Konfiguration abgeschlossen wird.
     - Plant die laufende Erfassung wichtiger Ereignisse.
     - Ermöglicht die Aktualisierung wichtiger Ereignisse, wenn ein SIR-Incident erstellt und geschlossen wird.
     - Weist die Rolle Security Incident Analyst (sn_si.analyst) zu.
     - Benutzer mit der Rolle sn_si.analyst arbeiten mit Security Incidents.

   Weitere Informationen finden Sie unter Managing roles .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Weisen Sie die Benutzerrolle Splunk zu.

   Weisen Sie in Splunk ES die Benutzerrolle „Sicherheitsanalyst“ (ess_analyst) zu, um alle integrationsbezogenen Aktivitäten auf dem Server Splunk ] auszuführen.

3. Vergewissern Sie sich, dass Sie Version 7.2.6 oder höher der Splunk -API verwenden. Frühere Versionen werden nicht unterstützt.

   Wenn Sie Zugriff auf die Konsole Splunk Enterprise Security haben, haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein weiteres spezielles Setup erforderlich.

4. Vergewissern Sie sich, dass Sie einen MID Server installiert und konfiguriert haben.

   Ein MID-Server in Ihrer Now Platform® -Instanz ist erforderlich, um eine Verbindung zum Splunk -Service herzustellen, wenn der Splunk -Server in Ihrem Unternehmensnetzwerk bereitgestellt wird. Weitere Informationen finden Sie unter MID Server .

   Wenn Sie den Cloud-Service [ Splunk Enterprise Security verwenden, ist MID-Server nicht erforderlich.

5. Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind.

   Das Plugin „ Security Incident Response Dependency“ (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung des Produkts Security Incident Response erforderlich sind. Installieren und aktivieren Sie dieses Plugin, bevor Sie die anderen für die Integration erforderlichen Security Operations -Anwendungen installieren und aktivieren.

   Vergewissern Sie sich, dass die folgenden Security Operations Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.

   a. Security Incident Response
   b. Security Integration Framework
   c. Sicherheitssupport Allgemein

   Weitere Informationen zur Installation der Kernanwendungen Security Operations finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab und Aktivieren Sie eine Anwendung ServiceNow Store ..

Sie haben Ihre Instanz Now Platform® erfolgreich für die Integration eingerichtet. Der nächste Schritt besteht darin, die Anwendung Splunk Enterprise Security Notable Event Ingestion aus dem ServiceNow Store für die -Integration zu installieren. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Security Notable Event Ingestion.

Wenn Sie wichtige Ereignisse manuell und bei Bedarf aus Ihrer Splunk Enterprise Security -Konsole für die Integration exportieren möchten, finden Sie weitere Informationen unter Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Integration von Splunk Enterprise Security Notable Event Ingestion ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Security Notable Event Ingestion

Führen Sie diese Installations- und Konfigurationsschritte aus, bevor Sie die Integration in Ihrer Instanz von Now Platform® ausführen, damit die Anwendung ordnungsgemäß in die Produkte Security Incident Response und Security Operations in Ihrer Instanz von Now Platform® integriert wird.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Wenn Sie die Anwendung Splunk Enterprise Security Event Ingestion nicht aus dem ServiceNow Store für die Integration installiert haben, lesen Sie Installieren Sie eine Security Operations -Integration, und führen Sie die Schritte zur Installation aus.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** , und suchen Sie die Kachel Splunk „ Event Ingestions“.
3. Um die Anwendung zu konfigurieren, klicken Sie auf **Neu**.

4. Wenn auf einer Kachel die Schaltfläche **Konfigurieren** angezeigt wird, klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im angezeigten Dialogfeld „Konfiguration der Event-Erfassung“ die Felder aus.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für die Konfiguration einer lokalen Version von Splunk Enterprise Security mit einem MID Server.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder Splunk Enterprise Security erkennbare Event-Typ, den Sie über Ihre Splunk Enterprise Security Incident-Überprüfungskonsole erfassen, erfordert ein eindeutiges Event-Profil in Ihrer Now Platform® -Instanz. Die Quelle, die Sie im Formular Event-Erfassungskonfiguration konfigurieren, kann jedoch für mehrere Now Platform® -Profile wiederverwendet werden, solange jedes Profil eindeutige wichtige Event-Typen erfasst.

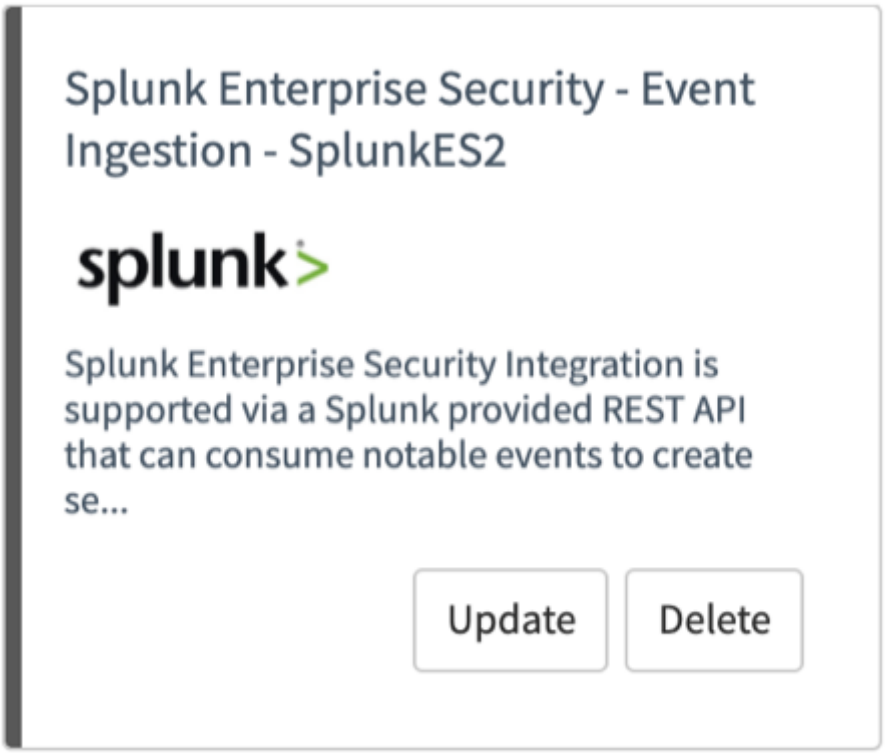
6. Klicken Sie auf **Absenden**.
   Nach erfolgreicher Validierung wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel werden die Schaltflächen **Aktualisieren** und **Löschen** angezeigt (siehe folgende Abbildung).

**Hinweis:**
Benutzer müssen entweder die Standardauthentifizierung oder die tokenbasierte Authentifizierung verwenden. Wenn Sie beides aktivieren, wird der folgende Fehler ausgegeben.

**Hinweis:**
Wenn Benutzer die vorhandenen Konfigurationskacheln auf Token-basierte aktualisieren möchten, müssen sie diese Einstellung aktivieren, um vorhandene Splunk Quellkonfigurationen für die Einstellung Token-basierte Authentifizierungsunterstützung im Modul Splunk Enterprise-Einstellungen zu aktualisieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Nach erfolgreicher Validierung und Übermittlung wird jede Serverkonfiguration für Event-Erfassungen Splunk auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, wählen Sie in der oberen rechten Ecke der Seite in der Liste Konfigurationen anzeigen die Option **Ja**aus.

### Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Event-Profil zu erstellen.

#### Konfigurieren Sie die Einstellungen für Splunk Enterprise Security

Verwenden Sie die Einstellungen für Splunk Enterprise Security (ES), um die voreingestellten Konfigurationen und ihre Werte gemäß Ihren Anforderungen zu ändern.

### Vorbereitungen
Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Splunk ES-Integration** > **Splunk ES-Einstellungen**.
2. Füllen Sie die Felder im Formular aus.

**Splunk ES-Einstellungen**

| Feld | Beschreibung |
|---|---|
| Erzwingen Sie eine Begrenzung der Anzahl der wichtigen Ereignisse, die zu einem einzelnen Incident zusammengefasst werden können. | Option, um ein Limit für die Anzahl der wichtigen Ereignisse zu erzwingen, die Sie zu einem einzelnen Incident zusammenfassen möchten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Standardmäßig ist der Wert auf 100 festgelegt. |
| Erzwingen Sie eine Begrenzung der Anzahl von Security Incidents, die innerhalb von 24 Stunden erstellt werden können. | Option zum Erzwingen einer Begrenzung der Anzahl von Security Incidents, die in einem Zeitraum von 24 Stunden erstellt werden können.<br><br>Standardmäßig ist der Wert auf 1000 festgelegt. |
| Erzwingen Sie eine Begrenzung der Anzahl der Werte, die in jedem von Splunkempfangenen Feld analysiert werden sollen. | Option, um ein Limit für die Anzahl der Werte zu erzwingen, die Sie für jedes von Splunkempfangene Feld analysieren möchten.<br><br>Standardmäßig ist der Wert auf 1000 festgelegt. |
| Anzahl der Korrelationsregeln, die aus Splunkabgerufen werden sollen. | Option zum Definieren der Anzahl der Korrelationsregeln, die aus Splunkabgerufen werden sollen.<br><br>Standardmäßig ist der Wert auf 500 festgelegt. |
| Der Parameter für die Gültigkeitsdauer für den Suchauftrag Splunk in Sekunden. | Option zum Definieren des Parameters „Lebensdauer“ für die Suche Splunk in Sekunden.<br><br>Standardmäßig ist der Wert auf 600 festgelegt. |
| Anzahl der wichtigen Typen, die in einer Suche zusammengefasst werden sollen. | Option zum Definieren der Gesamtzahl der wichtigen Typen, die in einer einzigen Suche als Batch angezeigt werden sollen.<br><br>Standardmäßig ist der Wert auf 20 festgelegt. |
| Anzahl der Tage, für die die Metadaten des Suchauftrags Splunk ] in ServiceNowaufbewahrt werden sollen | Option zum Definieren der Anzahl von Tagen, für die Sie die Metadaten des Splunk-Suchauftrags in ServiceNowaufbewahren möchten.<br><br>Standardmäßig ist der Wert auf 30 festgelegt. |
| Das Trennzeichen zum Aufteilen der Werte in Feldzuordnungen. | Option zum Definieren des Trennzeichens zum Aufteilen der Werte in Feldzuordnungen.<br><br>Standardmäßig ist der Wert auf (,) festgelegt. |
| Anzahl der Überlappungsminuten, die beim Abrufen der Ereignisse aus Splunk hinzugefügt werden sollen (um die Indizierungsverzögerung von Splunk zu überwinden) | Option zum Definieren der Anzahl der Überlappungsminuten, die beim Abrufen der Events aus Splunk [] hinzugefügt werden sollen, um die Indizierungsverzögerung von Splunkzu überwinden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Standardmäßig ist der Wert auf 30 festgelegt. |
| Rufen Sie aktualisierte wichtige Ereignisse ab | Option zum Abrufen aktualisierter wichtiger Ereignisse.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |
| Aktivieren Sie diese Einstellung, um vorhandene Splunk Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung zu aktualisieren. Sie müssen die Integrationskonfiguration mit Tokendetails aktualisieren, nachdem diese Einstellung aktiviert wurde. | Option zum Aktualisieren der vorhandenen Splunk -Quellkonfiguration auf die Unterstützung der tokenbasierten Authentifizierung von einer vorhandenen Version.<br><br>**Hinweis:**<br>Nach dem Upgrade auf die neue Version ist das Tokenfeld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung zu erhalten. Anschließend müssen Sie die Integrationskonfiguration mit Tokendetails aktualisieren.<br><br>Standardmäßig ist der Wert auf Nein festgelegt. |

3. Klicken Sie auf **Speichern**.

### Authentifizierungsfehler

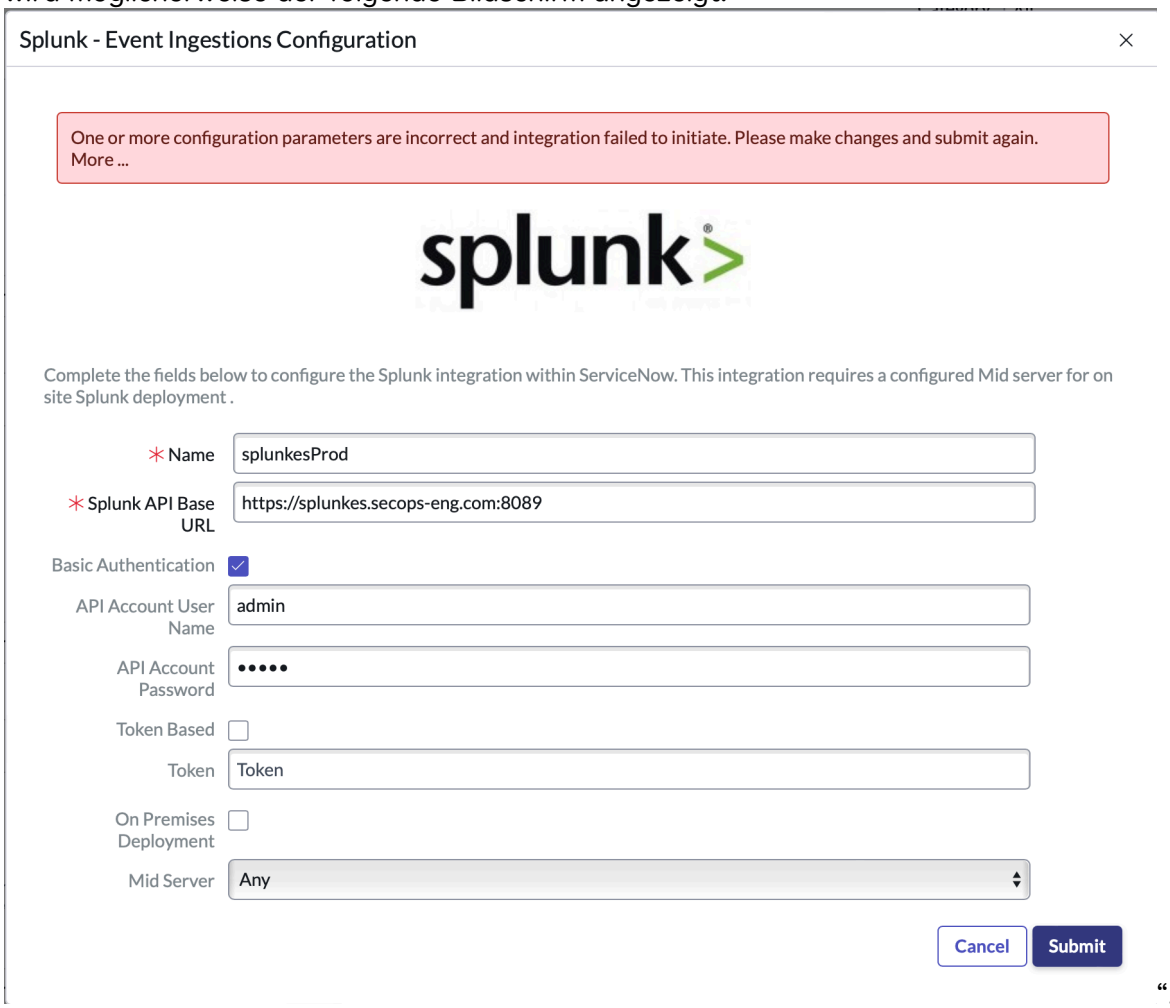
In diesem Abschnitt werden einige häufige Authentifizierungsfehler und ihre Behebung beschrieben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Problem bei der Zertifikatvalidierung

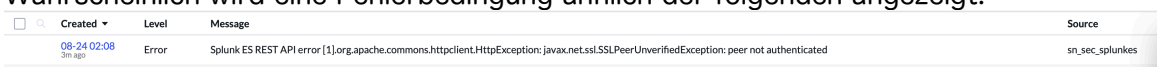
Wenn während der Authentifizierung ein Fehler auftritt, wird möglicherweise der folgende Bildschirm angezeigt:




“.

Wenn Sie überprüft haben, dass Ihre API-Kontoanmeldeinformationen und die Splunk-Basis-URL-Informationen korrekt sind, kann dieser Fehler auf ein Problem mit dem Splunk-Zertifikat für die Kommunikation über Port 8089 zurückzuführen sein. Die Instanz ServiceNow® erfordert ein gültiges Zertifikat mit einem allgemeinen Namen, der dem Hostnamen des Servers entspricht, um sichere Verbindungen herzustellen. Weitere Informationen finden Sie unter Zertifikate. Wenn dieser Fehler angezeigt wird, können Sie anhand der Systemprotokolle überprüfen, ob das Problem auf ein Zertifikatproblem zurückzuführen ist.

Wahrscheinlich wird eine Fehlerbedingung ähnlich der folgenden angezeigt:




Um mit der Authentifizierung fortzufahren, müssen Sie das Splunk-Standardzertifikat ersetzen, das für den API-Zugriff an Port 8089 bereitgestellt wird. Ausführliche Anweisungen zum Ersetzen des SSL-Zertifikats finden Sie unter KB0778285.

### Erstellen und benennen Sie ein Event-Profil für die Splunk Enterprise Security Event Ingestion-Integration

Sie erstellen ein Event-Profil in Ihrer Instanz Now Platform und bestimmen, welche wichtigen Splunk -Ereignisse Security Incidents verursachen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Bevor Now Platform Security Incident Response (SIR) Security Incidents aus erfassten wichtigen Events erstellt werden, werden die Feldwerte aus Warnungen in einem Layout eines Now Platform Security Incident angezeigt, sodass Sie eine Vorschau des tatsächlichen Security Incident anzeigen können.

Aus Perspektive der Integration mit den verfügbaren APIs werden Splunk ES wichtige Ereignisse einzeln und manuell als diskrete wichtige Ereignisse weitergeleitet, oder sie werden abhängig vom definierten Profiltyp automatisch in der Security Operations -Umgebung Ihrer Now Platform -Instanz erfasst.

Die Integrations-Workflows erfassen verschiedene Arten von wichtigen Ereignissen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese wichtigen Events werden basierend auf den Profilen erfasst, die Sie in der Security Operations -Umgebung Ihrer Instanz konfigurieren.

Alle wichtigen Elemente werden anfänglich für einen konfigurierten Korrelationssuchtyp in einem Profil erfasst. Erfasste wichtige Elemente können dann weiter gefiltert werden, um anzugeben, welche wichtigen Elemente Security Incidents erstellen. Beispielsweise könnten Sie Filter bevorzugen, die Security Incidents nur für wichtige Ereignisse erstellen, die als hohes Risiko identifiziert wurden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten wichtigen Ereignissen erstellt, werden einzelne Feldwerte in den wichtigen Ereignissen den entsprechenden Feldern in einem Layout des Security Incident für eine Vorschau zugeordnet.

### Prozedur

1. Namen für die Event-Profile in Ihrer Instanz Now Platform müssen eindeutig sein und können jeweils nur einem aktiven Event-Profil zugeordnet werden.
2. Now Platform erfasst bestimmte wichtige Elemente mithilfe der Workflows der Integration.
   Alle wichtigen Events, die die Auswahlkriterien in Ihrer Splunk ES -Konsole erfüllen, werden anfänglich in Ihrer Now Platform -Instanz erfasst.
3. Ein Profil in Now Platform ist eine Einkapselung eines wichtigen Ereignisses in Ihrer Splunk ES -Konsole. Es besteht eine Eins-zu-eins-Beziehung zwischen mit einem Profil erfassten wichtigen Ereignissen und Verbindungen zu Ihrer Splunk ES -Konsole: ein erkennbarer Ereignistyp für eine Verbindung.
4. Informationen zum Erstellen von Profilen für geplante wichtige Ereignisse finden Sie unter Richten Sie ein Profil für die geplante Erfassung wichtiger Ereignisse ein.
5. Informationen zum Erstellen von Profilen für die manuelle Event-Weiterleitung finden Sie unter Richten Sie ein Profil für die manuelle Event-Weiterleitung ein.

#### Richten Sie ein Profil für die geplante Erfassung wichtiger Ereignisse ein

Abhängig vom definierten Profil werden Splunk ES wichtige Ereignisse automatisch in der Security Operations -Umgebung Ihrer Now Platform -Instanz erfasst.

Die folgende Tabelle zeigt die Liste der Aufgaben, die Sie ausführen müssen, um ein Profil für die geplante Erfassung wichtiger Ereignisse einzurichten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Schritte zum Einrichten eines Profils für die geplante Erfassung wichtiger Ereignisse**

| Aufgabe | Abschnitt |
|---|---|
| Erstellen Sie ein Event-Profil | Siehe Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse |
| Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationssuche aus | Siehe Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für die Integration von Splunk ES Event Ingestion aus |
| Ordnen Sie Felder für wichtige Ereignisse zu | Siehe Zuordnung wichtiger Event-Felder für die Splunk Enterprise Security -Integration |
| Erstellen Sie benutzerdefinierte Zuordnungen | Siehe Zuordnungen für Splunk ES Incident-Überprüfung für wichtiges Event und beitragende Event-Details erstellen (geplante Erfassung) |
| Zeigen Sie eine Vorschau des Security Incident an | Siehe Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an |
| Planen Sie neue und aktualisierte wichtige Ereignisse, und rufen Sie sie ab | Siehe Planen und rufen Sie neue und aktualisierte wichtige Events für die Splunk Enterprise Security Event Ingestion-Integration ab |
| Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status | Siehe Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status |

## Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse

Sie können ein Profil so einrichten, dass wichtige Ereignisse automatisch erfasst werden.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

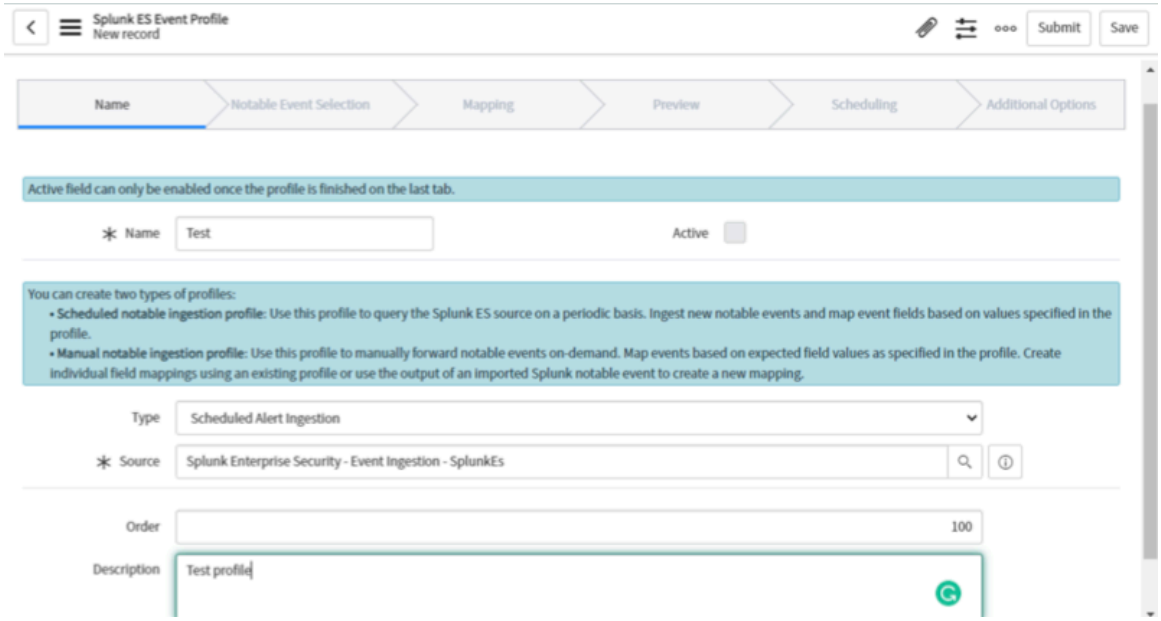
1. Um ein Event-Profil für ein wichtiges Event oder einen Korrelationsregeltyp in Ihrer Now Platform -Instanz zu erstellen, navigieren Sie zu **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wenn das Formular Splunk Event-Profil nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Name**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für einen geplanten wichtigen Ereignistyp.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Wählen Sie für ein Profil mit einem geplanten wichtigen Ereignis eine Option aus, um mit der Profilkonfiguration fortzufahren.

### Nächste Maßnahme

Der nächste Schritt besteht darin, wichtige Ereignisse für die automatische Erfassung auszuwählen.

## Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für die Integration von Splunk ES Event Ingestion aus

Nachdem Sie ein Profil für die geplante Erfassung eines erkennbaren Ereignistyps erstellt haben, wählen Sie den Namen einer Splunk Enterprise Security -Korrelationsregel für dieses Profil aus, für das Sie die entsprechenden erkennbaren Ereignisse einem Now Platform Security Incident Response -Security Incident zuordnen möchten.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelationsregeln in Ihrer Now Platform -Instanz an, damit Sie wissen, für welche wichtigen Event-Typen Sie Security Incidents erfassen und erstellen möchten. Wählen Sie eine Korrelationsregel aus. Sie können ein oder mehrere wichtige Ereignisse aus der Liste in diesem Formular auswählen.

### Prozedur

1. Wenn die Seite „Auswahl für wichtiges Ereignis“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
2. Wählen Sie in der Liste „Korrelationsregel“ eine der folgenden Optionen aus, um eine einzelne Korrelationsregel oder mehrere Korrelationsregeln auszuwählen, sie zu verschieben und sie aus der Spalte Verfügbar in die Spalte Ausgewählt zu verschieben.

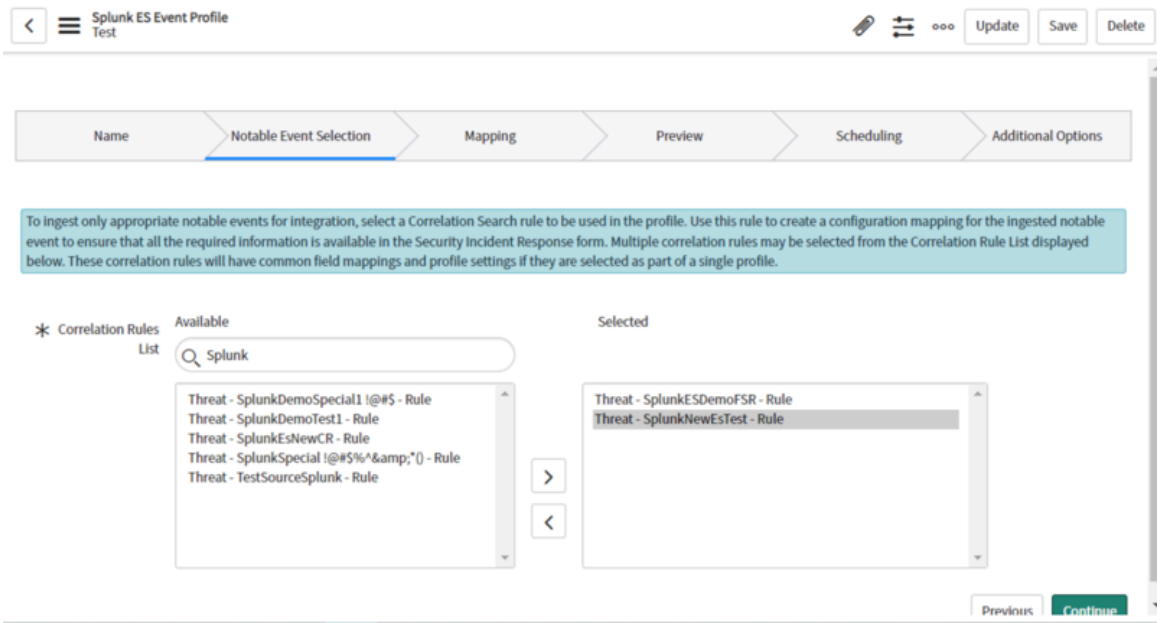
   Die Liste der Korrelationsregeln in diesem Formular stimmt mit der Liste der Korrelationsregeln in Ihrer Splunk ES Incident Review-Konsole überein. In diesem Formular werden bis zu 500 Korrelationsregeln angezeigt. Wenn in Splunk ESmehr als 500



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln aufgeführt sind, werden nur die ersten 500 wichtigen Ereignisse in diesem Formular in Ihrer Instanz Now Platform angezeigt.

| Option | Beschreibung |
|---|---|
| Geben Sie im Suchfeld Korrelationsregelliste Text ein. | Die Spalte unter dem Suchfeld wird basierend auf dem von Ihnen eingegebenen Text mit verfügbaren Optionen gefiltert. Wählen Sie eine Korrelationsregel aus, und verschieben Sie den ausgewählten Alarm mit den Pfeiltasten von **Verfügbar** zu **Ausgewählt**. |
| Doppelklicken Sie in der Liste der Korrelationsregeln auf eine Korrelationsregel. | Die Spalte **Ausgewählt** wird mit Ihrer Auswahl ausgefüllt. |
| Klicken Sie in der Liste der Korrelationsregeln einmal auf eine Korrelationsregel. | Die Korrelationsregel ist ausgewählt. Verschieben Sie die ausgewählte Korrelationsregel mit den Pfeiltasten von **Verfügbar** zu **Ausgewählt**. |




**3.** Wählen Sie eine Option aus, um fortzufahren.

## Nächste Maßnahme

Sie haben erfolgreich eine Korrelationsregel für ein geplantes Splunk Enterprise Security Profil ausgewählt. Der nächste Schritt besteht darin, wichtige Event-Werte den Feldern in einem Security Incident zuzuordnen.

### Zuordnung wichtiger Event-Felder für die Splunk Enterprise Security -Integration

Nachdem Sie die spezifische Korrelationsregel und den Typ des erkennbaren Ereignisses für das Profil identifiziert haben, besteht der nächste Schritt darin, einzelne Felder für erkennbare Ereignisse den Feldern in einem Now Platform Security Incident Response (SIR) Security Incident zuzuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

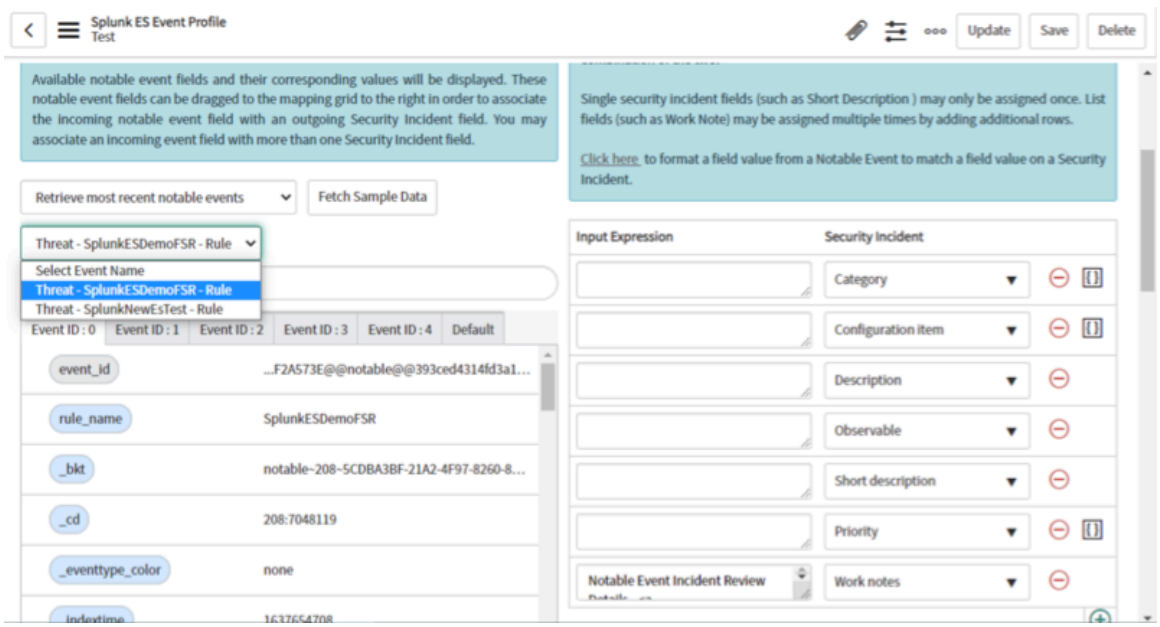
## Übersicht

Für den Zuordnungsschritt können Sie Beispiele für wichtige Ereignisse für die ausgewählte Korrelationsregel erfassen oder Daten für wichtige Ereignisse für manuell weitergeleitete wichtige Ereignisse exportieren. Der Event-Zuordnungsprozess ist unabhängig vom Profiltyp, den Sie erstellen, identisch.

Die folgenden Abbildungen sind Beispiele für die Standardzuordnungskonfigurationen, die für jeden Typ von Event-Profil bereitgestellt werden. Sie können die Felder anpassen, die den Security Incident ausfüllen. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten Felddaten für wichtige Ereignisse der entsprechenden Stelle im SIR-Incident-Formular zugeordnet werden, und dann den SIR-Incident im Vorschaubereich visualisieren.

Wenn mehrere Korrelationen verwendet werden, können wichtige Ereignisse abgerufen werden, indem das erforderliche Ereignis ausgewählt wird. Verwenden Sie den **Warnungsnamen**, um eine Warnung auszuwählen, wenn Sie mehrere Warnungen für die Erfassung konfiguriert haben.

Nachdem Sie auf geklickt haben, um Daten abzurufen, werden die Feldnamen für wichtige Ereignisse Splunk und die entsprechenden Werte auf der linken Seite des Formulars ausgefüllt. Dies sind die Splunk Felder für erkennbare Ereignisse, die den SIR Security Incident-Feldern zugeordnet werden können. Einige Felder können mehrmals den SIR-Security Incident-Feldern zugeordnet werden.




Möglicherweise ziehen Sie es vor, einige Beispiele für wichtige Ereignisse in Ihrer Splunk -Konsole zu überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird in der Fortschrittsleiste als Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**. Sie können bis zu fünf Beispiele für wichtige Ereignisse aus Splunk Enterprise Security erfassen, um den Prozess der Feldzuordnung für wichtige Ereignisse zu unterstützen. Es gibt Optionen, um entweder die fünf letzten nennenswerten Ereignisse für die ausgewählte Korrelationsregel zu erfassen oder bis zu fünf bestimmte wichtige Ereignisse basierend auf den IDs der erkennbaren Ereignisse zu erfassen.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen wichtiger Ereignisse erforderlich sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geplante Beispieldatenerfassung für Notable-Event: Für Beispieldaten, die für automatisch erfasste Profile für Notable-Events verwendet werden, werden verfügbare Notable-Event-Felder und ihre entsprechenden Werte in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt, sobald die Beispieldaten abgerufen wurden. Registerkarten werden angezeigt, um die Werte für eine bestimmte ID eines wichtigen Ereignisses anzuzeigen, die Sie abgerufen haben. Vergewissern Sie sich, dass alle kritischen Felder aus dem Abschnitt „Erfassung von Beispielen für wichtige Ereignisse“ auf der linken Seite des Formulars den Security Incident-Feldern ServiceNow auf der rechten Seite des Formulars zugeordnet sind.
- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Felder für wichtige Ereignisse von der linken Seite ziehen und sie im Abschnitt ServiceNow SIR-Incident-Zuordnung auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das eingehende Feld für ein wichtiges Ereignis einem ausgehenden Security Incident-Feld zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder mithilfe des Symbols + am unteren Rand des Abschnitts „SIR-Incident-Feldzuordnung“ hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder mit der angegebenen Farbcodierung nach (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um anzugeben, welche wichtigen Ereignisse Security Incidents erstellen sollen und welche wichtigen Ereignisse herausgefiltert werden sollen, z. B. wichtige Ereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Bedingungen für Incident-Generierung“, der sich unter dem Abschnitt „Zuordnung für wichtige Ereignisse“ befindet.
- Event-Zusammenfassungskriterien: Definieren Sie zusätzliche Event-Zusammenfassungskriterien, die ein eingehendes wichtiges Event zu einem vorhandenen SIR Security Incident zusammenfassen, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Durch die Verwendung von Wertkriterien für den Feldabgleich für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Daten zu wichtigen Sicherheitsereignissen in einem einzigen Security Incident platziert werden.
- Formatfeldübersetzung: In bestimmten Fällen werden Event-Feldwerte in den Splunk wichtigen Enterprise-Events möglicherweise nicht direkt in die Felder im Security Incident SIR übersetzt. Für diese Werte können Sie einen Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Zum Beispiel kann mit dem Skript-Editor ein Kategoriewert von Malware-Warnung und Virusinfection unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können mit in eine gemeinsame böswillige Codeaktivität im Feld Kategorie des Security Incident SIR übersetzt werden Funktion „Formatfeldübersetzung“.

Der nächste Schritt besteht darin, wichtige Ereignisse zu erfassen und Werte den Security Incident-Feldern SIR zuzuordnen.

### Zuordnungen für Splunk ES Incident-Überprüfung für wichtiges Event und beitragende Event-Details erstellen (geplante Erfassung)

Während des Schritts der Feldzuordnung für ein wichtiges Event ordnen Sie einzelne Event-Felder aus „Bemerkbare Events“ Feldern in einem Now Platform Security Incident Response (SIR) Security Incident zu.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Das Zuordnungsraster kann für den in der Auswahl der Korrelationsregel ausgewählten Typ eines wichtigen Ereignisses angepasst werden. Die Farbcodierung der Event-Felder hilft Ihnen, die Event-Werte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Event-Informationen nicht zugeordnet wurden.

Ordnen Sie bis zu fünf wichtige Events aus der Spalte „Beispiel für wichtiges Ereignis“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardfelder, die in der Regel wichtige Felder sind, die im Security Incident Response-Formular ausgefüllt werden müssen, werden angezeigt. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mithilfe der Schaltflächen + und - angezeigt werden. Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk Felder zuordnen, die nicht im Standardzuordnungsraster des Security Incident SIR angezeigt werden.

### Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Klicken Sie für ein Profil mit einer geplanten Erfassung unter „Erfassung von Beispielen für wichtige Ereignisse“ auf Beispieldaten **abrufen**, um die neuesten Beispieldaten für wichtige Ereignisse für die ausgewählte Korrelationsregel aus der Konsole Splunk Enterprise abzurufen.

   **Hinweis:**
   Sie können entweder die neuesten Beispiele für wichtige Ereignisse abrufen oder die eindeutigen IDs für wichtige Ereignisse für die spezifischen wichtigen Ereignisse angeben, die Sie für die Zuordnung von wichtigen Ereignissen verwenden möchten.

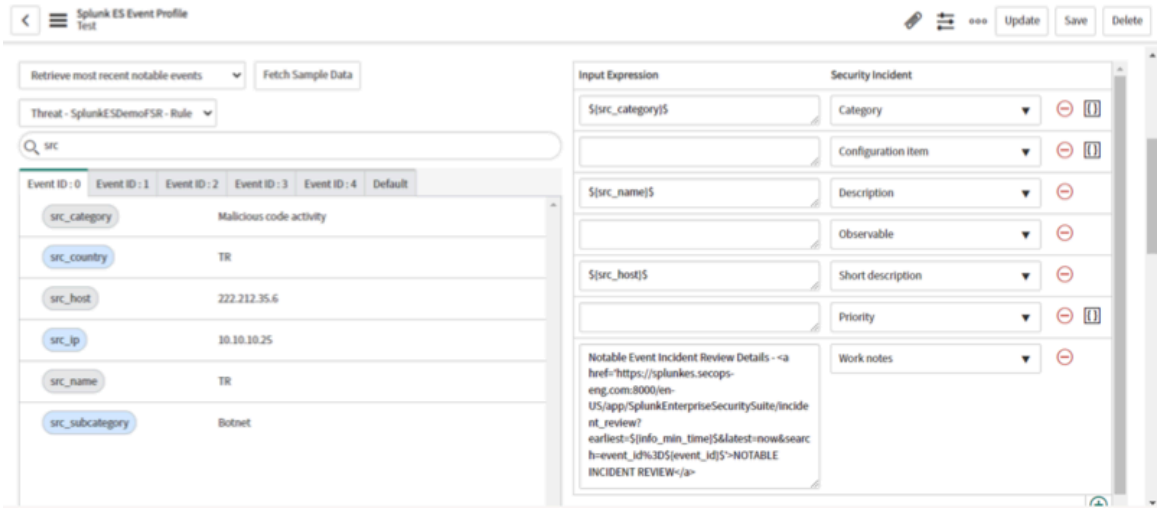
   Die Ergebnisse der Felder und Werte für wichtige Ereignisse werden als einzelne Registerkarten angezeigt. Sie können bis zu fünf wichtige Ereignisse erfassen.

   Der Abruf für beispielhafte wichtige Ereignisse kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

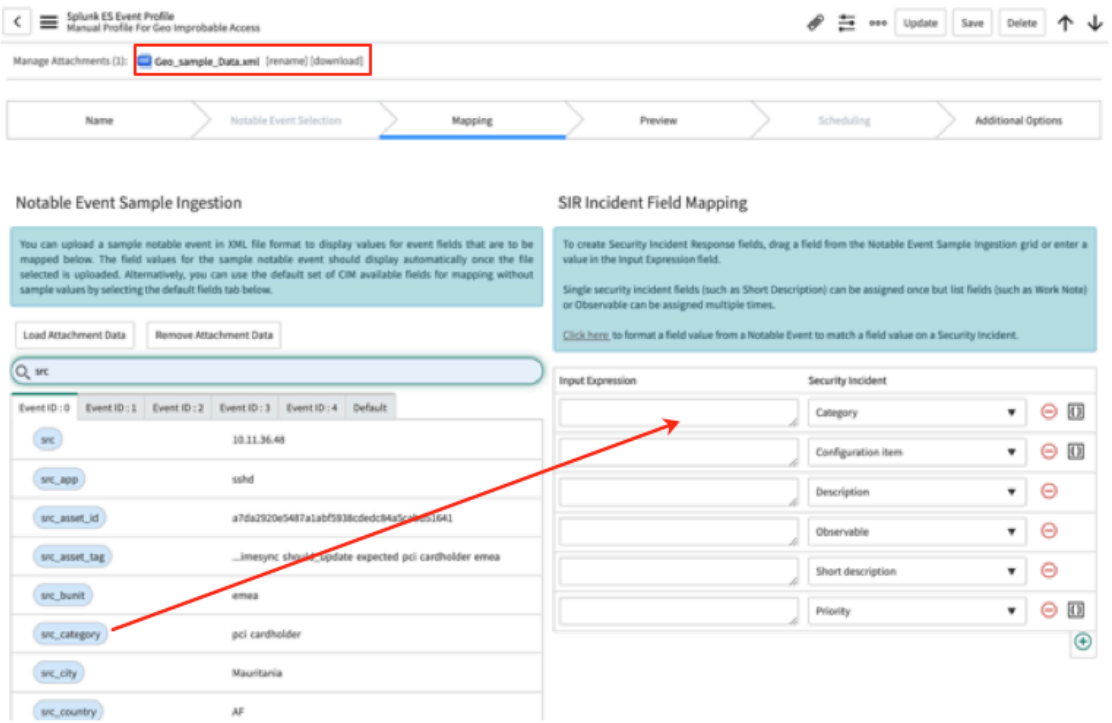
   In der folgenden Abbildung werden die Feldname-Wert-Paare für das erfasste wichtige Event oder die importierten Beispiel-Events auf der linken Seite dieses Formulars angezeigt, nachdem der Erfassungsabruf abgeschlossen ist. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken und halten Sie einen blauen Feldnamen auf der linken Seite des Formulars.
4. Ziehen Sie den Feldnamen, z. B. src_category, in ein Feld in der Spalte Eingabeausdruck neben einem Feldnamen in der Spalte Security Incident.




Der Feldwert wird in der Spalte Eingabeausdruck angezeigt. In der folgenden Abbildung wird src_category dem Kategoriefeld im Security Incident zugeordnet. Sie können jedoch jeden Wert auf der linken Seite mit einem Feld auf der rechten Seite abgleichen. Vergewissern Sie sich, dass der Wert während des Vorschauschritts dem Security Incident korrekt zugeordnet wurde.

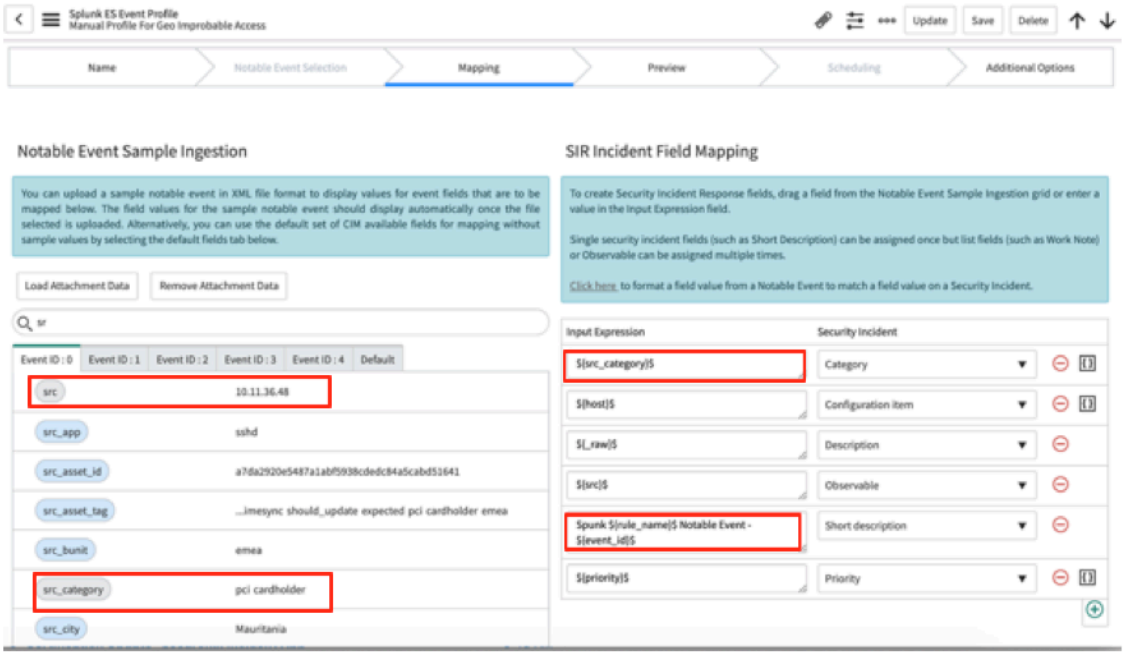
Um sicherzustellen, dass keine Event-Felder im Zuordnungsprozess übersehen oder dupliziert werden, sind die Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Feld für ein wichtiges Event ausgewählt und dem Security Incident



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugeordnet wurde. Möglicherweise möchten Sie ein eingehendes wichtiges Feld mit mehr als einem Feld in einem Security Incident verknüpfen.

Ein graues Feld zeigt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.




5. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

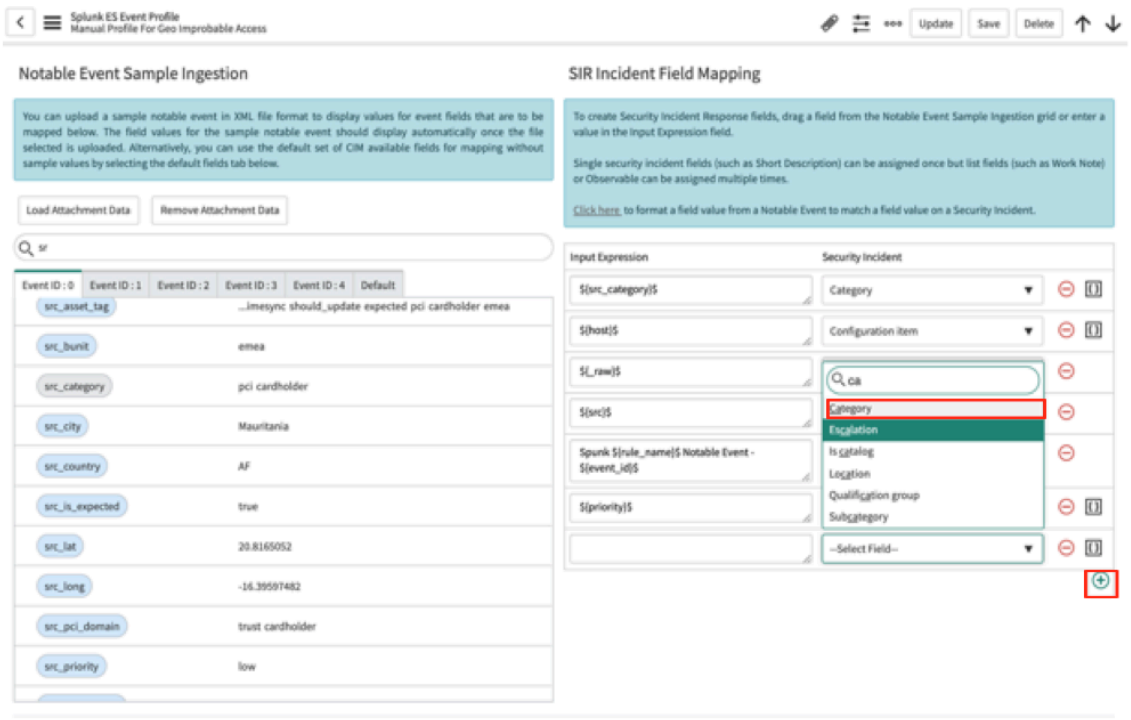
   a. Klicken Sie rechts im Formular im Abschnitt „SIR-Incident-Feldzuordnung“ am unteren Rand des Rasters auf das Plus-Symbol.
   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

   In der erweiterten Liste für das neue Feld sind einige Felder schattiert dargestellt. In der folgenden Abbildung hat die Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Felder für wichtige Ereignisse auf der linken Seite des Formulars hilft Ihnen diese Farbcodierung für die Security Incident-Felder auf der rechten Seite, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „Erkennbares Element“ mehrmals mit unterschiedlichen Werten zugeordnet werden. Ebenso unterstützen die Felder Konfigurationselement und Arbeitsnotizen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident eine Liste enthält, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

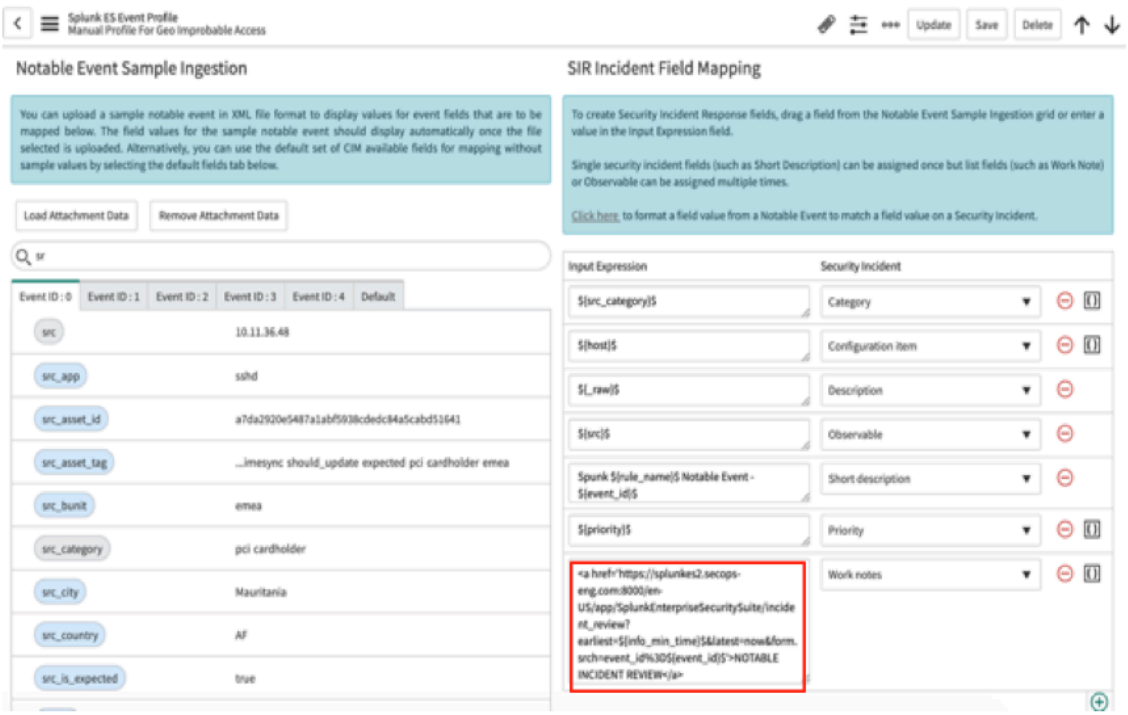
**c.** Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

**d.** Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um die **Event-ID** auszuwählen, die Sie im Feld Eingabeausdruck auswählen möchten.

**6.** Setzen Sie die Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder daraus entfernen.
Die folgende Abbildung zeigt ein Beispiel für eine bearbeitete Zuordnung. Im unteren Feld auf der rechten Seite wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Beachten Sie, dass Sie für das Feld mit langer Textzeichenfolge das Zuordnungsfeld erweitern können, um die vollständige Zeichenfolge anzuzeigen, und die Größe nach Bedarf ändern, indem Sie an der rechten unteren Ecke des Felds ziehen, wie im Screenshot unten mit dem hinzugefügten Feld „Arbeitsnotizen“ dargestellt:



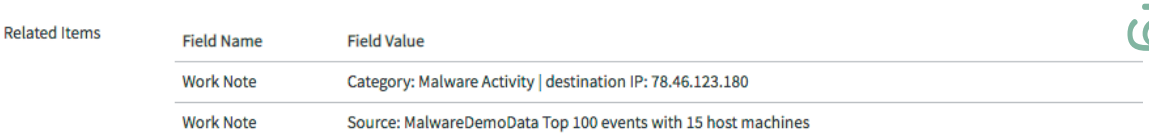
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Warnung:**
Bitte beachten Sie, dass im Abschnitt „ **SIR-Incident-Feldzuordnung** “ die im Feld „ **Eingabeausdruck** “ erwähnte URL und Portnummer nur ein Beispiel und nicht die vordefinierte URL oder Portnummer ist.

In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Zuordnungsabschnitt hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die Leerzeichen und Satzzeichen, die Sie in das Feld eingegeben haben, im Abschnitt „Zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

Die folgende Abbildung zeigt ein Beispiel dafür, wie die Werte in der vorherigen Abbildung im Security Incident angezeigt werden.




7. **Wahlweise:** Öffnen Sie den Skript-Editor, und setzen Sie die Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor, um Warnungswerte für die Splunk Enterprise Event Ingestion -Integration zu formatieren.

Einschließlich Hyperlinks für die Überprüfung wichtiger Event-Incidents und beitragende Events

Zusätzlich zu den Zuordnungsfeldern kann `sn_si.admin` einen Zeichenfolgenwert zuordnen, der es dem Sicherheitsanalysten, der an einem Incident arbeitet, ermöglicht, per Hyperlink sowohl zum wichtigen Event „Incident-Überprüfung“ in der Konsole Splunk



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enterprise Security als auch zu den zugrunde liegenden beitragenden Events, die Teil sind, zurückzukehren der Drilldown-Suche.

Die folgenden Zeichenfolgenwerte enthalten den Servernamen Splunk Enterprise Security und die entsprechenden Variablen, die für Hyperlinks zu diesen Details verwendet werden können:

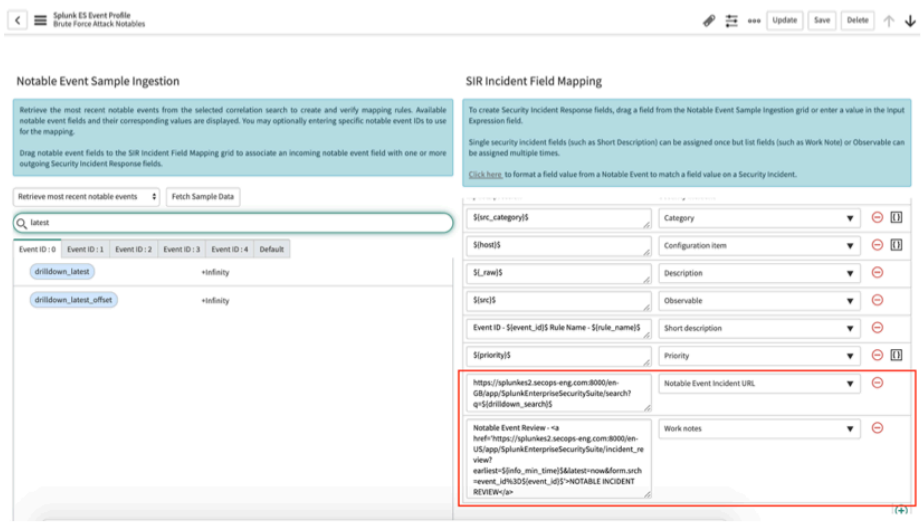
- **Hyperlink zur Überprüfung von Incidents für wichtige Ereignisse**: https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id} $

  wobei splunkes2.secops-eng.com:8000 die Splunk-Serverquelle ist und info_min_time und event_id Event-Feldwerte sind, die aus den wichtigen Events extrahiert wurden.

- **Bemerkenswerte Beitragsereignisse (Drilldown-Suche) Hyperlink**: https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$

  wobei splunkes2.secops-eng.com:8000 die Splunk-Serverquelle ist und Drilldown_search ein Event-Feldwert ist, der aus den wichtigen Events extrahiert wird.

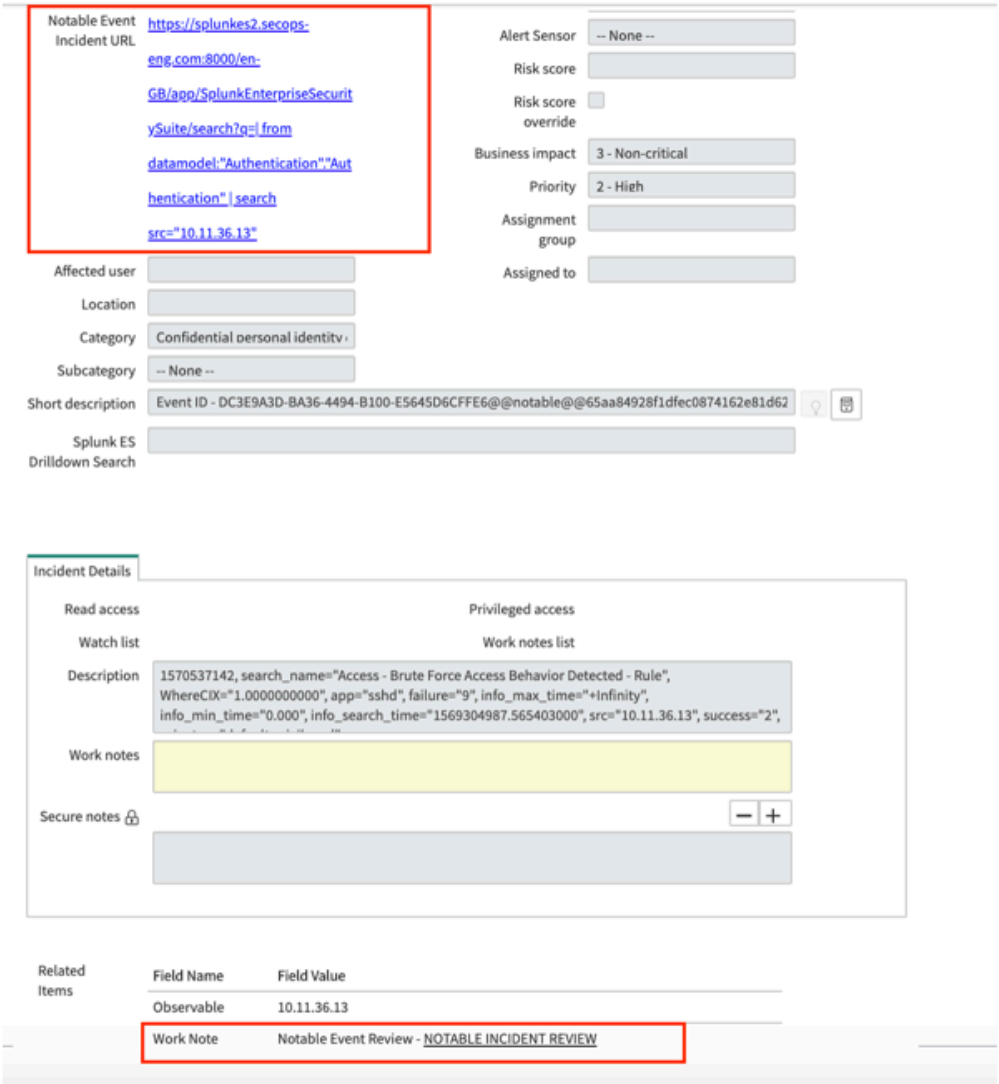
Die folgende Abbildung zeigt die URL zur Überprüfung von Notable Event Incidents, die dem Arbeitsnotizfeld zugeordnet ist, und den Hyperlink Notable Event Contributing Events (Drilldown-Suche), der einem benutzerdefinierten Feld mit der Bezeichnung Notable Event Incident URL zugeordnet ist:




Die folgende Abbildung zeigt die SIR-Incident-Vorschau mit dem Hyperlink „Überprüfung von Notable Event Incident“ und der URL für beitragende Ereignisse: Hyperlink für



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Filterbedingungen für die Incident-Generierung

8. **Wahlweise:** Nachdem Sie die vorherigen Schritte der Feldzuordnung abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Bedingungen für die Incident-Generierung verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes wichtiges Event erfüllen muss, um einen SIR Security Incident zu erstellen.
   Führen Sie die folgenden Schritte aus, um Bedingungen für die Incident-Generierung festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt „Bedingungen für Incident-Generierung“, und aktivieren Sie das Kontrollkästchen **Basierend auf Bedingungen** filtern, um die Option zu aktivieren.

      (Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den in den Feldern beschriebenen spezifischen Bedingungen entsprechen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

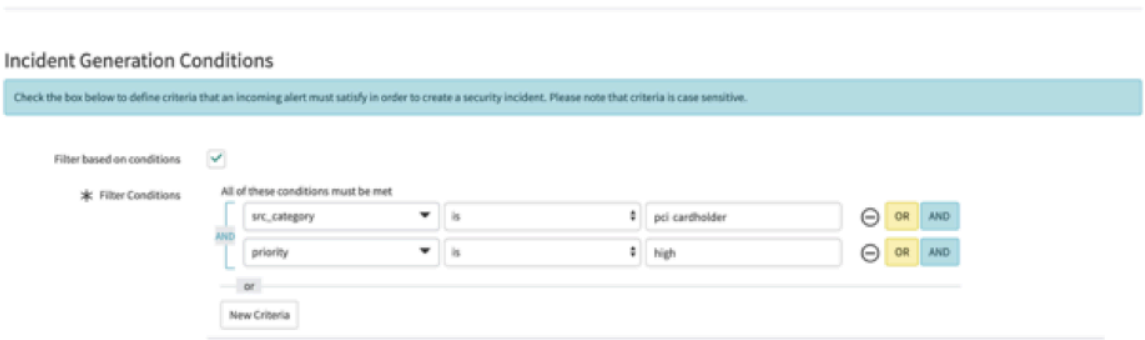
Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt Notable Event Sample Ingestion (Beispiel für wichtiges Event) für die von Ihnen erfassten Events angezeigt werden. Diese Felder sind dynamisch und ändern sich in Abhängigkeit von den Splunk bemerkbaren Events, die Sie erfassen, oder dem Event, das Sie für die manuell weitergeleiteten Beispiele für bedeutsame Events auswählen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen genau mit den Werten des wichtigen Ereignisses Splunk Enterprise Security übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu Ihrer Splunk Enterprise Security -Konsole zurück und überprüfen Ihre wichtigen Ereignisse auf die Stichwörter.

**b.** Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

**c.** Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** oder **ODER**. Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.

**d.** **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt sein müssen, bevor Security Incidents erstellt werden.




(Optional) Sie haben die Generierungsbedingungen für Incidents so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Filterung der Incident-Generierungsbedingung hilft Ihnen, die Sicherheits-Events einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche oder die Filter in



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunkzu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden Incidents nur nennenswerte Ereignisse zugeordnet, die allen Kriterien entsprechen.

**Hinweis:**
Wenn einer der Event-Feldnamen Sonderzeichen enthält, z. B. Anführungszeichen (“), Bindestriche ('), Unterstriche (-), (@) oder kaufmännische Und-Zeichen (&), müssen diese Zeichen möglicherweise für Zuordnungsübersetzungszwecke ersetzt werden und möglicherweise einen doppelten Ereignisnamen erstellen. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Event-Namen zu unterscheiden. Beispiel: Wenn das erste Event-Feld alerts.alert und das zweite Event-Feld alerts @alerts ist, können diese Felder nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Event-Feld ein Suffix hinzugefügt, und das Feld wird in alerts@alert(1)umbenannt.

(Optional) Event-Zusammenfassungskriterien zur Behandlung ähnlicher wichtiger Elemente und zur Verhinderung doppelter Incidents

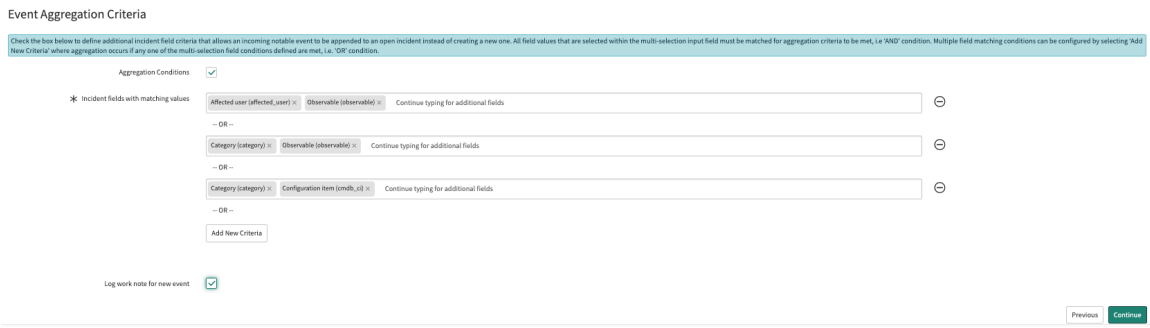
9. **Wahlweise:** Um die Erstellung doppelter Security Incidents zu vermeiden, definieren Sie zusätzliche Event-Zusammenfassungskriterien, sodass eingehende wichtige Events zu einem offenen Security Incident zusammengefasst werden.
Führen Sie die folgenden Schritte aus, um die Kriterien festzulegen.

   a. Scrollen Sie im Formular zum Abschnitt Event-Zusammenfassungskriterien, und aktivieren Sie das Kontrollkästchen **Bedingungen** zusammenfassen, um diese Option zu aktivieren.

   (Optional) Die Incident-Felder mit übereinstimmenden Werten werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle benutzerdefinierten Felder enthalten, die im Security Incident SIR konfiguriert wurden.

   b. Wählen Sie im Eingabefeld mit Mehrfachauswahl die Feldwerte aus, die Sie mit vorhandenen Security Incidents in Ihrem Now Platformabgleichen möchten.

   c. Verwenden **Sie Neue Kriterien hinzufügen**, um mehrere Feldabgleichbedingungen auszuwählen. Alle Feldwerte, die Sie im Mehrfachauswahl-Eingabefeld auswählen, werden anhand der UND-Bedingung mit Zusammenfassungskriterien abgeglichen. Klicken Sie auf **Neue Kriterien hinzufügen**, um mehrere Feldabgleichbedingungen auszuwählen, bei denen eine Zusammenfassung erfolgt, wenn eine der mehrfach ausgewählten Feldbedingungen, die definiert sind, mit der ODER-Bedingung erfüllt wird.

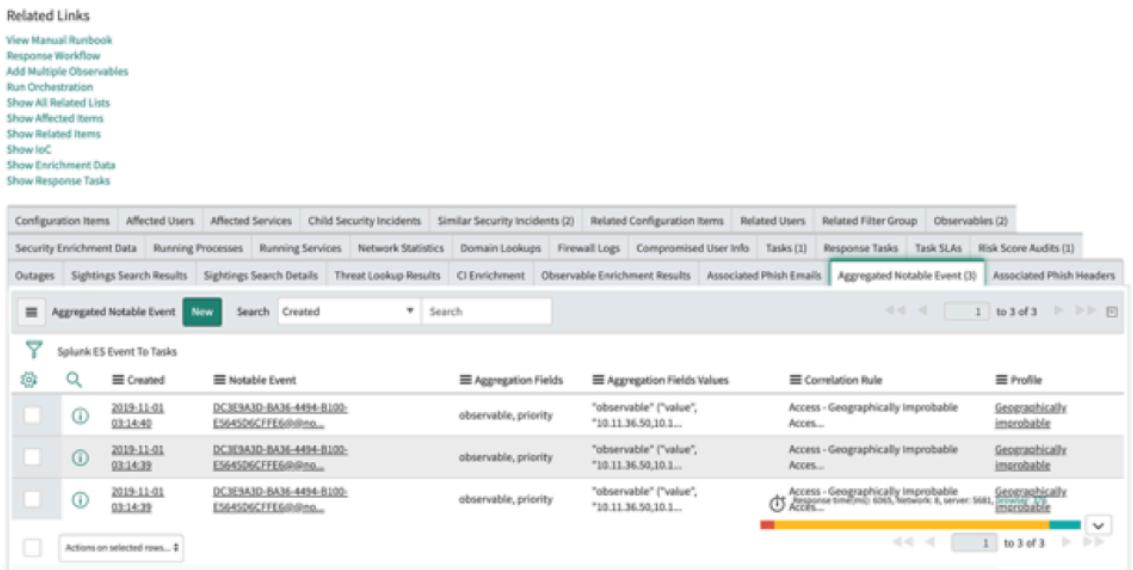



Wenn ein neues wichtiges Ereignis mit allen Werten übereinstimmt, die in den Zusammenfassungsfeldbedingungen im Zuordnungsschritt ausgewählt sind, wird das neue wichtige Ereignis automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.analyst, der an Security Incidents arbeitet, können Sie alle hinzugefügten zusammengefassten wichtigen Ereignisse in einer zugehörigen Liste zu einem Security Incident anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle zusammengefassten wichtigen Ereignisse für einen Security Incident werden in der zugehörigen Liste Splunk Event zu Aufgaben angezeigt. Diese Liste enthält die zugehörigen Zeitstempel und zusammengefassten Feldwerte. Diese Informationen helfen Ihnen zu verstehen, warum diese wichtigen Ereignisse zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie zur linken Seite des Datensatzes unter Zugehörige Links, und klicken Sie auf den Link **Alle zugehörigen Listen** anzeigen.




**d. Wahlweise:** Um eine Arbeitsnotiz für ein neues wichtiges Ereignis zu protokollieren, das kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. Die Arbeitsnotiz protokolliert, dass eine neue Notable hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und anderen Details, die dem Arbeitsnotizfeld in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

Sie haben Werte aus einem wichtigen Ereignis von Splunk erfolgreich Feldern in einem Security Incident von SIR zugeordnet. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung zu begrenzen. Sie haben auch wichtige Ereignisse an vorhandene SIR Security Incidents angehängt, wenn Ereignisfeldwerte mit den konfigurierten Zusammenfassungskriterien übereinstimmen.

**10.** Wählen Sie eines aus, um mit der Profilkonfiguration fortzufahren.

### Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau der Werte anzuzeigen, die Sie dem Security Incident zugeordnet haben.

#### Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem Now Platform® Security Incident Response (SIR)-Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle wichtigen Felder zugeordnet haben, die im Security Incident angezeigt werden sollen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin



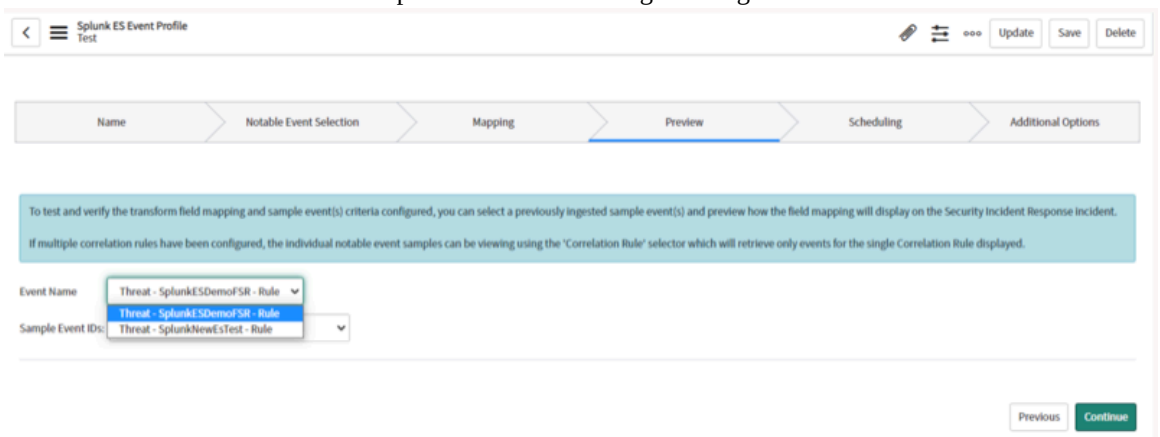
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie eine Vorschau eines Security Incident an, und bearbeiten Sie die Zuordnung bei Bedarf erneut, um Felder mit Fehlern zu korrigieren oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents im Produkt SIR gespeichert.

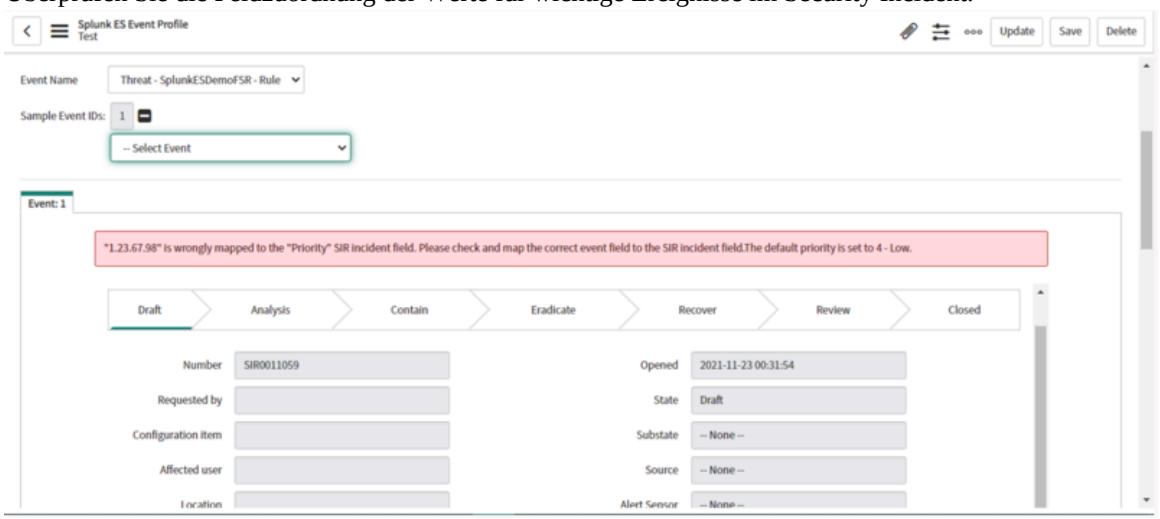
### Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Vorschau**.
2. Wählen Sie in der Auswahlliste Event-Name ein Element aus, wenn mehrere Events verwendet wurden.
3. Wählen Sie Event-IDs aus der Auswahlliste Beispiel-IDs für wichtiges Event aus.
4. Wählen Sie in der Auswahlliste Beispiel für IDs von wichtigem Ereignis ein Element aus.




Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incident wird nicht gespeichert.

5. Überprüfen Sie die Feldzuordnung der Werte für wichtige Ereignisse im Security Incident.



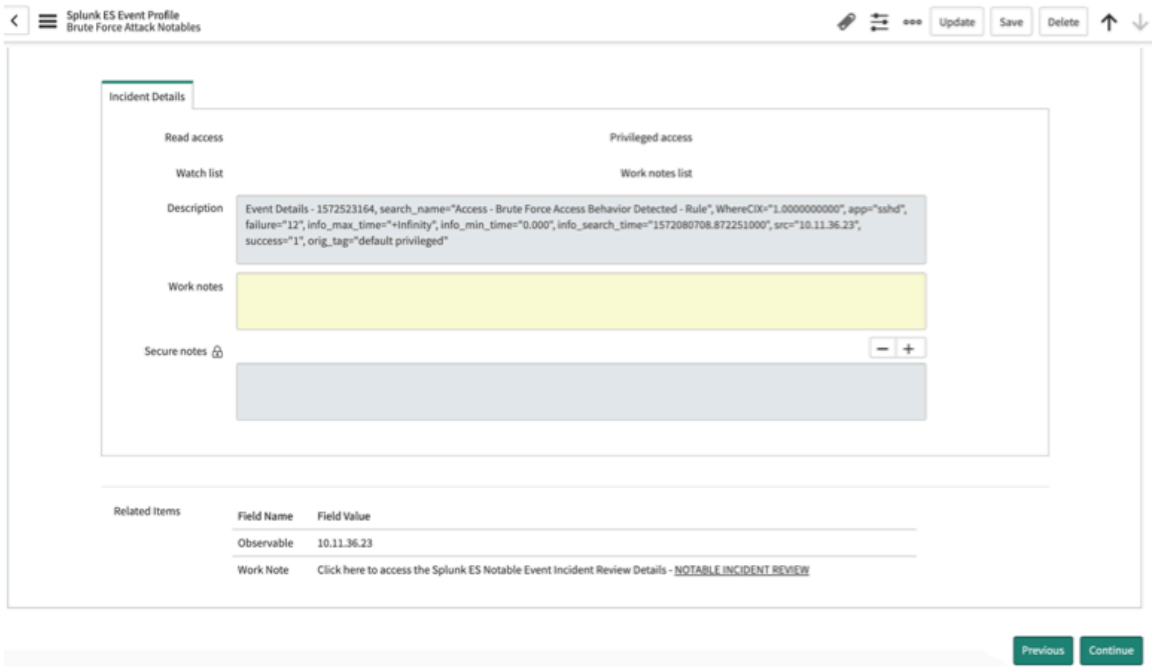

Die vorherige Abbildung zeigt eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem wichtigen Event keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Eine Fehlermeldung wird angezeigt, die angibt, dass für das Feld „ Konfigurationselement “ in der Kundenverwaltungsdatenbank (CMDB) ServiceNow® kein Eingabewert gefunden wurde. Daher wird dieser zugeordnete Feldwert nicht ohne weitere Änderung im SIR-Security Incident-Formular angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um diesen Fehler zu beheben, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.
7. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
8. Zeigen Sie eine erneute Vorschau der Zuordnung an, und fahren Sie mit der Behebung von Fehlern fort, die in Fehlermeldungen beschrieben werden.

   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Incident-Details“ in der unteren Hälfte eines SIR Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertpaaren ausgefüllt, die aus den Beispielen für wichtige Ereignisse Splunk Enterprise Security abgerufen wurden. Das erste Feld „Arbeitsnotizen“ hat keinen Wert. Dieses Feld wurde während des Zuordnungsschritts im Zuordnungsraster leer gelassen. Die zusätzlichen Arbeitsnotizfelder mit Werten wurden dem Zuordnungsabschnitt hinzugefügt.




9. Nachdem Sie alle Fehler behoben und überprüft haben, ob die Felder Ihren Vorstellungen entsprechen, wählen Sie eine Option aus, um fortzufahren.

### Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, führen Sie den nächsten Schritt zu Planen und rufen Sie Warnungen für die Splunk Enterprise Event Ingestion -Integration ab.

## Planen und rufen Sie neue und aktualisierte wichtige Events für die Splunk Enterprise Security Event Ingestion-Integration ab

Für automatisierte Profile für die Erfassung wichtiger Ereignisse ist dieser Schritt in der Konfiguration des Ereignisprofils erforderlich. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf wichtiger Ereignisse überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische wichtige Ereignisse mithilfe eines Datumsbereichs abrufen.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Bei Profilen für die automatisierte Erfassung wichtiger Ereignisse wählen Sie, ob Sie während des Schritts „Zeitplanung“ historische Ereignisse erfassen möchten. Sie können auch auswählen, wie oft zukünftige neue wichtige Ereignisse und aktualisierte wichtige Ereignisse, die der Warnungsprofilkonfiguration entsprechen, abgefragt werden sollen.

Bei automatisierten Profilen für die Erfassung wichtiger Ereignisse überprüfen und ändern Sie die Zeitplanung und den Warnungsabruf, bevor das Profil aktiviert wird. Dies ist ein erforderlicher Schritt für den gesamten Event-Profil-Konfigurationsprozess für geplante Warnungsprofile.

Sie konfigurieren diese Abfrageintervalle pro Profil. Die Leistung der Splunk -Integration der Event-Erfassung kann durch die unterschiedlichen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrage-Overheads auf dem Splunk Enterprise Security -Server gegen den Wunsch ausgleichen, so schnell wie möglich benachrichtigt zu werden, wenn ein wichtiges Event erstellt oder aktualisiert wird. Für jedes Profil wird ein Standardwert von fünf Minuten festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

Neue und aktualisierte wichtige Ereignisse werden abgerufen

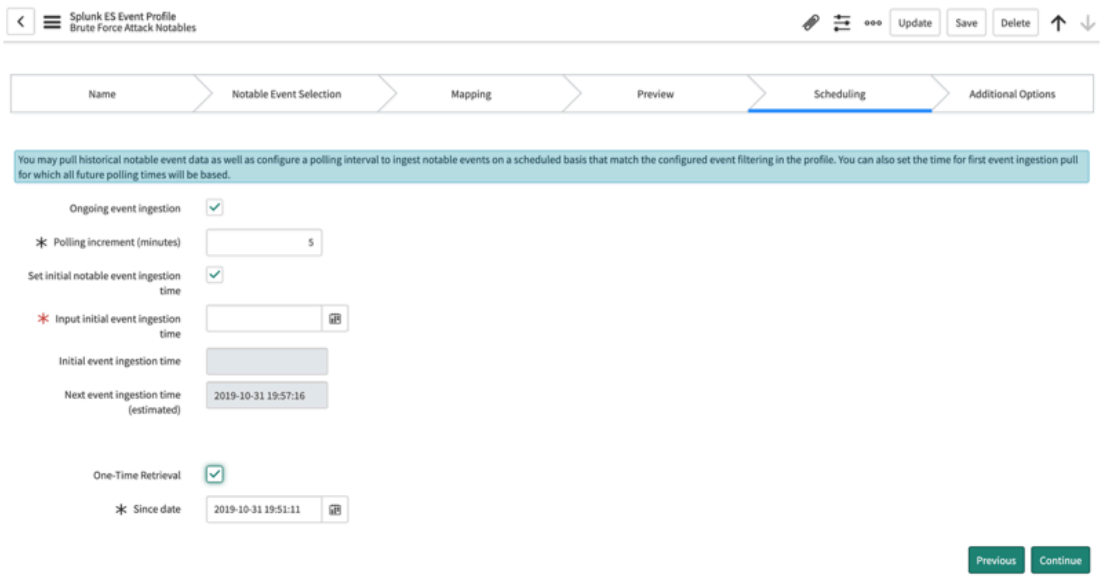
Wenn der Abfragezeitplan festgelegt ist, ruft die regelmäßige Aufgabe sowohl neue als auch aktualisierte wichtige Events ab, die zuvor abgerufen wurden, aber die Incident-Filterkriterien nicht erfüllt haben. Dies bietet Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die bei der ersten Erstellung eines wichtigen Ereignisses möglicherweise nicht vorhanden sind, aber nach einer Aktualisierung verfügbar werden, z. B. während der Untersuchungsphase. Sobald ein Incident für ein bestimmtes wichtiges Ereignis erstellt wurde, werden seine nachfolgenden Aktualisierungen ignoriert, da erwartet wird, dass der wichtige Hinweis jetzt als aktiver ServiceNow® Security Incident behandelt wird. Alle anderen Notables, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Kriterien für die Incident-Generierung überprüft, bis sie Teil eines aktiven Incident werden.

### Prozedur

1. Wenn die Seite „Zeitplanung“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zeitplanung**aus.
2. Wählen Sie einen aus, um zu planen, wie und wann wichtige Ereignisse aus der Konsole Splunk Enterprise Security abgerufen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Beispiel für die Planung einer ersten Erfassungszeit für wichtige Ereignisse: Wenn Sie eine tägliche Splunk Sicherheitsprüfung haben, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird, können Sie das entsprechende Profil für wichtige Ereignisse in Ihrer Instanz von Now Platform so einrichten, dass es um 16 Uhr ausgeführt wird :05 Uhr Ortszeit, um das Sicherheitsfehler-Event sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie 04 05 00 in das Feld Anfängliche Event-Erfassung ein. Geben Sie im Feld Increment (Minutes) (Schritt (Minuten)) 1440 (24 Stunden) ein, um die nächste Event-Erfassung für 24 Stunden nach der ersten Event-Erfassung zu planen. Sowohl die anfängliche Event-Erfassungszeit als auch die nächste Event-Erfassungszeit werden in den Feldern angezeigt.

3. Führen Sie die folgenden Schritte aus, um die Einstellungen für dieses Beispiel zu konfigurieren.

   a. Aktivieren Sie bei angezeigter Seite „Zeitplanung“ das Kontrollkästchen **Ongoing event ingestion** (Laufende Event-Erfassung), um diese Option zu aktivieren.

   b. Geben Sie im Feld Schritt (Minuten) den Wert 1440 (24 Stunden) ein.

   c. Klicken Sie auf das Kontrollkästchen **Anfängliche Event** -Erfassung auswählen, um die Bearbeitung der Felder Anfängliche Event-Erfassung und Nächste Event-Erfassung zu aktivieren.

   d. Geben Sie im Feld Anfängliche Event-Erfassung 04 05 00ein.
   Im Feld Nächste Event-Erfassung (geschätzt) wird die Zeit der nächsten Event-Erfassung angezeigt.

4. Klicken Sie auf eine der folgenden Optionen, um mit der Profilkonfiguration fortzufahren.

### Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Security Incidents können erstellt und aktualisiert werden, nachdem sie mit einer bidirektionalen Schnittstelle mit der Splunk Enterprise Security -Integration erstellt wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Die Splunk Enterprise Security -Integration verfügt über eine bidirektionale Schnittstelle, die es wichtigen Ereignissen ermöglicht, Security Incidents zu erstellen und die wichtigen Ereignisse zu aktualisieren, nachdem der Security Incident erstellt und/oder geschlossen wurde.

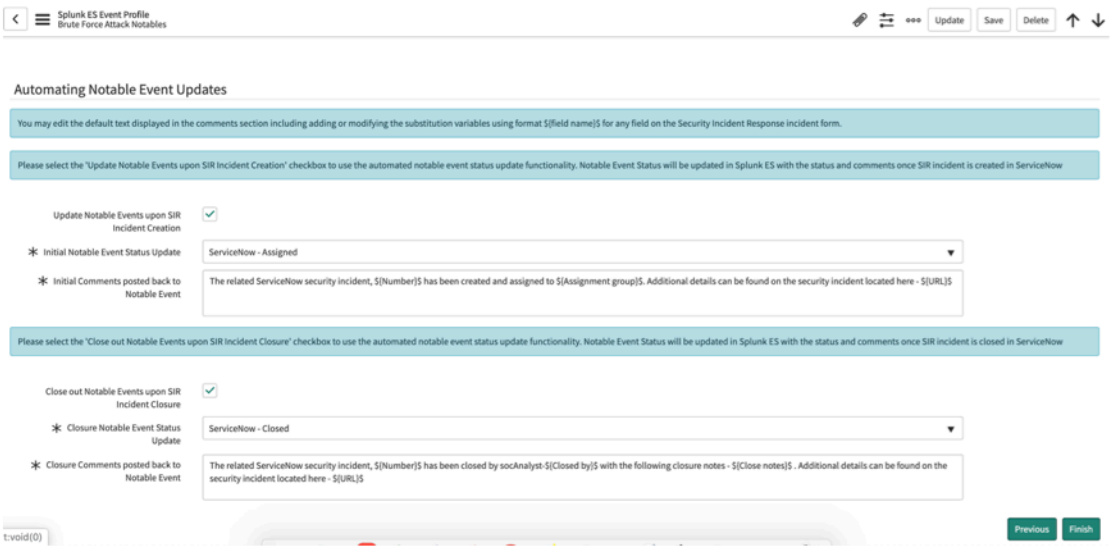
Zu den relevanten Incident-Details gehören SIR Incident-Nummer, Zuweisungsgruppe, SIR Incident-URL. Dieser Abschnitt ist der letzte Teil des Setups der Profilkonfiguration, der optionale Funktionen zum Aktualisieren der wichtigen Splunk Enterprise Security Events bereitstellt.

Erforderliche Rolle: sn_si.admin

## Prozedur

1. Wenn die Seite „Zusätzliche Optionen“ in der Fortschrittsleiste nicht angezeigt wird, wählen Sie **Zusätzliche Optionen**aus.
2. Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration für die Aktualisierung wichtiger Ereignisse basierend auf Security Incident-Updates abzuschließen.
3. **Klicken** Sie auf Fertigstellen, um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um basierend auf Ihrer Planung wichtige Ereignisse aus der Konsole Splunk Enterprise Security abzurufen. Es gibt ein Limit von 1.000 Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Bis zu 100 wichtige Ereignisse pro ausgelöster Warnung. Nachfolgende wichtige Ereignisse werden ignoriert, nachdem die Grenzwerte erreicht sind.

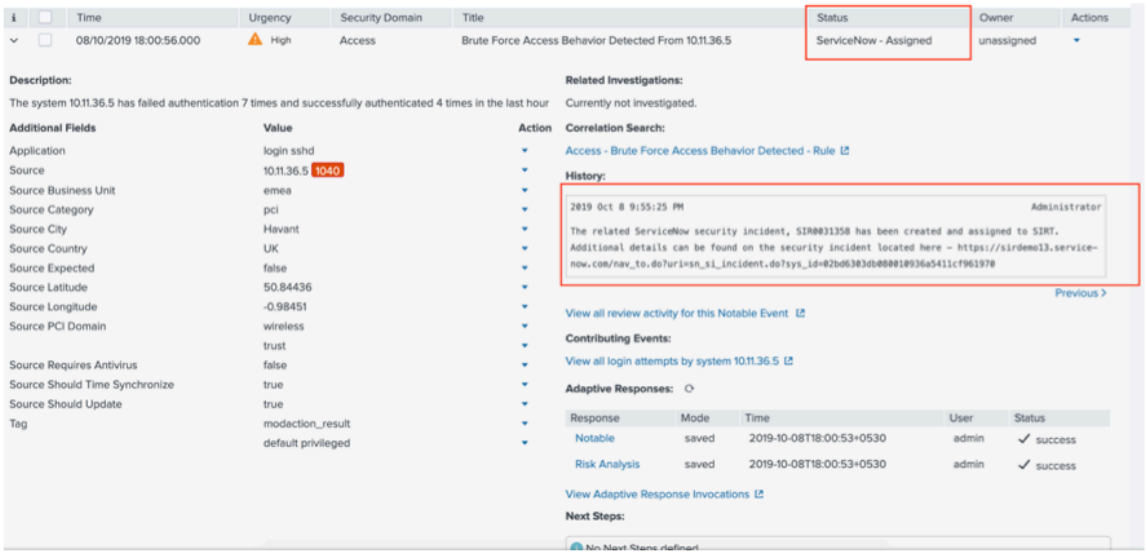
   Die folgende Abbildung zeigt die Registerkarte „Zusätzliche Optionen“ mit ausgefüllten Standardwerten:






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Konfiguration „Zusätzliche Optionen“ aktiviert ist, zeigt die Überprüfung von Incidents für wichtige Ereignisse die Statusänderung und eine Aktualisierung der Verlaufskommentare an:




### Richten Sie ein Profil für die manuelle Event-Weiterleitung ein

Abhängig vom definierten Profil werden Splunk ES Notable-Events manuell als diskrete Notable-Events an die Security Operations -Umgebung Ihrer Now Platform -Instanz weitergeleitet.

So richten Sie ein Profil für die manuelle Weiterleitung wichtiger Ereignisse ein:

| Aufgabe | Abschnitt |
|---|---|
| Erstellen Sie ein Event-Profil | Siehe Erstellen Sie Profile für manuell weitergeleitete Events |
| Ordnen Sie Felder für wichtige Ereignisse zu | Siehe Zuordnung wichtiger Event-Felder für die Splunk Enterprise Security -Integration |
| Erstellen Sie benutzerdefinierte Zuordnungen | Siehe Zuordnungen für Splunk ES Incident-Überprüfung eines wichtigen Ereignisses und beitragende Ereignisdetails erstellen (manuelle Weiterleitung) |
| Zeigen Sie eine Vorschau des Security Incident an | Siehe Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an |
| Richten Sie Ihre Splunk -Umgebung für die manuelle Erfassung ein | Siehe Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Integration von Splunk Enterprise Security Notable Event Ingestion ein |
| Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status | Siehe Automatisieren Sie die Aktualisierung und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status |

### Erstellen Sie Profile für manuell weitergeleitete Events

Sie können ein Profil für manuell weitergeleitete Events einrichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

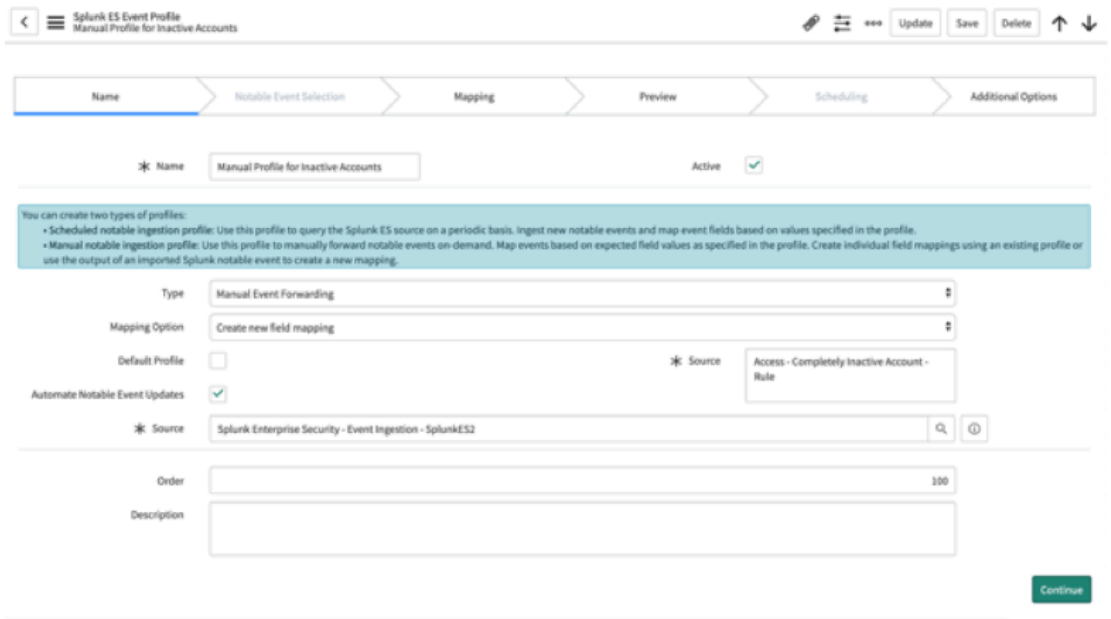
Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Event-Weiterleitung unterstützt.

Für Events, die Sie bei Bedarf von Ihrer Splunk Enterprise Security -Konsole aus weiterleiten, können Sie die einzelne Feldzuordnung auf ein vorhandenes Profil stützen. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangdaten erstellen. Events, die Sie manuell weiterleiten, werden nicht im Event-Profil geplant.

**a.** Wenn dies noch nicht geschehen ist, wählen Sie in der Auswahlliste für das Feld Typ die Option **Manuelle Event-Weiterleitung**aus.

**b.** Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

In den folgenden Abbildungen und Tabellen finden Sie weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen.




**Neue Feldzuordnungsoption erstellen**

| Option oder Feld | Beschreibung |
|---|---|
| Neue Feldzuordnungsoption erstellen | Neue Feldzuordnung für Ihr Event.<br><br>Wenn keine Feldzuordnung vorhanden ist, die dem von Ihnen erstellten Profil ähnelt, wählen Sie diese Option aus, um eine neue Zuordnung zu erstellen. |
| Standardprofil | Standardmäßiges Event-Weiterleitungsprofil für alle Splunk -Events. Der Standardwert ist deaktiviert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
| --- | --- |
| | Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Event-Weiterleitung. Dieses Profil wird verwendet, wenn es keine Übereinstimmung mit der Quelle aus dem manuell weitergeleiteten Event gibt. Es wird zum Standardprofil für alle Events mit unbekannten Quellen.<br><br>Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. |
| Quelle (Feld „Bemerkenswertes Ereignis“) | Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die den erkennbaren Wert ausgelöst hat, z. B. Brute-Force-Angriffe.<br><br>Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.<br><br>Falls verfügbar, ermöglicht dieses Feld eine eindeutige Event-Feldzuordnung zu Security Incident-Feldern basierend auf der Splunk-Korrelationsregel, die normalerweise für verschiedene Event-Typen unterschiedlich ist.<br><br>Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie basierend auf der Korrelationsregel verschiedene Profilereignisprofile erstellen, um diese Anforderung zu erfüllen. |
| Automatisieren Sie die Aktualisierung wichtiger Ereignisse | Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des wichtigen Ereignisses aktualisieren und zusätzliche Kommentare hinzufügen möchten, wenn ein SIR-Incident aus dem wichtigen Ereignis erstellt wird und/oder wenn der SIR-Incident geschlossen wird. Dies geschieht sowohl für die anfänglichen auslösenden nennenswerten Ereignisse, die den SIR-Incident erstellen, als auch für zusammengefasste Ereignisse. |
| Quelle (Splunk Server) | Der Server Splunk, den Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn Sie mehrere Splunk Server konfiguriert haben, wählen Sie den entsprechenden Server für die wichtigsten Ereignistypen aus, die für das Profil aktualisiert werden. Sie müssen einen Wert eingeben. |
| Reihenfolge | Der Standardwert ist 100. Belassen Sie diese Einstellung auf der Standardeinstellung. |

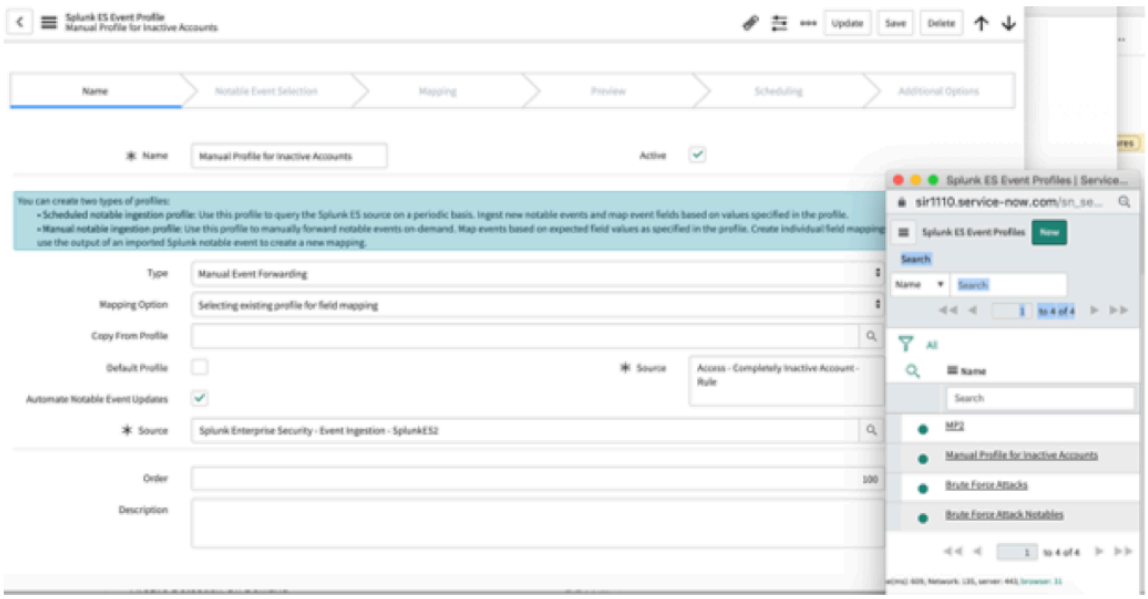


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
|---|---|
| | Wenn Sie eine große Anzahl von Profilen erstellt haben, gibt dieser Wert eine Ausführungszeitpriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität. |
| (Optional) Beschreibung | Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

Vergewissern Sie sich bei einem Profil mit einer neuen Feldzuordnung, dass Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fortfahren**, um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Für ein Profil mit einer vorhandenen Feldzuordnung finden Sie weitere Informationen in der folgenden Abbildung und Tabelle.




### Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

| Option oder Feld | Beschreibung |
|---|---|
| Wählen Sie ein vorhandenes Profil für die Feldzuordnung aus | Verwenden Sie eine vorhandene Feldzuordnung für Ihr neues Profil für wichtige Ereignisse erneut. Das Feld Aus Profil kopieren wird angezeigt.<br><br>Befolgen Sie diese Schritte, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren.<br><br>**i.** Klicken Sie links neben dem angezeigten Feld Aus Profil kopieren auf das Suchsymbol.<br><br>**ii.** Klicken Sie in der angezeigten Liste Splunk ES-Ereignisprofile auf den |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
|---|---|
| | Profilnamen mit der zu kopierenden Karte.<br><br>Der Profilname wird im Feld Aus Profil kopieren angezeigt. |
| Standardprofil | Standardmäßiges Event-Weiterleitungsprofil für alle Splunk wichtigen Events mit nicht abgeglichener Quelle. Der Standardwert ist deaktiviert.<br><br>Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Event-Weiterleitung.<br><br>Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. |
| Quelle (Feld „Bemerkenswertes Ereignis“) | Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die den erkennbaren Wert ausgelöst hat, z. B. Brute-Force-Angriffe.<br><br>Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.<br><br>Falls verfügbar, ermöglicht dieses Feld eine eindeutige Event-Feldzuordnung zu Security Incident-Feldern basierend auf der Splunk-Korrelationsregel, die normalerweise für verschiedene Event-Typen unterschiedlich ist.<br><br>Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie basierend auf der Korrelationsregel verschiedene Profilereignisprofile erstellen, um diese Anforderung zu erfüllen. |
| Automatisieren Sie wichtige Ereignisse | Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des wichtigen Ereignisses aktualisieren und zusätzliche Anmerkungen hinzufügen möchten, wenn ein Security Incident aus dem wichtigen Ereignis erstellt wird oder wenn der Security Incident geschlossen wird. Dies geschieht sowohl für die anfänglichen auslösenden wichtigen Ereignisse, die den Security Incident erstellen, als auch für zusammengefasste Ereignisse. |
| Quelle (Splunk Server) | Splunk -Server oder -Suchende, die Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn Sie mehrere Splunk Server konfiguriert haben, wählen Sie den entsprechenden Server für die wichtigsten Ereignistypen aus, die für das |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option oder Feld | Beschreibung |
|---|---|
| | Profil aktualisiert werden. Sie müssen einen Wert eingeben. |
| Reihenfolge | Der Standardwert ist 100. Belassen Sie diese Einstellung auf der Standardeinstellung.<br><br>Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Ausführungszeitpriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Der Workflow im Profil mit der niedrigsten Nummer hat die höchste Priorität. |
| (Optional) Beschreibung | Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

**Klicken** Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil auf Fertigstellen, um die Profilkonfiguration abzuschließen.

### Zuordnungen für Splunk ES Incident-Überprüfung eines wichtigen Ereignisses und beitragende Ereignisdetails erstellen (manuelle Weiterleitung)

Während des Zuordnungsschritts für das Feld für ein wichtiges Event ordnen Sie einzelne Event-Felder aus den Feldern für einen Now Platform Security Incident Response (SIR) Security Incident zu.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Ordnen Sie bis zu fünf wichtige Events aus der Spalte „Beispiel für wichtiges Ereignis“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardfelder, die in der Regel wichtige Felder zum Ausfüllen des SIR-Incident-Formulars sind, werden angezeigt. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mithilfe der Schaltflächen + und - angezeigt werden. Erstellen Sie benutzerdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie Splunk Felder zuordnen, die nicht im Standardzuordnungsraster des Security Incident SIR angezeigt werden.

#### Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, **klicken** Sie in der Fortschrittsleiste auf Zuordnung.
2. Befolgen Sie diese Schritte, um Anhangdaten in Ihre Now Platform® -Instanz hochzuladen.
   a. Wenn Sie noch nicht angemeldet sind, melden Sie sich bei Ihrer Splunk Enterprise -Konsole an.
   b. Navigieren Sie zur Registerkarte Suche, und geben Sie einen Namen für eine Suche ein, die die Daten zu wichtigen Ereignissen enthält, die Sie exportieren möchten.

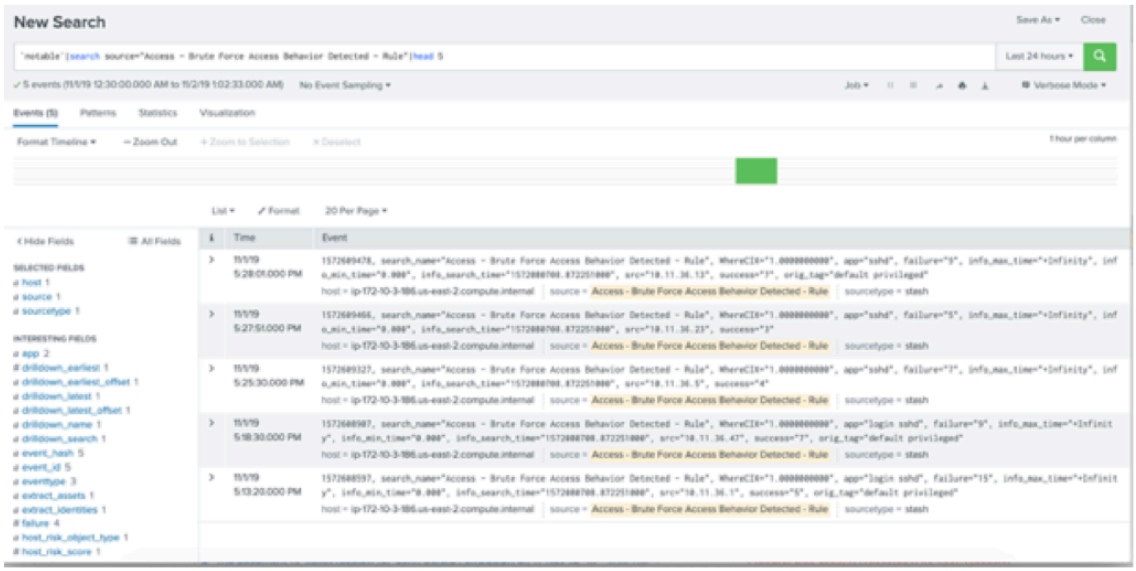


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel für ein Suchformat zum Abrufen von wichtigen Ereignissen für die Korrelationsregel für das Brute-Force-Zugriffsverhalten wäre: „notable“ | search source = „Zugriff – Brute-Force-Zugriffsverhalten erkannt – Regel“.

**c.** Erweitern Sie das wichtige Ereignis, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Seite „Zuordnung“ in Ihrer Instanz Now Platform® angezeigt werden.




**d.** Klicken Sie in der Konsole Splunk Enterprise oben rechts auf der Suchseite auf das Symbol **Exportieren**.

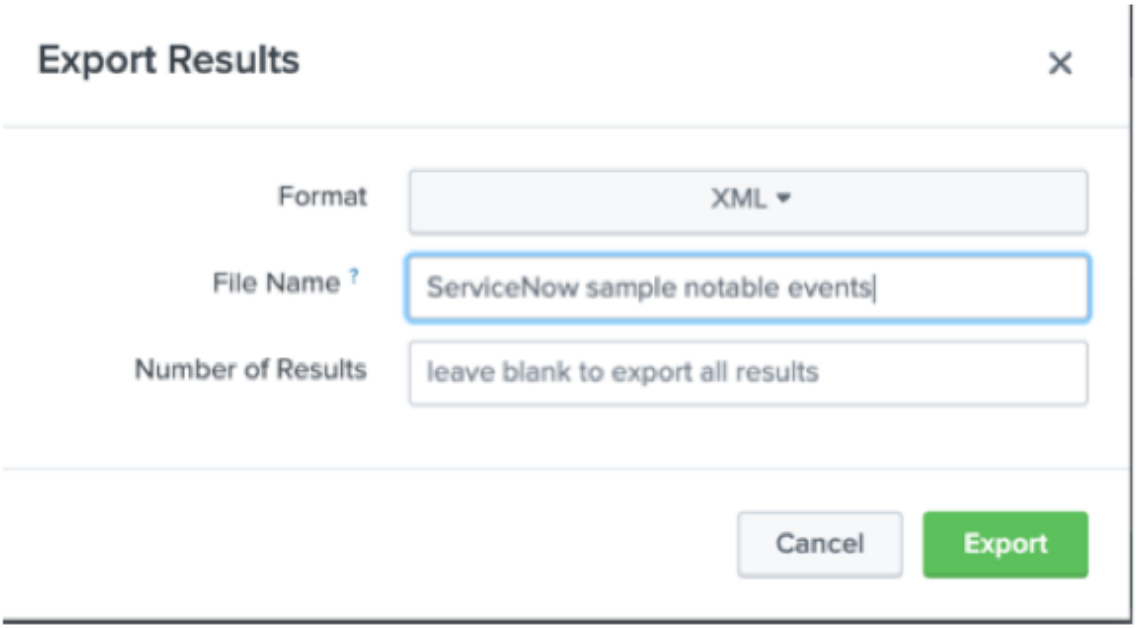
**e.** Klicken Sie in der Auswahlliste für das Feld Format im angezeigten Dialogfeld auf **XML-Format**.

**f. Wahlweise:** Geben Sie einen neuen Dateinamen ein.

**g.** Klicken Sie auf **Exportieren**.



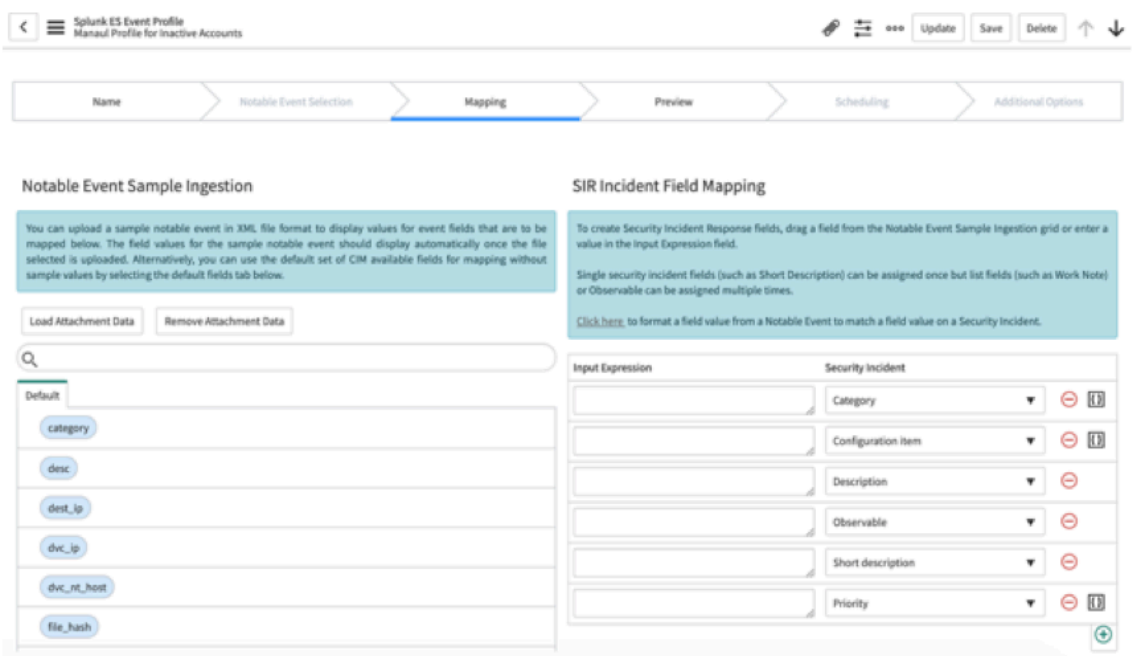
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die exportierte Splunk XML-Datei für wichtige Ereignisse muss jetzt in Ihre Instanz Now Platform® hochgeladen werden.

**h.** Wenn die Zuordnungsseite in Ihrer Instanz Now Platform® noch nicht angezeigt wird, klicken Sie in der Fortschrittsleiste auf **Zuordnung**.

**i.** Klicken Sie in der Spalte „Beispiel für wichtiges Ereignis“ auf **Anhangdaten**laden.




**j.** Klicken Sie im angezeigten Dialogfeld auf **Dateien** auswählen, navigieren Sie zur XML -Datei, die Sie exportiert haben, und klicken Sie auf **Öffnen**.
Nachdem Sie auf klicken, um Anhangdaten für manuell weitergeleitete Ereignisse zu laden, werden die Felder für wichtige Ereignisse Splunk ES auf der linken Seite des Formulars ausgefüllt. Diese Werte sind



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Feldwerte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.
Die Wertepaare für die Felder, die Sie für das Event exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

3. Führen Sie die Schritte 5 bis 10 im Abschnitt Zuordnungen für Splunk ES Incident-Überprüfung für wichtiges Event und beitragende Event-Details erstellen (geplante Erfassung) aus.

### Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Integration von Splunk Enterprise Security Notable Event Ingestion ein

Installieren und richten Sie die Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security in Ihrer Splunk Enterprise-Konsole oder Splunk Cloud-Instanz ein, wenn Sie Events manuell und bei Bedarf aus Ihrer Splunk Enterprise Security -Konsole für diese Integration exportieren möchten.

#### Vorbereitungen

Die Installation und Einrichtung der Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security in Ihrer Splunk Unternehmenskonsole oder Splunk Cloud-Instanz ist optional.

Vergewissern Sie sich, dass Sie die Anwendung für diese Integration aus dem ServiceNow Store installiert haben, bevor Sie das Add-on-Plugin von splunkbase installieren, das für die manuelle Event-Erfassung erforderlich ist. Wenn Sie die Anwendung für die Integration von ServiceNow Storenicht installiert haben, lesen Sie Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Security Notable Event Ingestion, und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: Splunk Enterprise Security Administrator

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Events manuell und bei Bedarf aus Ihrer Splunk Enterprise -Konsole für die -Integration exportieren möchten, laden Sie das ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Security aus splunkbase in Ihrer Splunk Enterprise Security -Konsole herunter, installieren Sie es und richten Sie es ein. Dieses Erweiterungs-Add-on ServiceNow ist erforderlich, damit Security Incidents aus manuell exportierten Events in Ihrer Now Platform -Instanz erstellt werden können. Diese Anwendung ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security ist auf splunkbase verfügbar.

Für die manuelle Event-Weiterleitung können Sie bis zu zwei verschiedene Now Platform -Endpunkte (Instanzen) in Ihrer Splunk Enterprise Security -Konsole identifizieren. Sie leiten die Events manuell an den Endpunkt oder die Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise sowohl eine Staging-Instanz (Entwicklungsinstanz) als auch eine Produktionsinstanz angeben. Indem Sie separate Instanzen angeben und primäre und sekundäre Workflows für jede Instanz benennen, können Sie auswählen, wohin Sie verschiedene Events weiterleiten möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn Sie das Add-on „ ServiceNow Security Operations Event Ingestion“ für Splunk Enterprise Securitynoch nicht installiert haben, führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu splunkbase .

   b. Suchen Sie nach dem Add-on „ ServiceNow Security Operations Security Operations Event Ingestion“ für Splunk Enterprise Security.

   **Hinweis:**
   Stellen Sie sicher, dass Sie ServiceNow Security Operations Event Ingestion Add-on für Splunk Enterprise Securityausgewählt haben. Es gibt zusätzliche ServiceNow Add-ons, die in dieser Liste angezeigt werden. Diese Add-ons sind für verschiedene ServiceNow Splunk -Integrationen vorgesehen und für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihr Konto Splunk Enterprise Security.

   e. Klicken Sie auf der Seite „Apps“ in der Dropdown-Liste des Menüs auf das Zahnradsymbol oder die Verknüpfung **Apps verwalten**.

   f. Klicken Sie oben links auf der angezeigten Seite „Apps“ auf **App aus Datei installieren**.

   g. Klicken Sie auf **Datei**auswählen, wählen Sie ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Securityaus, und klicken Sie auf **Hochladen**.

   h. Wenn Sie dazu aufgefordert werden, starten Sie Splunk Enterpriseneu.
   Das Add-on ServiceNow Security Operations Event Ingestion für Splunk Enterprise Security wird in Ihrer Splunk Enterprise Security -Konsole installiert. Der nächste Schritt zum Einrichten des Add-ons.

2. Führen Sie die folgenden Schritte aus, um das Add-on einzurichten.

   a. Klicken Sie in Splunk Enterprise Securityauf das Zahnradsymbol für **Apps** oder auf **Apps verwalten** in der Dropdown-Liste des Menüs.

   b. Klicken Sie in der Liste der angezeigten Anwendungen in der Spalte **Aktionen** auf **Setup** für ServiceNow Security Operations Event Ingestion Add-on for Splunk Enterprise Security.

   c. Füllen Sie das Formular aus.



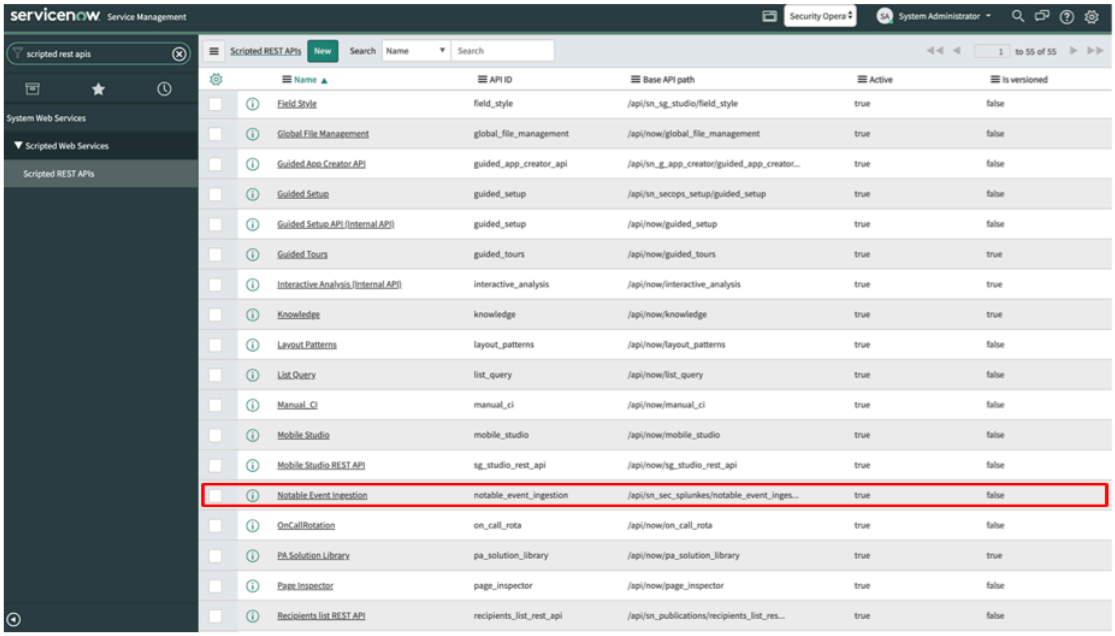
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular in der Konsole Splunk Enterprise Security.

Die folgende Abbildung zeigt ein Beispiel für die Liste der Scripted REST APIs in Now Platform. In der Liste wird die Position des Endpunktwerts einer Now Platform -Instanz angezeigt, die Sie im Formular als Teil des Setups für die Erweiterung ServiceNow „ Security Operations Event Ingestion Add-on for Splunk Enterprise Security “ in Ihrer Splunk Enterprise Security -Konsole eingegeben haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie im Setup-Formular in der Konsole Splunk Enterprise Security auf **Speichern**, um Ihre Änderungen zu speichern.

   Nach einigen Minuten wird oben links im Formular in Ihrer Splunk Enterprise Security -Konsole eine Meldung angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, sind die Namen (Workflow-Aktionsbezeichnungen) für Ihre Now Platform Instanzen, die Sie im Formular erstellt haben, in der Auswahlliste Ereignisaktionen für ein ausgewähltes Event einer Suche in Ihrer Splunk Enterprise Security -Konsole verfügbar.

## Nächste Maßnahme

Wenn Sie Suchen noch nicht in Ihrer Splunk Enterprise Security -Konsole gespeichert haben, besteht der nächste Schritt darin, Suchen als Warnungen in Ihrer Splunk Enterprise Security -Konsole zu speichern.

### Kopieren Sie ein Event-Profil für die Splunk Enterprise Security Event Ingestion-Integration

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, empfiehlt es sich, Alarmprofile zu kopieren, um Zeit zu sparen.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin

## Warum und wann dieser Vorgang ausgeführt wird

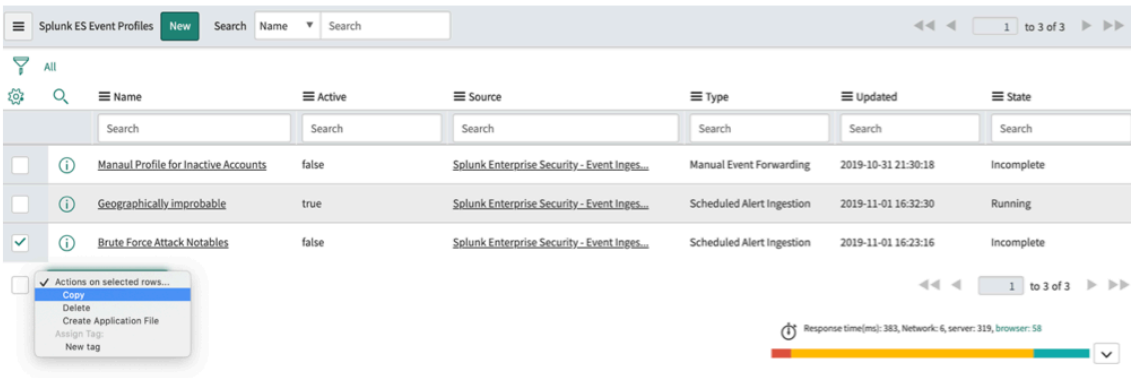
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), damit es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und überprüft haben.



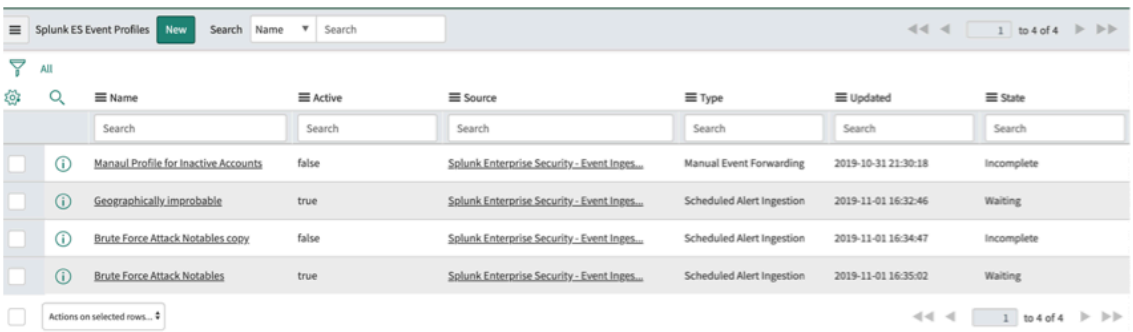
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Splunk-Integration** > **Splunk-Ereignisprofil**.
2. Wählen Sie in der angezeigten Liste Splunk Ereignisprofile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren**.




Das Profil wird kopiert und in der Liste angezeigt. Die Kopie enthält alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (true), ist die Kopie zu diesem Zeitpunkt deaktiviert (false). Möglicherweise möchten Sie die Werte des kopierten Profils bearbeiten und es umbenennen, damit die Konfigurationseinstellungen wie erforderlich auf das neue Profil angewendet werden.




Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

### Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren, nachdem Sie den Konfigurationsschritt abgeschlossen haben.

## Verwenden Sie den Skript-Editor, um Warnungswerte für die Splunk Enterprise Security Event Ingestion-Integration zu formatieren

Zusätzlich zu den direkt zugeordneten Feldern aus den erfassten Werten für wichtige Ereignisse und den Werten, die Sie manuell eingeben, verwenden Sie den Skript-Editor, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen werden die Werte für erkennbare Ereignisse Splunk Enterprise Security den Feldern „Kategorie“, „Configuration Item (CI)“ und „Erkennbares Element“ im Incident SIR nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert eines wichtigen Ereignisses Splunk Enterprise Security in einen Wert

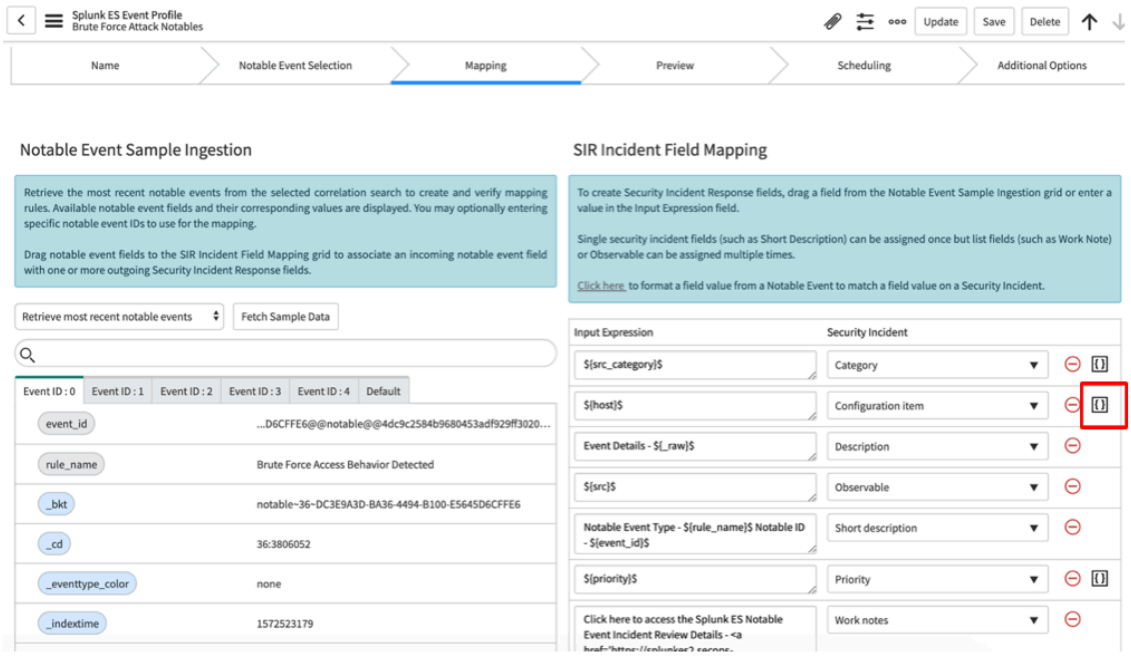
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übersetzen möchten, der von diesen Feldern im Security Incident SIR unterstützt wird, verwenden Sie den Skript-Editor.

### Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.




2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammersymbol [{}] neben einem Feld klicken, um den Skript-Editor für dieses Feld zu öffnen.

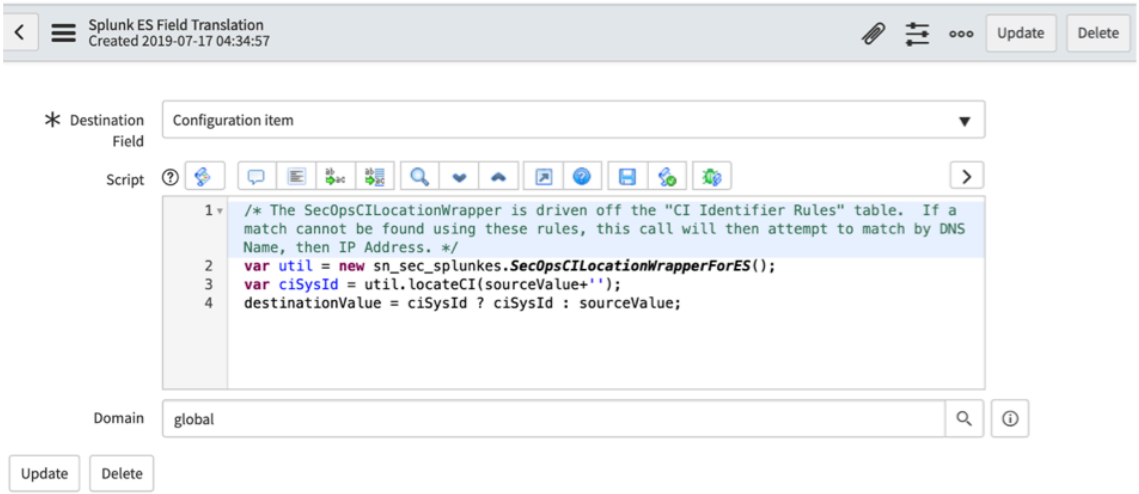
   In bestimmten Fällen kann eine Skripteinbindung für das Feld Configuration Item geeignet sein. Bei einem wichtigen Event stimmt beispielsweise ein Wert für das Konfigurationselement möglicherweise nicht überein.

   Wie in der folgenden Abbildung dargestellt, können Sie, wenn in der Now Platform® CMDB für das Feld „Konfigurationselement“ keine Übereinstimmung mit einem Hostnamen gefunden wird, die Regel so bearbeiten, dass das Feld „Konfigurationselement“ ausgefüllt wird, wenn eine IP-Adresse gefunden wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null gesetzt.

   Der Editor wird geöffnet, und das Feld wird in Zielfeld angezeigt. Die folgende Abbildung zeigt den Editor mit dem Feld Configuration Item als Zielfeld.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie Änderungen am Skript ein, und klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
   Die Tabelle Splunk „ Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Formular „Zuordnung“ zurückzukehren.

### Kopieren Sie Splunk Enterprise Security Profile mithilfe der Export-/Importfunktion von einer Instanz in eine andere

Sie können Splunk Enterprise Security -Profileinstellungen aus einer Now Platform -Instanz in eine andere Now Platform -Instanz exportieren und importieren.

#### Vorbereitungen
Zu den Einstellungen, die Sie exportieren und importieren können, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

Erforderliche Rolle: sn_si.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Mit dieser Funktionalität kann der Sicherheitsadministrator Profile, die in einer Now Platform -Instanz getestet und verifiziert wurden, z. B. außerhalb der Produktion, in eine andere Now Platform -Instanz kopieren, z. B. in der Produktion, ohne alle Konfigurationseinstellungen wiederholen zu müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel.

**Hinweis:**
Wenn Sie einen manuellen Event-Weiterleitungsprofiltyp exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangdaten kopiert, die Anhangdatei selbst wird jedoch nicht exportiert.

#### Prozedur

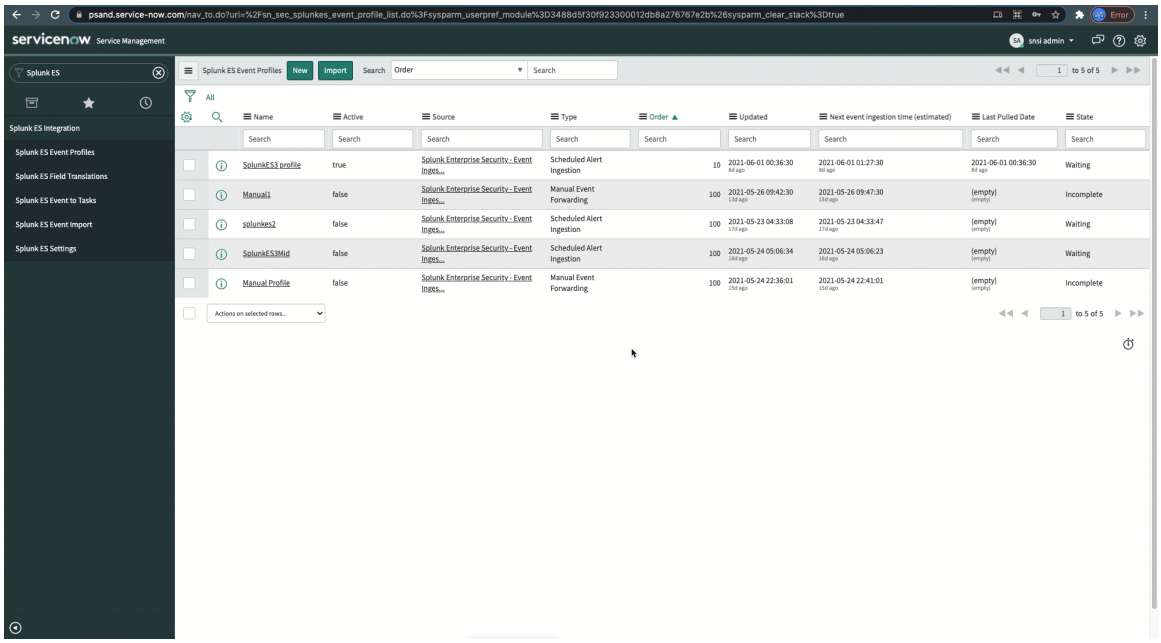
1. Navigieren zu **Alle** > **Splunk ES-Integration** > **Splunk ES-Ereignisprofile**.
2. Wählen Sie ein Profil aus, das Sie in eine andere Now Platform -Instanz exportieren möchten.
   Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Sobald die Meldung „Export abgeschlossen“ angezeigt wird, klicken Sie auf **Herunterladen**.

   Die folgende Abbildung zeigt das Exportieren eines Profils (SplunkES3profile) aus der Instanz Now Platform (psand.service-now.com).




   Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Quellinformationen der Konfigurationskachel. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben payload.xml-Datei angezeigt.

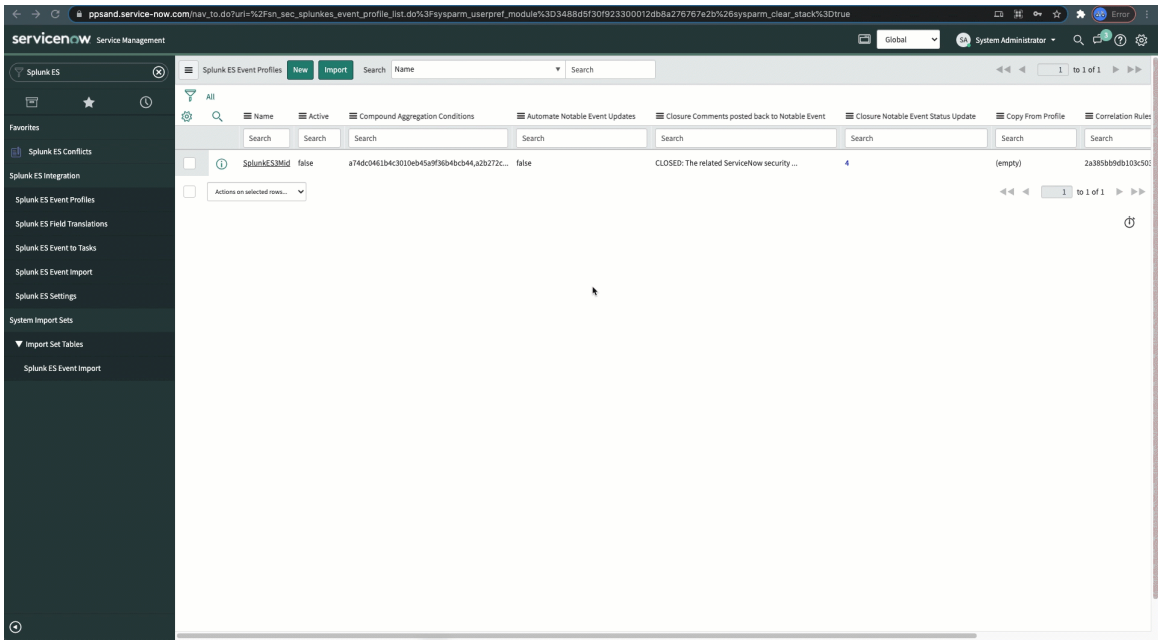
   Sie können jetzt das Profil in eine andere Now Platform -Instanz importieren.

5. Navigieren zu **Splunk ES-Integration** > **Splunk ES-Ereignisprofile**.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie auf **Datei** auswählen, und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie **auf Profile schließen und neu laden**.

   Die folgende Abbildung zeigt den Import eines Profils (SplunkES3profile) aus der Now Platform -Instanz (psand.service-now.com) in die Now Platform -Instanz (ppsand.service-now.com).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Sie haben das Profil erfolgreich aus einer anderen Now Platform -Instanz importiert.

Vergewissern Sie sich, dass die exportierte Quelle (Splunk API-Konto und Splunk Server-URL) und die MID Server-Konfigurationseinstellungen gültig und in der importierten Now Platform -Instanz verfügbar sind. Aktualisieren Sie bei Bedarf Ihre Splunk Enterprise Security -Konfiguration.

10. **Wahlweise:** Überprüfen Sie die MID Server-Einstellungen, nachdem Sie ein Profil importiert haben.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**.
12. **Wahlweise:** Wählen Sie die Konfigurationskachel Splunk Enterprise Security aus, und klicken Sie auf **Aktualisieren**.
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Quell- und MID Server-Details nach Bedarf.

### Prüfliste für die Integration von Splunk Enterprise Security Notable Event Ingestion

Verwenden Sie diese Prüfliste, um alle Aufgaben der Integration zu durchlaufen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

#### Vorbereitungen

Erforderliche Rolle: admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security -administrator

#### Warum und wann dieser Vorgang ausgeführt wird

Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration mit der folgenden Tabelle nach. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. In jeder Zeile der Tabelle werden Aufgaben aufgelistet und die Rollen angegeben, die zum Ausführen der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

Die für jede Aufgabe erforderlichen Rollen werden für jeden Schritt in der folgenden Tabelle aufgelistet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Verfolgen Sie Ihren Fortschritt bei der Einrichtung, Installation und Konfiguration der Integration nach. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren.
2. Führen Sie die Schritte in der Tabelle in der Reihenfolge aus, in der sie angezeigt werden.

**Prüfliste**

| | |
|---|---|
| ☐ | Richten Sie als Benutzer mit der Administratorrolle Now Platform ] Ihre Now Platform -Instanz ein.<br>○ Weisen Sie Benutzer mit den Rollen sn_si.admin und sn_si.analyst nach Bedarf zu.<br>○ Installieren und konfigurieren Sie einen MID Server, wenn der Server Splunk in Ihrem Unternehmensnetzwerk bereitgestellt wird.<br>○ Vergewissern Sie sich, dass die Plugins ServiceNow Security Incident Response für Ihr Release von Now Platformaktiviert sind.<br>○ (Optional) Wenn Sie Events manuell von Ihrer Splunk Enterprise Security -Konsole an Ihre Now Platform -Instanz weiterleiten möchten, vergewissern Sie sich, dass Sie die Rolle (sn_sec_splunkes.api_account_access) einem Benutzer mit der Administratorberechtigung Splunk Enterprise Security zugewiesen haben.<br>Weitere Informationen finden Sie unter Richten Sie Ihre Now Platform -Instanz für die Splunk Enterprise Security -Integration ein. |
| ☐ | Installieren und konfigurieren Sie als Benutzer mit der Administratorrolle Now PlatformSplunk Enterprise Security die Anwendung [] aus dem ServiceNow Store.<br>**a.** Laden Sie die Anwendung herunter, und installieren Sie sie in Ihrer Instanz Now Platform.<br>**b.** Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung zu Ihrer Splunk Enterprise Security -Konsole her.<br>Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung ServiceNow für die Integration von Splunk Enterprise Security Notable Event Ingestion. |
| ☐ | (Optional) Wenn Sie Events manuell aus Ihrer Splunk Enterprise Security -Konsole in Ihre Now Platform -Instanz exportieren möchten, führen Sie die folgenden Aufgaben aus: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | ○ Installieren, richten Sie als Splunk Enterprise Security ]-Administrator das Add-on „ ServiceNow Security Operations Event Ingestion“ für Splunk Enterprise Security aus splunkbase in Ihrer Splunk Enterprise Security -Konsole ein, richten Sie es ein und aktivieren Sie es.<br>○ Speichern Sie als Splunk Enterprise Security -Administrator, falls noch nicht konfiguriert, Suchen als wichtige Ereignisse in Ihrer Splunk Enterprise Security -Konsole.<br><br>Weitere Informationen finden Sie unter Richten Sie Ihre Splunk -Umgebung für die manuelle Event-Erfassung für die Integration von Splunk Enterprise Security Notable Event Ingestion ein. |
| ☐ | Erstellen und benennen Sie als Benutzer mit der Rolle Now Platform sn_si.admin ein Event-Profil.<br><br>Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Event-Profil, mit dem Sie Anhangdaten manuell aus Ihrer Splunk Enterprise Security -Konsole exportieren können.<br><br>○ Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus.<br>○ Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Zuordnung, oder kopieren Sie eine vorhandene Zuordnung.<br><br>Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Event-Profil für die Splunk Enterprise Security Event Ingestion-Integration. |
| ☐ | Ordnen Sie als Benutzer mit der Rolle Now Platform sn_si.admin erfasste Werte oder Anhangdaten, die aus Splunk Enterprise Security exportiert werden, zu Now Platform Security Incidents zu.<br><br>**a.** Rufen Sie Beispieldaten für eine geplante Warnung ab.<br>**b.** (Optional) Exportieren Sie Anhangdaten für ein Event manuell aus Splunk Enterprise Security.<br>**c.** Bearbeiten Sie die Standardzuordnungskonfiguration.<br>**d.** Fügen Sie optional Filterkriterien hinzu, hängen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skript-Editor.<br><br>Weitere Informationen finden Sie unter Zuordnung wichtiger Event-Felder für die Splunk Enterprise Security -Integration und Zuordnungen für Splunk ES Incident-Überprüfung für wichtiges Event und beitragende Event-Details erstellen (geplante Erfassung). |
| ☐ | ○ Zeigen Sie als Benutzer mit der Rolle Now Platform sn_si.admin eine Vorschau der Daten aus Splunk Enterprise an, die für einen Now Platform Security Incident angezeigt werden.<br>○ Beheben Sie alle Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | Weitere Informationen finden Sie unter Zeigen Sie eine Vorschau des Security Incident für die Splunk Enterprise Security Event Ingestion-Integration an. |
| ☐ | Planen Sie als Benutzer mit der Rolle Now Platform sn_si.admin den Warnungsabruf für ein Profil mit einer geplanten Warnung.<br><br>Weitere Informationen finden Sie unter Planen und rufen Sie neue und aktualisierte wichtige Events für die Splunk Enterprise Security Event Ingestion-Integration ab. |

Sie haben die Setup-Schritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration überprüft.

## Integration mit Splunk - Incident Enrichment

Die Integration Splunk – Incident-Ergänzung durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

| | |
|---|---|
| Erkunden<br><br>Integrationen mit Security Incident Response | Einrichtung<br><br>Erste Schritte mit der Splunk -Suchintegration für Security Operations |
| Verwenden<br><br>• Führen Sie eine Sichtungssuche aus<br>• Security Operations Integration - Sichtungs-such-Workflow<br>• Security Operations Integration - Splunk-Sichtungssuch-Workflow<br>• Sichtungssuchdetails anzeigen<br>• Sichtungssuchergebnisse anzeigen | Entwickeln<br><br>• ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und zusätzliche Informationen<br><br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Erste Schritte mit der Splunk -Suchintegration für Security Operations

Die SoftwareSplunk durchsucht, überwacht und analysiert maschinell generierte Big Data und lässt sich problemlos in Security Operationsintegrieren. Bevor Sie die Integration Splunk – Incident-Anreicherung verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und die entsprechende API-Basis-URL und Anmeldeinformationen hinzufügen.



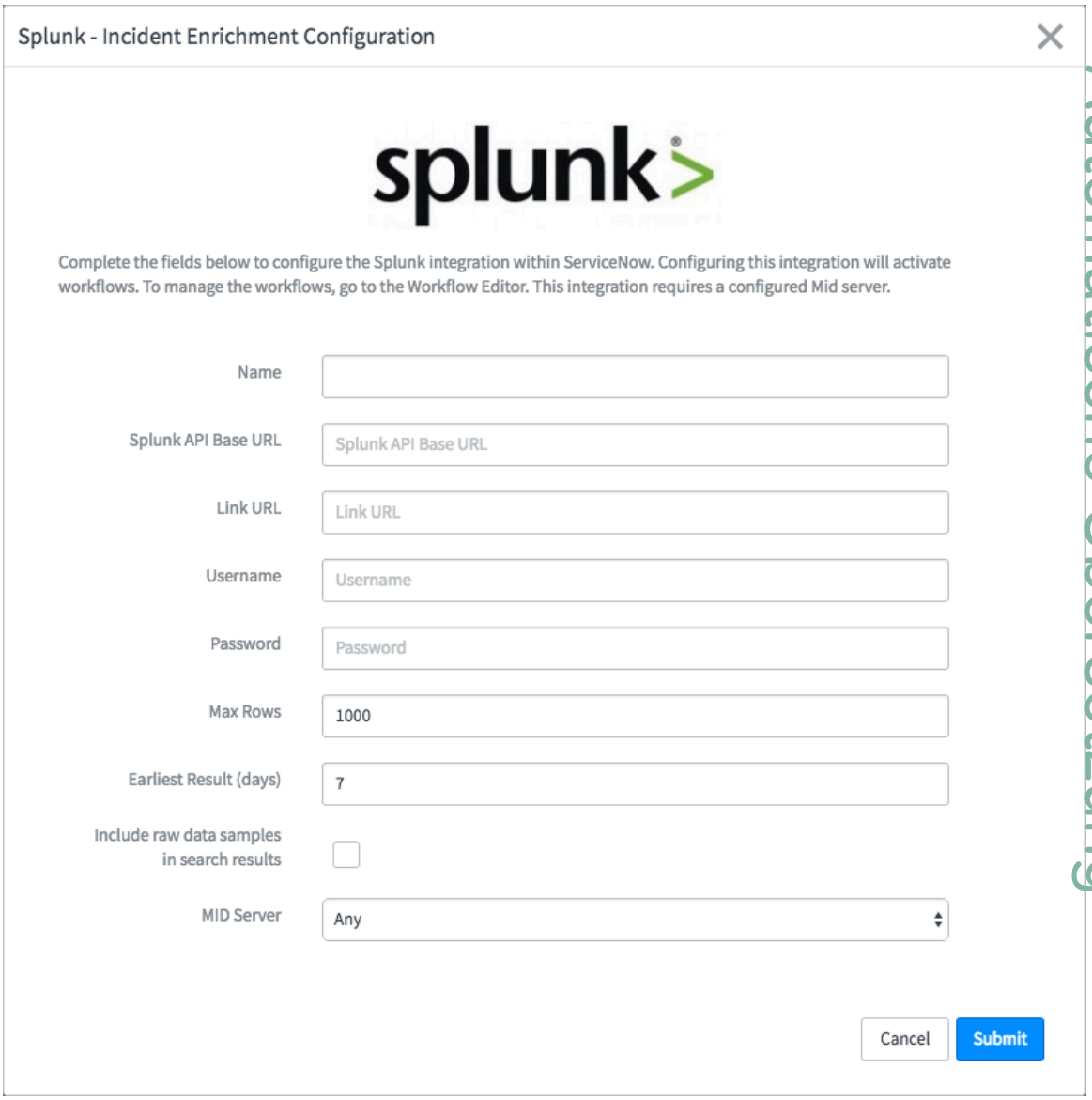
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_si_admin

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf Splunk zu, und rufen Sie den API-Schlüssel und die API-ID unter Ihrem Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie in der Karte „Splunk – Incident-Ergänzung“ auf **Neu**.




5. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name dieser Konfiguration. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Basis-URL der Splunk-API | Die Basis-URL, die Sie von der Website Splunk erhalten haben. |
| Link-URL | [Optional] Die Link-URL, die auf die Webschnittstelle Splunk verweist, sofern verfügbar. |
| Benutzername | Ihr Splunk-Benutzername. |
| Passwort | Ihr Splunk-Passwort. |
| Max. Zeilen | Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. |
| Erstes Ergebnis (Tage) | Die frühesten Ergebnisse, die Sie anzeigen möchten, in Tagen. |
| Rohdatenmuster in Suchergebnissen berücksichtigen | Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in der Eigenschaft „ **Anzahl der Zeilen der Rohdaten“** in Security Incident Response-Eigenschaftenab. |
| MID-Server | Wählen Sie **Beliebig** aus, um einen beliebigen aktiven MID Server zu verwenden, oder wählen Sie einen bestimmten MID Server-Namen aus. |

**Hinweis:**
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum **Workflow-Editor**.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf **Konfigurieren** oder **Löschen** klicken, um die Konfiguration zu ändern oder zu löschen.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie in der Dropdown-Liste **Konfigurationen** anzeigen die Option **Nein** aus.

## Integration „Tanium-Endpunktplattform“

Tanium-Endpunktplattform verwendet einen Workflow und Workflow-Aktivitäten, um laufende Prozesse für betroffene CIs zurückzugeben.

| | |
|---|---|
| Erkunden<br><br>Security Incident Response-Integrationen | Einrichtung<br><br>• Tanium-Endpunktplattform Integrationen-Setup<br>• Aktivieren und konfigurieren Sie die Integration von Security Operations Tanium<br>• Für MID Server-Zugriff konfigurieren<br>• Aktualisieren Sie Ihr X.509-Zertifikat |
| Verwenden<br><br>• Tanium – Workflow „Laufende Prozesse abrufen“.<br>• Tanium – Dateidetails-Workflow abrufen | Entwickeln<br><br>• ServiceNow Security Operations Entwicklungs-richtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | • Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und zusätzliche Hilfe<br><br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Tanium-Endpunktplattform Integrationen-Setup

Bevor Sie die Tanium-Integration verwenden können, müssen Sie das Plugin aktivieren und die Integration konfigurieren. Bei Bedarf müssen Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Immer wenn ein CI zu einem offenen Security Incident in Security Incident Responsehinzugefügt wird, wird der Workflow **Tanium – Laufende Prozesse abrufen** ausgelöst, wenn der Datensatz gespeichert wird. Tanium wird eine Frage zum Abrufen von Prozessen gestellt, und Tanium gibt die laufenden Prozesse für das betroffene CI in einer Tabelle zurück. Weitere Informationen zum Workflow und den zugehörigen Workflow-Aktivitäten finden Sie unter Tanium – Workflow „Laufende Prozesse abrufen“..

### Aktivieren und konfigurieren Sie die Integration von Security Operations Tanium

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich Tanium Integration, schnell aktivieren und einrichten. Bevor Sie die Tanium-Endpunktplattform -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

## Vorbereitungen

Erforderliche Rolle: sn_si_admin

## Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie auf der Tanium-Karte auf **Konfigurieren**.
4. Füllen Sie die entsprechenden Felder im Formular „Tanium-Konfiguration“ aus.

| Feld | Beschreibung |
|---|---|
| Tanium-Server-URL | Die URL für den Zugriff auf den SOAP-Endpunkt des Tanium-Servers. Normalerweise hat die URL ein ähnliches Format wie https://tanium.server.local/soap. Eine IP-Adresse kann ebenfalls verwendet werden. Beispiel: https//12.13.14.15/soap. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Tanium-Benutzername und -Passwort | Benutzername und Passwort für den Tanium-Integrationsadministrator (für Tanium Version 6.1 und höher). |
| Tanium-Sitzung (vor 6.1) | Der Tanium-Sitzungs-SOAP-Schlüssel (für Tanium-Versionen vor 6.1). Bei Installationen von Tanium 6.1 und höher bleibt dieses Feld normalerweise leer. |
| Sensor für laufende Prozesse | Der Name des zu verwendenden Sensors für laufende Prozesse. Beispiel: **Laufende Prozesse**. |
| IP-Adresssensor | Der Name des IP-Adresssensors, der zur Beschränkung einer Abfrage auf einen Satz bestimmter Clientcomputer verwendet werden soll. Beispiel: **IP-Adresse**. |
| Indexdateisensor | Der Name des Sensors, der zum Abrufen von Dateidetails verwendet wird. Dieses Feld ist standardmäßig auf Indexabfrage-Dateidetails festgelegt. |
| Max. Indexdateieinträge pro IP | Grenzwert für die Anzahl der pro Computer zurückgegebenen Dateien in einer Abfrage zum Abrufen von Dateidetails. Der Standardwert dieses Felds ist 10. |
| MID-Server verwenden | Wenn sich der Tanium-Server hinter einem MID-Server befindet, müssen die Anmeldeinformationen für die Authentifizierung im Textkörper der SOAP-Nachrichten enthalten sein. Die Anmeldeinformationen werden zusammen mit dem Rest des SOAP-Nachrichtentexts als Nur-Text im externen Kommunikationskanal (ECC-Warteschlange) gespeichert. |

5. Klicken Sie auf **Absenden**, um die Integrationskonfiguration zu speichern.

### Für MID Server-Zugriff konfigurieren

Wenn sich der Tanium-Server hinter einem MID-Server befindet, führen Sie diese zusätzlichen Konfigurationsschritte aus, um Anforderungen über den MID-Server weiterzuleiten. Alle über einen MID-Server gesendeten SOAP-Nachrichten werden asynchron ausgeführt.

#### Vorbereitungen

Erforderliche Rolle: admin

Es muss ein laufender MID Server vorhanden sein, der Ihrer Instanz zugeordnet ist.

Im Formular „Tanium-Konfiguration“ müssen Sie das Kontrollkästchen **MID Server** verwenden aktivieren.

#### Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **SOAP-Nachricht**.
2. Suchen Sie **Tanium-Server**und klicken Sie darauf.
3. Klicken Sie auf die Registerkarte **SOAP-Nachrichtenfunktionen**.
4. Legen Sie für jede der folgenden drei Funktionen das Feld **MID-Server** mit dem entsprechenden MID-Server fest, der für die Kommunikation mit dem Tanium-Server verwendet wird.
   - Laufende Prozesse abrufen – AddObject
   - GetResultData
   - GetResultInfo
5. Klicken Sie auf **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie für die Integration eine SSL-Verbindung benötigen, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie in der Adresszeile auf das Sperrsymbol.

   c. Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
   Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu**, und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

**Hinweis:**
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

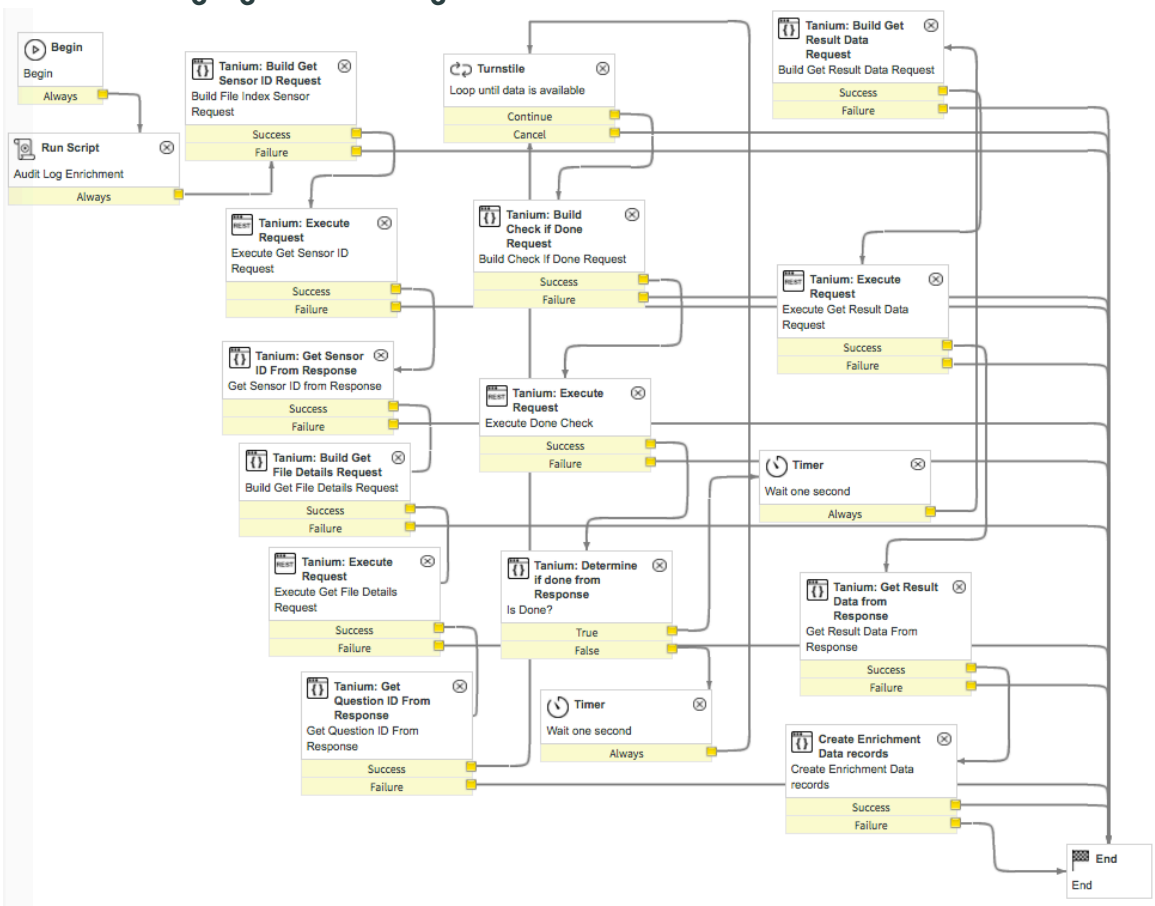
### Tanium – Dateidetails-Workflow abrufen

Dieser Workflow fragt den Tanium-Server nach Dateien mit einem bestimmten Hashwert oder Dateinamen ab. Die Aktivitäten erfassen die Ergebnisse und speichern sie als Ergänzungsdaten zu einem Security Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Sicherheitsvorgänge Tanium-Integration – Dateidetails abrufen-Workflow**




**Hinweis:**
Dieser Workflow veranschaulicht, wie Sie den Tanium-Server nach Dateien mit einem bestimmten Hashwert oder Dateinamen abfragen, die Daten erfassen und als Ergänzungsdaten für einen Security Incident speichern können. In seiner aktuellen Implementierung gibt der Workflow die angereicherten Daten nicht zur Verwendung durch das System zurück. Es wird bereitgestellt, um den Prozess zu veranschaulichen, mit dem Sie die Effektivität Ihrer Security Incident-Untersuchung erhöhen können.

Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Tanium: Aktivität zum Abrufen der Sensor-ID-Anforderung erstellen

Diese Aktivität verwendet einen Sensornamen und erstellt eine Anforderung, um eine Suche auf dem Tanium-Server durchzuführen. Sie gibt eine Sensor-ID zurück, die von nachfolgenden Aktivitäten verwendet wird.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| sensor_name [Zeichenfolge] | Eine Zeichenfolge, die den Sensornamen identifiziert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Aktivität „Sensor-ID aus Antwort abrufen“.

Diese Aktivität verarbeitet den als Eingabe bereitgestellten SOAP-Antworttext und gibt die entsprechende Sensor-ID aus.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | SOAP-Antworttext, der von Tanium zurückgegeben wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| sensor_id [Zeichenfolge] | Zeichenfolgensensor-ID, die dem angeforderten Sensor zugeordnet ist. |

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Frage-ID aus Antwortaktivität abrufen

Diese Workflow-Aktivität verarbeitet den Antworttext, um die Frage-ID zu erhalten.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der SOAP-Antworttext. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Tanium-Server zurückgegebene Frage-ID. |

#### Tanium: Aktivität „Überprüfen, ob fertig“ erstellt

Diese Workflow-Aktivität erstellt eine Anforderung des Tanium -Servers, um zu überprüfen, ob die Datenerfassung für die Frage abgeschlossen ist. Sie gibt die verschlüsselte Anforderung und andere Komponenten zurück, die zum Ausführen der Anforderung erforderlich sind.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Server Tanium zurückgegebene Frage-ID. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

#### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

#### Tanium: Bestimmen Sie, ob dies über die Antwortaktivität erfolgt

Diese Workflow-Aktivität bestimmt basierend auf dem Antworttext, ob eine Anforderung abgeschlossen wurde.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der von Tanium zurückgegebene SOAP-Anforderungstext. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| fertig [Boolean] | Gibt „true“ zurück, wenn die Anforderungsverarbeitung abgeschlossen ist. |

### Tanium: Aktivität „Ergebnisdatenanforderung abrufen“ erstellen

Dieser Workflow erstellt eine Anforderung zum Sammeln aller Daten, die von Tanium als Antwort auf eine Frage zurückgegeben werden. Er verwendet eine Frage-ID als Eingabe und stellt die Ausgabe zur Ausführung der Anforderung bereit, einschließlich einer verschlüsselten SOAP-Umschlagnutzlast.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Zeichenfolge] | Frage-ID der an Tanium gestellten Frage |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Eingabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Ergebnisdaten aus Antwortaktivität abrufen

Die Workflow-Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ verarbeitet den Antworttext aus den Ergebnisdaten und gibt ein Array von JSON-Objekten aus, die die Ergebnisse von Tanium darstellen.

Die Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ kann mit jedem Workflow verwendet werden, um Ergebnisdaten abzurufen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergebnisdaten abgerufen. |
| Fehler | Keine Daten abgerufen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| response_body | Verschlüsselte SOAP-Antwortinhalte |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| „implementierung_id“. | Implementierungsbezeichner. |
| impacted_ci | Betroffenes Konfigurationselement. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

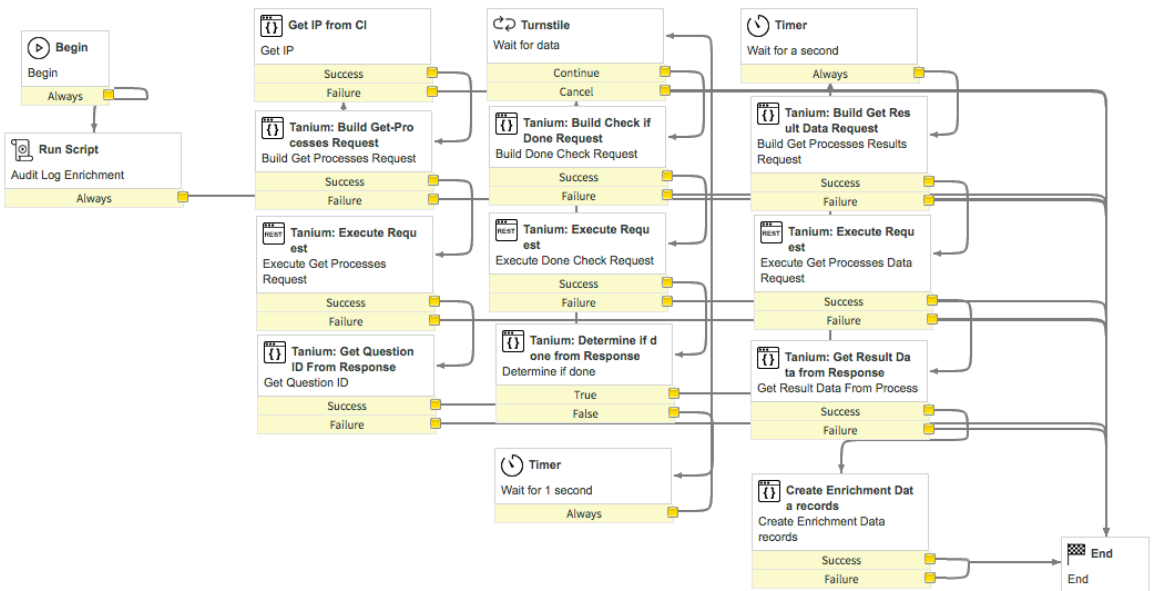
| Variable | Beschreibung |
|---|---|
| result_data | Array-Elementtyp von API-Variablen. Jedes Array enthält Schlüssel-Wert-Paare, die aus der Spalte und den vom Server zurückgegebenen Werten bestehen. Wenn keine Daten vom Server empfangen werden, ist die Ausgabe ein leeres Array. |
| Ausgabe | Formatierte Rückgabedaten zu laufenden Prozessen, die vom abstrakten Workflow verwendet werden. |

### Tanium – Workflow „Laufende Prozesse abrufen“.

Dieser Workflow erstellt einen Audit-Pfad, und die Aktivität Tanium: Get-Processes Question verwendet die IPv4-Adresse des CI als Eingabe und führt eine Abfrage auf dem Tanium-Server aus. Die Ausgabe ist eine Liste aller laufenden Prozesse auf dem betroffenen CI.

#### Sicherheitsvorgänge Tanium-Integration – Laufende Prozesse abrufen Workflow

Wenn das Feld **Configuration Item** in einem Security Incident geändert wird, wird dieser Workflow gestartet.




## Funktionsweise des Workflows

Bei Angabe einer Zeichenfolgen-Frage-ID (normalerweise das Ergebnis eines AddObject-Befehls) fragt die Aktivität „ **Tanium: Überprüfen, ob** abgeschlossen“ den Tanium-Server ab, um zu überprüfen, ob die Datenerfassung abgeschlossen ist. Diese Aktivität verwendet die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Skripteinbindung sn_sec_tanium.TaniumEndpointUtil** und basiert auf der SOAP-Nachricht **GetResultInfo** Tanium-Server.

Wenn die **Aktivität „Tanium: Überprüfen, ob abgeschlossen“ „** true“ zurückgibt, erfasst die Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ alle Daten, die vom Tanium-Server als Antwort auf die Frage „Get-Processes“ zurückgegeben werden. Die Ausgabe besteht aus einem Array von Objekten, die jeweils Schlüssel-Wert-Paare enthalten, die aus der Spalte und den vom Server zurückgegebenen Werten bestehen. Wenn keine Daten vom Server empfangen werden, ist die Ausgabe ein leeres Array.

Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### IP aus CI-Aktivität abrufen

Diese Workflow-Aktivität bestimmt die IPv4-Adresse, die einem Konfigurationselement (CI) zugeordnet ist.

Die Aktivität **IP aus CI** abrufen kann mit jedem Workflow verwendet werden, um die IPv4-Adresse eines CI abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| ci_sys_id [Zeichenfolge] | Systembezeichner des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| ip_addr [Zeichenfolge] | IPv4-Adresse Wenn die IP-Adresse nicht bestimmt werden kann, ist dieser Wert leer. |

## Austrittsbedingungen

Mögliche Ergebnisse für diese Aktivität sind:

**Bedingungen**

| Bedingung | Beschreibung |
|---|---|
| Erfolg | Eine IPv4-Adresse wurde zurückgegeben. |
| Fehler | Es konnte keine IPv4-Adresse ermittelt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Tanium: Anforderungsaktivität „Get-Processes“ erstellen

Diese Workflow-Aktivität verwendet die IPv4-Adresse eines CI, das einem Security Incident hinzugefügt wurde, und erstellt eine Anforderung an den Tanium-Server für alle laufenden Prozesse für dieses CI. Die Ausgabe sind die Details, die für die Ausführung der Anforderung erforderlich sind, wobei die Nutzlast verschlüsselt ist.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| ci_ip_address [Zeichenfolge] | Die IPv4-Adresse des CI, das einem Security Incident hinzugefügt wurde Dieses Eingabefeld ist ein Pflichtfeld. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Aktivität „Überprüfen, ob fertig“ erstellt

Diese Workflow-Aktivität erstellt eine Anforderung des Tanium -Servers, um zu überprüfen, ob die Datenerfassung für die Frage abgeschlossen ist. Sie gibt die verschlüsselte Anforderung und andere Komponenten zurück, die zum Ausführen der Anforderung erforderlich sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Server Tanium zurückgegebene Frage-ID. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Aktivität „Ergebnisdatenanforderung abrufen“ erstellen

Dieser Workflow erstellt eine Anforderung zum Sammeln aller Daten, die von Tanium als Antwort auf eine Frage zurückgegeben werden. Er verwendet eine Frage-ID als Eingabe und stellt die Ausgabe zur Ausführung der Anforderung bereit, einschließlich einer verschlüsselten SOAP-Umschlagnutzlast.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Zeichenfolge] | Frage-ID der an Tanium gestellten Frage |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Bestimmen Sie, ob dies über die Antwortaktivität erfolgt

Diese Workflow-Aktivität bestimmt basierend auf dem Antworttext, ob eine Anforderung abgeschlossen wurde.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der von Tanium zurückgegebene SOAP-Anforderungstext. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| fertig [Boolean] | Gibt „true“ zurück, wenn die Anforderungsverarbeitung abgeschlossen ist. |

## Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Tanium: Frage-ID aus Antwortaktivität abrufen

Diese Workflow-Aktivität verarbeitet den Antworttext, um die Frage-ID zu erhalten.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der SOAP-Antworttext. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Tanium-Server zurückgegebene Frage-ID. |

### Tanium: Ergebnisdaten aus Antwortaktivität abrufen

Die Workflow-Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ verarbeitet den Antworttext aus den Ergebnisdaten und gibt ein Array von JSON-Objekten aus, die die Ergebnisse von Tanium darstellen.

Die Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ kann mit jedem Workflow verwendet werden, um Ergebnisdaten abzurufen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergebnisdaten abgerufen. |
| Fehler | Keine Daten abgerufen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| response_body | Verschlüsselte SOAP-Antwortinhalte |
| „implementierung_id“. | Implementierungsbezeichner. |
| impacted_ci | Betroffenes Konfigurationselement. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| result_data | Array-Elementtyp von API-Variablen. Jedes Array enthält Schlüssel-Wert-Paare, die aus der Spalte und den vom Server zurückgegebenen Werten bestehen. Wenn keine Daten vom Server empfangen werden, ist die Ausgabe ein leeres Array. |
| Ausgabe | Formatierte Rückgabedaten zu laufenden Prozessen, die vom abstrakten Workflow verwendet werden. |

## Mobile Experience für Security Incident Response

Verwenden Sie Ihr Android- oder iOS-Mobilgerät, um Ihre Aufgaben im Security Operations Center (SOC) zu verwalten.

### Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

### Security Incident Response

Wenn Sie mit den grundlegenden Konzepten des Produkts Security Incident Response ( SIR) in Ihrer Instanz von Now Platform® ] nicht vertraut sind, finden Sie unter Security Incident Response-Übersicht weitere Informationen zu Threat Intelligence und wie dieses Produkt Ihnen helfen kann, Cyberbedrohungen für Ihre Organisation zu priorisieren und zu beheben.

### Übersicht

Als SOC-Manager (Security Operations Center) oder Benutzer mit der Rolle „ Now Platform Sicherheitsanalyst“ (sn_si.analyst) können Sie sich direkt über Ihr Mobilgerät bei einer Now Platform -Instanz anmelden. Mit Security Incident Response Mobile-Appkönnen Sie Ihre aktuellen und kritischsten SIR Security Incidents und Reaktionsaufgaben anzeigen, bearbeiten und zuweisen. Benachrichtigungen informieren Sie, wenn Ihnen zugewiesene kritische Security Incidents eintreffen.

Mit Security Incident Response Mobile-Appkönnen Sie die folgenden SIR -bezogenen Aufgaben von Ihrem Mobilgerät aus ausführen:

- Zeigen Sie eine Liste der kritischen Security Incidents und Reaktionsaufgaben an.
- Erhalten Sie detaillierte Benachrichtigungen für Security Incidents und Aufgaben, die vordefinierte Benachrichtigungskriterien erfüllen.
- Zeigen Sie Gruppierungen von Security Incidents oder Aufgaben an, die auf einem vordefinierten Satz von Abfragen oder Filtern basieren.
- Zeigen Sie die Arbeitsnotizen und zugehörigen Listen von Security Incidents an.
- Aktualisieren Sie Security Incidents, und fügen Sie Arbeitsnotizen oder Anhänge hinzu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bearbeiten Sie die Felder in Security Incidents.
- Weisen Sie Security Incidents sich selbst oder anderen Mitgliedern Ihres Sicherheitsteams zu.

Wenn sie ausgefüllt sind, können Sie die folgenden zugehörigen Listen zu SIR Security Incidents mit dem Security Incident Response Mobile-Appanzeigen:

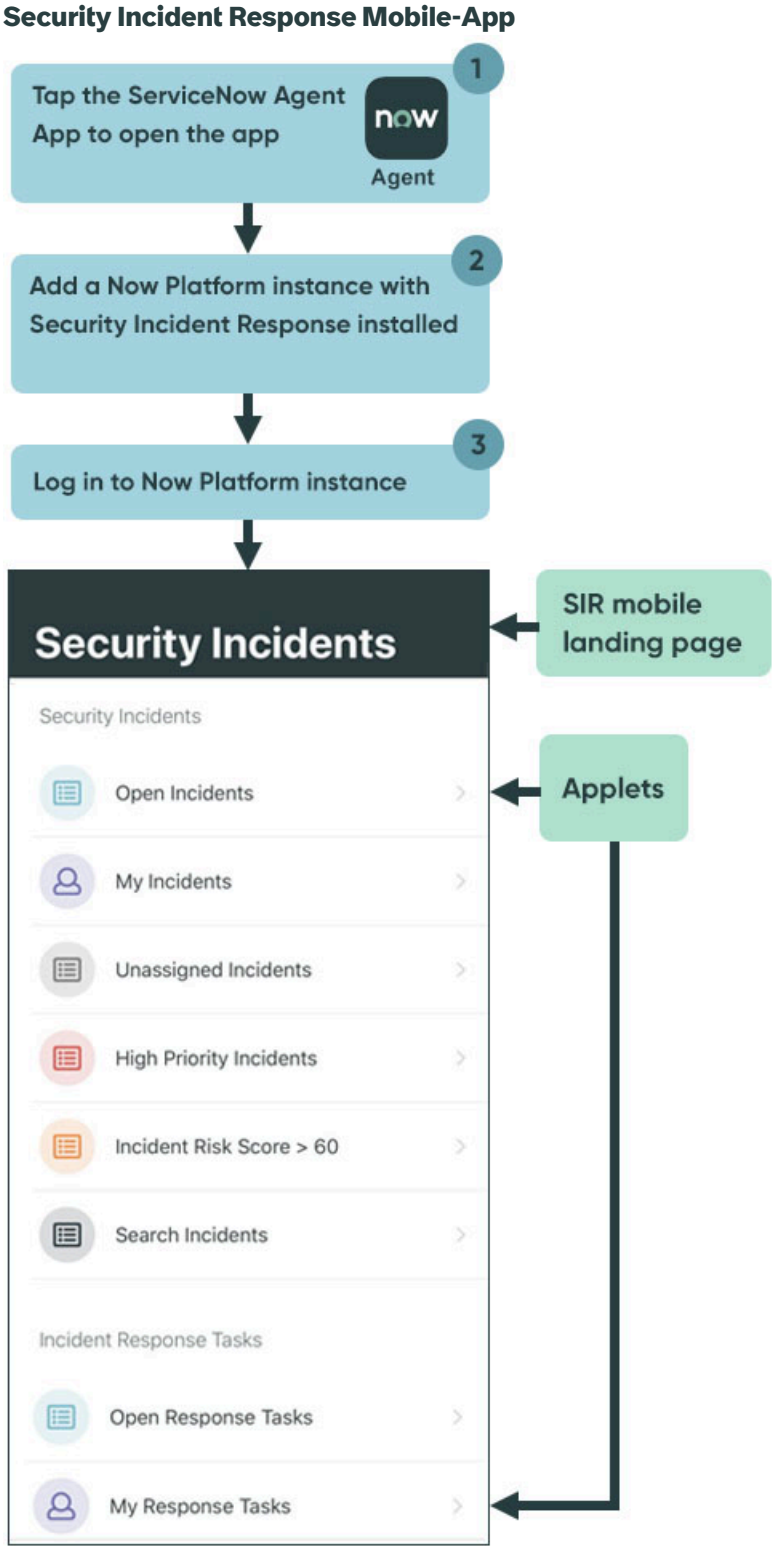
- Konfigurationselement
- Betroffener Anwender
- Betroffene Services
- Untergeordnete Security Incidents
- Ähnliche Security Incidents (von Now Platform nicht unterstützt)
- Erkennbare Elemente
- Antwortaufgaben
- Aufgaben
- Aufgaben-SLA
- Anhänge (von Now Platform nicht unterstützt)

Die folgende Abbildung zeigt, wie Sie sich von Ihrem Mobilgerät aus bei der Instanz Now Platform anmelden und wie der Zielbildschirm von Security Incident Response Mobile-App aufgebaut ist, der nach der Anmeldung abgespielt wird.

Eine Schritt-für-Schritt-Anleitung zum Einrichten der Instanz Now Platform und zur Installation von Security Incident Response Mobile-Appfinden Sie unter Richten Sie eine Prüfliste für ein Security Incident Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich beim an Security Incident Response Mobile-App.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Automatische Übersetzung

**Anwendungen**

Anwendungen sind die ServiceNow® -Softwarekomponenten wie Security Incident Response (SIR), Vulnerability Response (VR) und Governance, Risk und Compliance (GRC), die bestimmte Features und Funktionen in Ihrer Now Platform -Instanz bereitstellen. Nachdem Sie die Kernanwendung Security Incident Response und Security Incident Response Mobile-App in Ihrer Instanz von Now Platform installiert haben, wird das Symbol für die Kernanwendung nach der Anmeldung unten auf Ihrem Mobilgerät Android oder iOS angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident Response Mobile-App Symbol (Security Incidents).**

**Ordner**

Jede ServiceNow® Mobile Anwendung enthält Ordner, die die Applets nach Kategorien trennen. In der vorherigen Abbildung der Zielseite sind „ **Security Incidents** “ und „ **Reaktionsaufgaben** für Incidents“ Ordner.

**Applets**

Applets sind die verschiedenen Optionen in der Anwendung. Die Symbole unter den Abschnitten „ **Security Incidents** “ und „ **Aufgaben zur Reaktion** auf Incidents“ sind die verfügbaren Applets von Security Incident Response Mobile-App.

## Richten Sie eine Prüfliste für ein Security Incident Response Mobile-App

Die folgende Prüfliste enthält die Setupaufgaben, die Sie in Ihrer Instanz Now Platform® und auf Ihrem Mobilgerät ausführen müssen, bevor Sie Security Incident Response Mobile-Appverwenden können.

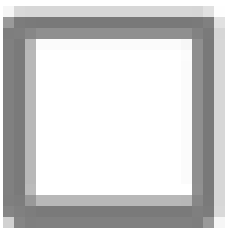
### Vorbereitungen

Alternativ können Sie diese Prüfliste drucken und sie durch die Setup-Aufgaben führen, die für Security Incident Response Mobile-Apperforderlich sind. Stellen Sie sicher, dass jedes Element in der Liste abgeschlossen ist, damit Sie SIR Security Incidents auf Ihrem Mobilgerät anzeigen und bearbeiten können.

Die Prüflistenelemente werden in hervorgehobenem Text angezeigt. Weitere Informationen folgen jedem Element in der rechten Spalte. Geschätzte Zeit bis zum Abschluss dieser Aufgabe: 15 bis 20 Minuten.

Erforderliche Rolle: admin, sn_si.analyst

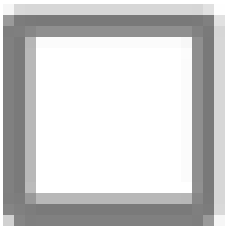
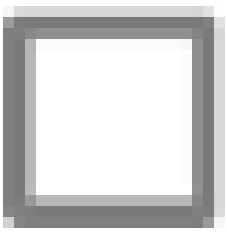
**Prüfliste für Mobilgeräte**

| Element | Beschreibung |
|---|---|
|  | Stellen Sie als Benutzer mit der Administratorrolle sicher, dass Sie die Kernanwendung Security Incident ResponseNow Platform in einer Instanz von [] installiert haben. Dies ist die Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen.<br>**Hinweis:**<br>Die Kernanwendung Security Incident Response und die Instanz Now Platform müssen aus demselben Familien-Release stammen.<br>1. Um sicherzustellen, dass die Kernanwendung in Ihrer Instanz installiert ist, navigieren Sie zu **Plugins**, und suchen Sie nach Security Incident Response.<br>2. Wenn die Kernanwendung Security Incident Response noch nicht installiert ist, klicken Sie auf **Installieren**, um sie zu installieren.<br>Weitere Informationen zur Installation der Kernanwendung Security Incident Response finden Sie unter Security Incident Response installieren und konfigurieren.<br>Wenn die Kernanwendung Security Incident Response in Plugins nicht sichtbar ist, finden Sie weitere Informationen zur Installation von |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste für Mobilgeräte (Fortsetzung)**

| Element | Beschreibung |
|---|---|
| | Kernanwendungen und Berechtigungen für Anwendungen unter Security Operations und ServiceNow Store. |
|  | Stellen Sie als Benutzer mit der Administratorrolle sicher, dass [ Now Platform in der Instanz von Security Incident Response Mobile-App installiert ist, die Sie auf Ihrem Mobilgerät anzeigen möchten.<br><br>**Hinweis:**<br>Die Instanzen Security Incident Response Mobile-App und Now Platform müssen aus demselben Familien-Release stammen.<br><br>Laden Sie Security Incident Response Mobile-App aus dem ServiceNow Store in Ihrer Now Platform -Instanz herunter, und installieren Sie sie.<br><br>Wenn Sie Security Incident Response Mobile-Appinstallieren, werden die zugehörigen Abhängigkeiten com.glide.sg und com.glide.sg.agent_native_client ebenfalls installiert.<br><br>So überprüfen Sie, ob diese Abhängigkeiten installiert sind:<br>**1.** Navigieren Sie zu **Plugins**.<br>**2.** Suchen Sie nach den Plugin-IDs (com.glide.sg und com.glide.sg.agent_native_client).<br>**3.** Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für Security Incident Response Mobile-Apperforderlich.<br><br>Weitere Informationen zur Installation von Anwendungen und Berechtigungen für Anwendungen finden Sie unter Security Operations und ServiceNow Store. |
|  | Vergewissern Sie sich als Benutzer mit der Administratorrolle Now Platform, dass Sie Mobile-Benutzern die erforderlichen Rollen in Ihrer Instanz von Now Platform zugewiesen haben.<br>**1.** Um die einem Benutzer zugewiesenen Rollen anzuzeigen, navigieren Sie zu **Benutzer und Gruppen** > **Anwender**.<br>**2.** Wählen Sie den Benutzernamen gefolgt von der zugehörigen Liste der Rollen aus. Alle diesem Benutzer zugewiesenen Rollen werden angezeigt.<br>**3.** Vergewissern Sie sich, dass ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der IT Infrastructure Library-Rolle (itil) zu. Benutzer mit der Rolle itil können Security Incidents erstellen, öffnen, aktualisieren und schließen. Nur Benutzern mit der Rolle „itil“ können Aufgaben zugewiesen werden.<br>**4.** Vergewissern Sie sich, dass ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle „Sicherheitsanalyst“ (sn_si.analyst) zu. Benutzer mit der Rolle „sn_si.analyst“ können Security Incident- |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste für Mobilgeräte (Fortsetzung)**

| Element | Beschreibung |
|---|---|
| | Datensätze lesen und bearbeiten. Diese Rolle wird automatisch hinzugefügt, wenn Sie die itil-Rolle zuweisen.<br>**5.** Vergewissern Sie sich, dass Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Benutzer zugewiesen haben.<br>**Hinweis:** Wenn Sie eine große Anzahl von Benutzern für die mobile Anwendung haben, können Sie die Rolle „sn_si.analyst“ alternativ einer Gruppe zuweisen. Jeder Benutzer, den Sie der Gruppe hinzufügen, erbt diese Rolle.<br>Weitere Informationen zu Sicherheitsanalysten finden Sie unter Zuweisen von Sicherheitsanalysten.<br>Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration . |
| ☐ | Laden Sie als Benutzer mit der Rolle „sn_si.analyst“ die aktuelle Agent-App ServiceNow® auf Ihr Mobilgerät herunter.<br>Die aktuelle Version der App „ServiceNow Agent“ ist im Apple App Store GoogleiOS und im Play Store [] verfügbar. |
| ☐ | Vergewissern Sie sich als Benutzer mit der Rolle sn_si.analyst, dass Benachrichtigungen auf Ihrem Mobilgerät und in Ihrer Now Platform -Instanz aktiviert sind.<br>Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Security Incidents zugewiesen werden. Um Sie bei der rechtzeitigen Korrektur zu unterstützen, klicken Sie nach der Aktivierung von Benachrichtigungen auf eine Benachrichtigung in Security Incident Response Mobile-App, um direkt zum Security Incident zu navigieren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste für Mobilgeräte (Fortsetzung)**

| Element | Beschreibung |
|---|---|
| | Führen Sie die folgenden Schritte aus, um Benachrichtigungen in Ihrer Now Platform -Instanz zu aktivieren, damit sie auf Ihrem Mobilgerät angezeigt werden.<br>**1.** Vergewissern Sie sich, dass Sie [] heruntergeladen und in Ihrer Instanz von Now PlatformSecurity Incident Response Mobile-App installiert haben.<br>**2.** Überprüfen Sie in den Systemeinstellungen in Ihrer Instanz Now Platform unter Benachrichtigungen, ob die **ServiceNow Mobile-Anwendung**aktiviert ist.<br>Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Benutzerbenachrichtigungseinstellungen in der Core-UI festlegen .<br>Now Platform -Benachrichtigungen werden auch auf dem Nachrichtenbildschirm Ihres Mobilgeräts angezeigt. Stellen Sie sicher, dass Benachrichtigungen auch in den Einstellungen Ihres Mobilgeräts aktiviert sind. |

Sie haben Ihr Mobilgerät und Now Platform erfolgreich für Security Incident Response Mobile-Appeingerichtet. Der nächste Schritt besteht darin, sich mit Ihrem Mobilgerät bei Ihrer Now Platform -Instanz anzumelden.

## Melden Sie sich beim an Security Incident Response Mobile-App

Öffnen Sie die Security Incident Response Mobile-App, und fügen Sie Ihrem Mobilgerät eine Now Platform® -Instanz mit Security Incident Response hinzu.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

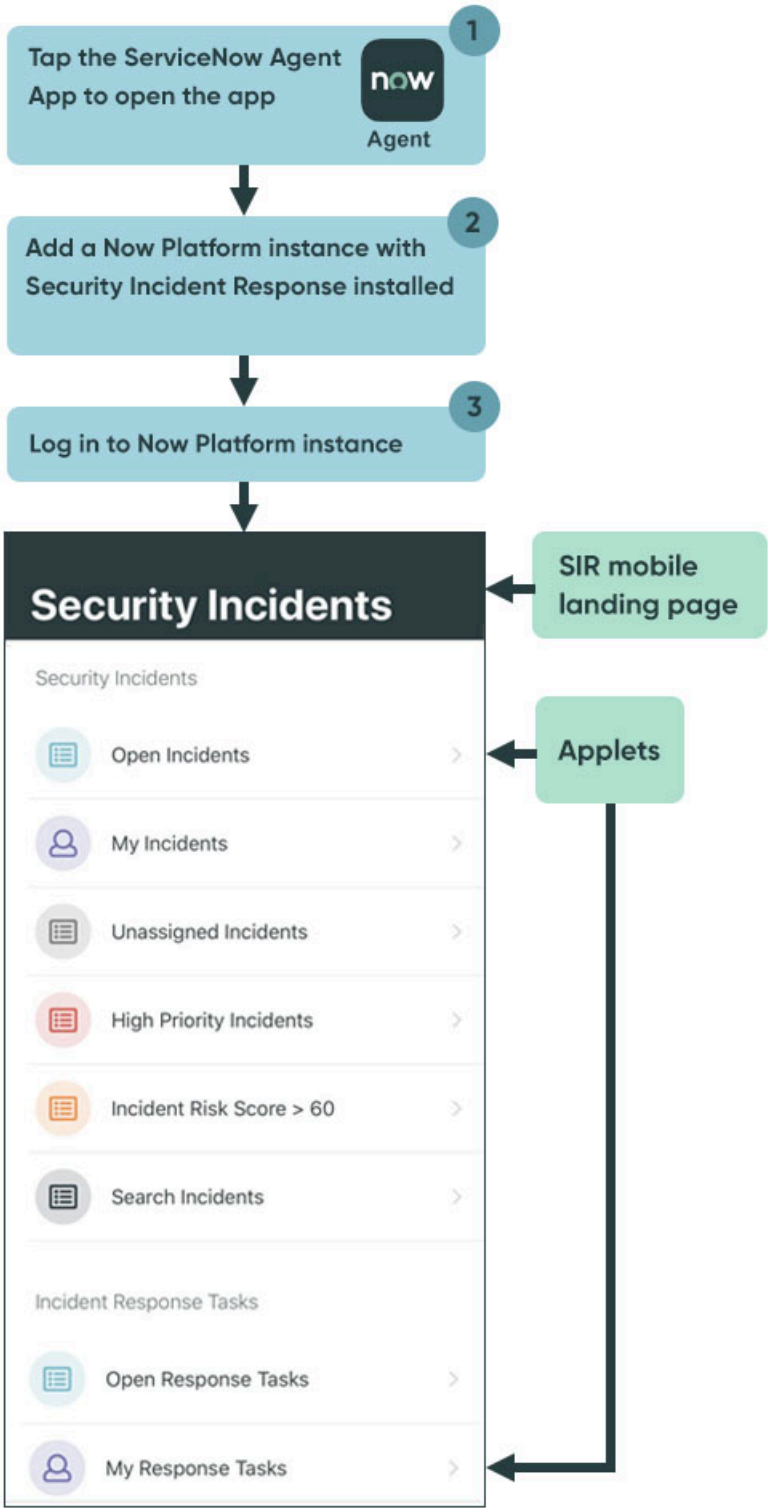
Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

Vergewissern Sie sich, dass Sie die in Richten Sie eine Prüfliste für ein Security Incident Response Mobile-Appbeschriebenen Setup-Schritte abgeschlossen haben.



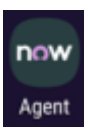
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Security Incident Response Mobile-App**




## Prozedur

**1.** Tippen Sie auf Ihrem Mobilgerät auf die App **ServiceNow Agent**, um sie zu öffnen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie noch nicht bei einer Now Platform -Instanz angemeldet sind, wird der Bildschirm „Instanzen“ angezeigt.

2. Wenn die Instanz Now Platform mit der Kernanwendung Security Incident Response noch nicht zu Ihrem Mobilgerät hinzugefügt wurde, führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

   a. Tippen Sie im angezeigten Bildschirm „Instanzen“ auf das .
   Ein Bildschirm wird angezeigt, in dem Sie aufgefordert werden, eine Adresse einer Now Platform -Instanz einzugeben und zu speichern.

   b. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Geben Sie die Instanzadresse ein, oder scannen Sie einen QR-Code. | Wählen Sie eine aus, um fortzufahren:<br>▪ Geben Sie vor .service-now.comden Namen Ihrer Instanz Now Platform ein, z. B. sirmobileny.<br>▪ Geben Sie eine Adresse ein. Diese Adresse ist die URL Ihrer Now Platform -Instanz, die Sie auf Ihrem Mobilgerät anzeigen möchten, z. B. https://sirmobileny.service-now.com.<br>▪ Scannen Sie einen QR-Code. |
| (Optional) Geben Sie einen Kurznamen ein | Geben Sie einen Spitznamen für diese Instanz ein. Wenn dem Gerät mehrere Instanzen hinzugefügt wurden, können Spitznamen Ihnen dabei helfen, eine Now Platform-Instanz schnell zu finden. |

   c. Tippen Sie auf **Speichern und anmelden**.

3. Geben Sie auf dem angezeigten Anmeldebildschirm ServiceNow den Benutzernamen und das Passwort für die Instanz Now Platform ein, die Sie hinzufügen möchten, und tippen Sie auf **Anmelden**.
   Der Zielbildschirm Security Incidents wird angezeigt. Sie haben sich erfolgreich bei Security Incident Response Mobile-Appangemeldet.
4. Überprüfen Sie nach der Anmeldung, ob Benachrichtigungen in Security Incident Response Mobile-Appaktiviert sind.

   a. Tippen Sie unten im Zielbildschirm auf **Benachrichtigung**.

   b. Tippen Sie im Bildschirm „Benachrichtigungen“ auf **Benachrichtigungen** aktivieren, wenn diese Option nicht aktiviert ist.
   Benachrichtigungen von Now Platform werden auf dem Bildschirm „Benachrichtigungen“ in Security Incident Response Mobile-App] angezeigt.

5. Nachdem Sie sich bei einer Instanz auf Ihrem Mobilgerät angemeldet haben, ist dies die Standardinstanz Now Platform auf dem Gerät.
   Wenn Sie eine andere Now Platform auf dem Gerät anzeigen möchten, müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

   a. Tippen Sie auf das Einstellungssymbol.

   b. Tippen **Sie auf Abmelden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bildschirm „Instanzen“ wird mit allen Now Platform Instanzen angezeigt, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich anzumelden, oder führen Sie alternativ die vorherigen Schritte aus, um eine weitere Instanz hinzuzufügen.

Wenn der Instanzbildschirm für Security Incident Response Mobile-App nicht angezeigt wird, nachdem Sie auf Ihrem Gerät auf die **ServiceNow Agent** -App getippt haben, stellen Sie sicher, dass **ServiceNow Agent** als vertrauenswürdige App auf Ihrem Gerät zugelassen ist. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und der allgemeinen Geräteverwaltung, und tippen Sie auf die Option (App vertrauen usw.), um den Zugriff zu gewähren.

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie Ihre Anmeldeinformationen auf dem Anmeldebildschirm eingegeben haben, überprüfen Sie, ob Ihr Benutzername und Ihr Passwort für die Instanz Now Platform korrekt sind.

Wenn Sie Probleme beim Anzeigen des Zielbildschirms haben, überprüfen Sie Ihre Netzwerkverbindung.

Wenn Sie den Bildschirm „Instanzen“ nicht anzeigen können, nachdem Sie auf die **ServiceNow Agent** -App getippt haben, versuchen Sie, sie von Ihrem Gerät zu deinstallieren. Vergewissern Sie sich, dass Sie die aktuelle Version der App aus dem Apple iOS App Store oder dem Google Play Store haben, und versuchen Sie, sie erneut zu installieren.

## Mit dem können Sie offene Security Incidents anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Als Security Incident-Analyst können Sie offene Security Incident Response (SIR) Security Incidents auf Ihrem Mobilgerät anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Auditpfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie sich in der Liste der Datensätze einen offenen Security Incident zu, oder weisen Sie ihn neu zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

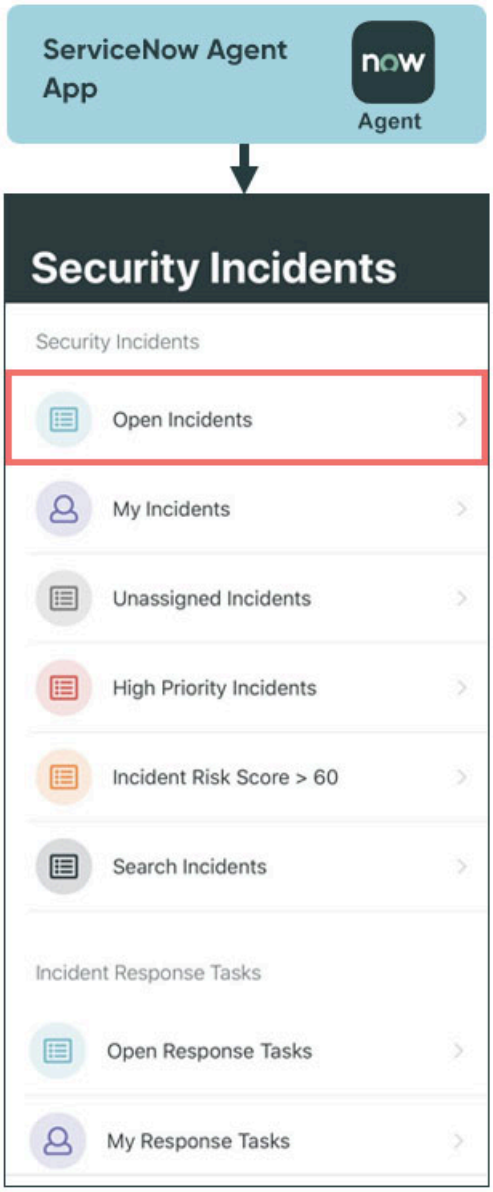
### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Tippen Sie auf der Zielseite von Security Incidents auf **Offene Incidents**.

Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.



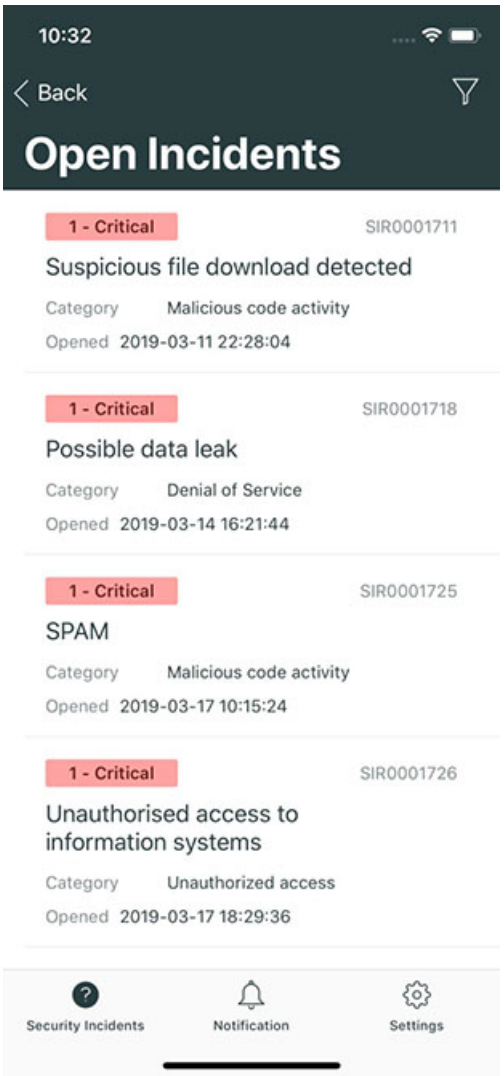
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der Bildschirm „Offene Incidents“ wird mit einer Liste offener Security Incident-Datensätze angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

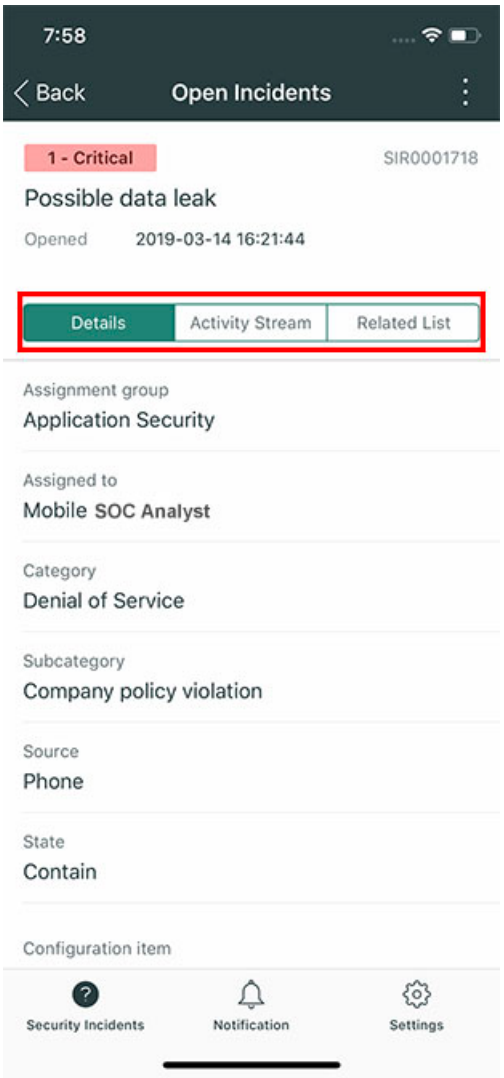



3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.
4. Um einen Incident sich selbst zuzuweisen oder ihn direkt aus der Liste der offenen Security Incidents neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.
5. Wählen Sie eine Option aus dem angezeigten Menü aus, um fortzufahren.
6. Alternativ können Sie im Bildschirm „Offene Incidents“ auf einen Datensatz in der Liste tippen, um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Mit dem können Sie Ihnen zugewiesene Security Incidents anzeigen, bearbeiten und neu zuweisen Security Incident Response Mobile-App

Als Security Incident-Analyst können Sie Security Incident Response (SIR) Incidents anzeigen, bearbeiten und neu zuweisen, die Ihnen zugewiesen sind. Zeigen Sie zugehörige Listen und den Auditpfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

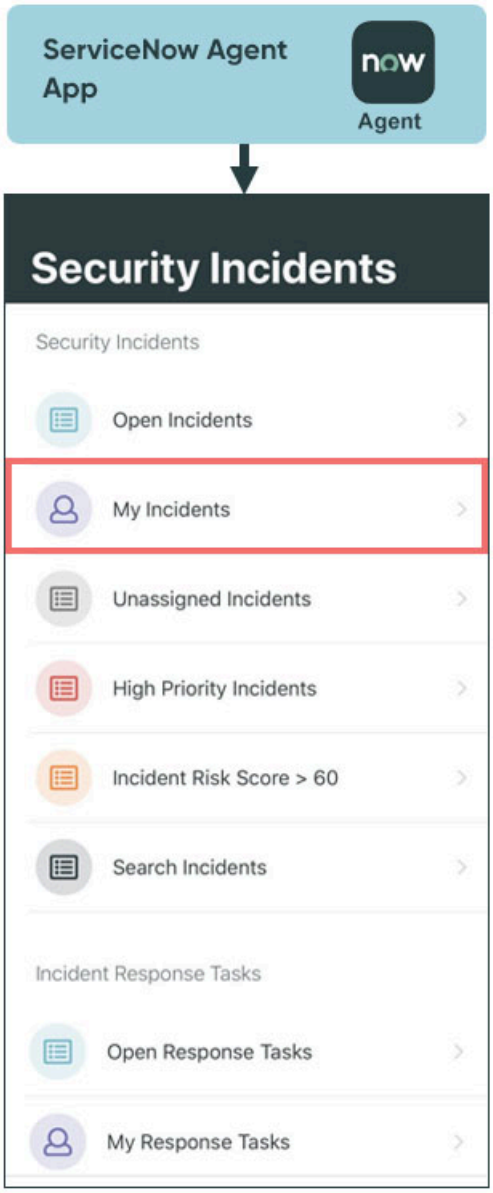
Weisen Sie einen offenen Security Incident aus der Liste der Datensätze einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Tippen Sie im Zielbildschirm von Security Incidents auf **Meine Incidents**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

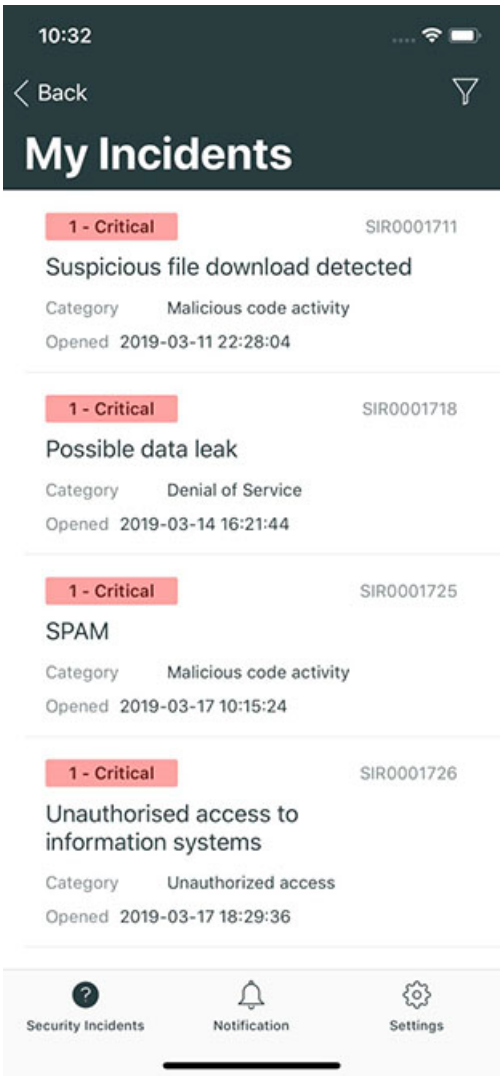
Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm Meine Incidents wird mit einer Liste offener Security Incident-Datensätze angezeigt, die Ihnen zugewiesen sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



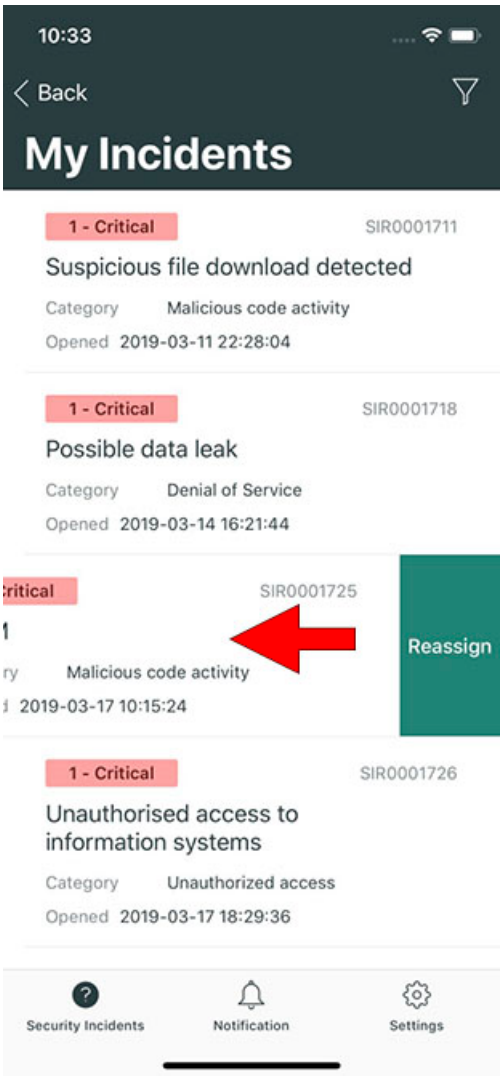

3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.

4. Um einen Incident direkt aus der Liste neu zuzuweisen, wischen Sie in der Liste der offenen Security Incident-Datensätze auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



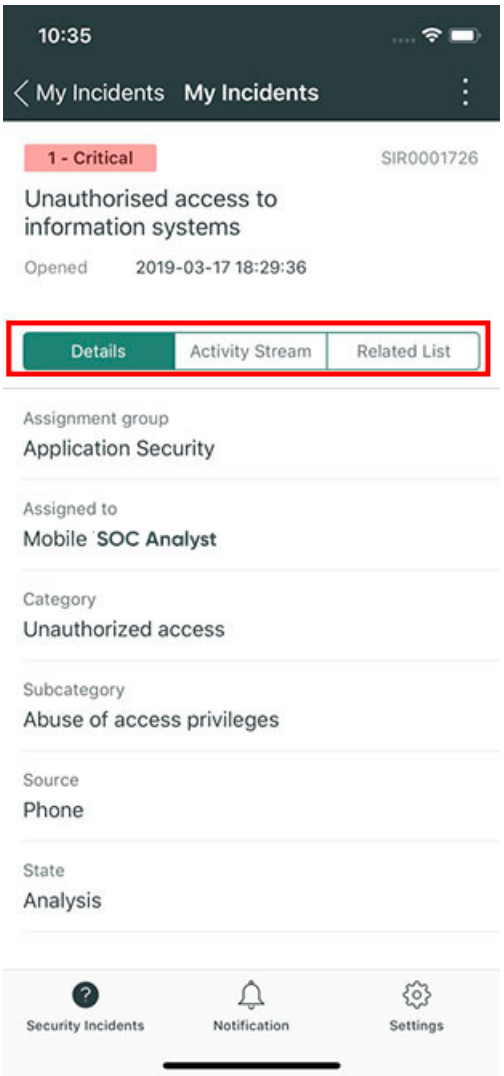

5. Bearbeiten Sie im angezeigten Menü die Felder Zuweisungsgruppe oder Zugewiesen an.

6. Um die Details des offenen Security Incident-Datensatzes anzuzeigen, tippen Sie im angezeigten Bildschirm „Meine Incidents“ auf einen Datensatz in der Liste.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Mit können Sie nicht zugewiesene Security Incidents anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Auf Ihrem Mobilgerät können Sie nicht zugewiesene Security Incident Response (SIR) Incidents anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Auditpfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie in der Liste der Datensätze einen offenen, nicht zugewiesenen Security Incident sich selbst oder einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

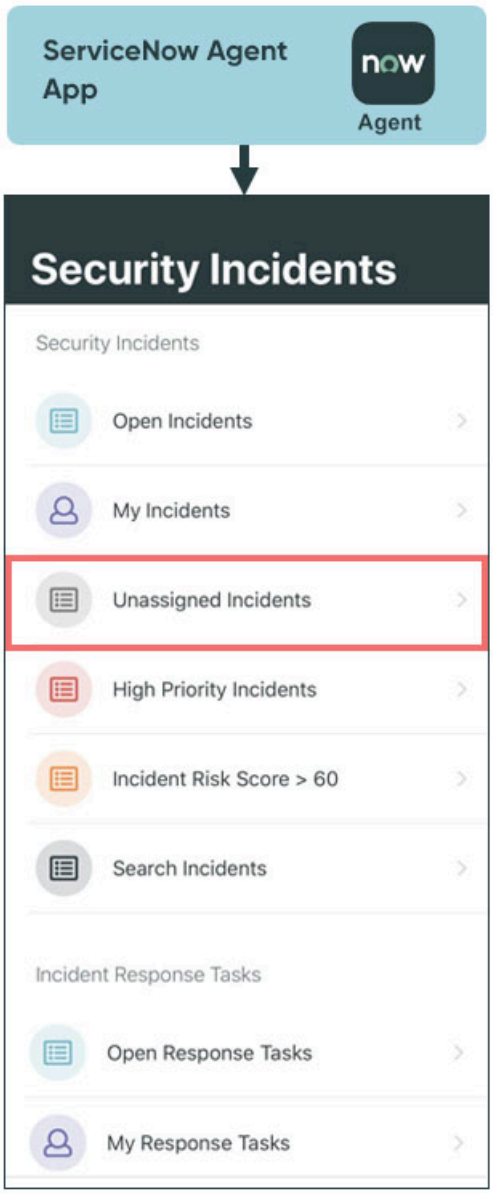


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Wenn der Zielbildschirm für Security Incidents angezeigt wird, tippen Sie auf **Nicht zugewiesene Incidents**.

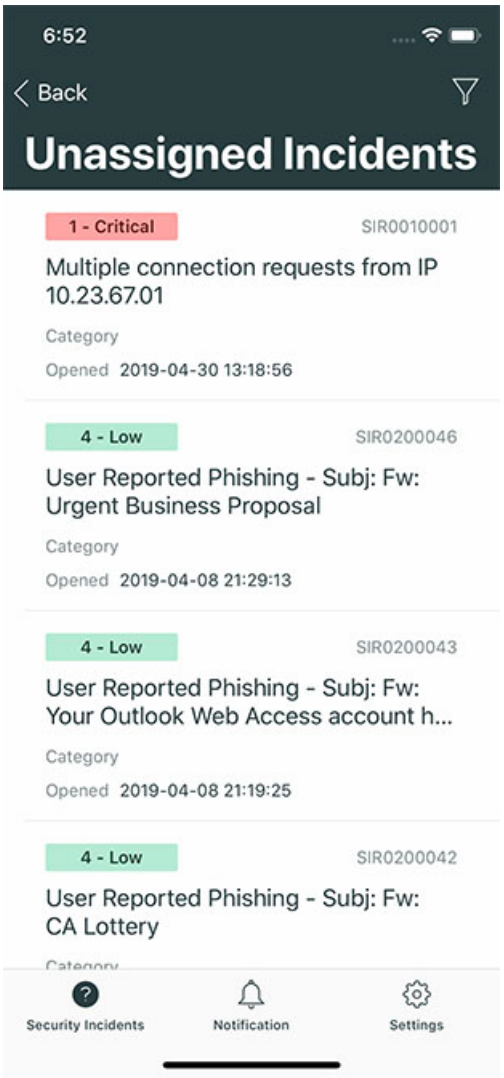
   Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm Nicht zugewiesene Incidents wird mit einer Liste nicht zugewiesener Security Incident-Datensätze angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



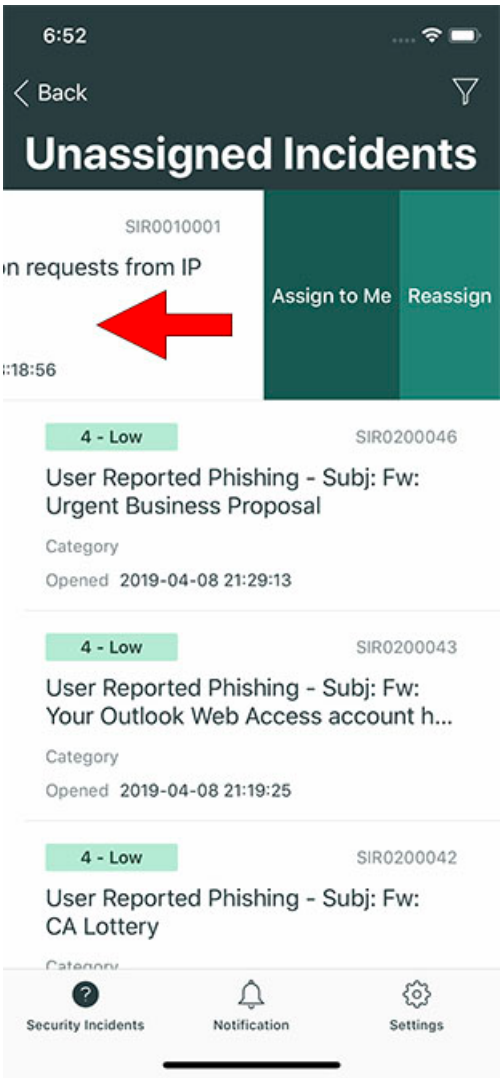

3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.

4. Um einen offenen Security Incident-Datensatz direkt aus der Liste zuzuweisen oder neu zuzuweisen, wischen Sie in der Liste der offenen, nicht zugewiesenen Security Incident-Datensätze auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



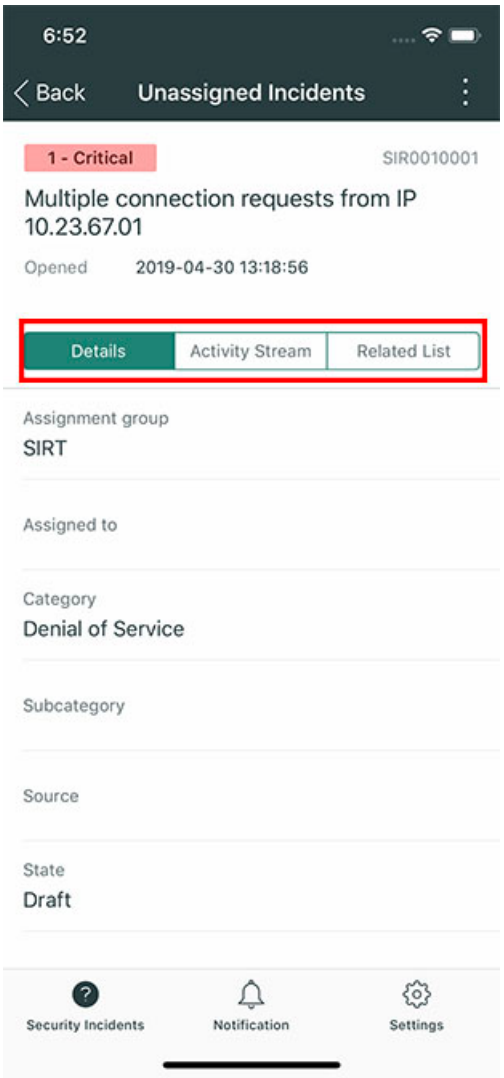

5. Wählen Sie eine Option aus dem Menü aus, um fortzufahren.

6. Alternativ können Sie bei angezeigtem Bildschirm Nicht zugewiesene Incidents auf einen Datensatz in der Liste tippen.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Mit können Sie Incidents mit hoher Priorität anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Auf Ihrem Mobilgerät können Sie Incidents mit hoher Priorität Security Incident Response (SIR) anzeigen, bearbeiten und zuweisen. Zeigen Sie zugehörige Listen und den Auditpfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

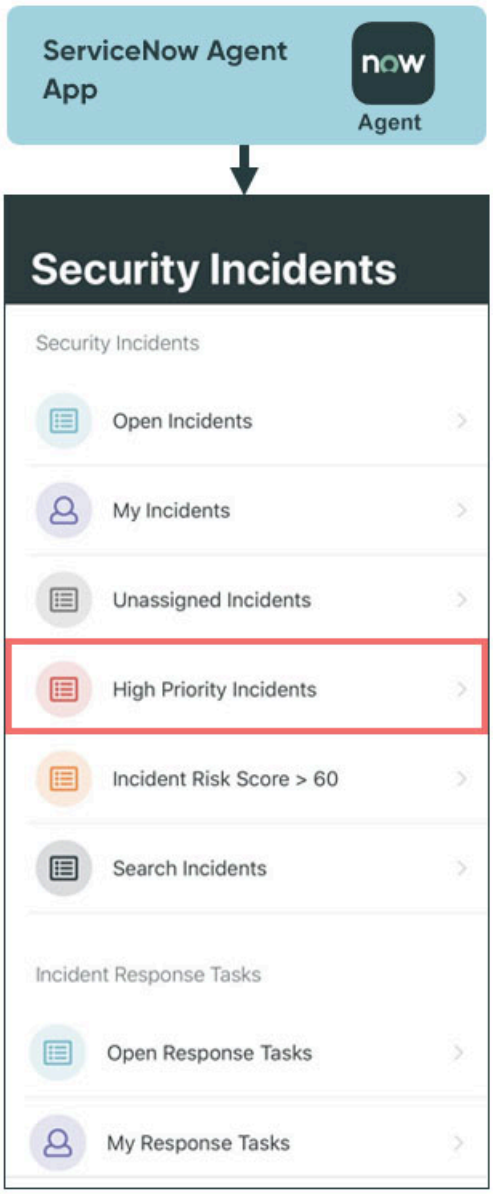
Weisen Sie in der Liste der Datensätze einen offenen, kritischen Security Incident sich selbst oder einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Wenn der Zielbildschirm für Security Incidents angezeigt wird, tippen Sie auf **Incidents mit hoher Priorität**.

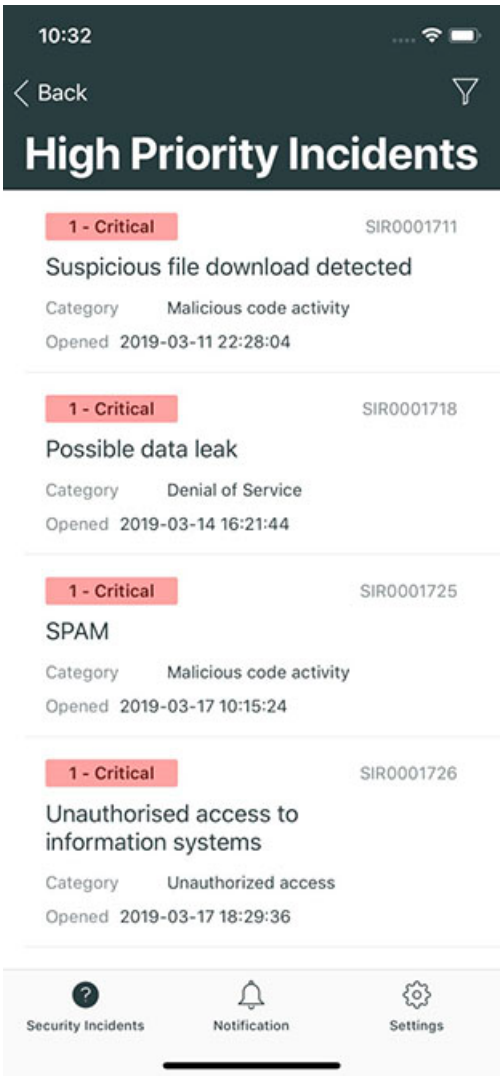
   Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm Incidents mit hoher Priorität wird mit einer Liste der kritischen Security Incidents (mit hoher Priorität) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



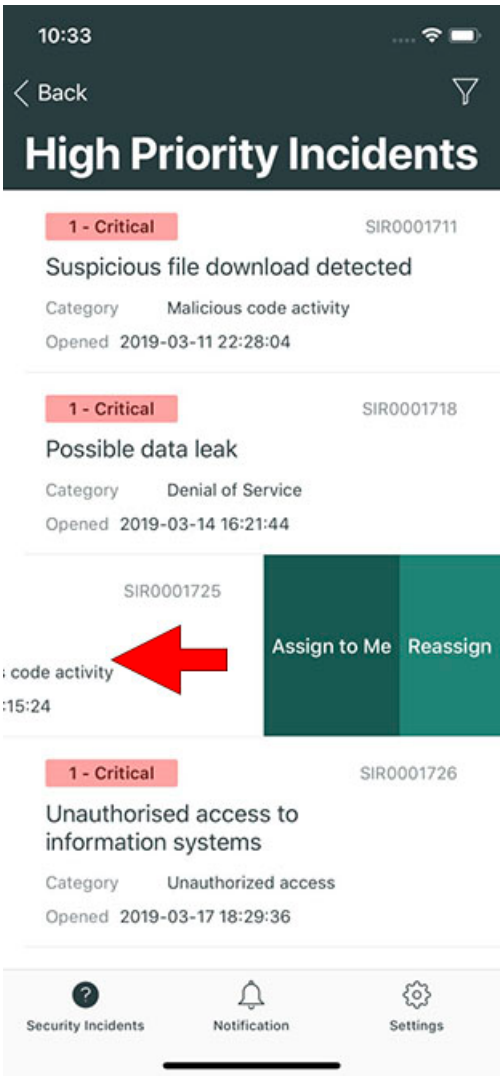

3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.

4. Wenn die Liste der offenen Security Incident-Datensätze mit hoher Priorität angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



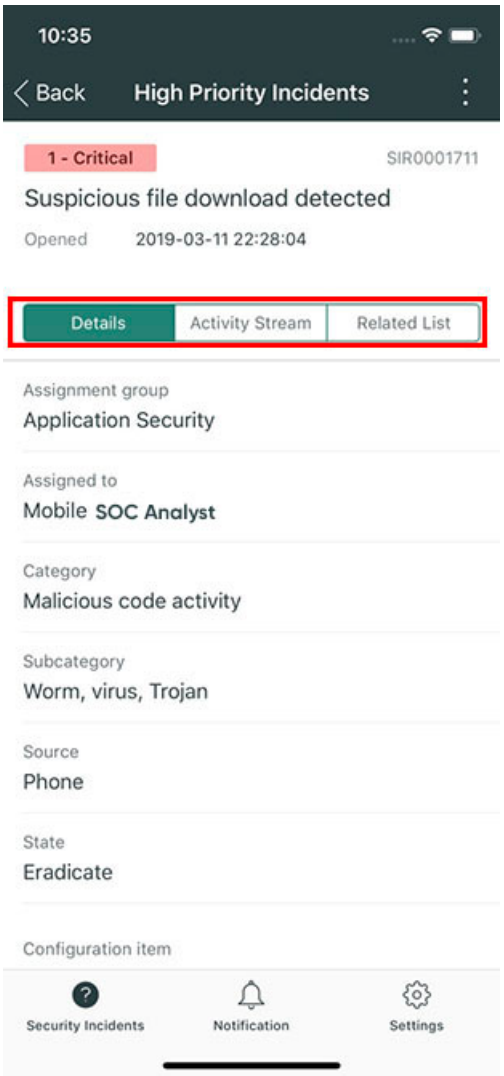

5. Wählen Sie eine, um fortzufahren.

6. Um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, tippen Sie im angezeigten Bildschirm „Incidents mit hoher Priorität“ auf einen Datensatz in der Liste.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Mit dem können Sie Security Incidents mit einer Risikopunktzahl von mehr als 60 anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Zeigen Sie auf Ihrem Mobilgerät Security Incident Response (SIR) Incidents mit einem Wert im Feld „Risikopunktzahl“ an, der größer als 60 ist, und bearbeiten Sie sie. Zeigen Sie zugehörige Listen und den Auditpfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

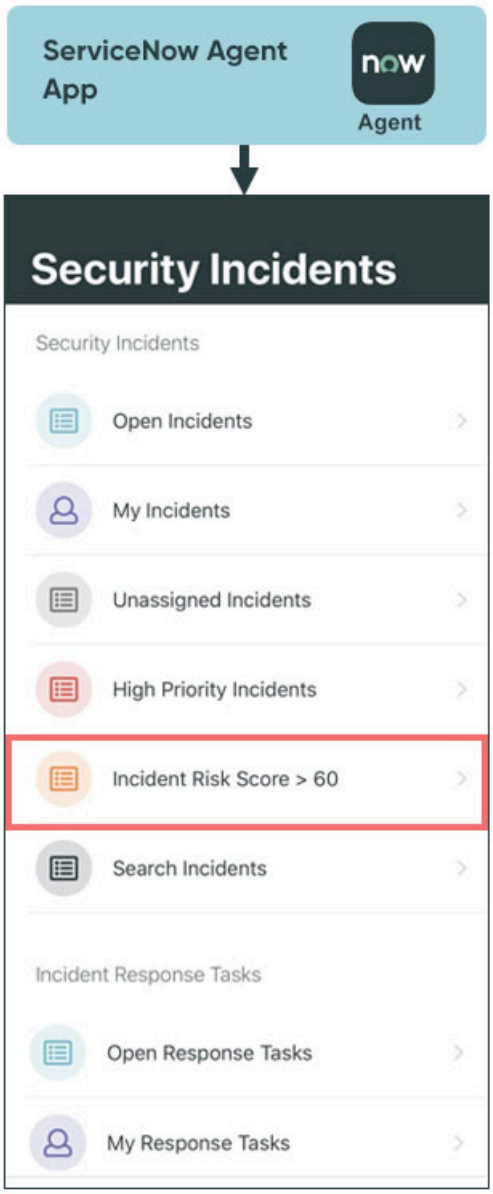
Weisen Sie aus der Liste der Datensätze einen offenen Security Incident mit einer Risikopunktzahl größer als 60 sich selbst oder einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Tippen Sie im Zielbildschirm von Security Incidents auf **Risikopunktzahl > 60**.

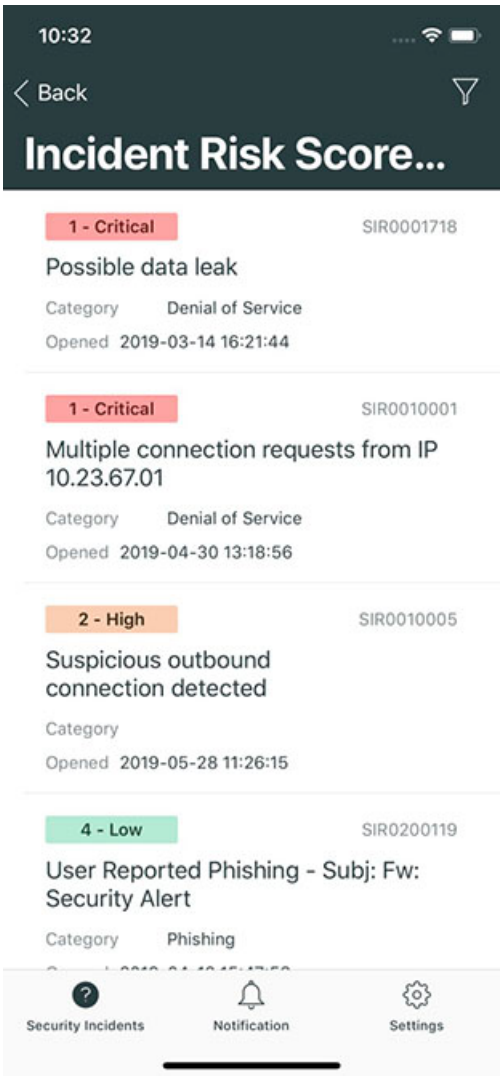
   Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm „Incident-Risikopunktzahl“ wird mit einer Liste von Security Incidents angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



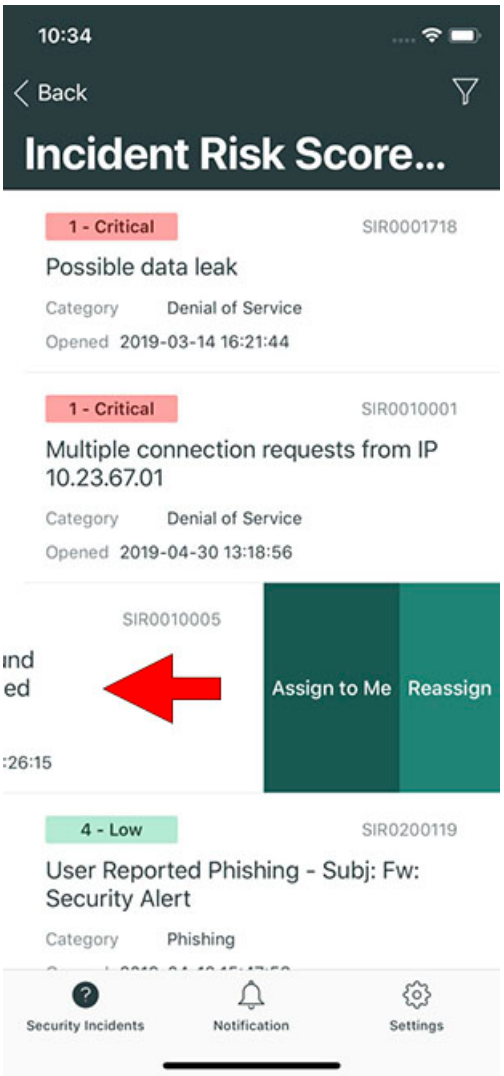

3. **Wahlweise:** Informationen zur Suche nach Security Incidents, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.

4. Um einen Security Incident sich selbst zuzuweisen oder ihn direkt aus der Liste der angezeigten offenen Security Incident-Datensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

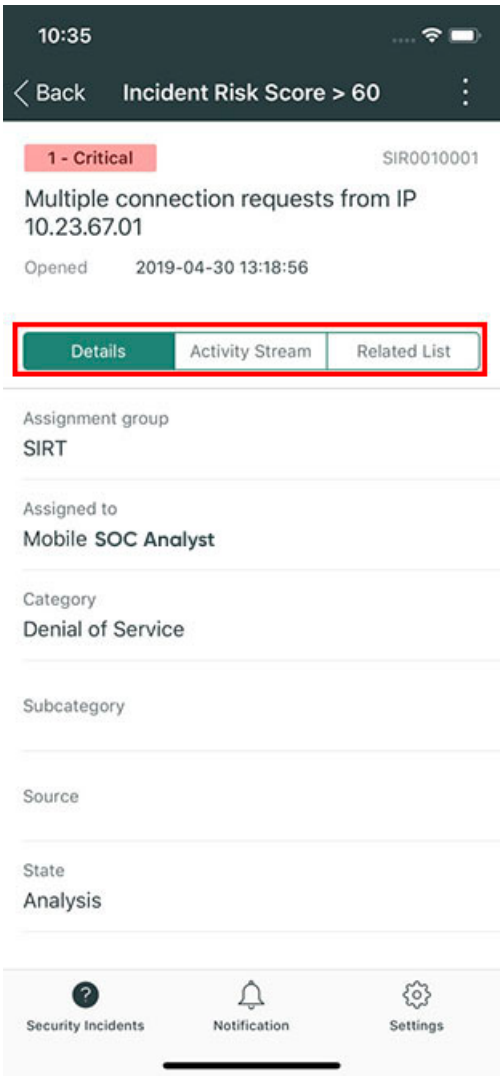



5. Wählen Sie eine, um fortzufahren.

6. Alternativ können Sie im Bildschirm „Incident-Risikopunktzahl“ auf einen Datensatz in der Liste tippen, um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App

Suchen Sie nach Security Incident Response (SIR) Security Incidents in einer Now Platform® -Instanz. Es werden nur Incidents angezeigt, die den von Ihnen eingegebenen spezifischen Suchkriterien entsprechen.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

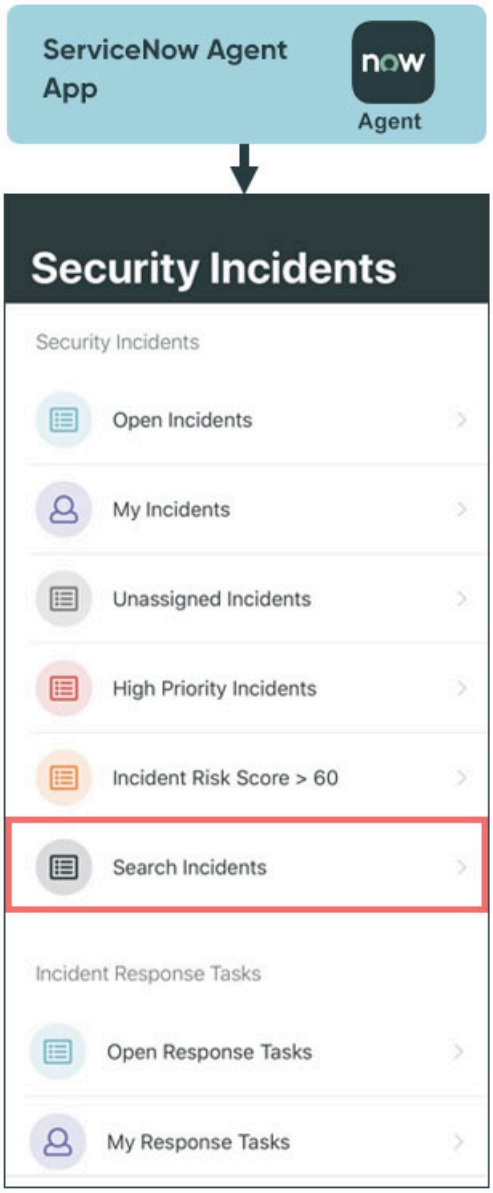
Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Wenn der Zielbildschirm „Security Incidents“ angezeigt wird, tippen **Sie auf Incidents durchsuchen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie nach der Anmeldung den Security Incident Response Mobile-App verlassen, können Sie jederzeit auf den Now Agent tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




3. Um die Anzahl der zurückgegebenen Suchergebnisse zu begrenzen, füllen Sie im Formular möglicherweise so viele Felder wie möglich aus.
   Informationen zum Hinzufügen von Suchkriterien finden Sie in der folgenden Tabelle. Befolgen Sie die Anweisungen nach der Tabelle, um vorhandene Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu übermitteln.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | Zum Hinzufügen von und Eingabe auf iOS -Geräten |
|---|---|---|
| Nummer | Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004. Diese Nummer | Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004. Diese Nummer |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | Zum Hinzufügen von und Eingabe auf iOS -Geräten |
|---|---|---|
| | wird oben rechts im Security Incident angezeigt.<br><br>Die Funktion sucht nach numerischen Zeichenfolgen und partiellen numerischen Zeichenfolgen. Geben Sie für eine detailliertere Suche weitere Ziffern ein. Platzhalter (*) werden nicht akzeptiert.<br><br>Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder auf das , um eine Suche zu übermitteln. | wird oben rechts im Security Incident angezeigt.<br><br>Die Funktion sucht nach numerischen Zeichenfolgen und partiellen numerischen Zeichenfolgen. Geben Sie für eine detailliertere Suche weitere Ziffern ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder auf Suche, um eine **Suche** zu übermitteln. |
| Kurzbeschreibung | Geben Sie Text in das Feld ein, z. B. Malware.<br><br>Die Funktion durchsucht Textzeichenfolgen und Teiltextzeichenfolgen aus dem Feld Kurzbeschreibung. Geben Sie für eine detailliertere Suche mehr Text ein. Platzhalter (*) werden nicht akzeptiert.<br><br>Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder auf das , um eine Suche zu übermitteln. | Geben Sie Text in das Feld ein, z. B. Malware.<br><br>Die Funktion durchsucht Textzeichenfolgen und Teiltextzeichenfolgen aus dem Feld Kurzbeschreibung. Geben Sie für eine detailliertere Suche mehr Text ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien einzugeben, oder auf Suche, um eine **Suche** zu übermitteln. |
| Priorität | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchensymbol, um zum Bildschirm Incidents durchsuchen zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren. |
| Kategorie | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchensymbol, um zum | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | Zum Hinzufügen von und Eingabe auf iOS -Geräten |
|---|---|---|
| | Bildschirm Incidents durchsuchen zurückzukehren. | |
| Status | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchensymbol, um zum Bildschirm Incidents durchsuchen zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren. |
| Zugewiesen an | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. |
| Zuweisungsgruppe | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. |

Wählen Sie für Android -Geräte bei angezeigtem Bildschirm „Incidents suchen“ und Eingabe aller Kriterien eines aus, um fortzufahren.

4. Wählen Sie für iOS -Geräte bei angezeigtem Bildschirm „Incidents durchsuchen“ eines aus, um fortzufahren.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie Filtern Sie Datensätze mit Security Incident Response Mobile-App, um die Suchergebnisse einzugrenzen.

## Mit dem können Sie offene Antwortaufgaben anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Offene Antwortaufgaben anzeigen, bearbeiten und zuweisen. Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incident gespeichert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

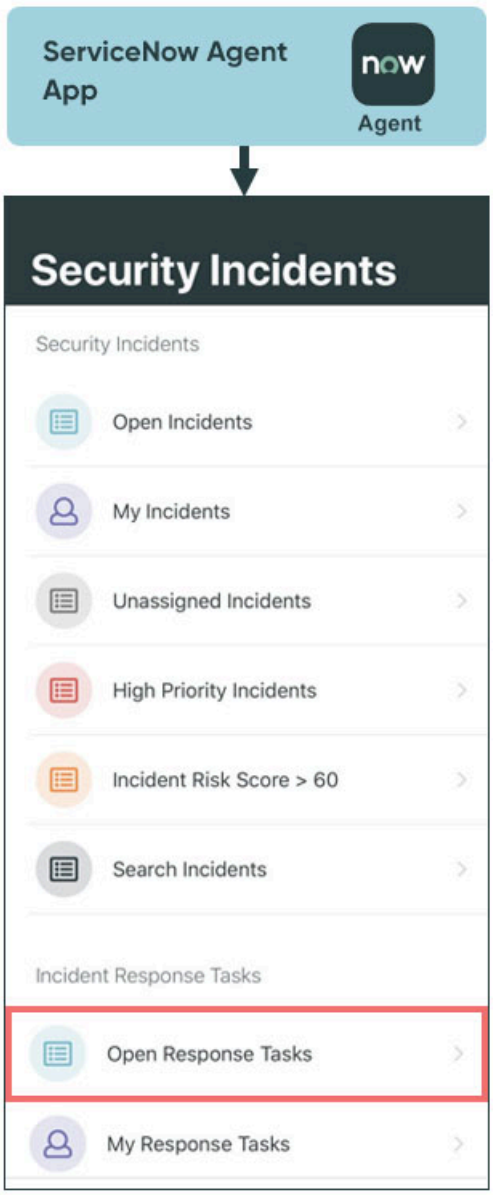
## Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie sich selbst oder einem anderen Analysten in Ihrer Gruppe aus der Liste der Datensätze eine offene, nicht zugewiesene Antwortaufgabe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

## Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Tippen Sie im Zielbildschirm von Security Incidents auf **Offene Antwortaufgaben**.

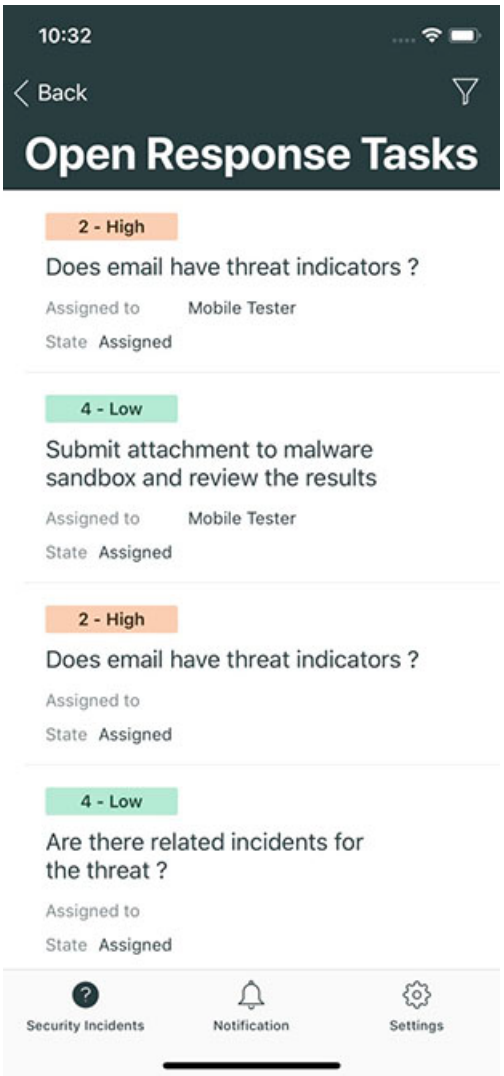
   Wenn Sie Security Incident Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm Offene Antwortaufgaben wird mit einer Liste offener Aufgaben angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

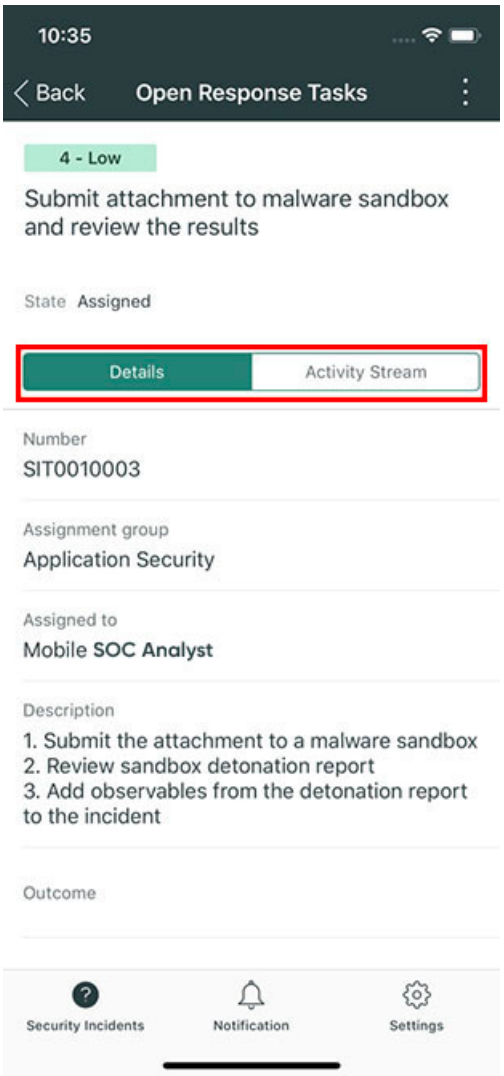



3. **Wahlweise:** Informationen zur Suche nach Aufgaben, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.
4. Wenn die Liste der offenen Antwortaufgaben angezeigt wird und Sie sie direkt aus der Liste zuweisen oder neu zuweisen möchten, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.
5. Wählen Sie eine, um fortzufahren.
6. Alternativ können Sie zum Anzeigen der Details eines offenen Antwortaufgabendatensatzes im angezeigten Bildschirm „Offene Antwortaufgaben“ auf einen Datensatz in der Liste tippen.
7. Wenn die Registerkarten im Antwortaufgabendatensatz angezeigt werden, wählen Sie eine aus der folgenden Tabelle aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Mit dem können Sie Ihre Antwortaufgaben anzeigen, bearbeiten und neu zuweisen Security Incident Response Mobile-App

Ihnen zugewiesene Antwortaufgaben anzeigen, bearbeiten und neu zuweisen. Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incident gespeichert.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

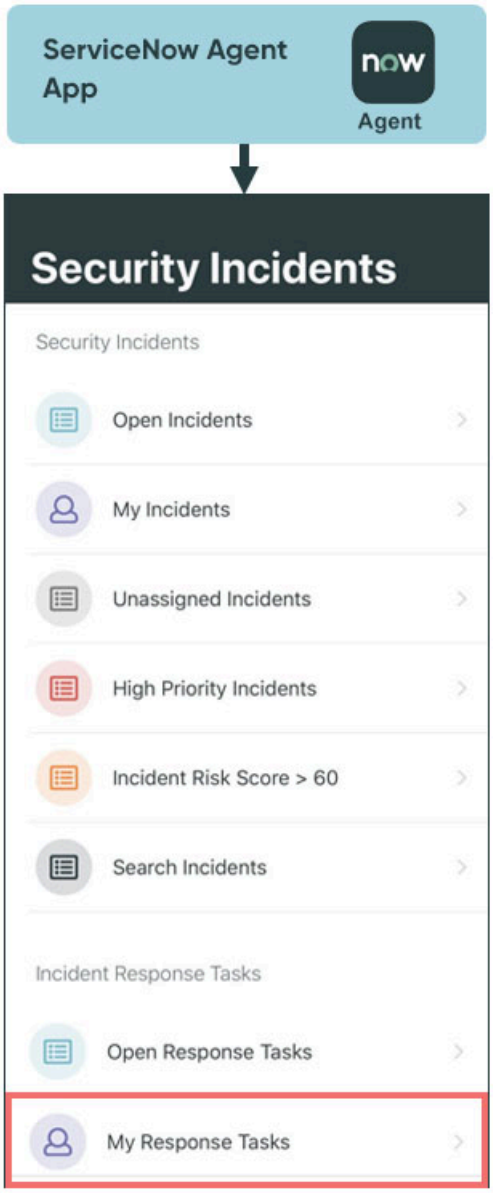
Weisen Sie in der Liste der Datensätze eine offene Antwortaufgabe, die Ihnen zugewiesen ist, einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Neuzuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

### Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Now Platform-Instanz angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Security Incident Response Mobile-App.
2. Tippen Sie im Zielbildschirm von Security Incidents auf **Meine Antwortaufgaben**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

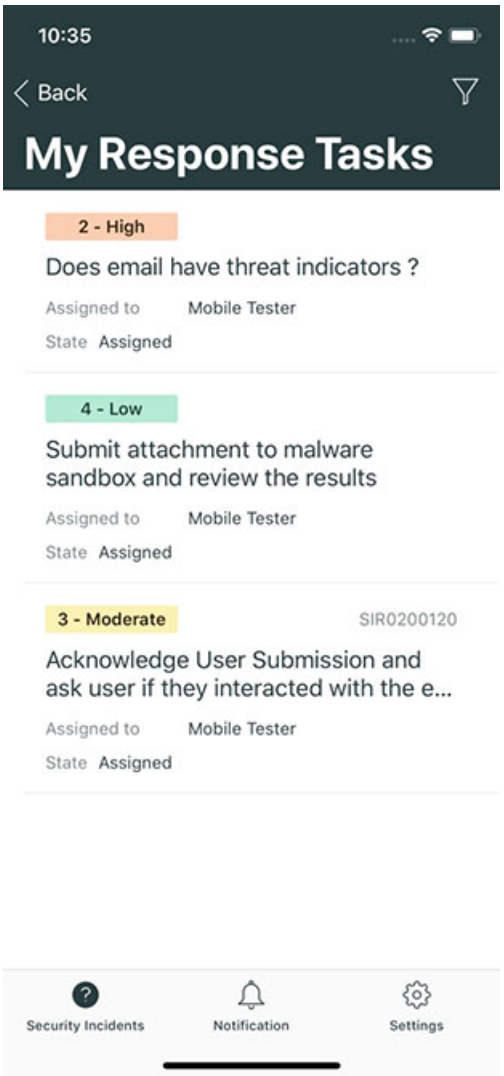
Wenn Sie nach der Anmeldung den Security Incident Response Mobile-App verlassen, können Sie jederzeit auf die App Now Agent (Erfüller) tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Der Bildschirm Meine Antwortaufgaben wird mit einer Liste der Antwortaufgaben angezeigt, die Ihnen zugewiesen sind.



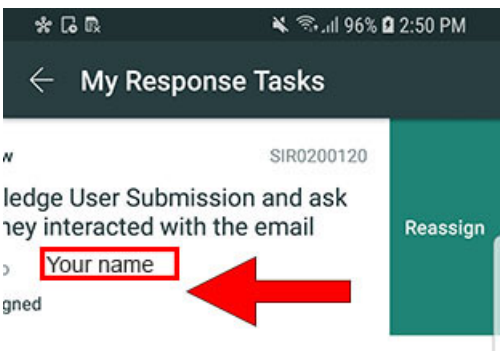
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. **Wahlweise:** Informationen zur Suche nach Aufgaben, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App.

   Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator in der Now Platform.

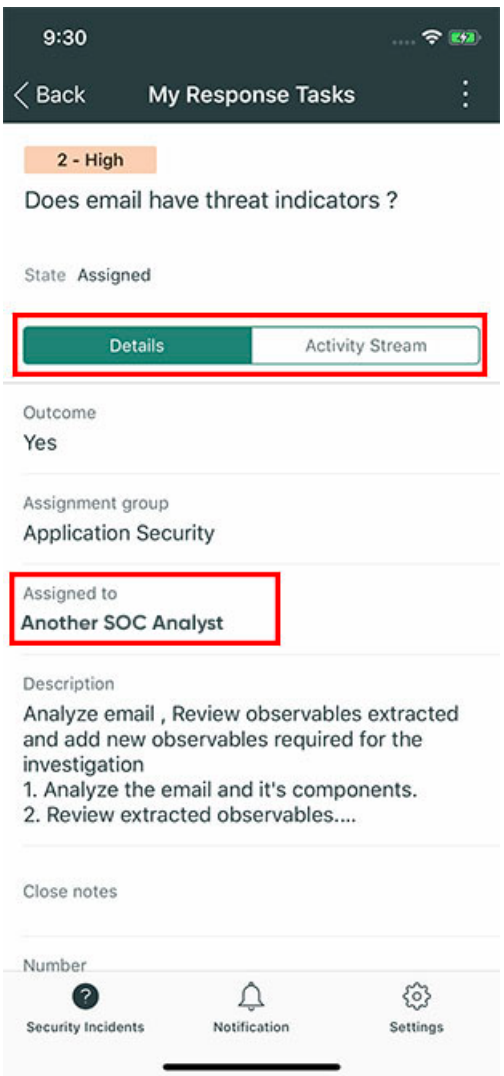
4. Um eine Aufgabe direkt aus der Liste der Ihnen zugewiesenen Aufgabendatensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Tippen **Sie auf Neu zuweisen**.
6. Tippen Sie im angezeigten Bildschirm Antwortaufgabe an andere zuweisen auf ein Feld, um es zu erweitern, und wählen Sie eine andere Gruppe oder einen anderen Benutzer für die Aufgabe aus.
7. Tippen Sie auf das Senden-Symbol ( ) oder auf **Absenden**, um Ihre Änderungen zu speichern und die Antwortaufgabe zu aktualisieren.
   Eine Nachricht wird angezeigt, die bestätigt, dass der Datensatz aktualisiert wurde. Die Aufgabe wird einem neuen Benutzer im übergeordneten Security Incident zugewiesen, und Ihre Instanz Now Platform wird aktualisiert.
8. Um die Details einer offenen Antwortaufgabe und die Arbeitsnotizen anzuzeigen, tippen Sie im angezeigten Bildschirm „Meine Antwortaufgaben“ auf einen Datensatz in der Liste.
9. Wenn die Felder in der Antwortaufgabe angezeigt werden, wählen Sie eines aus der folgenden Tabelle aus, um fortzufahren.




Automatische Übersetzung

## Filtern Sie Datensätze mit Security Incident Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird
Zeit bis zum Abschluss dieser Aufgabe: 5 Minuten.

### Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien für eine beliebige Liste von Datensätzen einzugeben, tippen Sie auf das Filtersymbol ( ).
2. Wenn der Bildschirm „Filter“ angezeigt wird, tippen Sie auf ein Feld, um es zu erweitern.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf den Zurück-Pfeil ( ) oder auf **FERTIG**, um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden auf dem Filter-Bildschirm angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird auch oben auf dem Bildschirm angezeigt. Tippen Sie auf **ZURÜCKSETZEN**, um alle Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 bei angezeigtem Filter-Bildschirm, um mit dem Festlegen Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Schnittmengensymbol Symbol um AND-Bedingungen zu erstellen.
   Alternativ können Sie auf das Schnittmengensymbol  um OR-Bedingungen zu erstellen.
7. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, tippen Sie im angezeigten Bildschirm „Filter“ auf **FERTIG**.
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

## Security Incident Response Orchestration

Security Incident Response Orchestration -Aktivitäten ermöglichen Benutzern die Interaktion mit und das Abrufen von Daten aus Windows- oder UNIX-basierten Systemen und Umgebungen mithilfe der Workflow-Orchestration.

### Security Incident Response Orchestration einrichten

Bevor Sie Security Incident Response Orchestrationverwenden, führen Sie die Schritte zum Einrichten verschiedener Teile des Systems durch, einschließlich Ausfüllen der CMDB, Konfigurieren des MID-Servers und Konfigurieren der Anmeldeinformationen.

#### Vorbereitungen
Erforderliche Rolle: admin
Um Security Incident Responsezu verwenden, benötigen Sie eine vollständig mit Domänennamen ausgefüllte CMDB. Weitere Informationen finden Sie unter Discovery .

#### Warum und wann dieser Vorgang ausgeführt wird

#### Prozedur

1. Aktivieren Sie das Plugin Security Incident Response.
2. MID Server konfigurieren .
3. Konfigurieren Sie Anmeldeinformationen für den Windows MID Server-Service .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Machen Sie sich mit den Workflows und Workflow-Vorlagen von Security Incident Response Orchestration vertraut

Das Basissystem von Security Incident Response enthält eine Reihe von Workflows und Workflow-Vorlagen, die für die Arbeit mit Security Incident-Datensätzen entwickelt wurden.

### Vorbereitungen

Erforderliche Rolle: sn_si.basic

### Warum und wann dieser Vorgang ausgeführt wird

Sie können alle Workflows und Workflow-Vorlagen an Ihre Anforderungen anpassen, vorausgesetzt, Sie haben die entsprechende Rolle: sn_sec_cmn.admin. Workflows werden im gesamten Security Operations-System verwendet, um eine Vielzahl von Aufgaben auszuführen.
Workflow-Vorlagen werden jedoch ausgelöst, indem ein Wert im Feld **Kategorie** in einem Security Incident ausgewählt wird. In diesem Fall startet die der Auswahl zugeordnete Workflow-Vorlage eine Workflow-Vorlage, die die Sicherheitsanalysten anweist, wie mit einer bestimmten Art von Bedrohung umgegangen werden soll.

Wenn Sie beispielsweise **Denial of Service** aus dem Feld **Kategorie** in einem Security Incident auswählen, wird die Vorlage „ **Security Incident – Denial of Service – Vorlage“** ausgeführt, und der Analyst wird angewiesen, zu bestimmen, ob das Ziel des DOS geschäftskritisch ist. Wenn dies der Fall ist, bewirkt die nächste Aufgabe, dass die Priorität des Security Incident auf **1 - Kritisch**festgelegt wird, und führt dann die nächste Aufgabe aus. Und so weiter.

Daher sind Security Incident Response Workflows und Workflow-Vorlagen im Wesentlichen identisch, außer dass die Vorlagen für einen bestimmten Satz von Funktionen innerhalb eines Security Incident verwendet werden.

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Workflows** > **Sicherheitsworkflows anzeigen**.
2. Eine Liste der Workflows und Workflow-Vorlagen, die im Basissystem enthalten sind, wird angezeigt. Alle neuen Workflows, die Sie in der Anwendungssuite Security Operations erstellt haben, sind ebenfalls in der Liste enthalten.
3. Klicken Sie auf den Namen des Workflows oder der Workflow-Vorlage, die Sie anzeigen möchten.

**Hinweis:**
Workflows können auf verschiedene Arten ausgelöst werden. Beachten Sie, dass die Zuordnung eines Workflows zu einem Workflow-Auslöser nicht unbedingt bedeutet, dass der Workflow aktiv ist.

#### Security Incident Response Orchestration Workflows und Aktivitäten

Security Incident Response Orchestrationenthält mehrere Workflows und Aktivitäten.

Nur Benutzer mit der Rolle „sn_sec_cmn.admin“ können Workflow-Editor .

#### Workflow „Suchanforderung für IoC-Änderungen erstellen“.

Der Workflow „ **Security Incident Response – Suchanforderung für IoC-Änderungen erstellen“** wird durch eine Geschäftsregel ausgelöst, die automatisch ausgeführt wird, wenn ein IoC hinzugefügt oder geändert wird. Malware-Scans werden nur ausgelöst, wenn neue Daten eingegeben werden, und nur die neuen Daten werden gescannt.

### Vorbereitungen

Erforderliche Rolle: sn_si.basic



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

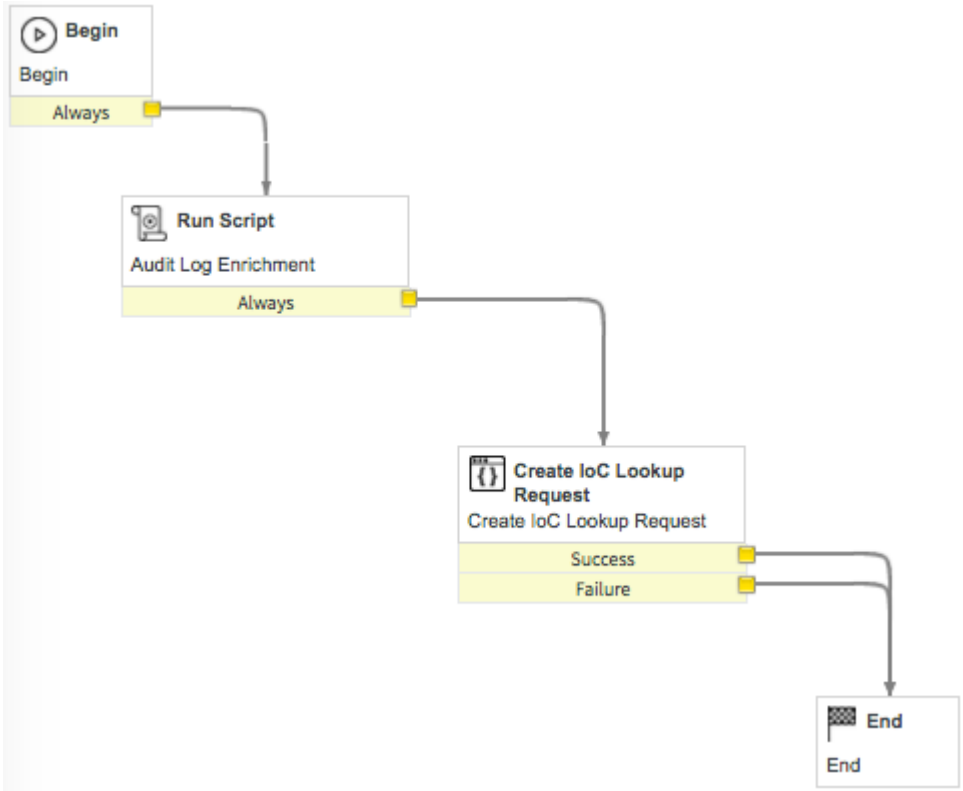
**Warum und wann dieser Vorgang ausgeführt wird**
Wenn das IoC leer ist, wird der Workflow nicht ausgeführt. Historische Scans werden beibehalten und können auf der Registerkarte „ **Sicherheitsscananforderungen“**und in den Arbeitsnotizen des Security Incident angezeigt werden.

Vorhandene Security Incidents werden automatisch aktualisiert.

Workflow-Prozessaktivitäten umfassen:

- Führen Sie das Audit-Protokollskript aus.
- Erstellen Sie die Aktivität „IoC-Suchanforderung“.

**Workflow für IoC-Änderungen**




### Erstellen Sie die Aktivität „IoC-Suchanforderung“.

Die Aktivität **IoC-Suchanforderung erstellen** kann mit jedem Workflow verwendet werden, um eine Malware-Suchanforderung für hinzugefügte oder geänderte IoC-Felder zu erstellen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Suchanforderung erstellt. |
| Fehler | Suchanforderung nicht erstellt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| iocZeichenfolge | JSON-formatierte IoC-Informationen. IP, Hash, URL. |
| siId | Security Incident-Systembezeichner |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| scnReqID | Bezeichner der Suchanforderung |

### Workflow „Security Incident Response – Netzwerkstatistiken abrufen“.

Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** Der Workflow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident im Status **„Analyse“**hinzugefügt wird.

### Vorbereitungen

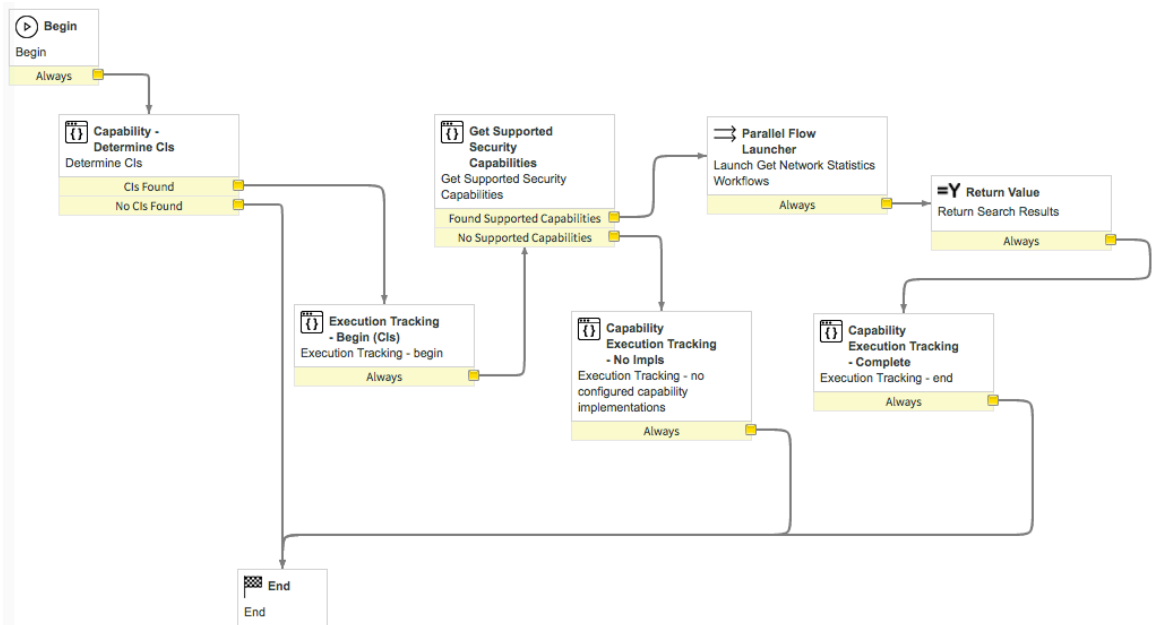
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Workflow automatisch ausgeführt, wenn sich der Status in **Analyse**ändert.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status „ **Analyse** “ befinden und ein neues Konfigurationselement hinzufügen.

### Netzwerkstatistiken abrufen




Workflow-Prozessaktivitäten umfassen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivität „FQDN für Konfigurationselement abrufen“.

Bestimmen Sie das Shell-Skript nach Betriebssystem

If-Anweisung wird von PowerShell ausgeführt

Ausführungsnachverfolgung: Beginn der Aktivität

Ruft Netzwerkstatistiken über die Aktivität „netstat“ ab

Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.

Aktivität „Ergänzungsdatensätze erstellen“.

Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“. Gibt die Ergänzungs-ID zurück.

Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

### Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie den **Status** auf **Analyse**, falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Netzwerkstatistikinformationen im bereit **Zugehörige Links** > **Security Incident-Ergänzungen** Registerkarte. Weitere Informationen finden Sie unter Security Operations -Ergänzungsdatenzuordnung.

Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## Workflow „Security Operations System Command Integration – Laufende Prozesse abrufen“.

Der Workflow „Security Operations System Command Integration - Get Running Processes“ ruft die laufenden Prozesse eines Konfigurationselements ab, wenn ein Windows- oder Unix-basierter Security Incident im Status **„Analyse“**hinzugefügt oder aktualisiert wird.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Bei neuen Security Incidents wird der Workflow automatisch ausgeführt, wenn Sie den Incident mit einem ausgewählten Konfigurationselement übermitteln und sich der Status automatisch in **Analyse**ändert. Wenn er im Status **Entwurf** bleibt, wird er nicht ausgeführt.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status „ **Analyse** “ befinden und ein neues Konfigurationselement hinzufügen.

Workflow-Prozessaktivitäten umfassen:

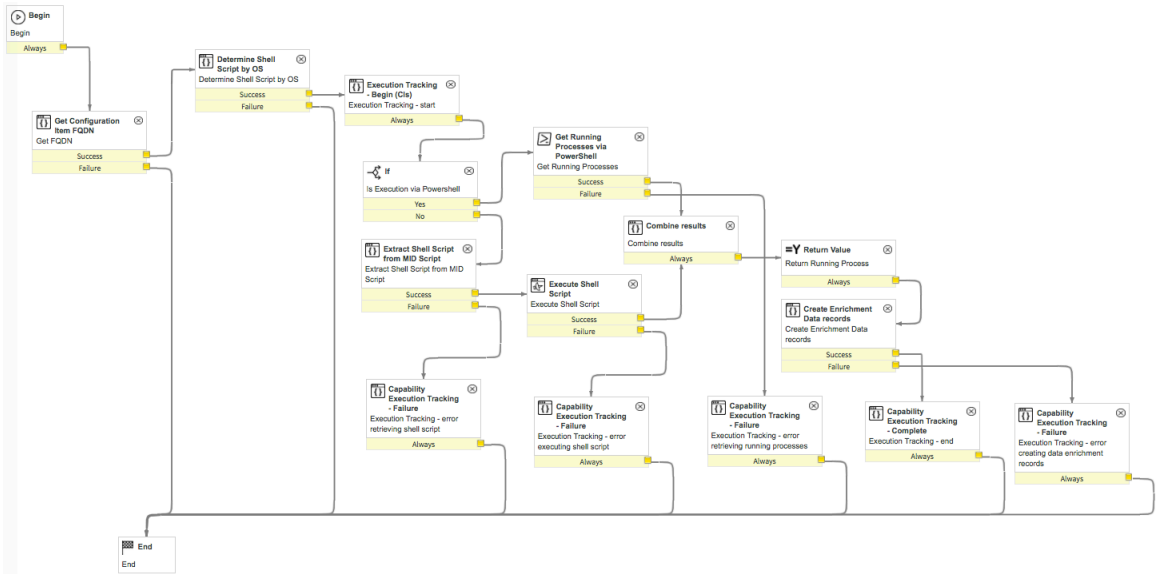
- Aktivität „FQDN für Konfigurationselement abrufen“.
- Bestimmen Sie das Shell-Skript nach Betriebssystemaktivität
- Ausführungsnachverfolgung: Beginn der Aktivität
- Ruft laufende Prozesse über PowerShell ab
- Aktivität „Shell-Skript ausführen“.
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivität „Shell-Skript aus MID-Skript extrahieren“
- Kombinieren Sie Ergebnisseund Rückgabewerte in einem Array
- Aktivität „Ergänzungsdatensätze erstellen“.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

**Laufende Prozesse abrufen**




## Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie den **Status** auf **Analyse**, falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Informationen zum laufenden Prozess in der bereit **Zugehöriger Link** > **Security Incident-Ergänzungen**Registerkarte. Weitere Informationen finden Sie unter Security Operations -Ergänzungsdatenzuordnung.

   Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Workflow „Security Incident Response – Laufende Services abrufen“.

Der **Workflow „Security Incident Response – Laufende Services** abrufen“ ruft eine Liste der ausgeführten Services aus Windows-basierten, ServiceNow, Konfigurationselementen (Cls) ab. Dieser Workflow wird für die Ergänzung von Incidents während Untersuchungen verwendet.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Der **Workflow „Security Incident Response – Laufende Services abrufen** “ wird automatisch ausgeführt, wenn Sie einem Windows-Security Incident ein neues Konfigurationselement hinzufügen, nachdem sich der Status in **„Analyse“**geändert hat. Die Informationen, die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dieser Workflow erhält, werden auf den Registerkarten **Ergänzungsdaten** anzeigen für den Security Incident angezeigt.

**Hinweis:**
Wenn der Security Incident im Status „ **Entwurf** “ bleibt, wird der **Workflow „Security Incident Response – Laufende Services abrufen** “ nicht ausgeführt.

Zu den Workflow-Aktivitäten gehören:

Aktivität „Audit-Protokollergänzungsskript“.

Aktivität „FQDN für Konfigurationselement abrufen“.

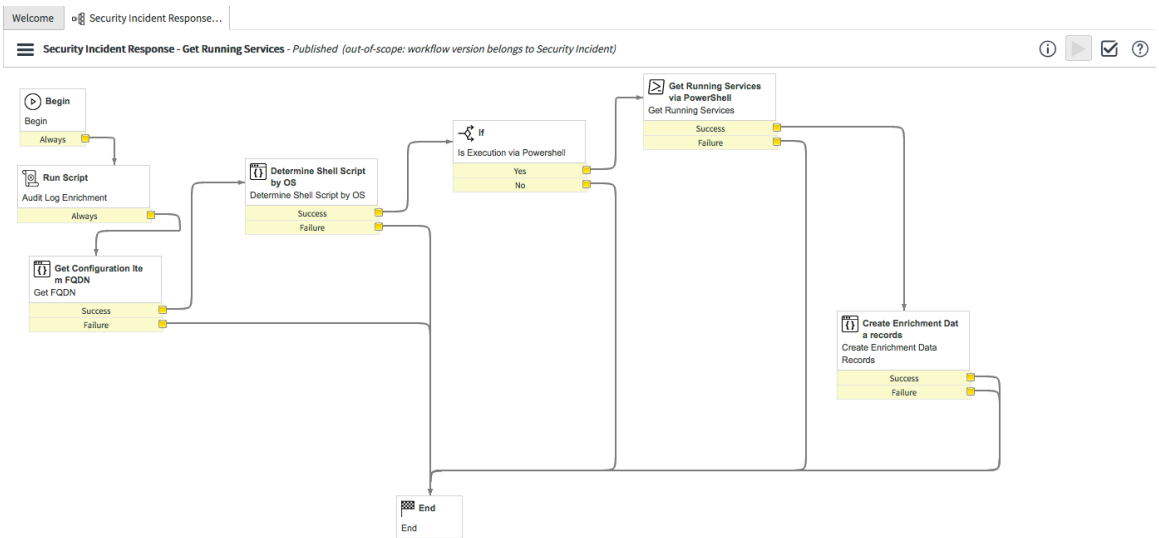
Bestimmen Sie das Shell-Skript nach Betriebssystemaktivität

Ist Ausführung über PowerShell-Aktivität

Aktivität „Laufende Services abrufen – WMI-Ergänzung“.

Aktivität „Ergänzungsdatensätze erstellen“.

**Laufende Services abrufen**




## Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie den **Status** auf **Analyse**, falls erforderlich.
3. Fügen Sie ein Windows-basiertes Konfigurationselement (Server, Laptop oder ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response stellt Informationen zu laufenden Services im bereit **Zugehörige Links** > **Security Incident-Ergänzungen**Registerkarte. Weitere Informationen finden Sie unter Security Operations -Ergänzungsdatenzuordnung.

### Aktivität „FQDN für Konfigurationselement abrufen“.

Die zugehörigen Listen namens **Security Common Orchestration** > **Ruft den FQDN des Konfigurationselements ab** Die Workflow-Aktivität ruft den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität „FQDN für Konfigurationselement abrufen“ kann mit jedem Workflow verwendet werden, um den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| cmdb_ci.id [Zeichenfolge] | Der Systembezeichner (sys_id) eines Configuration Item-Datensatzes. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| fqdn [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) des Konfigurationselements. |

## Zusätzliche Hinweise

Das Feld „fqdn“ im Konfigurationselement muss ausgefüllt werden.

### Bestimmen Sie das Shell-Skript nach Betriebssystemaktivität

Die Workflow-Aktivität „Shell-Skript nach Betriebssystem bestimmen“ bestimmt, welches Betriebssystem im Workflow verwendet werden soll

Die Aktivität „Shell-Skript nach Betriebssystem bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welches Shell-Skript basierend auf dem Betriebssystem ausgeführt werden soll, das auf dem System ausgeführt wird, das das Konfigurationselement enthält.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Betriebssystem gefunden. |
| Fehler | Kein Betriebssystem gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| ciSysId | Systembezeichner des Konfigurationselements. |
| processType | Interner Bezeichner, der definiert, welches Skript aus der Tabelle abgerufen werden soll. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| processScript | ECC-Agent, der den laufenden Prozess erfasst. |
| Ausführungsvorlage | Bestimmt, ob das Skript über eine Probe oder mit PowerShell ausgeführt wird. |
| anreicherungMappingId | Systembezeichner der Ergänzungszuordnung, die zum Transformieren der Antwortdaten verwendet wird. |

### Laufende Services abrufen – WMI-Ergänzung

Der Workflow „ **Security Incident Response – Laufende Services** abrufen“ erfasst laufende Services für ein Konfigurationselement, das einem Security Incident hinzugefügt wurde.

Die Aktivität **„Laufende Services abrufen – WMI-Ergänzung** “ wird automatisch gestartet, um Informationen zu laufenden Services für einen Windows-Host abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Ziel [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) des Zielsystems. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Antwort [Zeichenfolge] | Eine JSON-Zeichenfolge, die die aktuell ausgeführten Services auf dem Zielsystem darstellt.<br>JSON-Daten umfassen:<br>**Name**<br>Der Name des Service<br>**pid** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| | Der Prozessbezeichner des ausgeführten Service<br>**service_type**<br>(Optional) Der Typ des ausgeführten Service.<br>**start_name**<br>Der Systemname für den Service<br>**path**<br>Der Dateipfad der ausführbaren Datei des ausgeführten Service<br>**start_mode**<br>Der Startmodus des ausgeführten Service.<br>**display_name**<br>Der Name des ausgeführten Service, wie er dem Benutzer angezeigt wird |

## Beschränkungen

Der MID Server muss **PowerShell**unterstützen.

SHA-256-Hash erfordert PowerShell V4.

### Aktivität „Ergänzungsdatensätze erstellen“.

Die Workflow-Aktivität Ergänzungsdatensätze **erstellen** erstellt oder aktualisiert Ergänzungsdatensätze, die im Workflow verwendet werden sollen.

Die Aktivität **Ergänzungsdatensätze erstellen** kann mit jedem Workflow verwendet werden, um Ergänzungsdatensätze im Workflow zu aktualisieren.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergänzungsdatensatz aktualisiert. |
| Fehler | Ergänzungsdatensatz nicht aktualisiert. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_id | Aufgabenbezeichner. |
| content | Rohinhalt (laufende Prozessdaten). |
| enreicherung_mapping_id | Identifier der Ergänzungszuordnung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| ci_id | Bezeichner des Konfigurationselements. |
| Referenzwert | Nicht verwendet. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis | Mit dem EnrichmentUtils-Skript erstellte GlideRecords. |

### Procdump-Workflow ausführen

Der Workflow **procdump ausführen** führt einen Prozess-Dump für einen angegebenen Prozess aus und speichert ihn in einer Datei, die von Sicherheitsanalysten als Ziel verwendet werden kann.

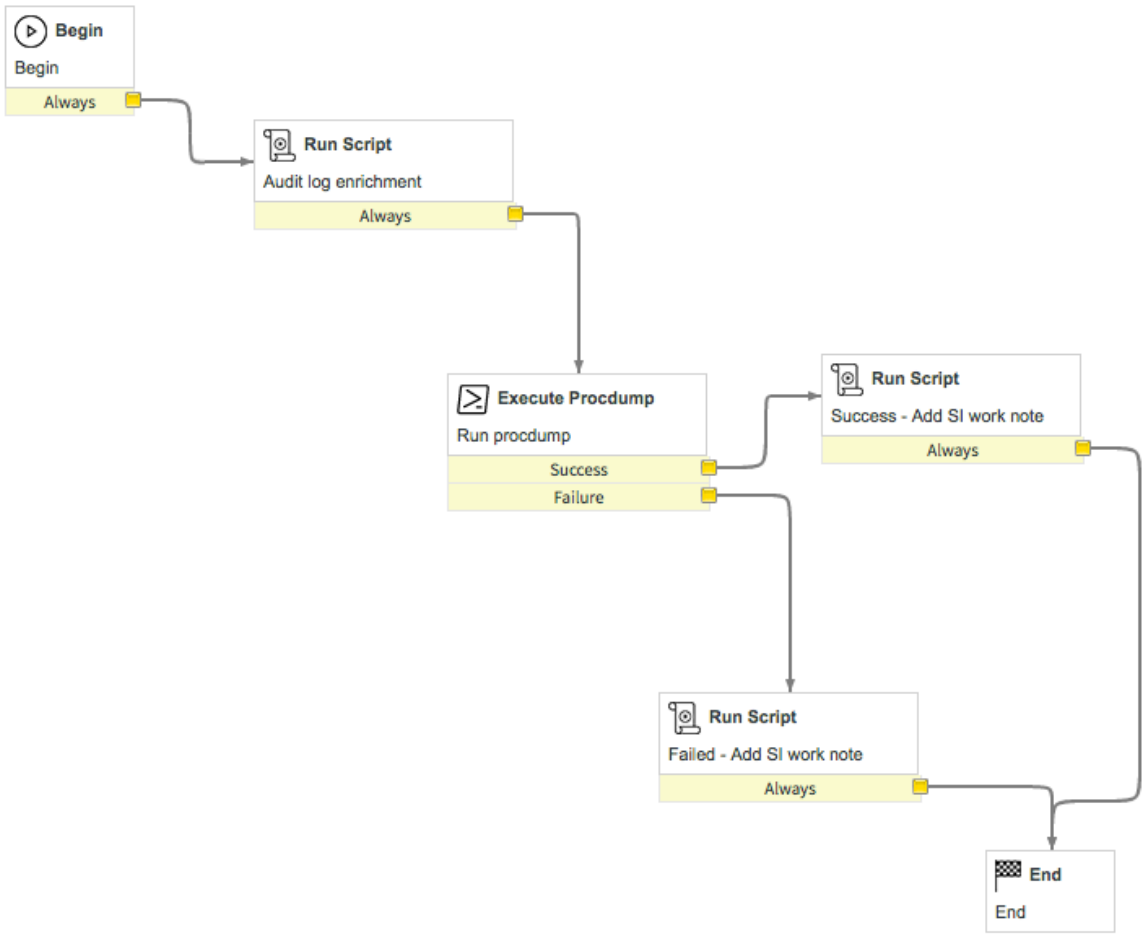
**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow wird ausgelöst, wenn angereicherte Prozesse ausgewählt werden und eine UI-Aktion **procdump ausführen** ausgeführt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Führen Sie procdump aus




Workflow-Prozessaktivitäten umfassen:

- Skript ausführen (Audit-Protokollanreicherung): Führt ein Skript aus, um dem Security Incident ein Audit-Protokoll hinzuzufügen.
- Führen Sie die Produktdump-Aktivität aus
- Skript ausführen (Erfolg – SI-Arbeitsnotiz hinzufügen): Führt ein Skript aus, um eine Arbeitsnotiz hinzuzufügen, wenn der Procdump erfolgreich ist.
- Skript ausführen (Fehlgeschlagen – SI-Arbeitsnotiz hinzufügen): Führt ein Skript aus, um eine Arbeitsnotiz hinzuzufügen, wenn der Procdump fehlschlägt. Gründe für das Fehlschlagen des Produktdump:
  - Ungültiger Dump-Pfad
  - Ungültiger Dateifreigabepfad
  - Der vollständig qualifizierte Domänenname des Windows-Computers, auf dem der Produktdump ausgeführt wird, kann nicht abgerufen werden
  - Der Prozessname ist nicht angegeben
  - Die PROCDUMP-Umgebungsvariable wurde nicht gefunden
  - Eine Kopie der Dump-Datei kann nicht vom Dump-Pfad in den Dateifreigabepfad kopiert werden

### Führen Sie die Produktdump-Aktivität aus

**„Procdump ausführen“** ist eine PowerShell-Aktivität, die den Procdump für die ausgewählten Prozesse ausführt, die Daten in eine Datei speichert und sie an eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

freigegebene Site in einem internen Netzwerk sendet. Ein Analyst kann dann einen Deny-Listen-Prozess anzeigen, der in einem Security Incident rot hervorgehoben ist, und zusätzliche Analysen für die Datei durchführen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der procdump wurde erfolgreich für process_name ausgeführt, und die Details sind in activityOutput.response verfügbar. |
| Fehler | Der procdump konnte für „process_name“ nicht ausgeführt werden, und die Details sind in activityOutput.response verfügbar. |

## Eingabevariablen

Eingabevariablen werden verwendet, um die angeforderten Ausgaben zu erstellen.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| targetId | [Obligatorisch] Die Ziel-ID, auf der der Produktdump ausgeführt werden soll. |
| process_name | [Obligatorisch] Der Prozessname für den Produktdump. |
| dump_path | [Obligatorisch] Der lokale Dateipfad, in dem die generierte Dump-Datei gespeichert wird. |
| dump_filename | [Obligatorisch] Der Dateiname der vom Procdummp generierten Datei. Alle Sonderzeichen werden beim Generieren der Datei durch Bindestriche (-) aus dem Namen der Dump-Datei ersetzt. |
| file_share_path | [Obligatorisch] Der Dateifreigabepfad, in den die Dump-Datei kopiert wird. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Share_path | Der Dateifreigabepfad, in den die Dump-Datei kopiert wurde. |
| response | Eine JSON-Darstellung des Ergebnisses des Produktdumps. |
| Ergebnis | Das Ergebnis des Produktdumps. |

### Security Incident – Workflow „Ergebnis der Antwortaufgabe auswerten“.

Der Workflow „Security Incident – Antwort auswerten“ bestimmt die zu verwendende Aufgabe und ruft einen ausgewählten Workflow und ein Bewertungsskript basierend auf dem Ergebnisauswertungsdatensatz auf, der als Eingabe für den ausgewählten Workflow bereitgestellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vorbereitungen**
Erforderliche Rolle: sn_si.write

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow soll gleichzeitig mit der auszuwertenden Aktivität „Aufgabe erstellen“ ausgeführt werden. Das Bewertungsskript fragt die Artefakte (z. B. Sichtungssuchdatensätze oder laufende Prozesse) der konfigurierten Fähigkeit unter Verwendung von Kontextinformationen aus der Antwortaufgabe (z. B. dem übergeordneten Security Incident) ab, um das entsprechende Ergebnis für die Antwortaufgabe zu bestimmen. Das Ergebnis könnte möglicherweise von der Workflow-Aktivität abhängig sein, ist jedoch im Allgemeinen **Ja** oder **Nein**. Beim Erstellen eines Ergebnisauswertungsdatensatzes können nur Fähigkeiten ausgewählt werden, für die ein Workflow konfiguriert ist, bei denen das Kontrollkästchen **Ist aufgabenbasierte Fähigkeit** aktiviert ist und ein Aufgabeneingabevariablensatz festgelegt ist.

Workflow-Prozessaktivitäten umfassen:

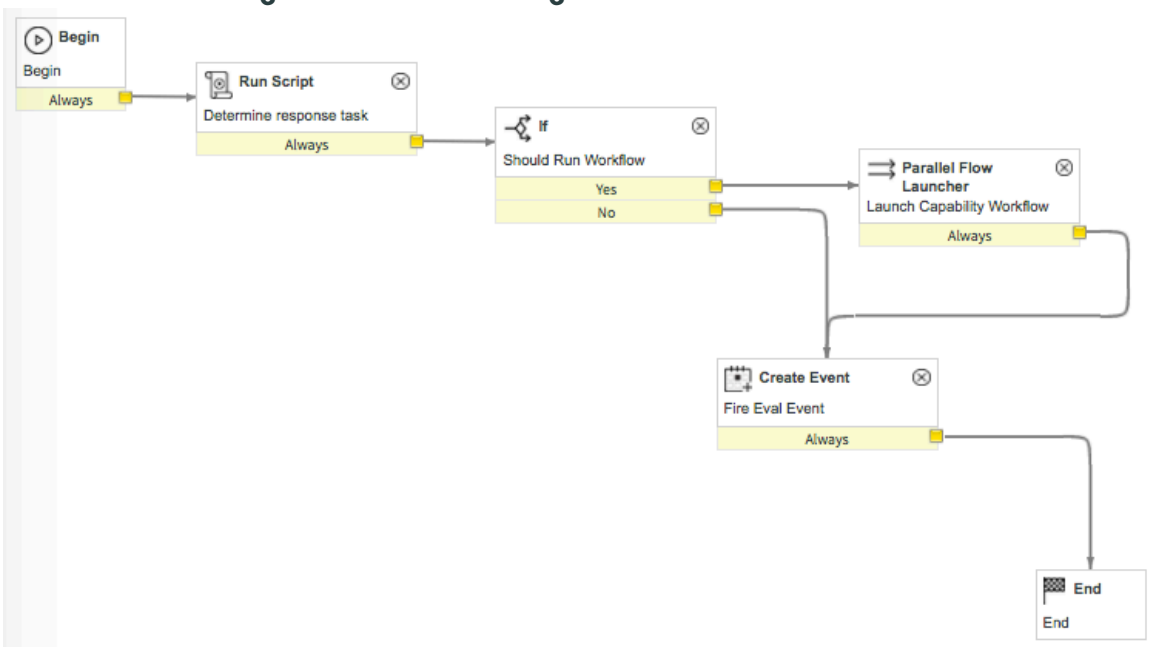
Skript ausführen, um die Antwortaufgabe zu bestimmen

Sollte Workflow ausführen

Startprogramm für paralleles Flow-Startprogramm – Workflow

Erstellen Sie ein Auswertungsereignis

**Bewerten Sie das Ergebnis der Antwortaufgabe**






### Security Incident Response-Workflow-Vorlagen

Workflow-Vorlagen werden mit Security Incident Response Orchestration bereitgestellt, damit Sie grundlegende Analyseverfahren im Zusammenhang mit Sicherheitsvorgängen durchführen können. Die Vorlagen können unverändert verwendet werden, oder Sie können sie anpassen, um Workflows zu erstellen, die Ihren spezifischen Anforderungen besser entsprechen. Die Workflow-Vorlagen sind standardmäßig deaktiviert.

Nur Benutzer mit der Rolle „sn_sec_cmn.admin“ können den Workflow-Editor verwenden.

### Workflow-Vorlage „Security Incident Confidential Data Exposure“.

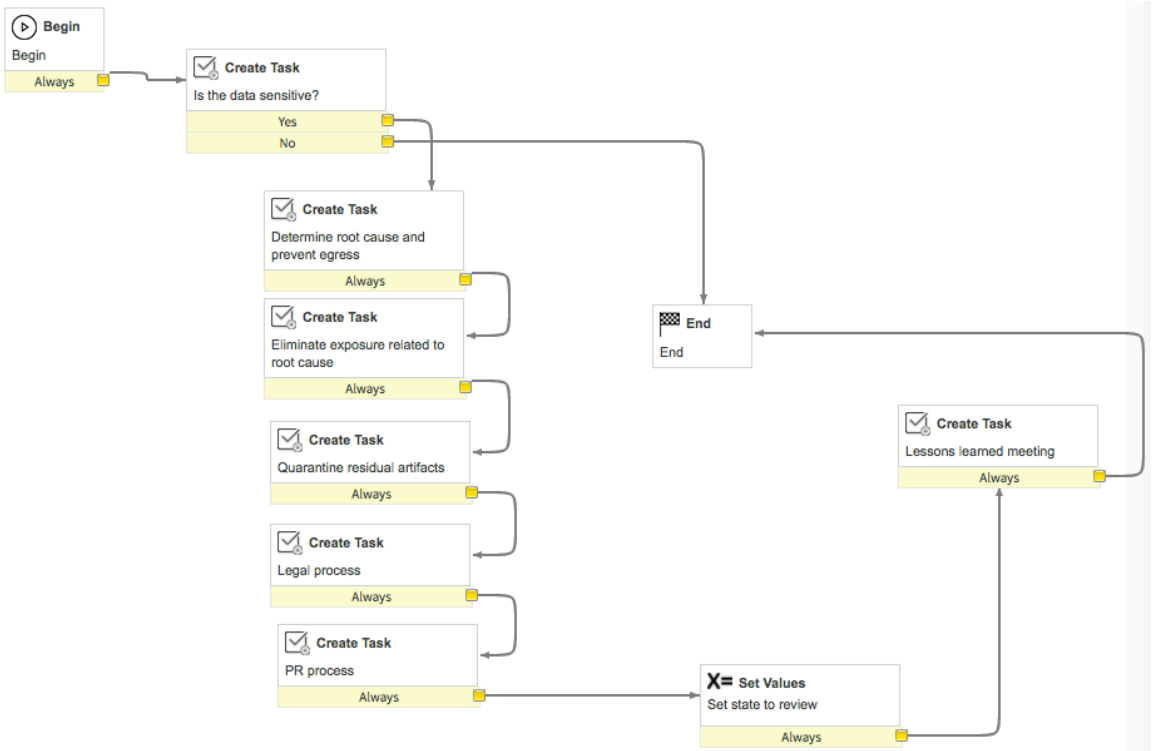
Mit der Vorlage Security Incident - Confidential Data Exposure - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Offenlegung vertraulicher Daten ausgelegt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **vertrauliche persönliche Identitätsdaten**festgelegt oder geändert wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

**Offenlegung von vertraulichen persönlichen Daten**




### Prozedur
1. Öffnen Sie den Security Incident, für den Sie die Gefährdung durch vertrauliche Daten behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Confidential personal Identity Data Exposure**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

**Antwortaufgaben in Vorlage für vertrauliche Daten**

| Antwortaufgabe | Beschreibung | Ergebnisse |
|---|---|---|
| Sind die Daten vertraulich? | Bestimmen Sie, ob die mit diesem Security Incident verknüpften Daten vertraulich sind. Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**ausgewählt haben, wird die nächste Antwortaufgabe ausgeführt.<br><br>Wenn Sie **Nein**ausgewählt haben, wird der Flow beendet. |
| Bestimmen Sie die Ursache, und | Ermitteln Sie die Ursache des Angriffs, und fügen Sie eine Ausgangsfilterung | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Beschreibung | Ergebnisse |
|---|---|---|
| verhindern Sie ausgehenden Datenverkehr | hinzu, um die **Exfilterung** zu stoppen, indem Sie das Feld Status in der Aufgabe entsprechend aktualisieren. | **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Beseitigen Sie das Gefährdungspotenzial im Zusammenhang mit der Ursache | Führen Sie basierend auf der Ursache die Schritte zum Beseitigen des Risikos aus, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Restartefakte unter Quarantäne stellen | Führen Sie die Schritte aus, um **Restartefakte** unter Quarantäne zu stellen, und aktualisieren Sie das Feld Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Rechtliches Verfahren | Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| PR-Prozess | Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die Arbeit an diesen vertraulichen Daten zu selektieren, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, bleibt der Security Incident im **Überprüfungsstatus**, bis Sie ihn schließen. |

### Workflow-Vorlage Security Incident Denial of Service

Mit der Vorlage „Security Incident – Denial of Service – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf Denial of Service-Angriffe (DOS) ausgelegt sind.

#### Vorbereitungen

Erforderliche Rolle: sn_si.write

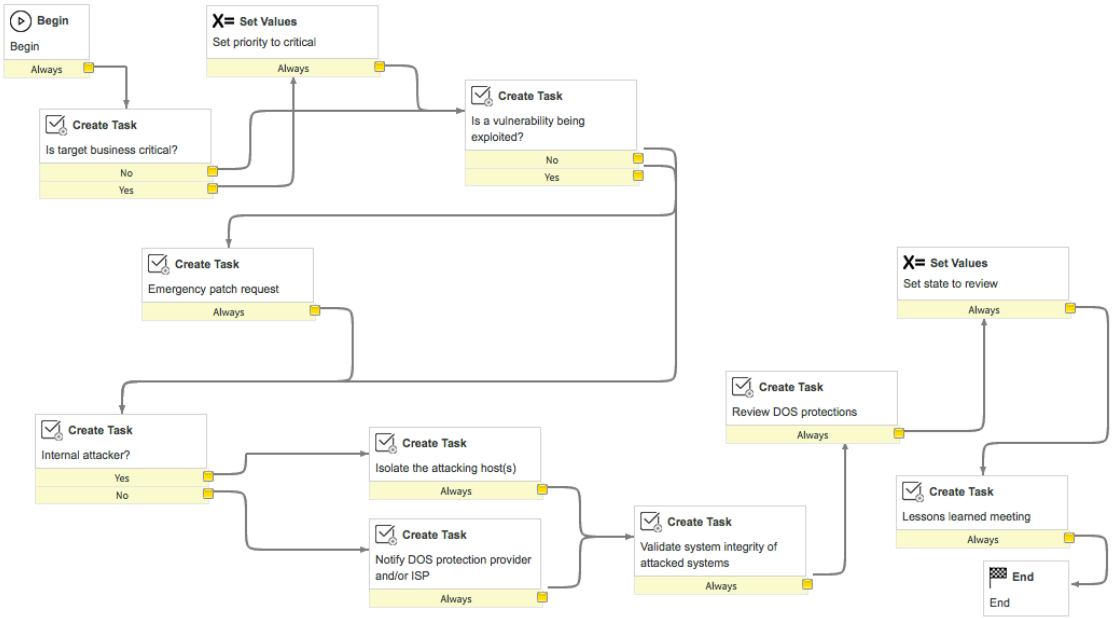
#### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Denial of Service**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Denial of Service (DOS)




## Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Denial of Service aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

### Antwortaufgaben in Denial of Service-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Ist das Ziel geschäftskritisch? | Stellen Sie fest, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe „ **Priorität auf kritische Priorität festlegen** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird das **Feld Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt. |
| Legen Sie die Priorität auf „Kritisch“ fest | Keine Aktion erforderlich. | Die **Priorität** des Security Incident wird automatisch in **Kritisch**geändert, und das **Feld Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt. |
| Wird eine Schwachstelle ausgenutzt? | Stellen Sie fest, ob dieser DOS-Angriff eine Softwareschwachstelle ausnutzt. | Wenn Sie **Ja**auswählen, wird die **Notfall-Patch-Anforderungsaufgabe** ausgeführt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Nein**auswählen, wird der **interne Angreifer?** Aufgabe wird ausgeführt. |
| Notfall-Patch-Anforderung | Geben Sie eine Notfall-Patch-Anforderung für die angegriffenen Systeme aus.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Interner Angreifer? | Bestimmen Sie, ob die Quelle dieses DOS-Angriffs intern in Ihrer Organisation liegt.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Angreifende Hosts isolieren** ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die **Notify-DOS-Schutzanbieter- und/oder ISP-** Aufgabe ausgeführt. |
| Angreifende Hosts isolieren | Führen Sie die erforderlichen Schritte aus, um den/die internen Host(s), der/die für den Angriff verantwortlich ist/sind, zu isolieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Nachdem Sie diesen Schritt abgeschlossen haben, wird die Aufgabe **Systemintegrität angegriffener Systeme validieren** ausgeführt. |
| Benachrichtigen Sie den DOS-Schutzanbieter und/oder ISP | Führen Sie die erforderlichen Schritte aus, um sich an Ihren Denial of Service-Schutzanbieter und/oder Ihren Internet Service Provider zu wenden und sie über den Angriff zu informieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Validiert die Systemintegrität angegriffener Systeme | Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Überprüfen Sie die DOS-Schutzmaßnahmen | Führen Sie eine Überprüfung Ihrer vorhandenen DOS-Schutzmaßnahmen und -Verfahren durch. Führen Sie alle erforderlichen Änderungen durch.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Denial of Service-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet. |

### Workflow-Vorlage „Security Incident – verlorene Ausrüstung“.

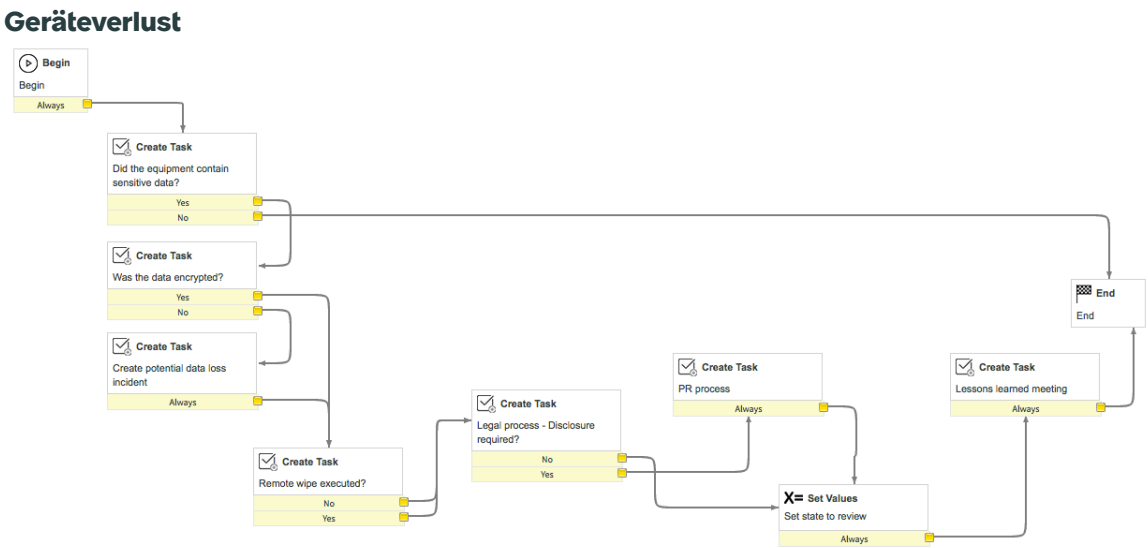
Mit der Vorlage „Security Incident - Lost Equipment - Template“ können Sie eine Reihe von Aufgaben ausführen, die auf den Umgang mit verlorenen Geräten ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Geräteverlust**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.




### Prozedur

1. Öffnen Sie den Security Incident für den Geräteverlust, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Option Geräteverlust**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Antwortaufgaben in Vorlage für verlorene Ausrüstung

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Enthält die Ausrüstung vertrauliche Daten? | Stellen Sie fest, ob die mit diesem Security Incident verknüpften Geräte sensible oder vertrauliche Informationen enthielten.<br><br>Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | Wenn Sie **Ja** auswählen, **wurde das Feld Wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Wurden die Daten verschlüsselt? | Stellen Sie fest, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden.<br><br>Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | Wenn Sie **Ja**auswählen, wird die **Remotelöschung erstellt?** Antwortaufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die **Incident-Antwortaufgabe für potenziellen Datenverlust erstellen**ausgeführt. |
| Erstellen Sie einen potenziellen Datenverlust-Incident | Führen Sie die erforderlichen Schritte aus, um einen potenziellen Datenverlust-Incident zu erstellen.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt. |
| Remotelöschung erstellt? | Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen.<br><br>Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | Die Aufgabe **„Rechtliches Verfahren – Offenlegung erforderlich** “ wird ausgeführt. |
| Rechtliches Verfahren – Offenlegung erforderlich? | Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen.<br><br>Wählen Sie **Ja**, wenn eine rechtliche Offenlegung erforderlich ist, **andernfalls Nein**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| PR-Prozess | Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Die Aufgabe **Status auf Überprüfung** festlegen wird ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Legen Sie den Status auf Überprüfung fest | Es ist keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Incident mit verlorenem Gerät durchgeführten Arbeiten zu selektieren.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Der Flow endet. |

### Workflow-Vorlage „Böswillige Software für Security Incident“.

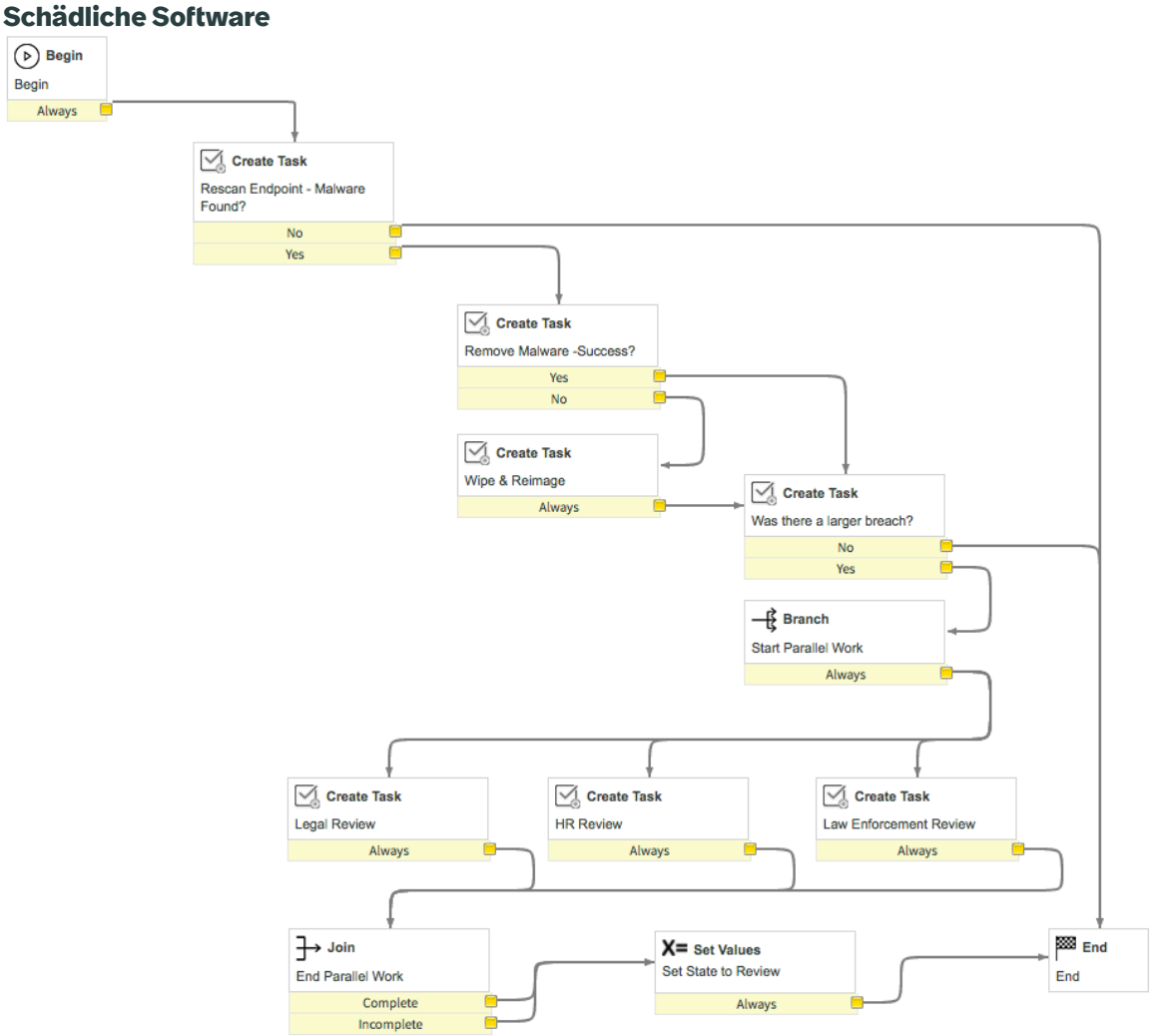
Mit der Vorlage Security Incident - Malicious Software - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung schädlicher Software in Ihrem Netzwerk ausgelegt sind.

#### Vorbereitungen
Erforderliche Rolle: sn_si.write

#### Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Böswillige Software**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






## Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität Böswilliger Code aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Vorlage für schädliche Software

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Scan-Endpunkt – Malware gefunden? | Stellen Sie nach dem Ausführen eines Scans fest, ob Malware gefunden wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Malware entfernen – Erfolg?** Aufgabe wird ausgeführt. |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Malware entfernen – Erfolg? | Stellen Sie fest, ob die Malware erfolgreich entfernt wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„Wipe & Reimage“** (Wipe & Reimage) ausgeführt. |
| Löschen und neues Image erstellen | Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern eine Löschung und ein neues Image durchzuführen. | Nach Abschluss der Aufgabe wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Gab es einen größeren Verstoß? | Stellen Sie fest, ob der durch die schädliche Software verursachte Verstoß größer ist als zuerst angenommen.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt:<br>○ Rechtliche Überprüfung<br>○ HR-Überprüfung<br>○ Überprüfung der Strafverfolgung<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Rechtliche Überprüfung<br><br>HR-Überprüfung<br><br>Überprüfung der Strafverfolgung | Führen Sie die für jede dieser Abteilungen erforderlichen Schritte aus, um den Prozess zur Entfernung der schädlichen Software zu überprüfen. | Wenn die Aufgaben abgeschlossen sind, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt. |
| Legen Sie Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und der Flow wird beendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Phishing-Workflow-Vorlage für Security Incident

Mit der Vorlage Security Incident - Phishing - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Verarbeitung von Spear-Phishing-E-Mails in Ihrem Netzwerk ausgelegt sind.

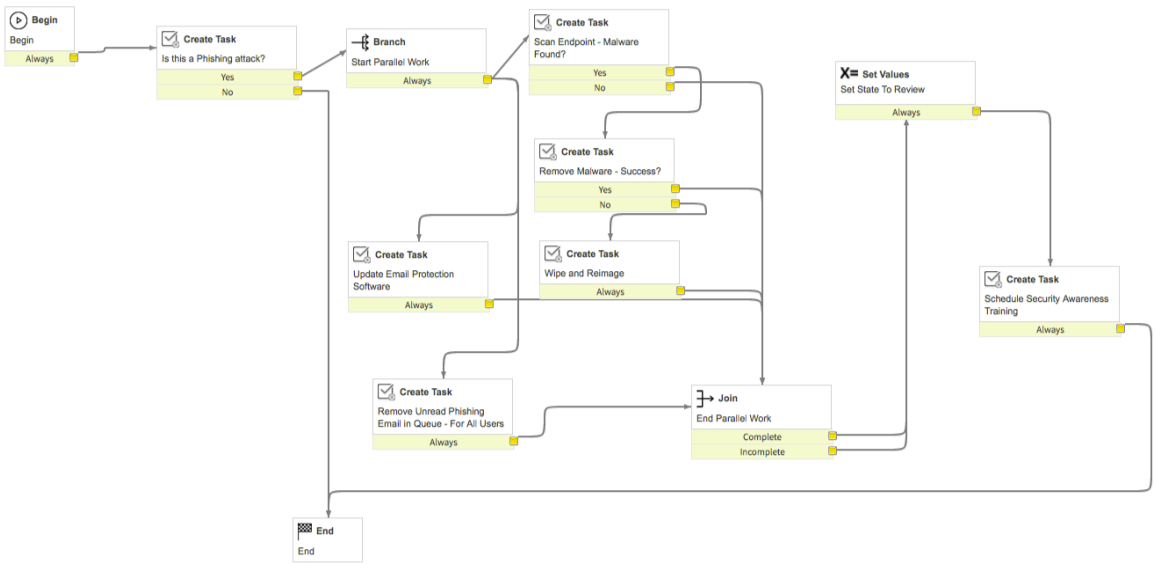
## Vorbereitungen

Erforderliche Rolle: sn_si.write

## Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Spear Phishing**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

### Spear-Phishing




## Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Spear Phishing**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Spear-Phishing-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Handelt es sich um einen Phishing-Angriff? | Stellen Sie fest, ob es sich um einen Phishing-Angriff handelt.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | ○ Scan-Endpunkt – Malware gefunden?<br>○ Aktualisieren Sie die E-Mail-Schutzsoftware<br>○ Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Scan-Endpunkt – Malware gefunden? | Stellen Sie nach dem Ausführen eines Scans fest, ob Malware gefunden wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Malware entfernen – Erfolg?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe „ **Status auf Überprüfung** festlegen“ ausgeführt. |
| Malware entfernen – Erfolg? | Stellen Sie fest, ob die Malware erfolgreich entfernt wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe „ **Status auf Überprüfung setzen** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„Wischen und Reimage“** ausgeführt. |
| Löschen und neues Image erstellen | Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern eine Löschung und ein neues Image durchzuführen. | Nach Abschluss der Aufgabe wird die Aufgabe **„Status auf Überprüfung setzen** “ ausgeführt. |
| Aktualisieren Sie die E-Mail-Schutzsoftware | Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren. | Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender | Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mails, die sich noch in der Warteschlange befinden, für alle Ihre Benutzer zu entfernen. | Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | **Überprüfung** festlegen“ ausgeführt. |
| Legen Sie Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.<br><br>Die Aufgabe **„Schulung für Sicherheitsbewusstsein planen“** wird ausgeführt. |
| Planen Sie ein Sicherheitsbewusstseinstraining | Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu schärfen.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn die Aufgabe abgeschlossen ist, endet der Flow. |

### Workflow-Vorlage „Security Incident Policy Violation“.

Mit der Vorlage „Security Incident – Richtlinienverstoß – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung von Verstößen gegen Sicherheitsrichtlinien ausgelegt sind.

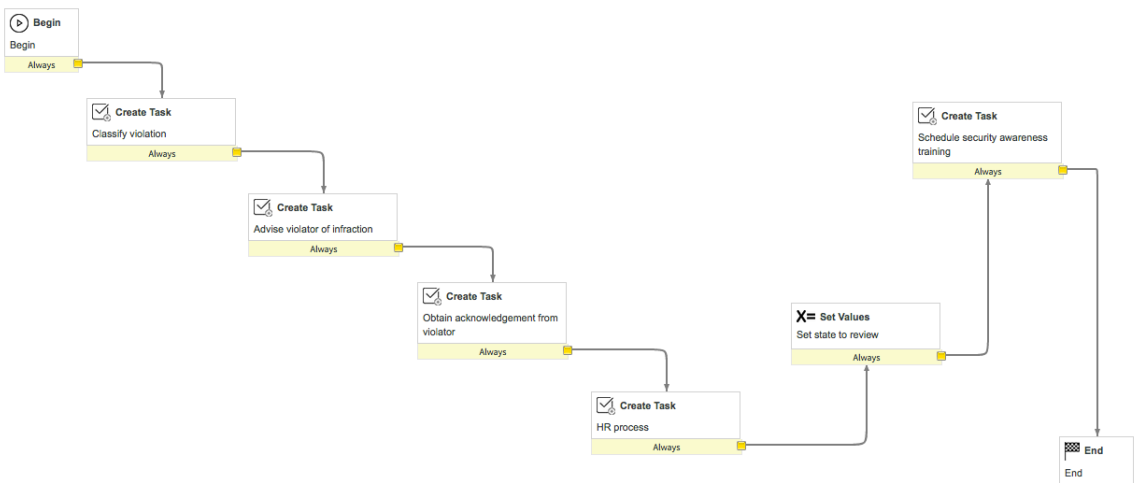
## Vorbereitungen

Erforderliche Rolle: sn_si.write

## Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Richtlinienverstoß**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

### Richtlinienverstoß




## Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Richtlinienverstoß**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Richtlinienverstoßvorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Klassifizieren Sie den Verstoß | Klassifizieren Sie, inwieweit dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe, nachdem Sie sie abgeschlossen haben. | Die Aufgabe **„Verletzer bei Verstoß** melden“ wird ausgeführt. |
| Benachrichtigen Sie den Zuwiderhandelnden über den Verstoß | Teilen Sie dem Verstoß die Art des Verstoßes mit.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe, nachdem Sie es mitgeteilt haben. | Die Aufgabe **„Bestätigung von** Antwort auf Verstoß abrufen“ wird ausgeführt. |
| Bestätigung vom Zuwiderhandelnden anfordern | Fordern Sie eine Bestätigung vom Verstoß an.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Die **HR-Prozessantwortaufgabe** wird ausgeführt. |
| HR-Prozess | Alle erforderlichen Informationen zu diesem Verstoß an HR übermitteln.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Die Antwortaufgabe **Status festlegen, um Überprüfung zu überprüfen** wird ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Es ist keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |
| Planen Sie eine Schulung zum Sicherheitsbewusstsein | Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um die Mitarbeiter darüber zu informieren, wie sie ähnliche Sicherheitsverletzungen in der Zukunft verhindern können.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet. |

### Workflow-Vorlage Security Incident Reconnaissance

Erkundung ist normalerweise ein vorläufiger Schritt zu einem weiteren Angriff, der darauf abzielt, ein Gerät oder System auszunutzen. Mit der Vorlage „Security Incident – Erkundung – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf die Erkundung in Ihrem Netzwerk ausgelegt sind.

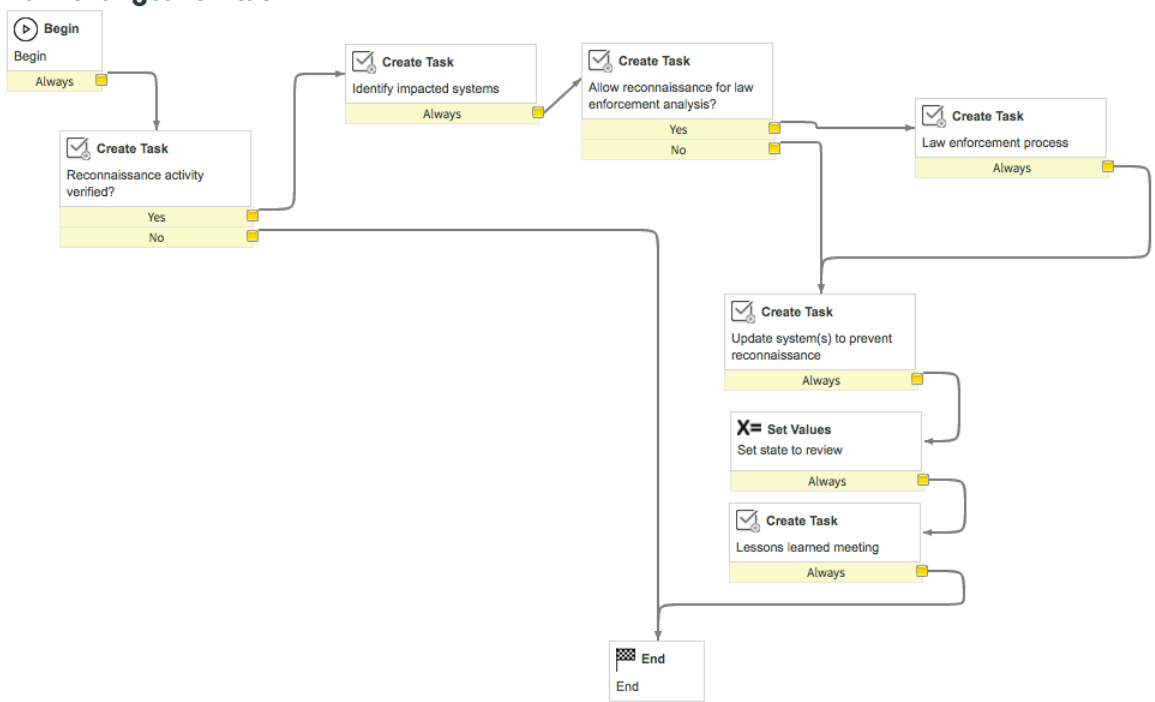


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Erkundungsaktivität**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

**Aufklärungsaktivität**




### Prozedur
1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität Reconnaissance aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

**Antwortaufgaben in der Reconnaissance-Vorlage**

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Erkundungsaktivität verifiziert? | Stellen Sie fest, ob eine beobachtete Erkundung verifiziert wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Betroffene Systeme identifizieren** ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Identifizieren Sie betroffene Systeme | Bestimmen Sie die von der Erkundung betroffenen Systeme. | Wenn diese Aufgabe abgeschlossen ist, wird das **Feld Reconnaissance für** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | **die Analyse der Strafverfolgung zulassen?** Aufgabe wird ausgeführt. |
| Erkundung für Strafverfolgungsanalyse zulassen? | Legen Sie fest, ob die Erkundung von den Strafverfolgungsbehörden analysiert werden soll.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, **wird die Aufgabe „Strafverfolgungsprozess** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„System(e) aktualisieren, um Erkundungstour zu verhindern“** ausgeführt. |
| Strafverfolgungsprozess | Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren, um Erkundungstour zu verhindern“** ausgeführt. |
| Aktualisieren Sie die Systeme, um eine Erkundung zu verhindern | Führen Sie die erforderlichen Schritte aus, um die von der Erkundung betroffenen Systeme zu aktualisieren. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Erkundungs-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn diese Aufgabe abgeschlossen ist, endet der Flow. |

### Workflow-Vorlage für Security Incident Rogue Server oder Service

Mit der Vorlage „Security Incident – Nicht autorisierter Server oder Service“ können Sie eine Reihe von Aufgaben ausführen, die darauf ausgelegt sind, Aktivitäten von nicht autorisierten Servern oder Diensten zu verarbeiten, die sich auf Ihr Netzwerk auswirken.

#### Vorbereitungen

Erforderliche Rolle: sn_si.write

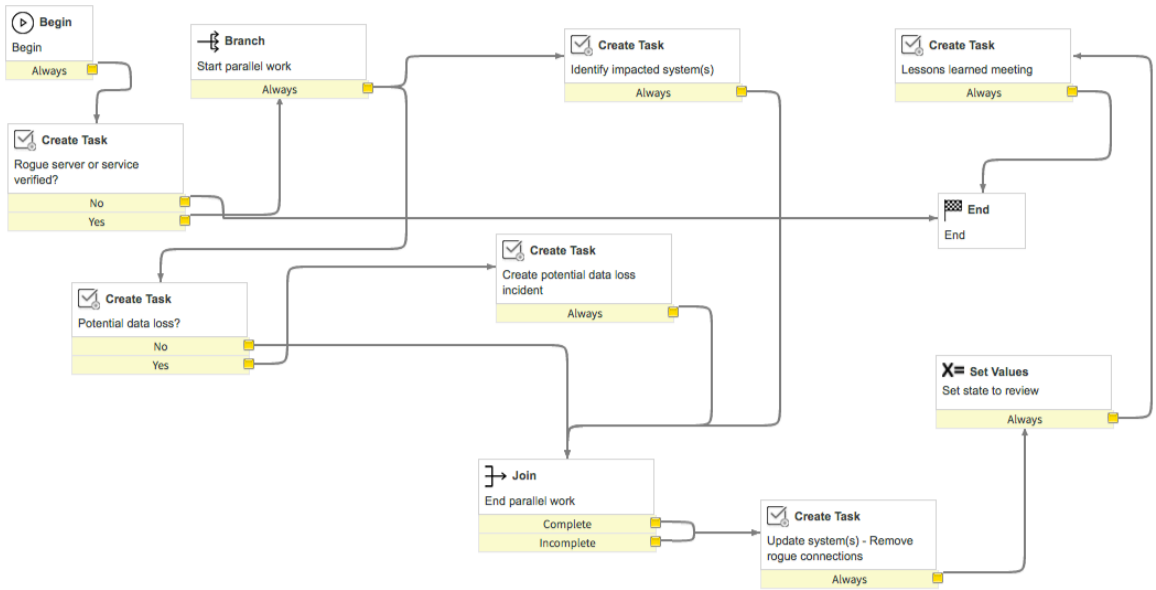
#### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Rogue-Server oder -Service**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nicht autorisierter Server oder Service




## Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität für nicht autorisierte Server oder Services aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Rogue-Server oder Servicevorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Nicht autorisierter Server oder Service verifiziert? | Stellen Sie fest, ob eine Verbindung mit einem nicht autorisierten Server oder Service in Ihrem Netzwerk verifiziert wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt:<br>○ **Betroffene Systeme identifizieren**<br>○ **Potenzieller Datenverlust?**<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Betroffene Systeme identifizieren | Bestimmen Sie die Systeme, die durch den Kontakt mit dem nicht autorisierten Server oder Service betroffen sind. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| Potenzieller Datenverlust? | Stellen Sie fest, ob die Verbindung mit dem nicht autorisierten Server oder Service potenziellen Datenverlust verursacht hat. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident mit potenziellem Datenverlust erstellen** ausgeführt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Nein**auswählen, wird die Aufgabe **„System aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| Erstellen Sie einen potenziellen Datenverlust-Incident | Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| System aktualisieren: Entfernen Sie nicht autorisierte Verbindungen | Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen nicht autorisierten Server oder Service-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn diese Aufgabe abgeschlossen ist, endet der Flow. |

### Security Incident-Spam-Workflow-Vorlage

Mit der Vorlage „Security Incident - Spam - Template“ können Sie eine Reihe von Aufgaben ausführen, die auf die Verarbeitung von E-Mail-Spam in Ihrem Netzwerk ausgelegt sind.

#### Vorbereitungen

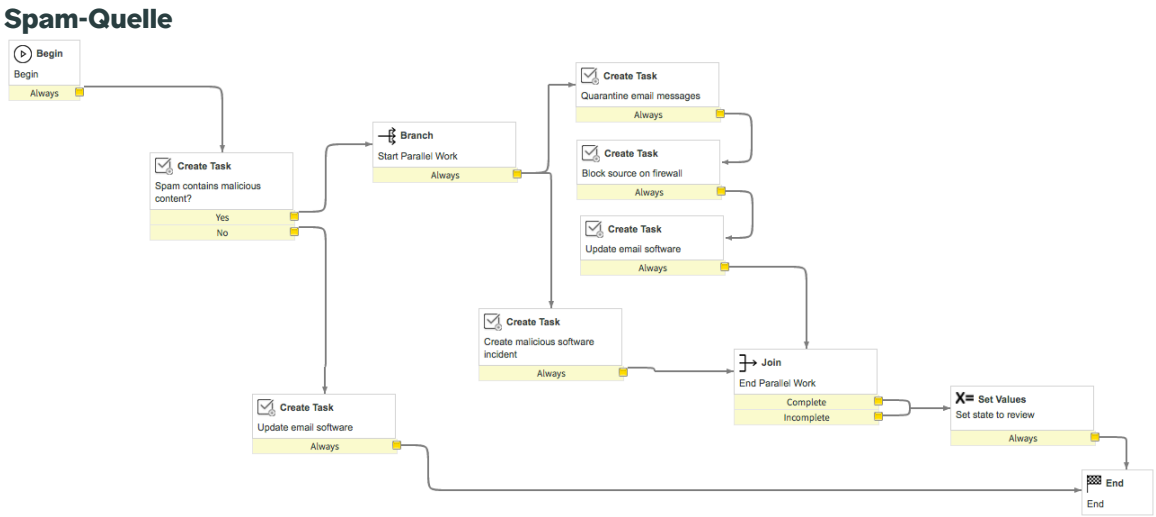
Erforderliche Rolle: sn_si.write

#### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident in **Spam-Quelle**festgelegt oder geändert wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam bearbeiten möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Spam-Quelle**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Spam-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Enthält Spam schädlichen Inhalt? | Stellen Sie fest, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**ausgewählt haben, werden die folgenden Antwortaufgaben ausgeführt:<br>○ **E-Mail-Nachricht unter Quarantäne stellen**<br>○ **Erstellen Sie einen Incident für schädliche Software**<br>Wenn Sie **Nein**ausgewählt haben, wird die **E-Mail-Software aktualisieren** ausgeführt. |
| Erstellen Sie einen Incident für schädliche Software | Führen Sie die Schritte zum Erstellen eines Security Incident aus, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wartet diese Antwortaufgabe, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incident wechselt dann zu **Überprüfung**. |
| E-Mail-Nachricht unter Quarantäne stellen | Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Blockquelle auf Firewall | Führen Sie die Schritte aus, um die E-Mail-Adresse auf der Firewall zu blockieren, | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | |
| Aktualisieren Sie die E-Mail-Software | Fügen Sie die E-Mail-Adresse Ihrer Sperrliste hinzu, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.<br>**Hinweis:**<br>Diese Antwortaufgabe wird auch ausgeführt, wenn Sie die Frage **„Enthält Spam schädlichen Inhalt?** “ mit **Nein** beantwortet haben. Antwortaufgabe. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |



### Workflow-Vorlage „Nicht autorisierter Zugriff“ für Security Incidents

Mit der Vorlage Security Incident - Unauthorized Access - Template können Sie eine Reihe von Aufgaben ausführen, die auf den Umgang mit nicht autorisiertem Zugriff auf Ihr Netzwerk ausgelegt sind.

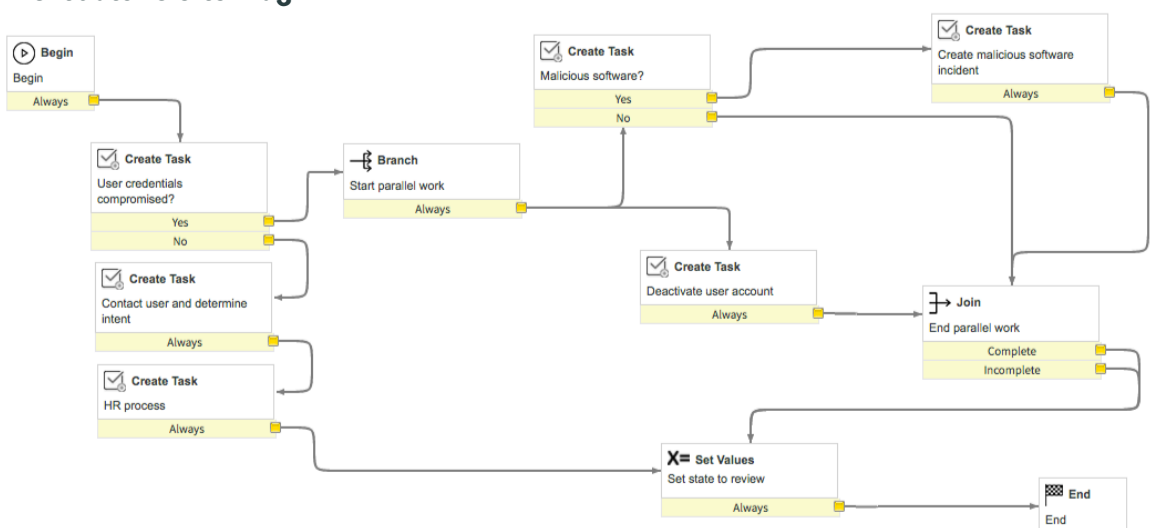
### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Zugriff**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

**Nicht autorisierter Zugriff**




### Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Nicht autorisierter Zugriff**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Vorlage für nicht autorisierten Zugriff

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Benutzeranmeldeinformationen gefährdet? | Stellen Sie fest, ob die Anmeldeinformationen von Benutzern gefährdet wurden.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt:<br>○ **Schädliche Software?**<br>○ **Benutzer-Account deaktivieren**<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe „ **Benutzer kontaktieren und Absicht bestimmen** “ ausgeführt. |
| Schädliche Software? | Stellen Sie fest, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident für schädliche Software erstellen** ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt. |
| Erstellen Sie einen Incident für schädliche Software | Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Benutzer-Account deaktivieren | Führen Sie die erforderlichen Schritte aus, um das gefährdete Benutzerkonto zu deaktivieren. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht | Führen Sie die erforderlichen Schritte aus, um den Benutzer zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und den Grund für den Zugriffsversuch zu ermitteln. | Wenn diese Aufgabe abgeschlossen ist, wird die **HR-Prozessaufgabe** ausgeführt. |
| HR-Prozess | Führen Sie die erforderlichen Schritte aus, um sich bei Bedarf an die | Wenn diese Aufgabe abgeschlossen ist, wird |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Personalabteilung zu wenden und Disziplinarmaßnahmen durchzuführen. | die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und der Flow wird beendet. |

### Workflow-Vorlage Security Incident Web/BBS Defacement

Mit der Vorlage „Security Incident – Web/BBS-Verunstaltung –“ können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung von Vandalismus ausgerichtet sind, der sich gegen eine der BBS- oder Websites Ihres Unternehmens richtet.

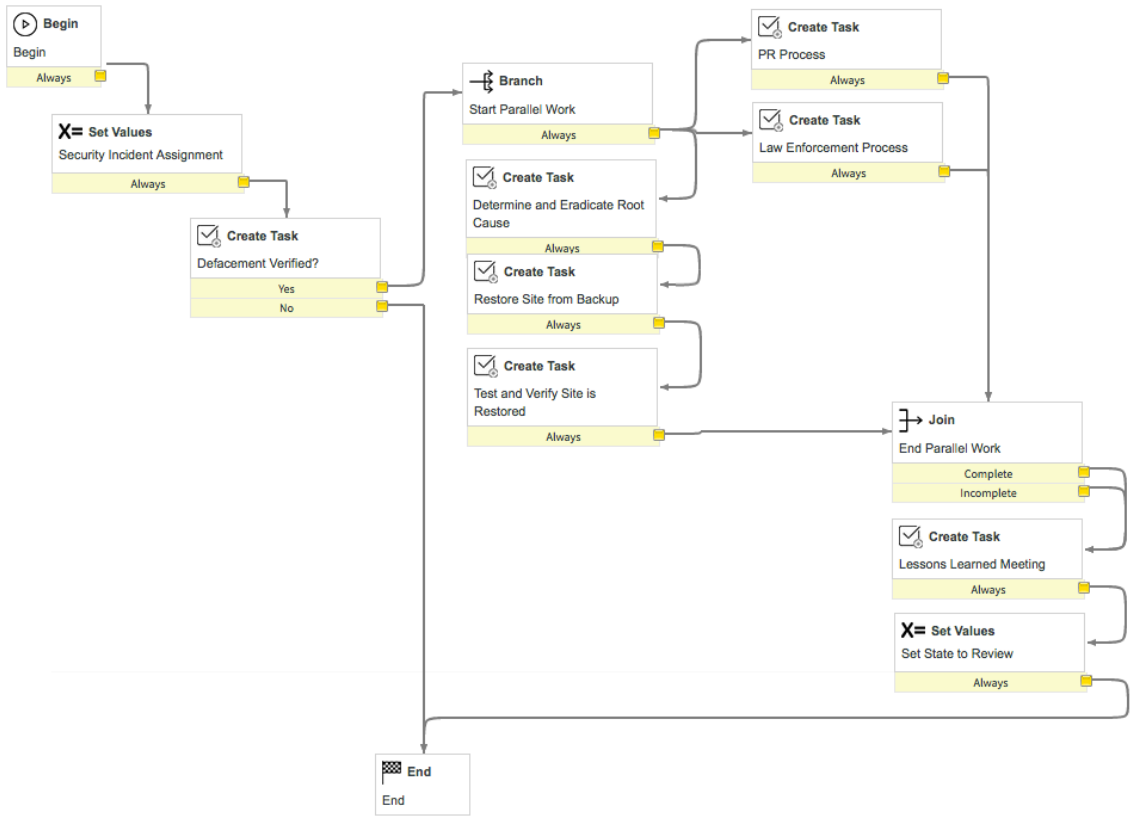
## Vorbereitungen

Erforderliche Rolle: sn_si.write

## Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Web/BBS-Defacement**festgelegt wird. Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

### Unleserlichmachen von Web/BBS




## Prozedur

1. Öffnen Sie den Security Incident für dieses Vorkommen einer Web- oder BBS-Verunreinigung, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Web/BBS-Verunreinigung**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

### Antwortaufgaben in Web/BBS-Veränderungsvorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Security Incident-Zuweisung | Erstellen Sie einen Security Incident für jeden gemeldeten Incident einer Website- oder BBS-Verunreinigung. | Die nächste Antwortaufgabe wird ausgeführt. |
| Verunreinigung verifiziert? | Stellen Sie fest, ob die Website oder BBS tatsächlich unkenntlich gemacht wurde.<br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden Antwortaufgaben ausgeführt:<br>○ **PR-Prozess**<br>○ **Strafverfolgungsprozess**<br>○ **Ursache ermitteln und beheben**<br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| PR-Prozess | Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu informieren, dass die Website oder BBS unkenntlich gemacht wurde.<br>Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig** fest. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Strafverfolgungsprozess | Führen Sie die erforderlichen Schritte aus, um die zuständigen Strafverfolgungsbehörden bezüglich des Angriffs zu beauftragen.<br>Wenn Sie fertig sind, setzen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Ursache ermitteln und beheben | Führen Sie die erforderlichen Schritte aus, um die Ursache der Verunreinigung zu ermitteln und zu beseitigen.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Site aus Sicherung wiederherstellen | Führen Sie die Schritte aus, die zum Sichern und Wiederherstellen der Website oder BBS erforderlich sind. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | |
| Testen Sie, ob die Site wiederhergestellt wurde | Vergewissern Sie sich, dass die Site wiederhergestellt wurde.<br><br>Wenn Sie fertig sind, setzen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Website-/BBS-Verunreinigungs-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der **Status zum Überprüfen** der Aufgabe festgelegt ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.<br><br>Der Flow endet. |

## Flow-Vorlagen für Security Incident Response

Das Security Incident Response Basissystem enthält eine Reihe von Workflow-Vorlagen, die mit dem Flow Designer erstellt wurden und mit Security Incident-Datensätzen arbeiten.

Nur Benutzer mit der Rolle sn_sec_cmn.admin können Sicherheitsvorgänge-Workflow-Vorlagen hinzufügen oder bearbeiten, und Benutzer mit der Rolle sn_si_admin sind erforderlich, um die Flow-Vorlagen zu aktualisieren.

### Wichtige Aktivierungsinformationen

Die mit dem Workflow-Editor erstellten Workflow-Vorlagen und die mit Flow Designer erstellten Flow-Vorlagen sind standardmäßig deaktiviert. Die Workflow-Vorlagen können mithilfe von Workflow-Auslöseraktiviert werden. Flow Designer-Vorlagen können mit Flow Designer aktiviert werden.

**Hinweis:**
Sie müssen darauf achten, nicht von jedem Typ dieselbe Vorlage zu aktivieren. Vermeiden Sie es beispielsweise, Workflow-Vorlage „Security Incident Confidential Data Exposure“. und Flow-Vorlage „Security Incident Confidential Data Exposure“.zu aktivieren. Dies kann dazu führen, dass sowohl der Workflow als auch der Flow ausgeführt werden und doppelte Informationen erstellt werden.

### Flow-Vorlage „Security Incident Confidential Data Exposure“.

Mit der Vorlage Security Incident - Confidential Data Exposure - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Offenlegung vertraulicher Daten ausgelegt sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **vertrauliche persönliche Identitätsdaten**festgelegt oder geändert wird.

### Prozedur
1. Öffnen Sie den Security Incident, für den Sie die Gefährdung durch vertrauliche Daten behandeln möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Confidential personal Identity Data Exposure**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe ausgeführt wird, oder der Flow wird beendet.

**Antwortaufgaben in Vorlage für vertrauliche Daten**

| Antwortaufgabe | Beschreibung | Ergebnisse |
|---|---|---|
| Sind die Daten vertraulich? | Bestimmen Sie, ob die mit diesem Security Incident verknüpften Daten vertraulich sind. Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**ausgewählt haben, wird die nächste Antwortaufgabe ausgeführt.<br>Wenn Sie **Nein**ausgewählt haben, wird der Flow beendet. |
| Bestimmen Sie die Ursache, und verhindern Sie ausgehenden Datenverkehr | Ermitteln Sie die Ursache des Angriffs, und fügen Sie eine Ausgangsfilterung hinzu, um die **Exfilterung** zu stoppen, indem Sie das Feld Status in der Aufgabe entsprechend aktualisieren. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Beseitigen Sie das Gefährdungspotenzial im Zusammenhang mit der Ursache | Führen Sie basierend auf der Ursache die Schritte zum Beseitigen des Risikos aus, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Restartefakte unter Quarantäne stellen | Führen Sie die Schritte aus, um **Restartefakte** unter Quarantäne zu stellen, und aktualisieren Sie das Feld Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Rechtliches Verfahren | Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| PR-Prozess | Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Beschreibung | Ergebnisse |
|---|---|---|
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die Arbeit an diesen vertraulichen Daten zu selektieren, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, bleibt der Security Incident im **Überprüfungsstatus**, bis Sie ihn schließen. |

## Flow-Vorlage für Security Incident Denial of Service

Mit der Vorlage „Security Incident – Denial of Service – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf Denial of Service-Angriffe (DOS) ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Denial of Service**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Denial of Service aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Workflow beendet wird.

#### Antwortaufgaben in Denial of Service-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Ist das Ziel geschäftskritisch? | Stellen Sie fest, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe „ **Priorität auf kritische Priorität festlegen** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird das **Feld Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt. |
| Legen Sie die Priorität auf „Kritisch“ fest | Keine Aktion erforderlich. | Die **Priorität** des Security Incident wird automatisch in **Kritisch**geändert, und das **Feld Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt. |
| Wird eine Schwachstelle ausgenutzt? | Stellen Sie fest, ob dieser DOS-Angriff eine Softwareschwachstelle ausnutzt.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die **Notfall-Patch-Anforderungsaufgabe** ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | Wenn Sie **Nein**auswählen, wird der **interne Angreifer?** Aufgabe wird ausgeführt. |
| Notfall-Patch-Anforderung | Geben Sie eine Notfall-Patch-Anforderung für die angegriffenen Systeme aus.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Interner Angreifer? | Bestimmen Sie, ob die Quelle dieses DOS-Angriffs intern in Ihrer Organisation liegt.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Angreifende Hosts isolieren** ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die **Notify-DOS-Schutzanbieter- und/oder ISP-** Aufgabe ausgeführt. |
| Angreifende Hosts isolieren | Führen Sie die erforderlichen Schritte aus, um den/die internen Host(s), der/die für den Angriff verantwortlich ist/sind, zu isolieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Nachdem Sie diesen Schritt abgeschlossen haben, wird die Aufgabe **Systemintegrität angegriffener Systeme validieren** ausgeführt. |
| Benachrichtigen Sie den DOS-Schutzanbieter und/oder ISP | Führen Sie die erforderlichen Schritte aus, um sich an Ihren Denial of Service-Schutzanbieter und/oder Ihren Internet Service Provider zu wenden und sie über den Angriff zu informieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Validiert die Systemintegrität angegriffener Systeme | Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Überprüfen Sie die DOS-Schutzmaßnahmen | Führen Sie eine Überprüfung Ihrer vorhandenen DOS-Schutzmaßnahmen und -Verfahren durch. Führen Sie alle erforderlichen Änderungen durch.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Denial of Service-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet. |

## Flow-Vorlage „Security Incident – verlorene Ausrüstung“.

Mit der Vorlage „Security Incident - Lost Equipment - Template“ können Sie eine Reihe von Aufgaben ausführen, die auf den Umgang mit verlorenen Geräten ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Geräteverlust**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen Denial of Service-Vorfall, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Option Geräteverlust**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

#### Antwortaufgaben in Vorlage für verlorene Ausrüstung

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Enthält die Ausrüstung vertrauliche Daten? | Stellen Sie fest, ob die mit diesem Security Incident verknüpften Geräte sensible oder vertrauliche Informationen enthielten.<br><br>Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | Wenn Sie **Ja** auswählen, **wurde das Feld Wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Wurden die Daten verschlüsselt? | Stellen Sie fest, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden. | Wenn Sie **Ja**auswählen, wird die **Remotelöschung erstellt?** Antwortaufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die **Incident-Antwortaufgabe** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | **für potenziellen Datenverlust erstellen**ausgeführt. |
| Erstellen Sie einen potenziellen Datenverlust-Incident | Führen Sie die erforderlichen Schritte aus, um einen potenziellen Datenverlust-Incident zu erstellen.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt. |
| Remotelöschung erstellt? | Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen.<br><br>Wählen Sie in der Aufgabe unter **Ergebnis** die Option **Ja** oder **Nein** aus. | Die Aufgabe **„Rechtliches Verfahren – Offenlegung erforderlich** “ wird ausgeführt. |
| Rechtliches Verfahren – Offenlegung erforderlich? | Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen.<br><br>Wählen Sie **Ja**, wenn eine rechtliche Offenlegung erforderlich ist, **andernfalls Nein**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| PR-Prozess | Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Die Aufgabe **Status auf Überprüfung** festlegen wird ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Es ist keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Incident mit verlorenem Gerät durchgeführten Arbeiten zu selektieren.<br><br>Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf „ **Abgeschlossen** “ oder „ **Unvollständig** “ fest. | Der Flow endet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Flow-Vorlage für Security Incident Böswillige Software

Mit der Vorlage Security Incident - Malicious Software - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung schädlicher Software in Ihrem Netzwerk ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Aktivität böswilliger Code**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität Böswilliger Code aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

**Antwortaufgaben in Vorlage für schädliche Software**

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Scan-Endpunkt – Malware gefunden? | Stellen Sie nach dem Ausführen eines Scans fest, ob Malware gefunden wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Malware entfernen – Erfolg?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Malware entfernen – Erfolg? | Stellen Sie fest, ob die Malware erfolgreich entfernt wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„Wipe & Reimage“** (Wipe & Reimage) ausgeführt. |
| Löschen und neues Image erstellen | Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern eine Löschung und ein neues Image durchzuführen. | Nach Abschluss der Aufgabe wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Gab es einen größeren Verstoß? | Stellen Sie fest, ob der durch die schädliche Software verursachte Verstoß größer ist als zuerst angenommen.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt:<br>○ Rechtliche Überprüfung<br>○ HR-Überprüfung<br>○ Überprüfung der Strafverfolgung<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Rechtliche Überprüfung<br><br>HR-Überprüfung<br><br>Überprüfung der Strafverfolgung | Führen Sie die für jede dieser Abteilungen erforderlichen Schritte aus, um den Prozess zur Entfernung der schädlichen Software zu überprüfen. | Wenn die Aufgaben abgeschlossen sind, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt. |
| Legen Sie Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und der Flow wird beendet. |

## Phishing-Flow-Vorlage für Security Incident

Mit der Vorlage Security Incident - Phishing - Template können Sie eine Reihe von Aufgaben ausführen, die auf die Verarbeitung von Spear-Phishing-E-Mails in Ihrem Netzwerk ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Spear Phishing**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Spear Phishing**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Antwortaufgaben in Spear-Phishing-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Handelt es sich um einen Phishing-Angriff? | Stellen Sie fest, ob es sich um einen Phishing-Angriff handelt.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden Aufgaben parallel ausgeführt:<br>○ Scan-Endpunkt – Malware gefunden?<br>○ Aktualisieren Sie die E-Mail-Schutzsoftware<br>○ Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Scan-Endpunkt – Malware gefunden? | Stellen Sie nach dem Ausführen eines Scans fest, ob Malware gefunden wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird das **Feld Malware entfernen – Erfolg?** Aufgabe wird ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe „ **Status auf Überprüfung** festlegen“ ausgeführt. |
| Malware entfernen – Erfolg? | Stellen Sie fest, ob die Malware erfolgreich entfernt wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe „ **Status auf Überprüfung setzen** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„Wischen und Reimage“** ausgeführt. |
| Löschen und neues Image erstellen | Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern eine Löschung und ein neues Image durchzuführen. | Nach Abschluss der Aufgabe wird die Aufgabe **„Status auf Überprüfung setzen** “ ausgeführt. |
| Aktualisieren Sie die E-Mail-Schutzsoftware | Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie | Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren. | **Überprüfung** festlegen“ ausgeführt. |
| Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender | Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mails, die sich noch in der Warteschlange befinden, für alle Ihre Benutzer zu entfernen. | Wenn die Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.<br><br>Die Aufgabe **„Schulung für Sicherheitsbewusstsein planen“** wird ausgeführt. |
| Planen Sie ein Sicherheitsbewusstseinstraining | Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu schärfen.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn die Aufgabe abgeschlossen ist, endet der Flow. |

## Flow-Vorlage für Sicherheitsvorfall-Richtlinienverstöße

Mit der Vorlage „Security Incident – Richtlinienverstoß – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung von Verstößen gegen Sicherheitsrichtlinien ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Richtlinienverstoß**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Richtlinienverstoß**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Antwortaufgaben in Richtlinienverstoßvorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Klassifizieren Sie den Verstoß | Klassifizieren Sie, inwieweit dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe, nachdem Sie sie abgeschlossen haben. | Die Aufgabe **„Verletzer bei Verstoß** melden“ wird ausgeführt. |
| Benachrichtigen Sie den Zuwiderhandelnden über den Verstoß | Teilen Sie dem Verstoß die Art des Verstoßes mit.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe, nachdem Sie es mitgeteilt haben. | Die Aufgabe **„Bestätigung von** Antwort auf Verstoß abrufen“ wird ausgeführt. |
| Bestätigung vom Zuwiderhandelnden anfordern | Fordern Sie eine Bestätigung vom Verstoß an.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Die **HR-Prozessantwortaufgabe** wird ausgeführt. |
| HR-Prozess | Alle erforderlichen Informationen zu diesem Verstoß an HR übermitteln.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Die Antwortaufgabe **Status festlegen, um Überprüfung zu überprüfen** wird ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Es ist keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |
| Planen Sie eine Schulung zum Sicherheitsbewusstsein | Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um die Mitarbeiter darüber zu informieren, wie sie ähnliche Sicherheitsverletzungen in der Zukunft verhindern können.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der Flow beendet. |



## Flow-Vorlage für Security Incident Reconnaissance

Erkundung ist normalerweise ein vorläufiger Schritt zu einem weiteren Angriff, der darauf abzielt, ein Gerät oder System auszunutzen. Mit der Vorlage „Security Incident – Erkundung – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die auf die Erkundung in Ihrem Netzwerk ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Erkundungsaktivität**festgelegt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität Reconnaissance aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

### Antwortaufgaben in der Reconnaissance-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Erkundungsaktivität verifiziert? | Stellen Sie fest, ob eine beobachtete Erkundung verifiziert wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Betroffene Systeme identifizieren** ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Identifizieren Sie betroffene Systeme | Bestimmen Sie die von der Erkundung betroffenen Systeme. | Wenn diese Aufgabe abgeschlossen ist, wird das **Feld Reconnaissance für die Analyse der Strafverfolgung zulassen?** Aufgabe wird ausgeführt. |
| Erkundung für Strafverfolgungsanalyse zulassen? | Legen Sie fest, ob die Erkundung von den Strafverfolgungsbehörden analysiert werden soll.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, **wird die Aufgabe „Strafverfolgungsprozess** “ ausgeführt.<br><br>Wenn Sie **Nein**auswählen, wird die Aufgabe **„System(e) aktualisieren, um Erkundungstour zu verhindern“** ausgeführt. |
| Strafverfolgungsprozess | Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren, um Erkundungstour zu verhindern“** ausgeführt. |
| Aktualisieren Sie die Systeme, um eine Erkundung zu verhindern | Führen Sie die erforderlichen Schritte aus, um die von der Erkundung betroffenen Systeme zu aktualisieren. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die | Wenn diese Aufgabe abgeschlossen ist, endet der Flow. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | für diesen Erkundungs-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | |

## Flow-Vorlage für Security Incident Rogue-Server oder -Service

Mit der Vorlage „Security Incident – Nicht autorisierter Server oder Service“ können Sie eine Reihe von Aufgaben ausführen, die darauf ausgelegt sind, Aktivitäten von nicht autorisierten Servern oder Diensten zu verarbeiten, die sich auf Ihr Netzwerk auswirken.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Rogue-Server oder -Service**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Aktivität für nicht autorisierte Server oder Services aus**.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

#### Antwortaufgaben in Rogue-Server oder Servicevorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Nicht autorisierter Server oder Service verifiziert? | Stellen Sie fest, ob eine Verbindung mit einem nicht autorisierten Server oder Service in Ihrem Netzwerk verifiziert wurde.<br><br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt:<br>○ **Betroffene Systeme identifizieren**<br>○ **Potenzieller Datenverlust?**<br><br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| Betroffene Systeme identifizieren | Bestimmen Sie die Systeme, die durch den Kontakt mit dem nicht autorisierten Server oder Service betroffen sind. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| Potenzieller Datenverlust? | Stellen Sie fest, ob die Verbindung mit dem nicht autorisierten Server oder Service potenziellen Datenverlust verursacht hat. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident mit potenziellem Datenverlust erstellen** ausgeführt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Nein**auswählen, wird die Aufgabe **„System aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| Erstellen Sie einen potenziellen Datenverlust-Incident | Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„System(e) aktualisieren – Nicht autorisierte Verbindungen entfernen“** ausgeführt. |
| System aktualisieren: Entfernen Sie nicht autorisierte Verbindungen | Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen nicht autorisierten Server oder Service-Incident durchgeführte Arbeit zu selektieren.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn diese Aufgabe abgeschlossen ist, endet der Flow. |

## Security Incident-Spam-Flow-Vorlage

Mit der Vorlage „Security Incident - Spam - Template“ können Sie eine Reihe von Aufgaben ausführen, die auf die Verarbeitung von E-Mail-Spam in Ihrem Netzwerk ausgelegt sind.

### Vorbereitungen

Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident in **Spam source**festgelegt oder geändert wird.

### Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam bearbeiten möchten, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die **Spam-Quelle**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Antwortaufgaben in Spam-Vorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Enthält Spam schädlichen Inhalt? | Stellen Sie fest, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**ausgewählt haben, werden die folgenden Antwortaufgaben ausgeführt:<br>○ **E-Mail-Nachricht unter Quarantäne stellen**<br>○ **Erstellen Sie einen Incident für schädliche Software**<br>Wenn Sie **Nein**ausgewählt haben, wird die **E-Mail-Software aktualisieren** ausgeführt. |
| Erstellen Sie einen Incident für schädliche Software | Führen Sie die Schritte zum Erstellen eines Security Incident aus, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wartet diese Antwortaufgabe, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incident wechselt dann zu **Überprüfung**. |
| E-Mail-Nachricht unter Quarantäne stellen | Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Blockquelle auf Firewall | Führen Sie die Schritte aus, um die E-Mail-Adresse auf der Firewall zu blockieren, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt. |
| Aktualisieren Sie die E-Mail-Software | Fügen Sie die E-Mail-Adresse Ihrer Sperrliste hinzu, und aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Abgeschlossen** oder **Abgebrochen**ändern, wird die nächste Antwortaufgabe ausgeführt.<br>**Hinweis:**<br>Diese Antwortaufgabe wird auch ausgeführt, wenn Sie die Frage **„Enthält Spam schädlichen Inhalt?** “ mit **Nein** beantwortet haben. Antwortaufgabe. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert. |

## Flow-Vorlage für nicht autorisierten Security Incident

Mit der Vorlage Security Incident - Unauthorized Access - Template können Sie eine Reihe von Aufgaben ausführen, die auf den Umgang mit nicht autorisiertem Zugriff auf Ihr Netzwerk ausgelegt sind.

**Vorbereitungen**
Erforderliche Rolle: sn_si.write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Nicht autorisierter Zugriff**festgelegt wird.

### Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Nicht autorisierter Zugriff**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

**Antwortaufgaben in Vorlage für nicht autorisierten Zugriff**

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Benutzeranmeldeinformationen gefährdet? | Stellen Sie fest, ob die Anmeldeinformationen von Benutzern gefährdet wurden.<br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, werden die folgenden beiden Aufgaben parallel ausgeführt:<br>○ **Schädliche Software?**<br>○ **Benutzer-Account deaktivieren**<br>Wenn Sie **Nein**auswählen, wird die Aufgabe „ **Benutzer kontaktieren und Absicht bestimmen** “ ausgeführt. |
| Schädliche Software? | Stellen Sie fest, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat.<br>Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | Wenn Sie **Ja**auswählen, wird die Aufgabe **Incident für schädliche Software erstellen** ausgeführt.<br>Wenn Sie **Nein**auswählen, wird die Aufgabe **Status auf Überprüfung** festlegen ausgeführt. |
| Erstellen Sie einen Incident für schädliche Software | Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Benutzer-Account deaktivieren | Führen Sie die erforderlichen Schritte aus, um das gefährdete Benutzerkonto zu deaktivieren. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | | **Überprüfung** festlegen“ ausgeführt. |
| Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht | Führen Sie die erforderlichen Schritte aus, um den Benutzer zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und den Grund für den Zugriffsversuch zu ermitteln. | Wenn diese Aufgabe abgeschlossen ist, wird die **HR-Prozessaufgabe** ausgeführt. |
| HR-Prozess | Führen Sie die erforderlichen Schritte aus, um sich bei Bedarf an die Personalabteilung zu wenden und Disziplinarmaßnahmen durchzuführen. | Wenn diese Aufgabe abgeschlossen ist, wird die Aufgabe **„Status auf Überprüfung** festlegen“ ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert, und der Flow wird beendet. |

## Flow-Vorlage für Security Incident Web/BBS-Veränderung

Mit der Vorlage „Security Incident – Web/BBS-Verunstaltung –“ können Sie eine Reihe von Aufgaben ausführen, die auf die Behandlung von Vandalismus ausgerichtet sind, der sich gegen eine der BBS- oder Websites Ihres Unternehmens richtet.

### Vorbereitungen
Erforderliche Rolle: sn_si.write

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn die **Kategorie** in einem Security Incident auf **Web/BBS-Defacement**festgelegt wird.

### Prozedur
1. Öffnen Sie den Security Incident für dieses Vorkommen einer Web- oder BBS-Verunreinigung, oder erstellen Sie einen neuen Security Incident.
2. Wählen Sie unter **Kategorie**die Option **Web/BBS-Verunreinigung**aus.
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie die zugehörige Liste **Antwortaufgaben**.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, führt Ihre Antwort auf die vorherige Aufgabe entweder dazu, dass die nächste Antwortaufgabe erstellt wird, oder der Flow beendet wird.

#### Antwortaufgaben in Web/BBS-Veränderungsvorlage

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| Security Incident-Zuweisung | Erstellen Sie einen Security Incident für jeden gemeldeten Incident einer Website- oder BBS-Verunreinigung. | Die nächste Antwortaufgabe wird ausgeführt. |
| Verunreinigung verifiziert? | Stellen Sie fest, ob die Website oder BBS tatsächlich unkenntlich gemacht wurde. | Wenn Sie **Ja**auswählen, werden die folgenden Antwortaufgaben ausgeführt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | Wählen Sie in der Aufgabe **Ja** oder **Nein** in **Ergebnis**aus. | ○ **PR-Prozess**<br>○ **Strafverfolgungsprozess**<br>○ **Ursache ermitteln und beheben**<br>Wenn Sie **Nein**auswählen, wird der Flow beendet. |
| PR-Prozess | Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu informieren, dass die Website oder BBS unkenntlich gemacht wurde.<br>Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig** fest. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Strafverfolgungsprozess | Führen Sie die erforderlichen Schritte aus, um die zuständigen Strafverfolgungsbehörden bezüglich des Angriffs zu beauftragen.<br>Wenn Sie fertig sind, setzen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Ursache ermitteln und beheben | Führen Sie die erforderlichen Schritte aus, um die Ursache der Verunreinigung zu ermitteln und zu beseitigen.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Site aus Sicherung wiederherstellen | Führen Sie die Schritte aus, die zum Sichern und Wiederherstellen der Website oder BBS erforderlich sind.<br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**geändert haben, wird die nächste Antwortaufgabe ausgeführt. |
| Testen Sie, ob die Site wiederhergestellt wurde | Vergewissern Sie sich, dass die Site wiederhergestellt wurde.<br>Wenn Sie fertig sind, setzen Sie den Status der Aufgabe auf **Abgeschlossen** oder **Unvollständig**. | Die **Besprechungsaufgabe „Erlernte Lektionen“** wird ausgeführt. |
| Besprechung der gelernten Lektionen | Führen Sie eine Besprechung mit gelernten Lektionen durch, um die für diesen Website-/ | Wenn Sie den Status der Aufgabe in **Geschlossen – vollständig** oder **Abgebrochen**ändern, wird der |



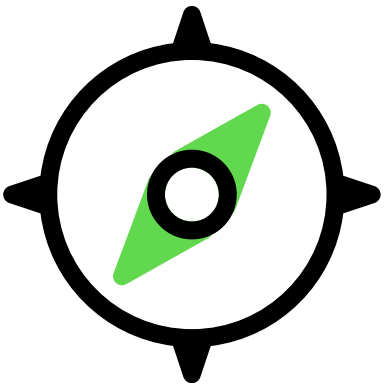
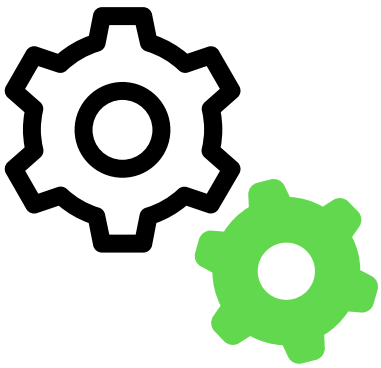
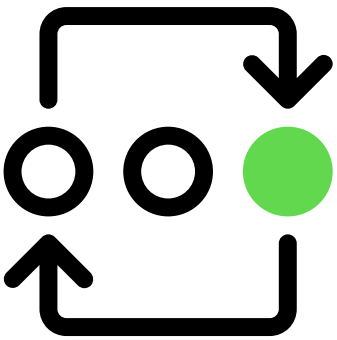
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Antwortaufgabe | Aktion | Ergebnisse |
|---|---|---|
| | BBS-Verunreinigungs-Incident durchgeführte Arbeit zu selektieren.<br><br>Aktualisieren Sie das **Feld** Status in der Aufgabe entsprechend. | **Status zum Überprüfen** der Aufgabe festgelegt ausgeführt. |
| Legen Sie den Status auf Überprüfung fest | Keine Aktion erforderlich. | Der **Status** des Security Incident wird automatisch in **Überprüfung**geändert.<br><br>Der Flow endet. |

## Sicherheitsstatus-Überwachung

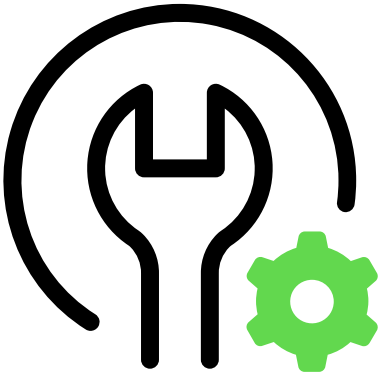
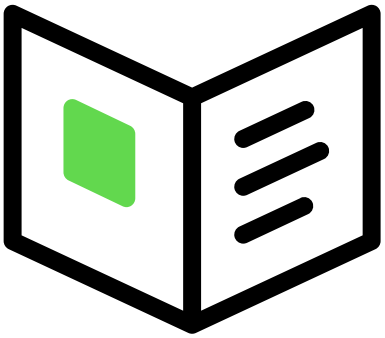
Verschaffen Sie sich einen Überblick über den Bestand an Unternehmens-Assets und die Abdeckung von Sicherheitstools. Verwenden Sie die mit dem Produkt bereitgestellten Richtlinien, oder erstellen Sie eigene, um Assets zu identifizieren, bei denen wichtige Sicherheitstools wie Endpunktschutz, Konfigurationsverwaltung und Schwachstellen-Scans fehlen. Überwachen Sie Assets auf Sicherheitstool-Konfigurationen, die für Ihre Umgebung spezifisch sind, und automatisieren Sie den Korrektur-Workflow für Sicherheitslücken in der Anwendung Configuration Compliance.

### Erste Schritte

| Erkunden | Installieren | integrieren |
|---|---|---|
|  |  |  |
| Erfahren Sie mehr über die Konzepte und Funktionen von Security Posture Control | Installieren Sie Security Posture Control-Anwendungen | Integrieren Sie Service Graph Connectors mit Security Posture Control |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Verwenden | | Referenz |
| --- | --- | --- |
|  | |  |
| Erfahren Sie, wie Sie den Arbeitsbereich verwenden, um Ihre Assets zu durchsuchen und Sicherheitslücken zu identifizieren | | Rufen Sie Details zu Szenarien ab, die Ihnen helfen, bestimmte Arten von Lücken bei der Toolabdeckung zu identifizieren |

### Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

## Sicherheitsstatus-Überwachung erkunden

Security Posture Control ermöglicht es Cybersicherheitsteams, Einblick in den gesamten Asset-Bestand des Unternehmens zu erhalten und die allgemeine Sicherheitslage zu bestimmen.

Sicherheitsanalysten erhalten Einblicke in die Bereitstellung von Sicherheitstools und die Abdeckung ihrer Assets basierend auf ihrem Asset-Bestand und importierten Daten aus Service Graph Connectors. Schwachstellenmanager können Einblicke aus Security Posture Control (SPC) verwenden, um die Korrektur von Kombinationen mit hohem Risiko für Internetgefährdung und Schwachstellen zu priorisieren, und benutzerdefinierte Richtlinien und Einblicke erstellen, um die Compliance von Assets mit internen Konfigurationsstandards für Sicherheitstools zu überwachen.

Sicherheitsstatus-Überwachung besteht aus zwei Anwendungen, die durch ein separates Abonnement von ServiceNow® Storeverfügbar sind:

- Security Posture Core
- Sicherheitsstatus-Management für Assets- (ASPM)

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

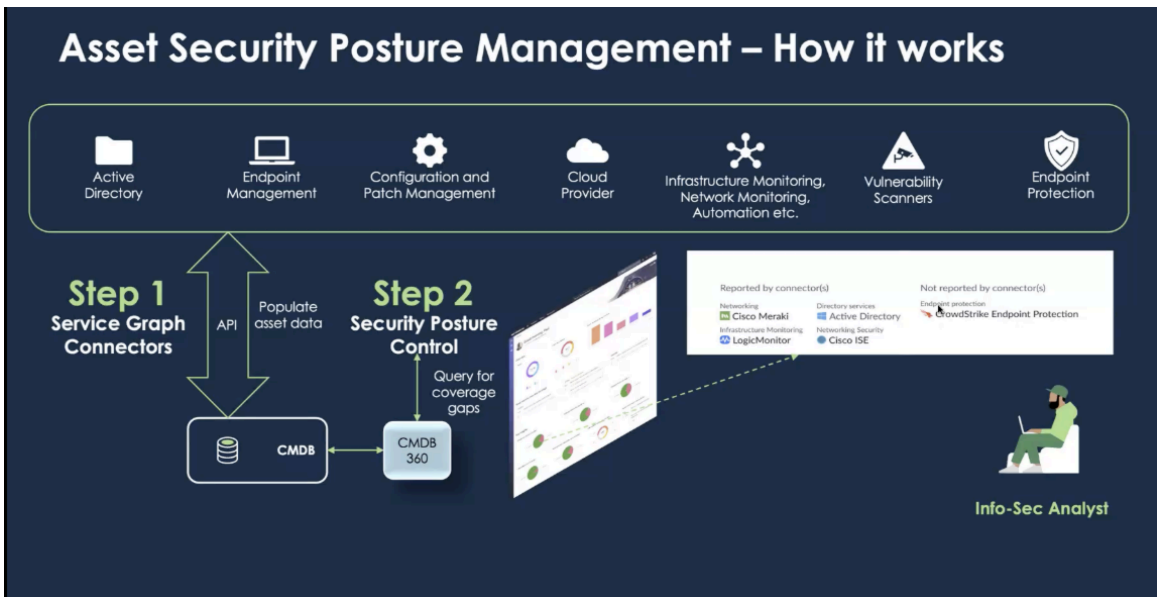
Mit dem Produkt SPC können Info-Sec-Teams die folgenden Aufgaben ausführen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie Einblicke in die Sicherheitslage für lokale und Cloud-Assets an.
- Überwachen Sie Assets auf ihre Compliance mit internen Konfigurationsstandards für Sicherheitstools, z. B. Überprüfen, ob die neueste Version eines Endpunktschutzprodukts verwendet wird.
- Automatisieren Sie Ihren Nachbesserungs-Workflow für Sicherheitslücken, die Sie mit der Anwendung „Configuration Compliance“ finden.
- Überprüfen Sie den Compliance-Status Ihrer Cloud-Umgebung für die Azure- und AWS-Cloud-Umgebungen anhand von Benchmark-Standards von Organisationen wie dem Center for Internet Security (CIS).
- Erstellen Sie benutzerdefinierte Richtlinien und Einblicke basierend auf Asset-Metadaten, Daten zur Abdeckung von Sicherheitstools und Schwachstellendaten.

## Funktionsweise von Sicherheitsstatus-Management für Assets




Sicherheitsstatus-Management für Assets identifiziert Lücken bei der Abdeckung von Sicherheitstools in Assets mithilfe von API-Integrationen mit verschiedenen Tools (Service Graph Connectors). Zu den Kategorien gehören unter anderem:

- Digitale Mitarbeiter-Experience
- Endpunktverwaltung
- Verwaltung externer Angriffsflächen
- IT Asset Management
- Infrastrukturüberwachung
- Netzwerk
- Netzwerksicherheit
- Überwachung der Netzwerkleistung
- Konfigurations- und Patch-Management
- Endpunktschutz
- Cloud-Provider
- Überwachung der Anwendungsleistung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verzeichnisdienste
- Schwachstellenbewertung

Weitere Informationen zu den unterstützten Service Graph Connectors finden Sie unter Service Graph Connectors . Unterstützte Service Graph Connectors sind über den ServiceNow® Store mit separaten Abonnements verfügbar.

ServiceNow Sicherheitsstatus-Management für Assets stützt sich auf die Asset-Daten, die aus verschiedenen Kategorien von Tools in Ihrer CMDB ausgefüllt wurden. Die Asset-Daten aus verschiedenen Quellen werden verglichen, um potenzielle Sicherheitslücken zu identifizieren. Angenommen, in der CMDB sind Asset-Daten ausgefüllt, die von Infrastrukturüberwachungs- und Netzwerkprodukten gemeldet werden. Angenommen, Daten für dieselben Assets werden nicht von Endpunktschutzprodukten gemeldet. Ein Vergleich der gemeldeten Asset-Daten in der CMDB in diesem Fall zeigt, dass den Assets ein Endpunktschutz-Agent fehlt.

Das Produkt Sicherheitsstatus-Überwachung findet Sicherheitstoollücken, indem es die folgenden Aufgaben ausführt.

1. Identifiziert die Liste aller eindeutigen Assets, die von verschiedenen Service Graph Connectors in der CMDB ausgefüllt werden.
2. Wertet Assets aus dem Bestand aus und identifiziert diejenigen, die nicht nach bestimmten Kategorien gemeldet werden, z. B. Endpunktschutz. Assets werden basierend auf einer aktivierten Richtlinie aus dem Bestand identifiziert.
3. Meldet Assets, die in der Anwendung „Configuration Compliance“ als „gemeldet“ oder „nicht gemeldet“ identifiziert wurden, als „Ergebnisse“ (Testergebnisse).
4. Priorisiert, gruppiert und weist Ergebnisse verschiedenen Teams zur Korrektur in der Anwendung „Configuration Compliance“ zu.

Um Lücken in Sicherheitstools zu identifizieren, müssen Sie die folgenden Schritte ausführen.

1. Richten Sie API-Verbindungen mit einem der Tools ein, die Sie in verschiedenen Kategorien verwenden, und aktivieren Sie sie.
2. Führen Sie eine oder mehrere Asset-Suchen basierend auf bestimmten Kriterien durch, um einen Bestand zu erhalten.
3. Aktivieren Sie die mit der Anwendung Sicherheitsstatus-Überwachung gelieferten Richtlinien, oder erstellen Sie eigene Richtlinien, und aktivieren Sie sie basierend auf den Ergebnissen Ihrer Asset-Suchen.
4. Aktivieren Sie benutzerdefinierte Einblicke, oder erstellen und aktivieren Sie Ihre eigenen Einblicke, um Ihre Assets zu überwachen.
5. Richten Sie Regeln ein, um den Fehlerkorrektur-Workflow in der Anwendung Configuration Compliance zu automatisieren.

Mit Sicherheitsstatus-Management für Assetskönnen Sie auch Assets identifizieren, bei denen Sicherheitstools in Kombination mit kritischen Schwachstellen und Internetgefährdung fehlen. Derzeit wird nur das Internet-Gefahrenpotenzial für Amazon Web Services (AWS) unterstützt. Einige der mit der Anwendung Sicherheitsstatus-Überwachung gelieferten Richtlinien suchen nach Kombinationen mit hohem Risiko aus kritischen Schwachstellen und Lücken in der Sicherheitstool-Abdeckung. Damit diese Kombinationsrichtlinien funktionieren, müssen jedoch die Anwendung Vulnerability Response und mindestens ein Schwachstellenscanner-



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsprodukt wie Qualys, Rapid7oder Tenable Vulnerability Integration installiert sein. Diese Anwendungen sind mit separaten Abonnements über den ServiceNow Storeverfügbar.

## Installieren Sie die unterstützten Anwendungen für Security Posture Control

Die für diese Integration erforderlichen Anwendungen sind im ServiceNow Storeverfügbar. Einige Anwendungen weisen Abhängigkeiten auf, die Sie separat herunterladen und installieren müssen.

### Vorbereitungen

Erforderliche Rolle: admin für Download, Installation und Aktivierung aller Anwendungen.

### Prozedur

1. Laden Sie die erforderlichen Anwendungen aus ServiceNow Store in Ihre ServiceNow -Instanz herunter.

   Die Anwendung Security Posture Control (SPC Core) stellt das Kern-Framework bereit und ist für Asset Security Posture Management (ASPM) erforderlich. Mit der Anwendung Configuration Compliance und ihren Abhängigkeiten können Sie Korrekturaufgaben für die mit Asset Security Posture Management (ASPM) und Cloud Security Posture Management (CSPM) gefundenen Schwachstellen erstellen.

| Anwendung | App-ID |
|---|---|
| Asset Security Posture Management | (Plugin-ID: sn_sec_caasm) |
| ITOM Discovery-Lizenz | (Plugin-ID: com.snc.itom.discovery.license) |
| Security Posture Control Core | (Plugin-ID: sn_sec_spc_core) |
| Configuration Compliance (enthält untergeordnete App „secops_shared_components“) | (Plugin-ID: sn_vulc) |
| Vulnerability Response-Lizenzierung und -Nutzung | (Plugin-ID: sn_vul_licensing) |
| Cloud Security Posture Management-Anwendungen | |
| Discovery-Plugin | (Plugin-ID: com.snc.discovery) |
| Cloud Configuration Governance | (Plugin-ID: sn_itom_ccg) |
| CCG-Inhaltspaket | (Plugin-ID: sn_itom_ccg_cp) |
| CMDB CI Class Models | (Plugin-ID: sn_cmdb_ci_class) |
| Cloud-Aktionsbibliothek | (Plugin-ID: com.sn.itom.cal) |

   Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

   - Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store heruntean.
   - Aktivieren Sie eine Anwendung ServiceNow Store .an.

2. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
3. Suchen Sie die Anwendungen, die Sie heruntergeladen haben, und wählen **Sie Installieren** aus, um sie zusammen mit ihren Abhängigkeiten zu aktivieren.
   Alle abhängigen Anwendungen, die zusammen mit einer Anwendung ebenfalls automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die Anweisungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind.

Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

4. Nachdem Sie die Anwendungen installiert und aktiviert haben, weisen Sie Benutzer den folgenden Security Posture Control-Gruppen zu:

   Diese Gruppen erben alle Rollen, die zum Lesen und Bearbeiten von SPC-Datensätzen erforderlich sind.

   **SPC-Administratorgruppe**

   Benutzer in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, einschließlich Lizenzierungsinformationen.

   **SPC-Analystengruppe**

   Benutzer in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, jedoch keine Schreibberechtigung. Sie können keine Lizenzierungsinformationen anzeigen.

   **Schreibgeschützte Gruppe für SPC-Analysten**

   Benutzer in dieser Gruppe können alle Datensätze für das Produkt anzeigen, haben jedoch keine Schreibberechtigung und können keine Lizenzierungsinformationen anzeigen.

## Der Security Posture Control-Arbeitsbereich

Der Security Posture Control-Arbeitsbereich enthält die Module, die Sie zum Konfigurieren, Verwenden und Überwachen der importierten Daten zu Ihren Assets verwenden.

## Die Module des Arbeitsbereichs

Um auf den Arbeitsbereich zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** Die Startseite (Zielseite) wird angezeigt. Der Security Posture Control-Arbeitsbereich enthält die folgenden Module:

### Module

| Modul | Beschreibung |
|---|---|
| Startseite | Die Abschnitte „Übersicht“, „Wichtige Einblicke“ und „Wichtige Anwendungsfallabdeckung“ enthalten Datenvisualisierungen, die Informationen zu Ihren Assets melden und überwachen. Diese Daten werden von den Richtlinien erstellt und aktualisiert, die in der Anwendung enthalten sind, nachdem Sie sie aktiviert haben. Siehe Wichtige Einblicke und benutzerdefinierte Einblicke für Security Posture Control und Richtlinien für Security Posture Control. |
| Benutzerdefinierte Einblicke | Datenvisualisierungen zu Ihren Assets, die Sie entweder mit Ihren eigenen Richtlinien oder den in der Anwendung enthaltenen Richtlinien erstellen. Weitere Informationen finden Sie unter Wichtige Einblicke und benutzerdefinierte Einblicke für Security Posture Control. |
| Asset-Suche | Suchen Sie schnell nach Assets in Ihrer Umgebung basierend auf den von Ihnen festgelegten Bedingungen. Vergewissern Sie sich, dass Sie |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Module (Fortsetzung)**

| Modul | Beschreibung |
|---|---|
| | Assets mit einer Reihe von Bedingungen finden können, bevor Sie diese Bedingungen für eine Police festlegen. Sie können diese Suchen verfeinern, sodass Sie eine Vorschau der Assets erhalten, die Ihren Suchkriterien entsprechen. Wenn Sie bereit sind, können Sie Ihre Bedingungen als Richtlinie speichern. Weitere Informationen finden Sie unter Erstellen Sie eine Asset-Suche in Security Posture Control. |
| Richtlinien und Ergebnisse | Richtlinien prüfen Ihre Assets, um Übereinstimmungen für potenzielle Verstöße zu finden. Einblicke, Visualisierungen und Anwendungsfälle hängen von Richtlinien ab. Weitere Informationen finden Sie unter Richtlinien für Security Posture Control. Die Ergebnisse entsprechen Ihren Richtlinien, die der Anwendung Configuration Compliance zur Korrektur zugeordnet sind. Weitere Informationen finden Sie unter Ergebnisse für Security Posture Control konfigurieren und anzeigen. |
| Setup für Connectors und Anwendungsfälle | Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Lücken bei der Toolabdeckung zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien, um Ihre Assets auf potenzielle Verstöße zu prüfen. Sie können auch eigene Richtlinien definieren, um die Anforderungen für Ihre spezifischen internen Sicherheitsstandards zu erfüllen. Weitere Informationen finden Sie unter Anwendungsfälle in Security Posture Control. |
| Konfiguration für benutzerdefinierte Einblicke | Sie können Ihre eigenen Einblicke erstellen, wenn Sie weitere Informationen wünschen, die nicht in den in der Anwendung enthaltenen wichtigen Einblicken enthalten sind. Sie können vorhandene Richtlinien oder Ihre eigenen benutzerdefinierten Richtlinien für die Bewertung verwenden. Ihre benutzerdefinierten Einblicke werden im Dashboard „Benutzerdefinierte Einblicke“ angezeigt. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie einen benutzerdefinierten Einblick für Security Posture Control. |

### Service Graph Connectors für Security Posture Control

Security Posture Control basiert auf API-Integrationen oder Service Graph Connectors (SGCs) als Schlüsselquelle für die Asset-Daten, die zur Identifizierung von Sicherheitslücken verwendet werden.

Security Posture Control unterstützt derzeit eine Vielzahl von Connectors, die im ServiceNow Storeverfügbar sind. Wählen Sie die Connectors aus, die Sie verwenden möchten, laden Sie die Anwendungen herunter und aktivieren Sie sie. Da Security Posture Control mehr Connectors unterstützt, wird die Liste der unterstützten Connectors, die im Store verfügbar sind, erweitert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Herunterladen, Konfigurieren und Aktivieren unterstützter Anwendungen für Service Graph Connectors finden Sie unter den folgenden Themen:

- Service Graph Connectors an.
- Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store herunter.
- Aktivieren Sie eine Anwendung ServiceNow Store .an.

Security Posture Control stellt zwei Asset-Klassen der obersten Ebene bereit, die als Teil von Richtlinien abgefragt oder ausgewertet werden können.

**Hardware-Asset**

Diese Klasse ist eine Abstraktion, die ein beliebiges lokales IP-Gerät darstellt, einschließlich PC-Geräte, Server, Netzwerkgeräte und andere Hardware.

**Virtueller Cloud-Computer**

Diese Klasse stellt einen virtuellen Computer in einer öffentlichen Cloud-Umgebung wie AWS, Azure oder GCP dar. Ein Beispiel sind EC2-Instanzen in AWS.

Richtlinien prüfen Ihre Assets auf potenzielle Verstöße basierend auf den importierten Daten aus SGCs.

Wenn eine Richtlinie versucht, eine Asset-Klasse abzurufen, die von einem bestimmten Service Graph Connector gemeldet oder nicht gemeldet wird, ordnet Security Posture Control alle relevanten Konfigurationselementklassen (Configuration Item, CI) zu, die sich auf diese Asset-Klasse in der CMDB beziehen und mit oder gefüllt werden nicht von diesem Service Graph Connector ausgefüllt.

Angenommen, eine Richtlinie sucht nach allen Hardware-Assets, die von Service Graph Connector Jamf Pro gemeldet werden. Es gilt die folgende Logik.

1. Security Posture Control identifiziert, welche CI-Klassen in der CMDB der Klasse „Hardware Asset“ für Jamf Pro zugeordnet sind.

   **Hinweis:**
   Verschiedene Service Graph Connectors füllen verschiedene CI-Klassen in der CMDB aus, und die Zuordnung von „Hardware Asset“ zu CI-Klassen variiert von Service Graph Connector zu Service Graph Connector.

2. Security Posture Control bestimmt, dass die CI-Klassen, Computer, Server und Drucker in der CMDB der Asset-Klasse „Hardware-Asset“ für Service Graph Connector Jamf Pro zugeordnet werden.
3. Security Posture Control fragt dann alle Asset-Datensätze ab, die in einer der folgenden drei CI-Klassen ausgefüllt sind: Server, Computer, Drucker, über Jamf Pro Service Graph Connector in der CMDB, und gibt diese Assets zurück.

   Sie können die Connectors und ihre Kategorien auch in der Connector-Tabelle [sn_sec_spc_core_connector] in Ihrer Instanz anzeigen.

   Sie können Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors in der Tabelle [sn_sec_spc_core_asset_type_connector] anzeigen.

   Um unterstützte Connectors im Arbeitsbereich anzuzeigen, ihren Online-Status zu überprüfen und das Setup für wichtige Anwendungsfälle anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Setup für Connectors und Anwendungsfälle** > **Registerkarte „Unterstützte Service Graph Connectors“**.

Jeder unterstützte Service Graph Connector fällt in eine der folgenden Kategorien.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Digitale Mitarbeiter-Experience
- Endpunktverwaltung
- Verwaltung externer Angriffsflächen
- IT Asset Management
- Infrastrukturüberwachung
- Netzwerk
- Netzwerksicherheit
- Überwachung der Netzwerkleistung
- Konfigurations- und Patch-Management
- Endpunktschutz
- Cloud-Provider
- Überwachung der Anwendungsleistung
- Verzeichnisdienste
- Schwachstellenbewertung

Die Spalte „Von SPC unterstützte CI-Klassen“ in der folgenden Tabelle gibt an, welche Klassen von CI-Datensätzen während einer Abfrage durch das Security Posture Control-Produkt im Rahmen einer Richtlinienbewertung berücksichtigt werden. Diese Tabelle ist keine vollständige Liste, aber Sie können sie verwenden, um zu sehen, wie erfasste Daten aus verschiedenen Kategorien und Quellen im Allgemeinen zugeordnet und abgefragt werden.

### Unterstützte SGCs

| Connector und Asset-Typ | Von SPC unterstützte CI-Klassen | Connector-Kategorie | Discovery-Quelle |
|---|---|---|---|
| Dynatrace<br><br>Hardware-Asset | cmdb_ci_server<br><br>cmdb_ci_computer | Überwachung der Anwendungsleistung | SGO-Dynatrace |
| New Relic<br><br>Hardware-Asset | cmdb_ci_server | Überwachung der Anwendungsleistung | SG-NewRelic |
| AppDynamics<br><br>Hardware-Asset | cmdb_ci_server | Überwachung der Anwendungsleistung | SG-AppDynamics |
| Azure<br><br>CloudVM | cmdb_ci_server<br><br>cmdb_ci_vm_instance | Cloud-Provider | SG-Azure |
| AWS<br><br>CloudVM | cmdb_ci_server<br><br>cmdb_ci_vm_instance | Cloud-Provider | SG-AWS |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Connector und Asset-Typ | Von SPC unterstützte CI-Klassen | Connector-Kategorie | Discovery-Quelle |
|---|---|---|---|
| GCP CloudVM | cmdb_ci_server<br>cmdb_ci_vm_instance | Cloud-Provider | SG-GCP |
| SCCM<br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_server | Konfigurations- und Patchverwaltung | SG-SCCM |
| Puppet<br>Hardware-Asset | cmdb_ci_server<br>cmdb_ci_computer | Konfigurations- und Patchverwaltung | SG-Puppet-Server |
| BigFix<br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_server | Konfigurations- und Patchverwaltung | SG-BigFix |
| VMware Workspace ONE UEM<br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_server<br>cmdb_ci_printer | Endpunktverwaltung | SG-Workspace ONE UEM |
| CrowdStrike<br>Hardware-Asset | cmdb_ci_server | Endpunktschutz | SG-CrowdStrike |
| ScienceLogic<br>Hardware-Asset | cmdb_ci_server<br>cmdb_ci_hc_device<br>cmdb_ci_computer<br>cmdb_ci_vm_instance<br>cmdb_ci_printer<br>cmdb_ci_iot | Infrastrukturüberwachung | SG-ScienceLogic |
| Datadog<br>Hardware-Asset | cmdb_ci_server | Infrastrukturüberwachung | SG-Datadog |
| LogicMonitor<br>Hardware-Asset | cmdb_ci_hc_device<br>cmdb_ci_printer<br>cmdb_ci_vm_instance<br>cmdb_ci_computer<br>cmdb_ci_server | Infrastrukturüberwachung | SG-LogicMonitor |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Connector und Asset-Typ | Von SPC unterstützte CI-Klassen | Connector-Kategorie | Discovery-Quelle |
|---|---|---|---|
| | cmdb_ci_iot | | |
| Forescout<br><br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_server<br>cmdb_ci_hc_device<br>cmdb_ci_printer<br>cmdb_ci_iot | Netzwerksicherheit | SG-Forescout |
| ExtraHop-Reveal(x)<br><br>Hardware-Asset | cmdb_ci_printer<br>cmdb_ci_server<br>cmdb_ci_computer<br>cmdb_ci_iot<br>cmdb_ci_hc_device | Netzwerksicherheit | SG-ExtraHop |
| Cisco Merak<br><br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_iot<br>cmdb_ci_hc_device<br>cmdb_ci_printer<br>cmdb_ci_server | Netzwerk | SG-Merki |
| Rapid7<br><br>Hardware-Asset | cmdb_ci_hardware | Schwachstellenbewertung | SG-Rapid7 |
| Tenable<br><br>Hardware-Asset | cmdb_ci_ot_control<br>cmdb_ci_ot_industrial_robot<br>cmdb_ci_hardware<br>cmdb_ci_hub_network<br>cmdb_ci_printer<br>cmdb_ci_ot_hmi<br>cmdb_ci_ot_industrial_actuator<br>cmdb_ci_storage_server<br>cmdb_ci_ot_plc<br>cmdb_ci_ot_historian<br>cmdb_ci_ot_rtu | Schwachstellenbewertung | SG-TenableForAssets |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Connector und Asset-Typ | Von SPC unterstützte CI-Klassen | Connector-Kategorie | Discovery-Quelle |
|---|---|---|---|
| | cmdb_ci_ot_cnc<br>cmdb_ci_computer<br>cmdb_ci_ip_firewall<br>cmdb_ci_iot<br>cmdb_ci_ot_ied<br>cmdb_ci_ot_industrial_drive<br>cmdb_ci_ot_evs<br>cmdb_ci_securitycmdb_ci_ip_switch<br>cmdb_ci_ups<br>cmbd_ci_server | | |
| Qualys-IDs<br>Hardware-Asset | cmdb_ci_computer<br>cmdb_ci_server | Schwachstellenbewertung | SCC Qualys |

### Richtlinien für Security Posture Control

Jeder Anwendungsfall hängt von einer Richtlinie oder Richtlinien ab, die Ihre Assets prüfen, um potenzielle Verstöße zu finden.

## Übersicht

Security Posture Control-Richtlinien basieren auf einem Entität-Beziehungen-Eigenschaften-Datenmodell. Sie können Richtlinien definieren, um nach einer Entität oder einem Asset zu suchen, die einem bestimmten Kriterium entspricht. Das Kriterium kann entweder in Form von Bedingungen für die Eigenschaften dieser Entität oder für die Eigenschaften einer zugehörigen Entität angegeben werden.

Derzeit können die folgenden primären oder obersten Entitäten oder Asset-Typen als Ausgangspunkt für die Definition der Richtlinien verwendet werden. Es gibt andere unterstützte Entitäten im Richtlinienschema der Security Posture Control, z. B. „Schwachstelle“ oder „Metadaten“, aber diese Entitäten können nicht der Ausgangspunkt sein. Sie können zu diesen sekundären Entitäten navigieren, indem Sie eine Beziehung aus den primären Entitäten oder den zugehörigen Entitäten verwenden.

Primäre Entitäten:

- Hardware-Asset
- Virtueller Cloud-Computer

**Entitäten und ihre Beziehungen zu sekundären Entitäten**

| Entität | Beziehung | Zielentität | Beschreibung |
|---|---|---|---|
| Hardware-Asset | Aus CI-Klasse | CMDB-Felder | Stellt Standardklassen in der CMDB oder Ihre benutzerdefinierten CI-Klassen in der CMDB dar. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Entitäten und ihre Beziehungen zu sekundären Entitäten (Fortsetzung)

| | | | |
|---|---|---|---|
| Hardware-Asset | Vom Connector gemeldet | Connector | Stellt einen Service Graph Connector dar, der diese Entität entweder gemeldet oder nicht gemeldet hat. |
| Hardware-Asset | Nicht gemeldet von | Connector | Stellt einen Service Graph Connector dar, der diese Entität entweder gemeldet oder nicht gemeldet hat. |
| Hardware-Asset | Mit Connector-Daten | Connector-Details | Stellt alle für dieses Asset verfügbaren Eigenschaften dar, die für den Service Graph Connector spezifisch sind. |
| Hardware-Asset | Mit CMDB-Metadaten | CMDBMetadaten | Stellt die Sammlung von CMDB-CI-Eigenschaften für dieses Asset dar. |
| Hardware-Asset | Mit Schwachstelle | Schwachstellendatensatz | Stellt ein angreifbares Element dar, das in diesem Asset vorhanden ist. |
| Virtueller Cloud-Computer | | | |
| Virtueller Cloud-Computer | Aus CI-Klasse | CMDB-Felder | Stellt Standardklassen in der CMDB oder Ihre benutzerdefinierten CI-Klassen in der CMDB dar. |
| Virtueller Cloud-Computer | Gemeldet von | Connector | Stellt einen Service Graph Connector dar, der dieses Cloud-Asset gemeldet hat. |
| Virtueller Cloud-Computer | Nicht gemeldet von | Connector | Stellt einen Service Graph Connector dar, der dieses Cloud-Asset nicht gemeldet hat. |
| Virtueller Cloud-Computer | Mit Connector-Daten | Connector | Stellt alle für dieses Cloud-Asset verfügbaren Eigenschaften dar, die für einen Service Graph Connector spezifisch sind. |
| Virtueller Cloud-Computer | Mit CMDB-Metadaten | CMDBMetadaten | Stellt die Sammlung von CMDB-CI-Eigenschaften für dieses Cloud-Asset dar. |
| Virtueller Cloud-Computer | Mit Schwachstelle | Schwachstellendatensatz | Stellt ein angreifbares Element dar, das in diesem Cloud-Asset vorhanden ist. |
| Virtueller Cloud-Computer | Hat Cloud-Metadaten | Cloud-Metadaten | Stellt die Sammlung von Cloud-Eigenschaften für dieses Cloud-Asset dar. |
| Virtueller Cloud-Computer | Der Port ist für das Internet verfügbar | Offener Port | Stellt einen Port in diesem Cloud-Asset dar, der für das Internet geöffnet ist. |

### Alle Entitäten und Eigenschaften, die für diese Entitäten unterstützt werden

| Entität | Eigenschaften |
|---|---|
| Hardware-Asset | Keine |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Alle Entitäten und Eigenschaften, die für diese Entitäten unterstützt werden (Fortsetzung)**

| | |
|---|---|
| Virtueller Cloud-Computer | • Cloud-Konto-ID<br>• Cloud-Region<br>• Cloud-Provider |
| Virtueller Cloud-Computer – Service Graph Connector | • Kategorie: Kategorie oder Typ von Service Graph Connector, z. B. Endpunktschutz.<br>• Produktname: Name des Produkts, das Assets über Service Graph Connector meldet. |
| Virtueller Cloud-Computer – Connector-Daten | Details, die für Kategorien und Typen von Connectors spezifisch sind, z. B. Softwaredetails, Asset-Details, Netzwerkschnittstellendetails |
| CMDB-Metadaten – Verbindung | • Enthält Modellinformationen: Modellname, Anzeigename, Hersteller.<br>• Mit installierter Software – Deinstallationszeichenfolge, Version, Name. |
| CMDB-Metadaten – Eigenschaft | Cloud-Eigenschaften wie Hostname, Seriennummer, BS-Domäne. |
| Cloud-Metadaten | • Cloud-Region<br>• Internet – Gefährdung<br>• Cloud-Provider<br>• Cloud-Konto-ID |
| Schwachstelle | • Hat-Exploit<br>• Schweregrad<br>• CVE-ID |
| Öffnen Sie Port | • Port (offener Port, z. B. 22)<br>• Protokoll (z. B. TCP). |

## In der Anwendung enthaltene Richtlinien

Es gibt einige Richtlinien, die in der Security Posture Control-Anwendung enthalten sind, die an wichtige Anwendungsfälle gebunden sind und letztendlich als wichtige Einblicke im Dashboard auf der Zielseite (Startmodul) im SPC-Arbeitsbereich angezeigt werden. Um diese Richtlinien anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Alle**.

Diese Richtlinien können nicht bearbeitet werden. Sie können die Metadaten jedoch ändern. Sie können diese Richtlinien klonen, um eigene benutzerdefinierte Richtlinien zu erstellen.

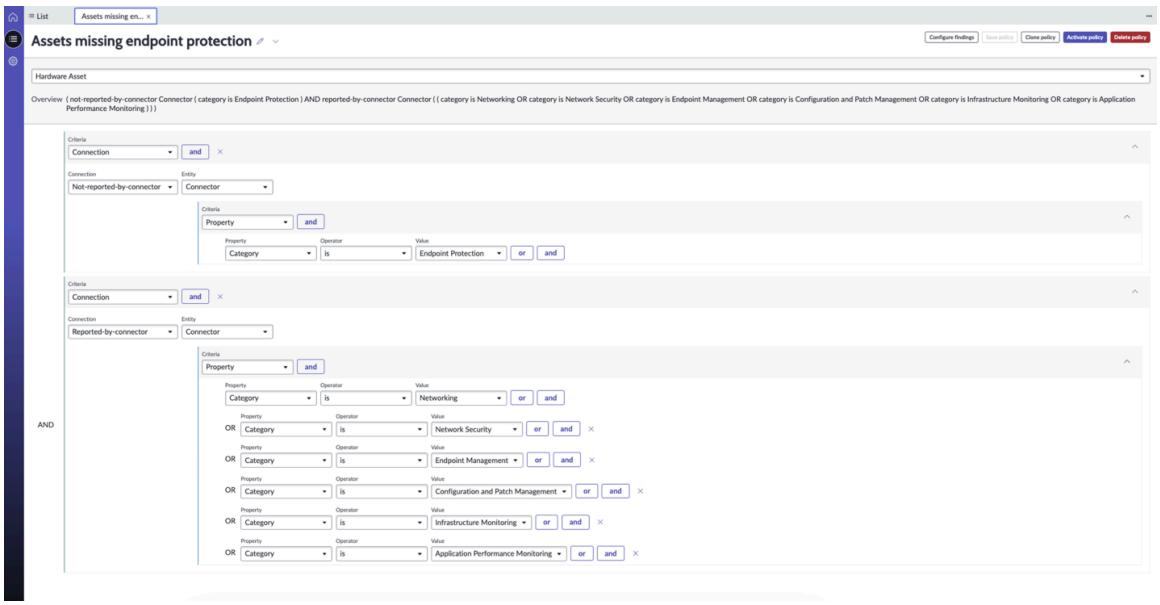


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie jedoch, dass die von Ihnen geklonten Richtlinien nicht als wichtige Einblicke im Dashboard auf der Zielseite der Homepage mit den anderen wichtigen Einblicken angezeigt werden.

Nachdem Sie die von Ihnen erstellten Richtlinien geklont und aktiviert haben, erstellen Sie Ihren eigenen benutzerdefinierten Einblickdatensatz im Modul „Generator für benutzerdefinierte Einblicke“ im Arbeitsbereich (letztes Modul im Navigationsbereich) und zeigen die Daten im Dashboard „Benutzerdefinierte Einblicke“ (das zweite Symbol von) an oben im Arbeitsbereich).

Die folgende Abbildung zeigt eine Richtlinie, die im Produkt enthalten ist und nach Assets ohne Endpunktschutz sucht. Die Bedingungen dieser Richtlinie suchen nach Assets, die nicht von Service Graph Connector der Kategorie „Endpunktschutz“ gemeldet werden und von Service Graph Connectors in einer der folgenden Kategorien gemeldet werden: Netzwerk, Infrastrukturüberwachung oder Cloud-Provider.




## Eigene Richtlinien erstellen

Sie können eigene Richtlinien erstellen, um Ihre Assets zu überwachen. Diese Richtlinien basieren auf Daten aus den verschiedenen von Ihnen installierten und aktivierten Service Graph Connectors, die Connector-spezifische Metadaten für die Assets enthalten, z. B.:

- CrowdStrike-Agent-Version
- Dem Internet ausgesetzt
- Kritische Schwachstellen

Sie können entweder eine vorhandene Richtlinie klonen und Bedingungen hinzufügen oder eine Richtlinie von Grund auf neu erstellen. Für Ihre benutzerdefinierten Richtlinien können Sie Bedingungen für Metadaten wie Betriebssystem, Betriebssystemversion und FQDN einbeziehen, um beispielsweise Assets mit älterer Software zu überwachen. Beachten Sie, dass es sich bei diesen Eigenschaften um allgemeine CMDB-Eigenschaften handelt, die von verschiedenen Service Graph Connectors für ein bestimmtes Asset ausgefüllt werden.

Sie können auch eine Bedingung für genehmigte Ausnahmen mit der Anwendung Governance, Risk, and Compliance (GRC) hinzufügen, die Sie nicht überwachen und in Ihre Asset-Anzahlen einbeziehen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Basisrichtlinien und untergeordnete Richtlinien

Sie können mehrere Richtlinien verwenden, um Ihre Assets zu bewerten und eigene benutzerdefinierte Einblicke zu erstellen. Sie können mehr als eine Richtlinie verwenden, wenn Sie die Anzahl der übereinstimmenden Assets aus einer großen Stichprobe reduzieren oder sich auf mehr als eine Übereinstimmungsbedingung konzentrieren möchten. Angenommen, Sie möchten ein Vergleichsdiagramm erstellen, das zeigt, wie viele Ihrer gesamten Assets, sowohl lokal als auch in der Cloud, nicht auf Schwachstellen gescannt wurden.

Sie können auch untergeordnete Richtlinien aus einem beliebigen Richtliniendatensatz erstellen, um Ihre Suchkriterien weiter zu verfeinern und spezifischere Übereinstimmungen zurückzugeben. Alle Bedingungen in der Basisrichtlinie werden auch in der untergeordneten Richtlinie geerbt.

Wenn Sie mehr als eine Richtlinie hinzufügen:

- Ebene 1 ist die Basis. Diese Richtlinie fragt eine umfangreiche Stichprobengröße in (N) ab, z. B. alle Ihre Assets in Active Directory, die vom Active Directory-Service Graph Connector gemeldet werden.
- Ebene 2 wertet die Ergebnisse der ersten Richtlinie aus. Diese Richtlinie wertet nur eine Teilmenge von (N) aus. Geben Sie beispielsweise von allen Assets in Active Directory nur die Assets mit Schwachstellenbewertungstools zurück, die nicht auf Schwachstellen gescannt wurden.
- Ebene 3 wertet die Ergebnisse der Richtlinien 1 und 2 aus usw. Beispiel: Von allen Assets in Active Directory mit Schwachstellenbewertungstools, die nicht auf Schwachstellen gescannt werden, geben Sie nur die fehlenden Endpunktschutz-Agents zurück.
- Hinweis: Sie können mehrere Richtlinien in einer Hierarchie haben. Mit der Hierarchie können Sie die verschiedenen Klassifizierungen anzeigen, wie Ihre Assets den einzelnen Ebenen in der Hierarchie entsprechen.

Um eine untergeordnete Richtlinie zu erstellen, wählen Sie in einem Richtliniendatensatz **Neue Richtlinie** aus, und legen Sie die gewünschten Bedingungen fest. Sie haben die Möglichkeit, die Bedingungen einer vorhandenen Richtlinie als Start zu verwenden und Ergebnisse aus vorhandenen Richtlinien und genehmigten Ausnahmen auszuschließen. Weitere Informationen finden Sie unter Erstellen, klonen und aktivieren Sie eine Richtlinie für Security Posture Control.

Wenn Sie Richtlinien für benutzerdefinierte Einblicke auswählen, können Sie keine untergeordnete Richtlinie auf derselben Ebene wie eine übergeordnete Richtlinie auswählen, es sei denn, Sie ändern die Hierarchie.

## Metadaten- und CMDB-Filterung

Für Ihre Sicherheitsteams kann es wichtig sein, Assets mit älterer Software zu überwachen. Sie können Richtlinienkriterien angeben, um die unten aufgeführten allgemeinen Eigenschaften einzubeziehen.

- BS
- BS-Version
- Hostname
- FQDN
- IP-Adresse
- IP-Version



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Netzmaske
- MAC-Adresse
- MAC-Hersteller
- Software
- RAM
- Seriennummer
- NIC
- Seriennummertyp
- Standort
- CPU-Anzahl
- Festplattenspeicher

**Hinweis:**
Um diese Metadaten zu erfassen, müssen die folgenden Eigenschaften in der CMDB-Metadatenverbindung verfügbar sein, die von Ihren Service Graph Connectors ausgefüllt wird.

## Ausnahmen bei der Anwendung Governance, Risk, and Compliance (GRC).

Eine IRM-Ausnahme (Integrated Risk Management) ist ein Asset mit einer genehmigten Ausnahme aus dem Governance, Risk, and Compliance (GRC)-Produkt. Sie haben die Möglichkeit, in einer Richtlinie eine Bedingung für eine Ausnahme hinzuzufügen, damit Sie diese Assets nicht überwachen und in Ihre Zählungen einbeziehen.

Beispielsweise können für einige Assets Ausnahmen für bestimmte Kontrollziele mit IRM genehmigt werden. Um die Anzahl der zurückgegebenen Übereinstimmungen zu reduzieren, möchten Informationssicherheitsteams diese Assets möglicherweise von der Überwachung auf Sicherheitskontrollen mit bereits genehmigten IRM-Ausnahmen ausschließen.

### Aktivieren Sie eine Richtlinie für einen Anwendungsfall in Security Posture Control

Richtlinien, die in der Anwendung enthalten sind, müssen aktiviert werden, bevor Security Posture Control die Assets überwachen kann, die dieser Richtlinie entsprechen. Standardmäßig ist keine der in der Anwendung enthaltenen Richtlinien aktiviert.

**Vorbereitungen**
Sie müssen Richtlinien manuell aktivieren, nachdem Sie sich vergewissert haben, dass alle erforderlichen Voraussetzungen erfüllt sind:

- Service Graph Connectors aktiviert.
- Alle erforderlichen Anwendungen wie Vulnerability Response werden installiert und aktiviert, falls für Anwendungsfälle zutreffend.

**Hinweis:**
Sie können eine Richtlinie, die in der Anwendung enthalten ist, nicht bearbeiten. Sie können jedoch die Metadaten bearbeiten (Bleistiftsymbol in der Nähe des Namens der Richtlinie im Datensatz) und eine neue Richtlinie basierend auf den Bedingungen einer vorhandenen Richtlinie klonen oder erstellen.

Erforderliche Rollen:

- SPC-Administratorgruppe
- SPC-Analystengruppe



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.
2. Wählen Sie einen Richtliniendatensatz aus, um ihn zu öffnen.
3. Für einen Richtliniendatensatz, der nicht aktiviert ist, haben Sie die folgenden Optionen:

| Option | Beschreibung |
|---|---|
| Richtlinie deaktivieren | Deaktivieren Sie eine aktive Richtlinie, wenn keine Assets überwacht oder anhand dieser Richtlinie ausgewertet werden sollen oder wenn Sie die Bedingungen bearbeiten möchten. Diese Bearbeitungsoption ist nur für aktive Policendatensätze sichtbar. |
| Richtlinie speichern | Speichern Sie Ihre Richtlinienbedingungen. |
| Ergebnisse konfigurieren | ○ Wählen Sie **Ja** aus, wenn Sie möchten, dass Ihre Ergebnisse gemäß den Regeln, die Sie in der Anwendung „Configuration Compliance“ eingerichtet haben, gruppiert und zur Korrektur zugewiesen werden. Diese Ergebnisse können Ergebnisse sein, die Sicherheitslücken aufdecken.<br>○ Wählen Sie **Nein**, wenn die Ergebnisse automatisch geschlossen werden sollen. Diese Ergebnisse können Ergebnisse sein, die keine Sicherheitslücken offenlegen.<br>○ Klicken Sie auf den Link Zuweisungsregeln **konfigurieren**, um Zuweisungsregeln in der Anwendung „Configuration Compliance“ einzurichten, um Ergebnisse für Ihre Richtlinie zur Lösung zuzuweisen. |
| Richtlinie klonen | Erstellen Sie eine neue Richtlinie mit denselben Bedingungen wie diese Richtlinie als Ausgangspunkt. Weitere Informationen finden Sie unter Erstellen, klonen und aktivieren Sie eine Richtlinie für Security Posture Control. |
| Erstellen Sie eine untergeordnete Richtlinie | Erstellen Sie eine untergeordnete Richtlinie, die die Bedingungen der aktuellen Richtlinie übernimmt. Die aktuellen Richtlinienbedingungen werden im Feld „Basisrichtlinie“ des neuen Datensatzes angezeigt, und Sie fügen weitere Bedingungen hinzu. |
| Richtlinie aktivieren | Aktivieren Sie diese Richtlinie, damit sie Assets durchsucht, Übereinstimmungen findet und Ergebnisse generiert. |
| Richtlinie löschen | Löschen Sie diese Richtlinie. Die Löschoption wird nicht für Richtlinien unterstützt, für die bereits |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | Ergebnisse generiert wurden. Sie können diese Richtlinien nur mit Ergebnissen deaktivieren. |

Um festzustellen, ob eine Richtlinie aktiviert ist, bestätigen Sie ihren Status (wahr oder falsch) in der Spalte Aktiv **Alle** > **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.

### Erstellen, klonen und aktivieren Sie eine Richtlinie für Security Posture Control

Erstellen Sie Ihre eigenen benutzerdefinierten Richtlinien, um Assets auf Toolabdeckung und andere Kombinationen mit hohem Risiko zu überwachen.

#### Vorbereitungen

Bevor Sie beginnen, lesen Sie den in Anwendungsfälle in Security Posture Control beschriebenen Anwendungsfall für die Erkennung von Assets mit Schwachstellen und Sicherheitstool-Abdeckungslücken, um sicherzustellen, dass Sie Service Graph Connector für das CrowdStrike-Produkt aktiviert und die Vulnerability Response-Anwendung installiert haben.

Um die zum Erstellen einer Richtlinie erforderlichen Schritte zu verstehen, folgen Sie dem folgenden Beispiel. Angenommen, Sie möchten für diese Richtlinie eine Richtlinie erstellen, die alle Assets findet, die vom CrowdStrike-Produkt nicht erkannt oder gemeldet werden und die die log4shell-Schwachstelle „CVE-2021-44228“ aufweisen.

Erforderliche Rollen:

- SPC-Administratorgruppe
- SPC-Analystengruppe

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**.
2. Wählen Sie **Neue Richtlinie**aus.
3. Wählen Sie oben neben dem Namen das Stiftsymbol aus, um die Metadaten zu ändern.

   Füllen Sie die Felder aus.

| Feld | Beschreibung |
| --- | --- |
| Name | Ein eindeutiger Name für Ihre Richtlinie. |
| Relevanz | Wählen Sie einen aus der Liste aus. |
| Kurzbeschreibung | Eine eindeutige Beschreibung für Ihre Richtlinie. |

4. Wählen **Sie Metadaten speichern aus**.
5. Wählen Sie im ersten Feld des Formulars **Hardware-Asset** aus der Liste aus.

   Beachten Sie die Optionen Basisrichtlinie und Ausschlussrichtlinien rechts auf der Seite.

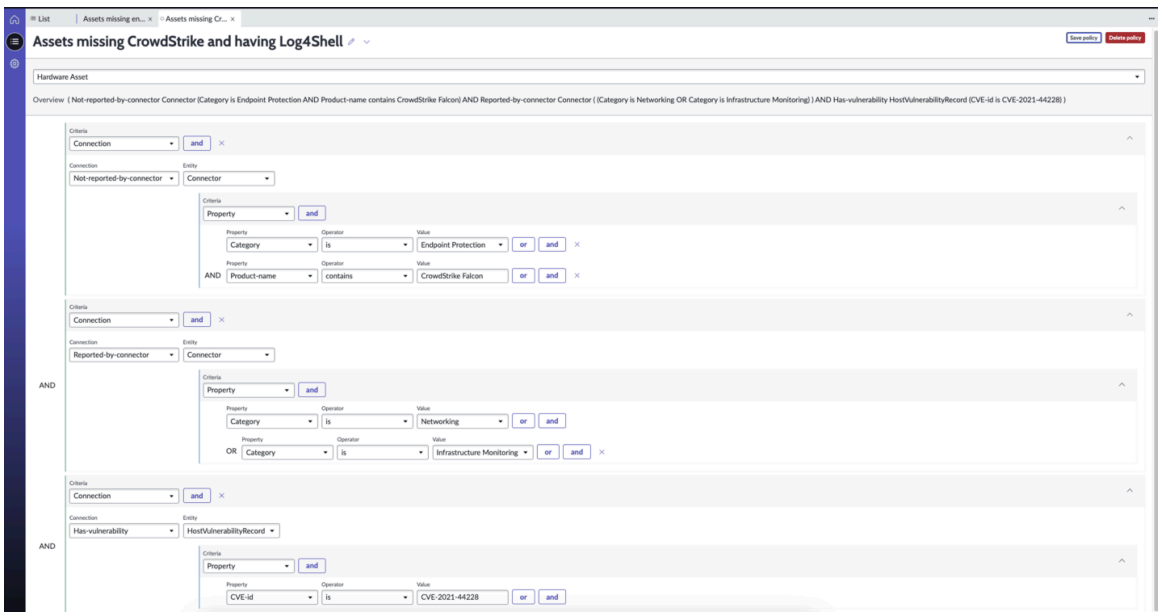
   - Basisrichtlinie – Sie können die Bedingungen einer vorhandenen Richtlinie erben, um sie als Basis für diese Richtlinie als Ausgangspunkt zu verwenden.
   - Ausschlussrichtlinien: Sie können übereinstimmende Assets aus einer vorhandenen Richtlinie oder Richtlinien ausschließen, sodass ihre Ergebnisse in dieser Richtlinie ignoriert werden. Mit dieser Option können Sie die zurückgegebenen Ergebnisse für diese Richtlinie weiter verfeinern oder genehmigte Ausnahmen für Assets ignorieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Felder Verbindung und Entität werden angezeigt.

6. Wählen Sie **Nicht gemeldet von** aus der Liste für das Feld Verbindung aus.
   Das Feld Zielentität wird automatisch mit Service Graph Connector ausgefüllt. Eine neue Bedingung mit dem Feld Kriterien wird mit den Feldern Eigenschaft, Operator und Wert angezeigt. Die Eigenschaft wird im Feld Kriterien angezeigt.
7. Wählen Sie **[Kategorie][ist][Endpunktschutz]** aus der angezeigten Werteliste aus.
8. Wählen Sie den Operator **und** rechts neben dem Feld Wert aus, das mit Endpunktschutz gefülltwird.
9. Wählen Sie im nächsten **Feldsatz [Product-name][is][CrowdStrike] aus**.
10. Wählen Sie den Operator **und** oben neben dem ersten mit Service Graph Connector ausgefüllten Entitätsfeld aus, um neue Verbindungs- und Entitätsfelder anzuzeigen.
11. Wählen Sie **Gemeldet von aus**.
    Das Feld Entität wird automatisch ausgefüllt (Service Graph Connector). Eine neue Bedingung (Kriterien) wird mit Feldern für Eigenschaft, Operator und Wert angezeigt. **Die Eigenschaft** wird im Feld Kriterien angezeigt.
12. Wählen Sie **[Kategorie][ist][Netzwerk] aus**.
13. Wählen Sie den Operator **und** neben dem mit Netzwerk ausgefüllten Feld Wert aus.
14. Wählen Sie **[Kategorie][ist][Infrastrukturüberwachung] aus**.
15. Wählen Sie den Operator **und** in der Sekunde aus, in der das mit Service Graph Connector ausgefüllteEntitätsfeld ausgefüllt wird.
16. Wählen Sie im neuen Feld Verbindung die Option **Mit Schwachstelle**aus.
    Das Feld Entität wird automatisch mit Schwachstelle ausgefüllt.
17. Wählen Sie **[CVE-id][is]** aus, und geben **Sie CVE-2021-44228 ein**.
    Die Richtlinienbedingungen müssen mit dem Image übereinstimmen.




18. Wählen **Sie Richtlinie speichern**aus, konfigurieren Sie die Ergebnisse, und aktivieren Sie die Richtlinie.

Nachdem Sie eine Richtlinie gespeichert und aktiviert haben, wertet sie die importierten Daten aus dem in der nächsten Ausführung geplanten SGC aus. Wenn Sie die Daten im Dashboard für benutzerdefinierte Einblicke im Arbeitsbereich anzeigen möchten, müssen Sie im Dashboard (letztes Symbol im Arbeitsbereich) im Konfigurationsmodul



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für benutzerdefinierte Einblicke einen neuen Einblick erstellen. Nachdem Sie den benutzerdefinierten Einblick aktiviert haben, werden seine Daten im Dashboard „Benutzerdefinierte Einblicke“ im Arbeitsbereich angezeigt (zweites Symbol).

19. Wählen Sie im Menü rechts neben Richtlinie speichern die **Option Ergebnisse konfigurieren**aus.
20. Füllen Sie die Felder aus.
21. Wählen **Sie Konfiguration speichern aus**.
22. **Wahlweise:** Wenn Sie diese Richtlinie oder eine vorhandene Richtlinie klonen möchten, wählen Sie im Menü neben **Richtlinie aktivieren die Option Richtlinieklonen**aus.

    (Optional) Sie können eine untergeordnete Richtlinie aus erstellen, indem Sie eine beliebige Richtlinie als Basis verwenden, um vorhandene Richtlinien zu erweitern, ohne die Bedingungen erneut eingeben zu müssen. Alle Bedingungen in der Basisrichtlinie werden auch in der untergeordneten Richtlinie geerbt. Ein neuer Richtliniendatensatz wird mit dem Namen der geklonten Richtlinie geöffnet, gefolgt von „Kopie“.

    Wählen Sie **Ausschlussrichtlinien** aus, und wählen Sie Richtlinien aus, die Sie von den Ergebnissen dieser Richtlinie ausschließen möchten. Alle Ergebnisse in Ihrer neuen Richtlinie, die einer vorhandenen Richtlinie oder Richtlinien entsprechen, werden nicht in Ihre Ergebnisse aufgenommen.
23. Wählen Sie **Basisrichtlinie** aus, und wählen Sie eine aktive Richtlinie als übergeordnete Richtlinie aus.

    Sie können diese Option auswählen, wenn Sie die Bedingungen einer vorhandenen Richtlinie als Ausgangspunkt für Ihre neue Richtlinie verwenden möchten.

    Wenn Sie mehr als eine Richtlinie hinzufügen, beachten Sie die folgende Hierarchie. Sie können mehrere Richtlinien in einer Richtlinienhierarchie haben. Für jede Richtlinie können Sie die verschiedenen Klassifizierungen anzeigen, wie Ihre Assets den einzelnen Ebenen entsprechen.

    - Ebene 1 ist die Basis. Diese Richtlinie fragt eine umfangreiche Stichprobengröße in (N) ab, z. B. alle Ihre Assets in Active Directory, die vom Active Directory-Service Graph Connector gemeldet werden.
    - Ebene 2 wertet die Ergebnisse der ersten Richtlinie aus. Diese Richtlinie wertet nur eine Teilmenge von (N) aus. Geben Sie beispielsweise von allen Assets in Active Directory nur die Assets mit Schwachstellenbewertungstools zurück, die nicht auf Schwachstellen gescannt wurden.
    - Ebene 3 wertet die Ergebnisse der Richtlinien 1 und 2 aus usw. Beispiel: Von allen Assets in Active Directory mit Schwachstellenbewertungstools, die nicht auf Schwachstellen gescannt werden, geben Sie nur die fehlenden Endpunktschutz-Agents zurück.

    **Hinweis:**
    Sie können mehrere Richtlinien in einer Hierarchie haben. Mit der Hierarchie können Sie die verschiedenen Klassifizierungen anzeigen, wie Ihre Assets den einzelnen Ebenen in der Hierarchie entsprechen.
24. Speichern Sie Ihre Richtlinie.
    Ihre Richtlinie wird in der Liste Alle im Listenmodul im Arbeitsbereich angezeigt.
25. Um eine Richtlinie zu aktivieren, öffnen Sie den Richtliniendatensatz und wählen Sie **Richtlinie aktivieren**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wichtige Einblicke und benutzerdefinierte Einblicke für Security Posture Control

Wichtige und benutzerdefinierte Einblicke bieten visuelle Berichte, die anhand der Bewertungskriterien erstellt und aktualisiert werden, die Ihren Assets entsprechen.

## Wichtige Einblicke

Die für die Bewertungen Ihrer Assets verwendeten Kriterien werden von den Richtlinien bereitgestellt, die in der Anwendung enthalten sind.

- Wichtige Einblicke verwenden die Richtlinien, die in der Anwendung enthalten sind.
- Benutzerdefinierte Einblicke können mithilfe der in der Anwendung enthaltenen Richtlinien, Ihrer eigenen benutzerdefinierten Richtlinien oder einer Kombination aus beidem erstellt werden.

Auf der Startseite (Zielseite) im Arbeitsbereich „Security Posture Control“ werden im Abschnitt „Wichtige Einblicke“ unter der Übersicht visuelle Berichte angezeigt, die anhand der in der Anwendung enthaltenen Richtlinien erstellt und aktualisiert werden. Diese Einblicke sind auch in der Anwendung enthalten und zeigen die folgenden Informationen an:

- Installierter Endpunktschutz-Agent: Gesamtzahl der Assets, die über Endpunktschutz verfügen oder nicht.
- Abdeckung verwalteter Geräte: Anzahl der verwalteten Assets im Vergleich zu nicht verwalteten Assets.
- Abdeckung durch Schwachstellenscan: Gesamtzahl der gescannten Assets im Vergleich zu den Assets, die nicht von einem Drittanbieter-Schwachstellenscanner auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Anzahl der Assets aus der Gesamtzahl der Assets mit kritischen Schwachstellen.
- Angreifbare Elemente nach Relevanz: Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach ihrem Schweregrad. Eine bekannte Schwachstelle, die einem Asset in Ihrer CMDB entspricht, führt zu einem angreifbaren Element. Für diesen Einblick müssen Sie die Anwendung Vulnerability Response und mindestens eine Scanner-Integration installieren: Qualys, Rapid7 oder Tenable Vulnerability Integration. Alle diese Anwendungen sind auf der ServiceNow® Storeverfügbar.
- Top-3-Richtlinien nach Ergebnissen: Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.

## Benutzerdefinierte Einblicke

Sie können eigene Einblicke erstellen, wenn Sie weitere Informationen wünschen, die nicht in den wichtigsten Einblicken enthalten sind. Sie können diese benutzerdefinierten Einblicke erstellen und vorhandene Richtlinien oder Ihre eigenen benutzerdefinierten Richtlinien für die Bewertung verwenden. Ihre benutzerdefinierten Einblicke werden im Dashboard-Modul „Benutzerdefinierte Einblicke“ angezeigt, dem zweiten Symbol von oben im Arbeitsbereich.

### Erstellen und aktivieren Sie einen benutzerdefinierten Einblick für Security Posture Control

Sie können Ihre eigenen Einblicke erstellen. Benutzerdefinierte Einblicke sind Einblicke, die Sie entweder mit vorhandenen Richtlinien oder Ihren eigenen benutzerdefinierten Richtlinien erstellen können.

**Vorbereitungen**
Sie müssen einen Einblicksdatensatz erstellen und aktivieren, bevor Sie Ihre Daten im Dashboard „Benutzerdefinierte Einblicke“ anzeigen können. Sie können bis zu sechs



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einblicke und 21 Diagramme im Dashboard-Modul „Benutzerdefinierte Einblicke“ im Arbeitsbereich haben.

Alle Richtlinien, die Sie für einen benutzerdefinierten Einblick verwenden, müssen aktiviert sein.

Erforderliche Rollen:

- SPC-Administratorgruppe
- SPC-Analystengruppe

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Generator für benutzerdefinierte Einblicke** (letztes Symbol im Arbeitsbereich).

   Auf dieser Zielseite gibt es drei Registerkarten:

   **Aktiv**

   Ihre aktivierten benutzerdefinierten Einblicke. Aktivierte benutzerdefinierte Einblicke werden auf der Zielseite „Benutzerdefinierte Einblicke“ angezeigt (zweite Symbol von oben im Arbeitsbereich).

   **Inaktiv**

   Ihre inaktiven benutzerdefinierten Einblicke. Deaktivierte Einblicke werden erst auf der Zielseite für benutzerdefinierte Einblicke angezeigt, wenn die Einblicke und die sie unterstützenden Richtlinien aktiviert sind.

   **Alle**

   Alle Ihre aktiven und inaktiven benutzerdefinierten Einblicke.

2. Wählen Sie rechts auf der Seite **Neuer Einblick** aus, um einen neuen Datensatz zu erstellen.
3. Wählen Sie im Feld Typ einen Einblick aus der Auswahlliste aus.

| Option | Beschreibung |
|---|---|
| Vergleichsdiagramm | Vergleichen Sie die Anzahl übereinstimmender Assets für bis zu fünf Policen. |
| Widget für Anzahl der Richtlinienübereinstimmungen | Die Gesamtzahl der Assets, die einer Police oder Policen entsprechen. |
| Diagramm für prozentuale Richtlinienübereinstimmung | Der Prozentsatz Ihrer gesamten Assets, die einer Police entsprechen oder nicht entsprechen. |
| Diagramm für Trend der Richtlinienübereinstimmung | Historischer Trend von Assets, die einer Police oder Policen entsprechen. |

4. Wählen Sie die Richtlinien und Einblicksbezeichnungen aus, die Sie für Ihre Einblicksdaten benötigen.
5. Wählen Sie **Speichern**.
   Ihr Einblick wird auf der Registerkarte Inaktiver Einblick gespeichert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um Ihren neuen Einblick zu aktivieren, öffnen Sie den Datensatz in der Liste „Inaktiv“ und wählen Sie **Aktivieren**aus.
   Daten werden aus dem nächsten geplanten Import für die Service Graph Connectors gesammelt, die den Richtlinien des Einblicks zugeordnet sind, und die Daten werden im Dashboard-Modul „Benutzerdefinierte Einblicke“ im Arbeitsbereich angezeigt.

### Ergebnisse für Security Posture Control konfigurieren und anzeigen

Sie können die Ergebnisse anzeigen, die durch die Auswertung von Richtlinien in Security Posture Control im Security Posture Control Workspace generiert wurden.

## Übersicht

Alle übereinstimmenden Assets werden als „Ergebnisse“ gemeldet. Sie können Ergebnisse konfigurieren, die aus der Ausführung von Richtlinien generiert werden sollen, sodass diese Ergebnisse verschiedenen Teams zur Korrektur zugewiesen oder für die Berichterstellung verwendet werden können. Security Posture Control veröffentlicht diese Ergebnisse als „Testergebnisse“ im Configuration Compliance-Modul. Alle administrativen Steuerungen in der Anwendung „Configuration Compliance“, die sich auf Zuweisung und Gruppierung beziehen, d. h. Generierung von Korrekturaufgaben, Korrekturzielen und Ausnahmen, werden für Ergebnisse unterstützt, die von Security Posture Control generiert werden.

Die Arten der Ergebnisse:

**Toolabdeckung**

Dieser Typ stellt eine Sicherheitstool-Abdeckungslücke dar. Dieser Ergebnistyp gilt für Richtlinien mit den Connector-Beziehungen „Gemeldet von“ und „Nicht gemeldet“.

**Internet-Gefahrenpotenzial**

Dieser Typ stellt die Internetgefährdung eines Cloud-Assets dar. Dieser Ergebnistyp gilt für Richtlinien, bei denen die Beziehung „Hat Port mit dem Internet verbunden“ auf virtuellen Cloud-Computern verwendet wird.

**Kombination mit hohem Risiko**

Dieser Typ stellt ein Problem dar, dem mehr als ein Risikofaktor zugeordnet ist, z. B. Assets mit kritischen Schwachstellen und ein fehlender Endpunktschutz-Agent.

**IRM-Ausnahme (Integrated Risk Management).**

Dieser Typ stellt ein Asset mit einer genehmigten Ausnahme vom Produkt Governance, Risk, and Compliance (GRC) dar. Wenn angegeben, werden diese Ausnahmen nicht in die Anzahl der Ergebnisse einbezogen.

Sicherheitsstatusbezeichnungen werden generiert und an die Testergebnisse angehängt. Eine Bezeichnung eines geeigneten Typs, z. B. „Toolabdeckung“, wird Testergebnissen basierend auf dem Typ der Police automatisch zugewiesen.

Durch die Verwendung von Sicherheitsstatusbezeichnungen, die den Ergebnissen zugeordnet sind, können Sie Zuweisungsregeln in Configuration Compliance schreiben, um diese Probleme zur Korrektur an die entsprechenden Teams weiterzuleiten. Sie können beispielsweise die Ergebnisse der Toolabdeckung an ein IT-Team und die Ergebnisse der Internetexposition an ein Anwendungsteam senden.

Wenn jedoch einer der Korrekturbesitzer das Problem in einer Kombination behebt, wird die andere Suche automatisch geschlossen, da diese Ergebnisse aus einer Richtlinie generiert werden, die nach der Kombination sucht. Wenn das IT-Betriebsteam beispielsweise die Suche nach „Toolabdeckung“ durch Installation des Endpunktschutz-Agent schließt, wird die aus dieser Richtlinie generierte Suche nach „Gefahrenpotenzial des Internets“ automatisch geschlossen, obwohl das Asset mit dem Internet verbunden ist, da diese Suche



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus generiert wird eine Richtlinie, die nach einer Kombination von Problemen sucht. Wenn Sie Probleme mit dem Internet-Gefahrenpotenzial für Assets nachverfolgen möchten, wird empfohlen, eine andere Richtlinie zu erstellen, die nur das Internet-Gefahrenpotenzial für die Assets ohne andere Risikofaktoren untersucht.

## Ort zum Anzeigen von Ergebnissen

Sie haben diese Optionen, um die Ergebnisse anzuzeigen, die durch die Bewertung von Richtlinien generiert wurden.

- Navigieren zu **Security Posture Control Workspace** > **Lists** > **Ergebnisse** > **Alle.**
- Wählen Sie in einem **Policendatensatz Ergebnisse anzeigen**aus. Die Liste zeigt Gruppen von Ergebnissen an, die sie in allgemeine Kategorien wie „Kombination mit hohem Risiko“, „Gefahrenpotenzial im Internet“ usw. einordnen. Diese Gruppen sind jedoch keine formalen Gruppierungen, die zur Korrektur verwendet werden können. Sie müssen Korrektur- und Zuweisungsregeln in Configuration Compliance für Ergebnisse einrichten.
- Wählen Sie in der Anwendung „Configuration Compliance“ **Testergebnisse** aus, und filtern Sie die Datensätze nach **Quelle ist ServiceNow SPC**.

## Das Dashboard

Im Security Posture Control-Arbeitsbereich werden auf der Startseite (Zielseite) die folgenden Visualisierungen angezeigt:

**Übersicht**

- Assets: Anzahl der lokal und in der Cloud überwachten Assets.
- Ergebnisse nach Relevanz: Anzahl der kritischen Ergebnisse aus Ihren Assets insgesamt.
- Von Top-5-Quellen überwachte Assets: Top 5 der Service Graph Connectors, die über Assets berichten.
- Cloud-Konten: Anzahl der von AWS und Azure überwachten Cloud-Konten.
- Offene und geschlossene Ergebnisse: Vergleich von Datensätzen, die noch verarbeitet werden oder auf eine Lösung warten, und Datensätzen, die gelöst wurden.

**Wichtige Einblicke**

- Installierter Endpunktschutz-Agent: Gesamtzahl der Assets mit oder ohne Endpunktschutz.
- Abdeckung verwalteter Geräte: Anzahl der verwalteten Assets im Vergleich zu nicht verwalteten Assets.
- Abdeckung durch Schwachstellenscan: Gesamtzahl der gescannten Assets im Vergleich zu der Anzahl, die nicht von einem Drittanbieter-Schwachstellenscanner auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Anzahl der Assets aus der Gesamtzahl der Assets mit kritischen Schwachstellen.
- Angreifbare Elemente nach Relevanz: Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach ihrem Schweregrad. Eine bekannte Schwachstelle, die einem Asset in Ihrer CMDB entspricht, führt zu einem angreifbaren Element.
- Top-3-Richtlinien nach Ergebnissen: Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Abdeckung wichtiger Anwendungsfälle

Wählen Sie einen Anwendungsfall aus, und wählen Sie **Hilfe bei der Aktivierung** oder **Hilfe bei der Verbesserung**, um anzuzeigen, welche Service Graph Connectors und Richtlinien für die wichtigsten Anwendungsfälle aktiviert werden sollen.

### Erstellen Sie eine Asset-Suche in Security Posture Control

Legen Sie Ihre Bedingungen fest, und suchen Sie nach Assets anhand bestimmter Service Graph Connector-Produkte oder nach Assets, deren bestimmte Daten von einem Connector gemeldet werden.

#### Vorbereitungen

Beispiel für Suche: Sie möchten Assets mit Windows-Servern und einer bestimmten Version identifizieren, die in den CrowdStrike-Metadatendetails gefunden wurde.

Erforderliche Rollen:

- SPC-Administratorgruppe
- SPC-Analystengruppe

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Asset-Suche**.
2. Wählen Sie einen aus.

| Option | Bezeichnung |
|---|---|
| **Option** | Beschreibung |
| **Hardware-Asset** | Durchsuchen Sie lokale Assets |
| **Virtueller Cloud-Computer** | Durchsuchen Sie Cloud-Assets |

   Wählen Sie für dieses Beispiel **Hardware-Asset** für Asset-Typ aus.
3. **Wahlweise:** Wählen Sie **Basisrichtlinie** und **Ausschlussrichtlinien** aus, wenn Sie die Bedingungen einer vorhandenen Richtlinie als Ausgangspunkt verwenden und Assets ausschließen möchten, die vorhandenen Richtlinien entsprechen.
   Die von Ihnen ausgewählten Richtlinien werden angezeigt.
4. Wählen Sie **Mit Connector-Daten** für das Feld Verbindung aus.
5. Wählen **Sie CrowdStrike-Gerätedetails** für die Entität aus.
6. Wählen Sie für Eigenschaft, Operator und Wert **[Agent-Version][ist]** aus, und geben Sie die Version ein, z. B. **6.26.14003.0**.
7. Wählen Sie den Operator und rechts neben dem Feld Entität mit CrowdStrike-Gerätedetails als Wert für eine weitere Bedingung aus.
8. Wählen Sie **Mit CMDB-Metadaten** für das Feld Verbindung aus.
   Das Feld Entität wird mit CMDB-Metadaten ausgefüllt.
9. Wählen Sie **Eigenschaft** für das Feld Kriterien aus.
10. Wählen Sie für Eigenschaft, Operator und Wert **[BS][enthält]**, und geben Sie **Windows-Server**ein.
11. Wählen Sie **Assets anzeigen aus**.
    Nach einiger Zeit werden die Ergebnisse auf der Registerkarte Übereinstimmende Assets angezeigt.
    Wenn keine Übereinstimmungen angezeigt werden, können Sie Ihre Suche verfeinern. Nachdem Sie die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen korrekt festgelegt haben, können Sie die Suche als Richtlinie speichern und aktivieren. Wie andere Richtlinien durchsucht sie Ihre Assets kontinuierlich mit einem Hintergrundauftrag, nachdem Sie sie aktiviert haben.

### Anwendungsfälle in Security Posture Control

Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Lücken bei der Toolabdeckung zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien, um Ihre Assets auf potenzielle Verstöße zu prüfen. Sie können auch eigene Richtlinien definieren, um die Anforderungen für Ihre spezifischen internen Sicherheitsstandards zu erfüllen.

## Anwendungsfälle

Die Anwendung Security Posture Control unterstützt verschiedene Anwendungsfälle, die in der Anwendung enthalten sind. Anwendungsfälle helfen Ihnen, bestimmte Arten von Toolabdeckungslücken in Ihren Assets, die Internetgefährdung von Cloud-Assets und Kombinationen mit Schwachstellen zu identifizieren. Die Richtlinien, die Sie für die unterstützten Anwendungsfälle benötigen, sind ebenfalls im Produkt enthalten.

Sie können den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle auf der Startseite (Zielseite) im Security Posture Control-Arbeitsbereich unter anzeigen **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Startseite** auf dem Startseitenmodul (Zielseite).

Alternativ können Sie die unterstützten Service Graph Connectors und den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle auf den Registerkarten „Unterstützte Service Graph Connectors“ und „Setup für wichtige Anwendungsfälle“ unter anzeigen **Alle** > **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Setup für Connectors und Anwendungsfälle** (das Zahnradsymbol).

### Hinweis:

Auf der Registerkarte „Wichtige Anwendungsfälle“ auf den Zielseiten der Homepage werden nicht alle möglichen Anwendungsfälle aufgelistet. Sie erhalten einige wichtige Anwendungsfälle, die Sie aktivieren, um Ihnen den Einstieg in die Bereitstellung von Security Posture Control-Produkten zu erleichtern.

Vergewissern Sie sich, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie Richtlinien für die mit der Anwendung bereitgestellten unterstützten Anwendungsfälle aktivieren.

- Sie haben alle in Installieren Sie die unterstützten Anwendungen für Security Posture Controlbeschriebenen erforderlichen Anwendungen installiert und konfiguriert.
- Sie müssen mindestens eine der folgenden Voraussetzungen für jeden Anwendungsfall erfüllt haben.

1. Sie verwenden derzeit oder installieren und aktivieren Service Graph Connectors für verschiedene Kategorien.

   Zu den Kategorien für die Anwendungsfälle gehören Service Graph Connectors, die Sie aktivieren müssen, um erste Einblicke zu erhalten, und Service Graph Connectors, die Sie aktivieren können, um die Abdeckung für die von Security Posture Control überwachten Assets zu verbessern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Sie verwenden derzeit oder installieren und aktivieren die Anwendung Vulnerability Response.
3. Sie verwenden derzeit oder konfigurieren den Cloud-Konto-Scan für Ihre AWS- und Azure-Konten unter „Cloud Security Posture Management“.

Spezifische Anforderungen für jeden unterstützten Anwendungsfall werden in den folgenden Abschnitten beschrieben. Darüber hinaus müssen Sie eine oder mehrere der mit Security Posture Control gelieferten Richtlinien für einen Anwendungsfall aktivieren. Dieses Konzept wird auch in den folgenden Abschnitten behandelt.

### Anwendungsfall Security Posture Control: Erkennen von Assets mit fehlendem Endpunktschutz

Um Assets zu erkennen, für die ein Endpunktschutz-Agent fehlt, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist. Abhängig von Ihrem Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

Wenn Ihr Ziel beispielsweise darin besteht, nur Cloud-Assets mit fehlendem Endpunktschutz zu überwachen, müssen Sie nur einen Service Graph Connector für Endpunktschutz und mindestens einen Cloud-Provider aktivieren: AWS, Azure oder GCP. Sie müssen keine separaten Service Graph Connectors für Netzwerk, Infrastrukturüberwachung usw. aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpunktschutz“.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Netzwerk (nur für lokale Assets erforderlich)
   b. Infrastrukturüberwachung (nur für lokale Assets erforderlich) .
   c. Verzeichnisdienste (nur für lokale Assets erforderlich. Diese Kategorie umfasst Active Directory.
   d. Cloud-Provider (erforderlich für die Überwachung von Cloud-Assets für diesen Anwendungsfall).
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von Security Posture Control gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Endpunktverwaltung.
   c. Konfigurations- und Patch-Management.
   d. Überwachung der Anwendungsleistung.

Nachdem Sie überprüft haben, ob diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors unter der Kategorie „Cloud-Provider“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Security Posture Control.

- Assets ohne Endpunktschutz
- Cloud-Assets ohne Endpunktschutz



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Anwendungsfall Security Posture Control: Erkennen von Assets, die von Tools zur Schwachstellenbewertung übersehen wurden

Um Assets zu erkennen, die von Tools zur Schwachstellenbewertung übersehen wurden, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist. Abhängig von Ihrem Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

Wenn Ihr Ziel beispielsweise darin besteht, nur Cloud-Assets zu überwachen, die von Tools zum Scannen von Schwachstellen übersehen wurden, müssen Sie nur einen Service Graph Connector für Endpoint Protection und mindestens einen Cloud-Anbieter aktivieren: AWS, Azure oder GCP. Sie müssen keine separaten Service Graph Connectors für Netzwerk, Infrastrukturüberwachung usw. aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Schwachstellenbewertung“.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Netzwerk (nur für lokale Assets erforderlich)
   b. Infrastrukturüberwachung (nur für lokale Assets erforderlich) .
   c. Verzeichnisdienste (nur für lokale Assets erforderlich. Diese Kategorie umfasst Active Directory.
   d. Cloud-Provider (erforderlich für die Überwachung von Cloud-Assets für diesen Anwendungsfall).
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von Security Posture Control gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Endpunktverwaltung.
   c. Konfigurations- und Patch-Management.
   d. Überwachung der Anwendungsleistung.

Nachdem Sie überprüft haben, ob diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors unter der Kategorie „Cloud-Provider“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Security Posture Control.

- Assets wurden nicht auf Schwachstellen gescannt.
- Cloud-Assets wurden nicht auf Schwachstellen gescannt.

### Anwendungsfall Security Posture Control: Nicht verwaltete Assets erkennen

Dieser Anwendungsfall umfasst zwei Teile: das Erkennen von Assets, bei denen Konfigurations- und Patch-Management-Agents fehlen.

Um Assets zu erkennen, für die Konfigurations- und Patch-Management-Tools fehlen, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängig von Ihrem Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren. Beispiel: Wenn Ihr Ziel darin besteht, nur Cloud-Assets zu überwachen, für die Konfigurations- und Patch-Management-Tools fehlen, müssen Sie nur einen Service Graph Connector für Endpoint Protection und mindestens einen Cloud-Anbieter aktivieren: AWS, Azure oder GCP. Sie müssen keine separaten Service Graph Connectors für Netzwerk, Infrastrukturüberwachung usw. aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus den Kategorien „Konfiguration“ und „Patch Management“.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Netzwerk (nur für lokale Assets erforderlich)
   b. Infrastrukturüberwachung (nur für lokale Assets erforderlich) .
   c. Verzeichnisdienste (nur für lokale Assets erforderlich. Diese Kategorie umfasst Active Directory.
   d. Cloud-Provider (erforderlich für die Überwachung von Cloud-Assets für diesen Anwendungsfall).
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von Security Posture Control gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Endpunktverwaltung.
   c. Endpunktschutz
   d. Schwachstellenbewertung
   e. Überwachung der Anwendungsleistung.

Nachdem Sie überprüft haben, ob diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors unter der Kategorie „Cloud-Provider“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Security Posture Control.

- Assets ohne Konfiguration und ohne Patch-Management.
- Cloud-Assets ohne Konfiguration und ohne Patch-Verwaltung.

### Anwendungsfall Security Posture Control: Erkennen von Assets, für die eine Endpunktverwaltungslösung fehlt

Um Assets zu erkennen, für die eine Endpunktverwaltungslösung fehlt, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist.

Abhängig von Ihrem Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren. Wenn Ihr Ziel beispielsweise darin besteht, nur Cloud-Assets mit fehlenden Endpunktverwaltungstools zu überwachen, müssen Sie nur einen Service Graph Connector für Endpunktschutz und mindestens einen Cloud-Anbieter aktivieren: AWS, Azure oder GCP. Sie müssen keine separaten Service Graph Connectors für Netzwerk, Infrastrukturüberwachung usw. aktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpoint Management“.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Netzwerk (nur für lokale Assets erforderlich)
   b. Infrastrukturüberwachung (nur für lokale Assets erforderlich) .
   c. Verzeichnisdienste (nur für lokale Assets erforderlich. Diese Kategorie umfasst Active Directory.
   d. Cloud-Provider (erforderlich für die Überwachung von Cloud-Assets für diesen Anwendungsfall).
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von Security Posture Control gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Endpunktverwaltung.
   c. Endpunktschutz
   d. Schwachstellenbewertung
   e. Überwachung der Anwendungsleistung.

Nachdem Sie überprüft haben, ob diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors unter der Kategorie „Cloud-Provider“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Security Posture Control.

- Assets mit fehlender Endpunktverwaltungslösung.
- Cloud-Assets ohne Endpunktverwaltungslösung.

### Anwendungsfall Security Posture Control: Erkennen von Assets mit Schwachstellen und Sicherheitstool-Abdeckungslücken

Sie können Assets mit kritischen Schwachstellen identifizieren, in denen kritische Sicherheitstools wie Endpunktschutz fehlen, um diese Assets für die Korrektur zu priorisieren. Im Lieferumfang von Security Posture Control sind einige Richtlinien zur Unterstützung dieses Anwendungsfalls enthalten.

Dieser Anwendungsfall erfordert die Installation der Vulnerability Response-Anwendung und einer Integration mit mindestens einem Schwachstellenbewertungsprodukt wie Qualys, Rapid7 oder Tenable.

Die folgenden Richtlinien sind im Produkt Security Posture Control enthalten, um diesen Anwendungsfall für Assets mit kritischen Schwachstellen zu unterstützen, für die auch keine Sicherheitstools abgedeckt sind.

1. Assets mit kritischen Schwachstellen und fehlendem Endpunktschutz
2. Assets mit kritischen Schwachstellen und fehlender Konfiguration und Patch-Verwaltung
3. Assets mit kritischen Schwachstellen und fehlender Endpunktverwaltung
4. Cloud-Assets mit kritischen Schwachstellen und fehlendem Endpunktschutz



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Cloud-Assets mit kritischen Schwachstellen und fehlender Konfiguration und Patch-Verwaltung
6. Cloud-Assets mit kritischen Schwachstellen und fehlender Endpunktverwaltung

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpoint Management“.
   - Endpunktschutz (erforderlich für Richtlinien 1 und 4).
   - Configuration and Patch Management (erforderlich für Richtlinien 2 und 4).
   - Endpoint Management (erforderlich für Richtlinien 3 und 6).
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Netzwerk (nur für lokale Assets erforderlich)
   b. Infrastrukturüberwachung (nur für lokale Assets erforderlich) .
   c. Verzeichnisdienste (nur für lokale Assets erforderlich. Diese Kategorie umfasst Active Directory.
   d. Cloud-Provider (erforderlich für die Überwachung von Cloud-Assets für diesen Anwendungsfall).
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von Security Posture Control gemeldet und überwacht werden.
   a. Netzwerksicherheit.
   b. Endpunktverwaltung.
   c. Endpunktschutz
   d. Schwachstellenbewertung
   e. Überwachung der Anwendungsleistung.

Nachdem Sie überprüft haben, ob diese Voraussetzungen erfüllt sind, müssen Sie mindestens eine der Richtlinien aktivieren. Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors unter der Kategorie „Cloud-Provider“ aktiviert sein. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Security Posture Control.

### Anwendungsfall Security Posture Control: Erkennen der Internetgefährdung von Cloud-Assets und Kombinationen mit hohem Risiko

Es ist wichtig, die potenzielle Internetgefährdung von Cloud-Assets (virtuelle Computer) an verschiedenen Ports zu überwachen, um sicherzustellen, dass Schwachstellen in diesen Assets nicht remote ausgenutzt werden. Dieser Anwendungsfall hilft Ihnen, diese Assets zu identifizieren.

Mit Security Posture Control können Sie die Konfiguration von Cloud-Assets auswerten, um die Assets mit Internetverbindung zu identifizieren, d. h. welche Assets von überall im Internet erreichbar sind und an welchen Ports sie vorhanden sind.

Security Posture Control kombiniert diese Einblicke mit Sicherheitstool-Abdeckungslücken und Schwachstellendaten von Drittanbieter-Scannern wie Qualys, Rapid7 und Tenable, um Kombinationen mit hohem Risiko zu identifizieren.

Derzeit unterstützt dieser Anwendungsfall AWS und erfordert die folgenden Voraussetzungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Service Graph Connector für AWS wird für von Ihnen konfigurierte AWS-Konten aktiviert.
2. Sie haben eine oder mehrere der im Produkt enthaltenen Richtlinien in Security Posture Control aktiviert.
   - Cloud-Assets mit SSH-Port 22, der für das Internet geöffnet ist.
   - Cloud-Assets mit SSH-Port 22, der für das Internet geöffnet ist, und ohne Endpunktschutz.
   - Cloud-Assets mit HTTP-Port 80, der für das Internet geöffnet ist, und ohne Endpunktschutz.
   - Cloud-Assets mit kritischen Schwachstellen und SSH-Port 22 offen für das Internet (Erfordert Vulnerability Response).
   - Cloud-Assets mit kritischen Schwachstellen, fehlendem Endpunktschutz und SSH-Port 22 offen für Internet (Erfordert Vulnerability Response).
   - Cloud-Assets mit für das Internet geöffneten HTTP-Ports, kritischen Schwachstellen und fehlendem Endpunktschutz (Erfordert Vulnerability Response).

[store-future: BEGIN review]

## Integration von Cloud Security Posture Management mit Amazon Web Services

Die von ServiceNow entwickelte CSPM-Anwendung (Cloud Security Posture Management) scannt Ihre Cloud-Umgebung kontinuierlich, um Nichteinhaltungen oder Konfigurationsverstöße gegen Compliance-Frameworks wie CIS zu identifizieren.

## Wichtige Begriffe und Konzepte

Derzeit unterstützt CSPM von ServiceNow CIS AWS Foundations Benchmark v1.4.0. Dieses Modul erfasst die Konfigurationsdaten von Cloud-Assets in Ihrer AWS-Umgebung direkt aus der Cloud, importiert sie in Ihre Now Platform-Instanz und prüft sie auf Compliance.

**Region**

Regionen beziehen sich auf einen geografischen Bereich, den Ihre AWS Cloud-Services unterstützen. Regionen haben Standardendpunkte, mit denen Sie auf die unterstützten Services für diese Region zugreifen können. Beispiele für Regionen sind „Virginia“ oder „OHO“ in den USA oder andere RECHENZENTRUM-Standorte außerhalb der USA.

**Ressource**

Ressource ist ein Begriff, der in der AWS-Umgebung verwendet wird und die AWS-Assets und ihre Konfigurationseinstellungen beschreibt. Ressourcen sind die Services in Ihren AWS-Umgebungen. In Ihrer Now Platform -Instanz werden Ressourcen als Ihre Assets oder Konfigurationselemente (CIs) bezeichnet.

**Center for Internet Security (CIS)**

CIS ist eine Community-orientierte, Non-Profit-Organisation, die für die CIS-Steuerungen ® und CIS-Benchmarks ™verantwortlich ist, global anerkannte Prozesse zur Sicherung von IT-Systemen und -Daten. Derzeit verwendet die CSPM-Anwendung ServiceNow die in CIS AWS Foundations 1.4.0 veröffentlichten Richtlinien, um die Compliance Ihrer Cloud-Assets zu prüfen.

**Richtlinie (Konfigurationsrichtlinien)**

Richtlinien sind Governance-Leitlinien. In Now Platformwerden Richtlinien als Konfigurationsrichtlinien bezeichnet. Die von ServiceNow entwickelte CSPM-Anwendung bietet Baseline-Konfigurationsrichtlinien, um Ihre Cloud-Umgebung anhand von Benchmark-Standards



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wie CIS zu bewerten. Zwischen den Konfigurationsrichtlinien und den in den Compliance-Frameworks bereitgestellten Richtlinien besteht eine 1:1-Zuordnung.

**Richtliniensatz (Konfigurationsrichtliniengruppen)**

Richtliniensätze sind Gruppen einzelner Richtlinien. In Now Platformwerden Richtliniensätze als Konfigurationsrichtliniengruppen bezeichnet.

**Cloud Security Posture Management**

Richtlinien (**Konfigurationsrichtlinien**) und Richtliniensätze (**Konfigurationsrichtliniengruppen**) befinden sich im Modul **Cloud Security Posture Management**, das in Ihrer Instanz für diese Integration erstellt wurde.

**Test**

Tests sind Bibliotheken von Datensätzen, die Scans Ihrer Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets geregelt werden soll, um die Compliance zu gewährleisten. Tests werden in der Anwendung Configuration Compliance verwendet, um Assets für die Korrektur zu gruppieren.

**Testergebnisse**

Testergebnisse (TR) werden in Ihrer Instanz erstellt, wenn bei einem Audit festgestellt wird, dass eine Ressource in Ihrer Cloud-Umgebung nicht konform ist. Testergebnisse werden in der Anwendung Configuration Compliance in Ihrem Now Platformgespeichert. Diese Datensätze zeigen die Ergebnisse (Bestanden/Fehlgeschlagen) der Audits an, die für Ihre Ressourcen ausgeführt werden.

**Testergebnisgruppen**

Testergebnisgruppen helfen Ihnen, Testergebnisse in logischen Gruppen zu organisieren und Ihre Korrekturaufgaben zu priorisieren.

## Erforderliche Now Platform-Rollen

Sicherheitsadministratoren mit der Rolle „sn_vul.cspm_security_admin“ können dieses Produkt verwenden. Cloud-Konto-Scans können auch von Benutzern mit der Rolle sn_vul.cspm_cloud_account_admin konfiguriert werden.

Eine vollständige Liste der erforderlichen Rollen für diese Integration finden Sie unter .

## Workflow

- Die in der Anwendung enthaltenen Richtliniensätze (**Konfigurationsrichtliniengruppen**) definieren, welche Daten Sie importieren.
- Importierte Ressourcenkonfigurationsdaten werden in temporären Tabellen in Ihrer Now Platform -Instanz gespeichert. Diese gespeicherten Daten werden dann auf Compliance mit den im CIS Amazon Web Services Foundations Benchmark v1.4.0 aufgeführten Richtlinien geprüft.
- Die Ergebnisse der Audits werden als Testergebnisse und Testergebnisgruppen in der Anwendung Configuration Compliance in Ihrer Plattforminstanz erstellt.
- Sie können Testergebnisse, Testergebnisgruppen und andere Configuration Compliance -Daten in Dashboards und in Datensätzen in der Anwendung Configuration Compliance anzeigen. Sicherheitsmanager, Schwachstellenmanager und Schwachstellenanalysten können diese Daten verwenden, um konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren, zu priorisieren und darauf zu reagieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Datenerfassung

Um die AWS Cloud-Konfigurationsdaten in Ihrer Umgebung zu erfassen, rufen Sie die Cloud-API AWS über einen MID Server in Ihrer Instanz Now Platform® auf. Sie rufen die Daten für die AWS-Ressourcen in Ihrer Unternehmensumgebung ab. Die Daten in Ihren Ressourcen können die folgenden Informationen enthalten, die Sie für Audits importieren können:

- Identitäts- und Zugriffsverwaltung (IAM)
- Speicher
- Protokollierung
- Überwachung
- Netzwerk

## Beispiele für Sicherheits- und Konfigurationsabweichungen in Ihren importierten Daten

Die folgende Liste enthält einige Beispiele für nicht konforme Ressourcen oder Abweichungen von einer ordnungsgemäßen Sicherheitspraxis bei der Asset-Konfiguration:

- Suchen Sie nach S3-Buckets, die zur öffentlichen Ansicht geöffnet sind.
- Suchen Sie nach S3-Buckets, die nicht verschlüsselt sind.
- IAM-Benutzerschlüssel werden nicht rotiert.
- Überprüfen Sie, ob der Zugriff auf VM-Images (VM) von bestimmten Anbietern eingeschränkt ist.
- Überprüfen Sie, welche Ihrer IP-Adressen öffentlich sind.
- Überprüfen Sie, ob die Multifaktor-Authentifizierung (MFA) für S3-Buckets aktiviert ist.

## Richtlinien und Benchmark-Standards

In der CIS Amazon Web Services Foundations Benchmark v1.4.0 sind 58 Richtlinien definiert. 47 dieser Richtlinien sind in Ihrer Instanz als Teil dieser Anwendung codiert. Die 11 manuellen Richtlinien, die auch im Benchmark aufgeführt sind, werden von dieser Anwendung nicht unterstützt.

[End]
[store-future: BEGIN review]

### Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für AWS

Die für diese Integration erforderlichen Anwendungen sind im ServiceNow® Store verfügbar und unter dem Link „Abhängigkeiten und Lizenzierung anzeigen“ auf der Seite mit der App-Liste aufgeführt. Einige Anwendungen weisen Abhängigkeiten auf, die Sie separat herunterladen und installieren müssen.

**Vorbereitungen**
Erforderliche Rolle: admin für Download, Installation und Aktivierung aller Anwendungen.

Der Administrator weist die folgenden Rollen zu. Diese Now Platform® Rollen sind für die Anwendung erforderlich.

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 
- Aktivieren Sie eine Anwendung ServiceNow Store .

### Prozedur

1. Klicken Sie auf den Link in der erhaltenen E-Mail, um auf die Anwendungen für diese Integration in der ServiceNow Storezuzugreifen.

   Um die Abhängigkeiten für eine Anwendung anzuzeigen, klicken Sie auf der Anwendungsseite in ServiceNow Storeauf **Abhängigkeiten und Lizenzierungsanforderungen anzeigen** unter „Abhängigkeiten und Lizenzierung“.

   **Hinweis:**
   Die Anwendung Cloud Security Posture Management befindet sich unter dem Link „ **Innovation Lab** “ von ServiceNow Store. Die anderen Anwendungen finden Sie unter **Apps und Lösungen**.

2. Installieren Sie die Anwendungen in der folgenden Reihenfolge.

| Anwendung | App-Version und Abhängigkeits-Plugins |
|---|---|
| Plattformversion | San Diego vx.xx |
| Vulnerability Response (Abhängigkeiten) | v x.xx |
| Configuration Compliance (Abhängigkeiten) | v x.xx |
| CMDB CI Class Models | Installieren Sie CMDB CI Class Models , branch Master |
| Security Support Common | Installieren Sie Security Support Common (Plugin-ID: com.snc.security_support.common) aus dem Repository , branch feature/ EPIC1037528_native_cspm |
| Security Integration Framework | Installieren Sie Security Integration Framework (Plugin-ID: com.snc.sec.int.framework) aus dem Repository , Verzweigungsfunktion/ EPIC1037528_native_cspm |
| Security Support Orchestration | Installieren Sie Security Support Orchestration (Plugin-ID: com.snc.secops.orchestration) aus dem Repository , Verzweigung „secops-dev“. |
| Vulnerability Response (Kernanwendung) | Installieren Sie Vulnerability Response (Plugin-ID: com.snc.vulnerability) aus dem Repository , Verzweigungsfunktion/EPIC1037528_native_cspm |
| Configuration Compliance (Kernanwendung) | Installieren Sie Configuration Compliance (Plugin-ID: com.snc.vulc) aus dem Repository , Verzweigungsfunktion/EPIC1037528_native_cspm |
| Vulnerability Response und Configuration Compliance für Cloud | Installieren Sie Vulnerability Response and Configuration Compliance for Cloud (Plugin-ID: com.snc.vul_cloud) aus dem Repository , Verzweigung Scratch/STRY53500471_overview |
| Performance Analytics for Vulnerability Response | Installieren Sie Performance Analytics for Vulnerability Response (Plugin-ID: com.snc.vulnerability.analytics) |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendung | App-Version und Abhängigkeits-Plugins |
|---|---|
| | aus dem Repository , branch feature/ EPIC1037528_native_cspm |
| ServiceNow IntegrationHub Enterprise Pack-Installationsprogramm | ServiceNow IntegrationHub Enterprise Pack Installer installieren (Plugin-ID: com.glide.hub.integrations.enterprise) |
| Cloud Provisioning and Governance Core | Cloud Provisioning and Governance Core installieren (Plugin-ID: com.snc.cloud.core) |
| Cloud-Aktionsbibliothek | Installieren Sie die Cloud-Aktionsbibliothek (Plugin-ID: com.sn.itom.cal) aus dem Repository , Verzweigung „Master“. |
| Cloud Configuration Governance | Installieren Sie Cloud Configuration Governance (Plugin-ID: com.sn.itom.ccg) , Verzweigung Master |
| Cloud Security Posture Management | Installieren Sie Cloud Security Posture Management (Plugin-ID: com.snc.secops.cspm) aus dem Repository , Verzweigung „Scratch/Develop“. |

3. Nachdem Sie die Anwendungen von ServiceNow Storeheruntergeladen haben, navigieren Sie in Ihrer Instanz von Now Platform zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
4. Suchen Sie die in der vorherigen Tabelle aufgeführten Anwendungen, und klicken Sie auf **Installieren**, um sie zu aktivieren.
   Alle abhängigen Anwendungen, die zusammen mit einer Anwendung ebenfalls automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die Anweisungen. Vergewissern Sie sich, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind.

   Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.
5. Nachdem Sie die Anwendungen installiert und aktiviert haben, weisen Sie die folgenden Rollen zu, sofern sie noch nicht zugewiesen sind.

   Diese Rollen sind für verschiedene Workflow-Aktivitäten in der -Integration erforderlich:

   - discovery_admin oder sn_cmmp.cloud_admin – richtet die Cloud-Servicekonten unter Now Platform für die entsprechenden AWS-Servicekonten ein.
   - cspm_security_admin Diese Rolle erbt auch die folgenden Rollen:
     - sn_itom_ccg.governor – erstellt neue Richtlinien, Richtliniensätze und Sammler. Die Rolle „Kontrolle“ führt die Testrichtlinie aus und erstellt neue Entitäten, die vom Planungsadministrator verwendet werden.
     - sn_itom_ccg.operator – der Operator Cloud Configuration Governance testet die Richtlinien und überprüft die Ergebnisse. Der Operator korrigiert auch Testergebnisse und Testergebnisgruppen.
     - sn_itom_ccg.scheduling_admin – richtet Cloud Configuration Governance für die AWS-Servicekonten ein. Erstellt Scan-Konfigurationen und Scan-Zeitplan. Hat Zugriff auf Scan-Ergebnisse, um importierte Entitäten und Richtlinien anzuzeigen.
   - cspm_cloud_account_admin Diese Rolle erbt auch die Rolle sn_itom_ccg.scheduling_admin.
   - mid_server – konfiguriert einen MID-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vulc.admin – konfiguriert die Anwendung Configuration Compliance, hat Transparenz für alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Configuration Compliance zu. Weitere Informationen zu Rollen in der Anwendung Configuration Compliance finden Sie unter Mit Configuration Compliance installierte Komponenten.
- sn_vuln.admin – konfiguriert die Anwendung Performance Analytics for Vulnerability Response.

Führen Sie die folgenden Schritte aus, damit Sie einen Scan-Datensatz erstellen können, um die Assets in Ihrer AWS-Umgebung zu scannen.

6. Wenn dies noch nicht geschehen ist, richten Sie AWS-Servicekonten und -Anmeldeinformationen sowie einen Alias für Anmeldeinformationen ein.
   Ein Benutzer mit der Rolle discovery_admin oder sn_cmmp.cloud_admin richtet die Servicekonten Amazon Web Services (AWS) ein. Weitere Informationen finden Sie unter . Diese Anmeldeinformationen werden in der Spalte Discovery-Anmeldeinformationen in den von Ihnen erstellten Cloud-Servicekonten-Datensätzen angezeigt.
7. Konfigurieren Sie Richtlinien mit der erforderlichen Berechtigungsebene, um Zugriff auf die AWS-Ressourcen für Cloud Discovery und Cloud Provisioning and Governance bereitzustellen.
   Platzieren Sie das folgende JSON-Objekt in Ihrem Anhang, um Ihre Berechtigungen zu erstellen. Kopieren Sie den Text, und nehmen Sie die erforderlichen Änderungen vor. Verwenden Sie diese Datei, um Ihre Richtlinienberechtigungen zu erstellen. Dies sind mindestens die Berechtigungen, die für diese Anwendung erforderlich sind. Weitere Informationen finden Sie unter .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GenerateCredentialReport",
    "access-analyzer:ListAnalyzers",
    "iam:GetPolicyVersion",
    "iam:GetAccountPasswordPolicy",
    "iam:ListServerCertificates",
    "s3:GetBucketLogging",
    "cloudtrail:GetTrailStatus",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeRegions",
    "logs:DescribeMetricFilters",
    "cloudtrail:GetEventSelectors",
    "iam:ListVirtualMFADevices",
    "s3:GetEncryptionConfiguration",
    "kms:GetKeyRotationStatus",
    "iam:ListAttachedUserPolicies",
    "rds:DescribeDBInstances",
    "iam:GetCredentialReport",
    "ec2:DescribeNetworkAcls",
    "iam:ListPolicies",
    "sns:ListSubscriptionsByTopic",
    "iam:ListEntitiesForPolicy",
    "iam:ListUserPolicies",
    "s3:GetBucketVersioning",
    "config:DescribeConfigurationRecorderStatus",
    "cloudtrail:DescribeTrails",
    "ec2:DescribeSecurityGroups",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "kms:ListKeys",
      "config:DescribeConfigurationRecorders",
      "ec2:DescribeVpcs",
      "cloudwatch:DescribeAlarms",
      "iam:GetLoginProfile",
      "iam:GetAccountSummary"
    ],
    "Resource": "*"
  }
 ]
}
```

8. Ein Benutzer mit der Rolle „sn_itom_ccg.scheduling_admin“ richtet ein Cloud-Servicekonto mit den AWS-Anmeldeinformationen in Cloud Configuration Governance für die Amazon Web Services Servicekonten ein, die Sie im vorherigen Schritt erstellt haben.

   Weitere Informationen zu den erforderlichen Schritten finden Sie unter .

9. Wenn dies noch nicht geschehen ist, richtet ein Benutzer mit der Rolle mid_server einen Now Platform MID Server ein, um Ihre Instanz mit Ihren AWS-Konten zu verbinden.

   Weitere Informationen finden Sie unter .

10. Nachdem Sie den MID Server eingerichtet haben, führt ein Benutzer mit der Rolle sn_itom_ccg.scheduling_admin die DATACENTER-Erkennung aus, um die DATACENTER mit den Servicekonten zu identifizieren.

    Weitere Informationen finden Sie unter .

    **Hinweis:**
    Wenn Sie die Tabelle im Cloud-Servicekonto nicht ausfüllen, wird die Integration nicht ordnungsgemäß ausgeführt.

11. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Gruppenregeln** und wählen Sie die **Zuweisungsgruppe, Testregel**, um den Datensatz zu öffnen und das Feld Aktiv auf **true**zu setzen.

    In Configuration Compliance sind die in der Anwendung enthaltenen Gruppen- und Zuweisungsregeln standardmäßig deaktiviert. Ein Benutzer mit der Rolle sn_vulc.admin aktiviert diese Regeln.

    Diese Regel gruppiert die während des Audits erstellten Testergebnisse. Alle Testergebnisse für eine bestimmte Richtlinie, deren Testergebnis „ falsch “ ist, werden in einer Testergebnisgruppe gruppiert.

    Standardmäßig werden Testergebnisgruppen der CI-Support-Benutzergruppe zugewiesen. Diese Zuweisungsregel ist standardmäßig inaktiv.

12. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Zuweisungsregeln** und wählen Sie den Datensatz An CI-Supportgruppe zuweisen aus, um ihn zu öffnen, und klicken Sie auf das Kontrollkästchen **Aktiv**, um ihn zu aktivieren.

    Diese Regel weist die Testergebnisgruppen Benutzern in der CI-Supportgruppe zu. Weisen Sie dieser Gruppe Benutzer zu, die an diesen Testergebnissen arbeiten sollen.

    Dies ist eine Standardzuweisungsregel, die abhängig von Ihren internen Vorgehensweisen möglicherweise nicht für die Zuweisung von Cloud-Konfigurationsproblemen in Ihrer



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Organisation geeignet ist. Möglicherweise möchten Sie stattdessen eine Zuweisungsregel erstellen, die Ihren Anforderungen entspricht. Sie können Cloud-Konto-Metadaten verwenden, indem Sie in der Tabelle „Erkanntes Element“ aus der Tabelle „Testergebnis“ Dot-Walk durchlaufen, um Zuweisungsregeln zu definieren.

13. Navigieren zu **Performance Analytics** > **Datenerfasser** > **Aufträge** und suchen Sie nach den täglichen Sammleraufträgen für PA CC, und vergewissern Sie sich, dass diese Aufträge aktiviert sind.

    Um die Audit-Ergebnisse in den Performance Analytics for Vulnerability Response -Dashboards anzuzeigen, aktiviert ein Benutzer mit der Rolle „sn_vuln.admin“ die Anwendung und die Datensammler.

    Sie haben das Setup für die Integration abgeschlossen. Sie sind bereit, einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.

[End]

[store-future: BEGIN review]

### Cloud-Konten mit der CSPM-Anwendung [] mit AWSServiceNow scannen

In diesem Abschnitt wird beschrieben, wie Sie Sicherheitsprüfungen für Ihre Cloud-Konten konfigurieren, um die Compliance Ihrer Ressourcen mit Benchmark-Frameworks zu überprüfen. Eine Beispielrichtlinie wird verwendet, um Ihnen diesen Prozess zu zeigen.

#### Vorbereitungen

Setup erforderlich: Dieses Beispiel beginnt mit der Erstellung eines Scan-Datensatzes. Wenn Sie die Informationen in Ihren Servicekonten für AWS einrichten oder überprüfen möchten, sehen Sie sich die Setup-Schritte unter an.

Erforderliche Rolle: sn_vul.cspm_cloud_account_admin

#### Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Administration** > **Cloud-Account-Scans** , um einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.
   Die Seite Richtlinienbewertungsregeln wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

   a. Geben Sie einen eindeutigen Namen für die Scan-Konfiguration ein.

   b. Geben Sie eine Kurzbeschreibung ein, damit Sie den Datensatz später finden können.

   c. Wählen Sie **Cloud-Servicekonten** und dann die gewünschten Zielservicekonten aus.
      Dies sind die Datensätze, die Sie für Ihre AWS-Konten erstellt und eingerichtet und in Cloud Configuration Governanceeingegeben haben.

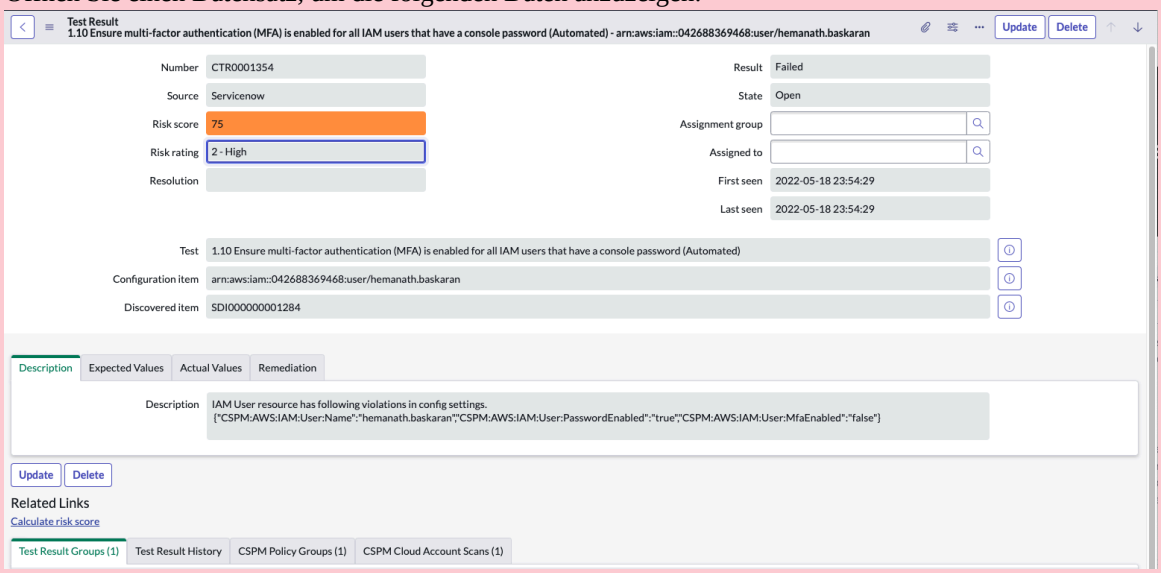
4. Aktivieren Sie die Checkbox **Hintergrundprüfung,** um sie zu aktivieren.
   Wenn der Scan stündlich ausgeführt werden soll, aktivieren Sie das Kontrollkästchen **Hintergrundscan,** um ihn zu aktivieren. Wenn das Kontrollkästchen nicht aktiviert ist, müssen Sie den Scan bei Bedarf starten.
5. Um die verknüpften untergeordneten Konten automatisch zu scannen, aktivieren Sie das Kontrollkästchen Verknüpfte untergeordnete Konten automatisch **scannen**.
6. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisse** > **Alle**.
   Die Liste der Testergebnisgruppen (CTR#), die aus dem Richtlinienaudit erstellt wurden, wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisdatensätze für Ihre nicht konformen Cloud-Ressourcen werden erstellt. Wenn Verstöße behoben werden, werden Testergebnisdatensätze geschlossen.

**7.** Öffnen Sie einen Datensatz, um die folgenden Daten anzuzeigen:




**Testfeld**

In diesem Feld wird die 1:1-Zuordnung zwischen der für das Audit verwendeten Richtlinie und dem Audit-Testdatensatz in Configuration Complianceangezeigt. Klicken Sie, um eine Vorschau anzuzeigen, den Testdatensatz zu öffnen und die Bezugsvermerke anzuzeigen, d. h. die autorisierende Quelle. In diesem Beispiel ist die autoritative Quelle CIS AWS Foundations Benchmark v1.4.0, und der angegebene Abschnitt, die Richtlinie, ist 1.10. Jede Richtliniengruppe, zu der diese Richtlinie gehört, wird angezeigt. Eine Richtlinie kann sich in mehr als einer Richtliniengruppe befinden. Außerdem wird die Anzahl der durch das Audit generierten Testergebnisse angezeigt.

**Feld „Konfigurationselement“**

Diese Daten beziehen sich auf eine Ressource in AWS.

**Feld „Erkanntes Element“**

Ein erkanntes Element in Now Platform ist der AWS-Ressource zugeordnet. Alle über die AWS-Ressource importierten Cloud-Metadaten, z. B. Region, Cloud-Konto und Ressourcentyp, werden im Datensatz „Erkanntes Element“ gespeichert.

**Registerkarte „Testergebnisgruppen“.**

Standardmäßig gruppiert die Anwendung Configuration Compliance die Testergebnisse basierend auf einer falschen Rückgabe des Audits in Testergebnisgruppen. Für eine Ressource wird nur ein Datensatz pro Testergebnis erstellt und nach Datenimporten aktualisiert. Wenn die Konfigurationseinstellung für eine Ressource in Ihrer AWS-Umgebung zwischen Scans geändert wird, wird der Datensatz in Ihrer Now Platform -Instanz aktualisiert.

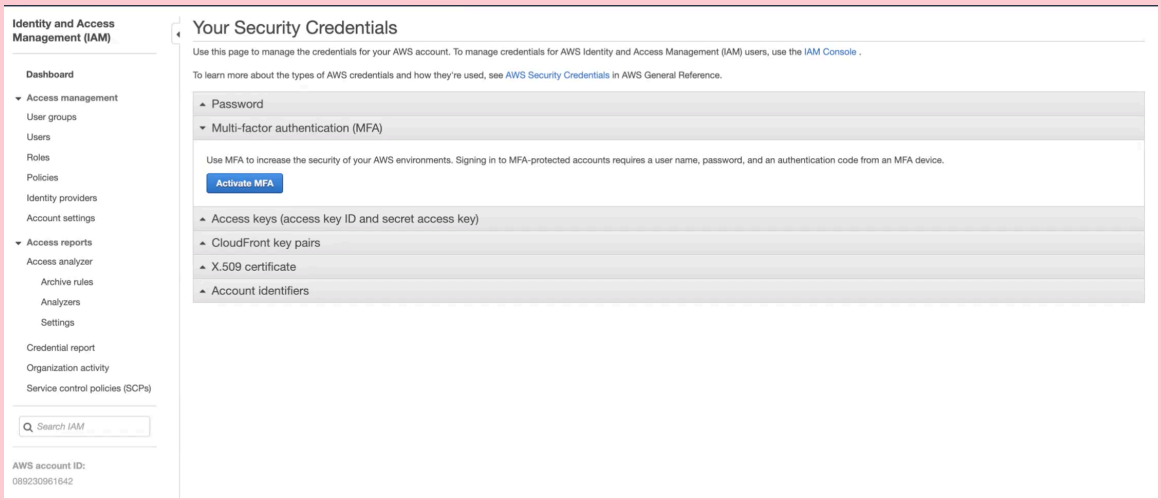
**8.** Um importierte Daten zu überprüfen, können Sie zum AWS-Benutzerkonto zurückkehren.

In diesem Beispiel zeigt eine Prüfung für diesen Account an, dass die Multifaktor-Authentifizierung nicht aktiviert ist (**MFA aktivieren**). Dieser Status stimmt mit den Sicherheitsdaten überein, die über die Ressourcen und Ressourcengruppen aus der Cloud importiert wurden. Nachdem Sie die Einstellung geändert haben und die Ressource konform ist, werden Ihre Änderungen im nächsten Datenimport berücksichtigt. Im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

folgenden Beispiel muss MFA in AWS für diese Ressource aktiviert werden, bevor der Testergebnisdatensatz geschlossen wird.




[End]

### Zeigen Sie AWS CSPM-Auditdaten in den Dashboards Performance Analytics for Vulnerability Response an

Diese Integration umfasst Dashboards in der Anwendung Performance Analytics for Vulnerability Response.

#### Vorbereitungen
Erforderliche Rolle: pa_viewer

#### Prozedur

1. Um das Dashboard anzuzeigen, navigieren Sie zu **Configuration Compliance** > **Übersicht**.

   Daten für die Dashboards werden täglich erfasst. Um die Einstellungen zu ändern, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.

   **Hinweis:**
   Wenn Sie andere Schwachstellenintegrationen von Drittanbietern ausführen, werden alle Ihre Schwachstellendaten und Audit-Ergebnisdaten zusammen in den Dashboard-Visualisierungen angezeigt. Sie können Ihre Filter so festlegen, dass Sie die CSPM-Daten herausfiltern können.

   Das Dashboard enthält drei Registerkarten:

   - Asset-Kategorie
   - Korrektur
   - Genehmigungen

2. Klicken Sie auf eine Registerkarte, um die Daten anzuzeigen.
3. Die in den Daten enthaltenen autorisierenden Quellen werden unter den Datenvisualisierungen aufgelistet.

### Erstellen Sie eine benutzerdefinierte Richtlinie für AWS in CSPM

Erstellen Sie eine Richtlinie, um Ihre benutzerdefinierten Compliance-Standards zu implementieren.

#### Vorbereitungen
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Konfigurationsrichtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

### Formular zur Erstellung benutzerdefinierter CSPM-Richtlinien

| Feld | Beschreibung | | |
|---|---|---|---|
| Richtlinienname | Eindeutiger Name der Richtlinie. | | |
| Beschreibung | Details der Richtlinie. | | |
| Ressourcentyp | | | |
| Cloud-Provider | Cloud-Bereitstellungsplattform für die Richtlinie. | | |
| Ressourcentyp | Typ der Ressource in der Cloud-Umgebung. Wenn der Ressourcentyp nicht vorhanden ist, erstellen Sie einen Ressourcentyp mithilfe der AWS- oder Azure-Konventionen. | | |
| Policenbedingung | | | |
| Typ | | | |
| Bedingung | Bedingung zum Erstellen eines Testergebnisses. Betrachten Sie die folgenden Szenarien. | | |
| | Konfigurationsschlüssel vorhanden? | Ressourcentyp vorhanden? | Nächste Schritte |
| | Ja | Ja, Ressourcentyp und die Flows zum Abrufen der Metadaten sind vorhanden. Beispiel für einen Subflow: CSPM: Azure Subscription Resource Collector. | Geben Sie die Bedingungen für die Richtlinie an. |
| | Nein | Ja | **a.** Erstellen Sie einen Konfigurationsschlüssel.<br>**b.** Erstellen Sie einen Ressourcensammler.<br>**c.** Erstellen Sie einen Konfigurationssammler.<br>**d.** Geben Sie die Bedingungen für die Richtlinie an. |
| Schweregrad | Schweregrad der Richtlinie. | | |

4. Wählen Sie **Absenden** aus, um die benutzerdefinierte Richtlinie zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Cloud Security Posture Management mit Microsoft Azure

Die von ServiceNow® entwickelte CSPM-Anwendung (Cloud Security Posture Management) scannt Ihre Cloud-Umgebung kontinuierlich, um Nichteinhaltungen oder Konfigurationsverstöße gegen Compliance-Frameworks wie CIS zu identifizieren.

## Wichtige Begriffe und Konzepte

Diese von ServiceNow entwickelte CSPM-Integration unterstützt CIS Microsoft Azure. Die Integration erfasst die Konfigurationsdaten von Cloud-Assets in Ihrer Microsoft Azure -Umgebung direkt aus der Cloud, importiert sie in Ihre Now Platform® -Instanz und prüft Ihre Assets auf Compliance.

Die folgenden Begriffe sollen Ihnen helfen, die Konzepte für diese CSPM-Integration zu verstehen. Weitere Informationen zu Azure-Produkten finden Sie unter Azure.com .

**Region**

Regionen beziehen sich auf geografische Gebiete, die von Ihren Microsoft Azure Cloud-Services unterstützt werden. Regionen haben Standardendpunkte, mit denen Sie auf die unterstützten Services für diese Region zugreifen können. Beispiele für Regionen sind „Virginia“ oder „OHO“ in den USA oder andere RECHENZENTRUM-Standorte außerhalb der USA.

**Ressource**

„Ressource“ ist ein Begriff, der in der Umgebung Microsoft Azure ] verwendet wird und Microsoft Azure Assets und ihre Konfigurationseinstellungen beschreibt. Ressourcen sind die Services in Ihren Microsoft Azure -Umgebungen. Virtuelle Computer, Speicherkonten, Web-Apps, Datenbanken und virtuelle Netzwerke sind Beispiele für gängige Ressourcen. In Ihrer Now Platform -Instanz werden Ressourcen als Ihre Assets oder Konfigurationselemente (CIs) bezeichnet.

**Ressourcengruppen**

Ressourcen in Ihren Microsoft Azure -Accounts können in Ressourcengruppen organisiert werden. Gruppen enthalten zugehörige Ressourcen für eine bestimmte Microsoft Azure Lösung oder ein bestimmtes Produkt. Ressourcen in einer Ressourcengruppe können sich in verschiedenen Regionen befinden, und sie können sich in einer Region außerhalb der Gruppe selbst befinden. Die Ressourcengruppe speichert Metadaten zu ihren Ressourcen. Wenn Sie einen Speicherort für die Ressourcengruppe angeben, geben Sie an, wo diese Metadaten gespeichert werden. Für Compliance müssen Sie wissen, dass Ihre Daten in einer bestimmten Region gespeichert werden.

**Center for Internet Security (CIS)**

CIS ist eine Community-orientierte, Non-Profit-Organisation, die für die CIS-Steuerungen ® und CIS-Benchmarks ™verantwortlich ist, global anerkannte Prozesse zur Sicherung von IT-Systemen und -Daten. Derzeit verwendet die CSPM-Anwendung ServiceNow die in Microsoft Azure (CIS Microsoft Azure Foundations Benchmark, Version 1.4.0) veröffentlichten Richtlinien, um die Compliance Ihrer Cloud-Assets zu überprüfen.

**Automatisiert**

Dieser Begriff bezieht sich auf die Empfehlungen, die sich aus einem Audit eines Assets oder einer technischen Kontrolle ergeben, die vollständig automatisiert und durch einen Pass/Fehlschlag-Status validiert werden kann. Diese Integration unterstützt automatisierte Bewertungen.

**Richtlinie (Konfigurationsrichtlinien)**

Richtlinien sind Governance-Leitlinien. In Now Platformwerden Richtlinien als Konfigurationsrichtlinien bezeichnet. Die von ServiceNow entwickelte CSPM-Anwendung bietet



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Baseline-Konfigurationsrichtlinien, um Ihre Cloud-Umgebung anhand von Benchmark-Standards wie CIS zu bewerten. Zwischen den Konfigurationsrichtlinien und den in den Compliance-Frameworks bereitgestellten Richtlinien besteht eine 1:1-Zuordnung.

**Richtliniensatz (Konfigurationsrichtliniengruppen)**

Richtliniensätze sind Gruppen einzelner Richtlinien. In Now Platformwerden Richtliniensätze als Konfigurationsrichtliniengruppen bezeichnet.

**Cloud Security Posture Management**

Richtlinien (**Konfigurationsrichtlinien**) und Richtliniensätze (**Konfigurationsrichtliniengruppen**) befinden sich im Modul **Cloud Security Posture Management**, das in Ihrer Instanz für diese Integration erstellt wurde.

**Test**

Tests sind Deskriptordatensätze, die für Konfigurationsrichtlinien erstellt werden. Für jede Konfigurationsrichtlinie im CSPM-Modul wird ein entsprechender Konfigurationstest automatisch im Configuration Compliance-Modul erstellt. Konfigurationstests werden von den Testergebnissen, also den Konfigurationsergebnissen des Scans, referenziert, um den Test oder die Richtlinie zu identifizieren, die für eine bestimmte Cloud-Ressource ausgewertet wurde.

**Testergebnisse**

Testergebnisse (TR) werden in Ihrer Instanz erstellt, wenn bei einem Audit festgestellt wird, dass eine Ressource in Ihrer Cloud-Umgebung nicht konform ist. Testergebnisse werden in der Anwendung Configuration Compliance in Ihrem Now Platformgespeichert. Diese Datensätze zeigen die Ergebnisse (Bestanden/Fehlgeschlagen) der Audits an, die für Ihre Ressourcen ausgeführt werden.

**Testergebnisgruppen**

Testergebnisgruppen helfen Ihnen, Testergebnisse in logischen Gruppen zu organisieren und Ihre Korrekturaufgaben zu priorisieren.

## Erforderliche Now Platform-Rollen

Sicherheitsadministratoren mit der Rolle „sn_vul.cspm_security_admin“ können dieses Produkt verwenden. Cloud-Konto-Scans können auch von Benutzern mit der Rolle sn_vul.cspm_cloud_account_admin konfiguriert werden.

Eine vollständige Liste der erforderlichen Rollen für diese Integration finden Sie unter .

## Workflow

- Die in der Anwendung enthaltenen Richtliniensätze (**Konfigurationsrichtliniengruppen**) definieren, welche Daten Sie importieren.
- Importierte Ressourcenkonfigurationsdaten werden in temporären Tabellen in Ihrer Now Platform -Instanz gespeichert. Diese gespeicherten Daten werden dann auf Compliance mit den im aufgeführten Richtlinien geprüft Microsoft Azure. . Es gibt 56 automatisierte Richtlinien, die von dieser Integration unterstützt werden. Die manuellen Richtlinien und neun der automatisierten Richtlinien werden nicht unterstützt.
- Die Ergebnisse der Audits werden als Testergebnisse und Testergebnisgruppen in der Anwendung Configuration Compliance in Ihrer Plattforminstanz erstellt.
- Sie können Testergebnisse, Testergebnisgruppen und andere Configuration Compliance -Daten in Dashboards und in Datensätzen in der Anwendung Configuration Compliance anzeigen. Sicherheitsmanager, Schwachstellenmanager und Schwachstellenanalysten können diese Daten verwenden, um konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren, zu priorisieren und darauf zu reagieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Datenerfassung

Um die Microsoft Azure Cloud-Konfigurationsdaten in Ihrer Umgebung zu erfassen, ruft ServiceNow die Microsoft Azure Cloud-API über einen MID Server von Ihrer NOW-Plattforminstanz auf. Die Konfigurationsdaten von Microsoft Azure-Ressourcen werden abgerufen, um Konfigurationsrichtlinien auszuwerten. Zu den Services oder Ressourcen, für die Konfigurationsdaten abgerufen werden, gehören:

- Identitäts- und Zugriffsverwaltung (IAM)
- Speicher
- Datenbankservices
- Protokollierung und Überwachung
- Netzwerk
- Virtuelle Computer
- Sicherheitsüberlegungen wie Schlüssel-Ablaufdaten
- AppService

## Beispiele für Sicherheits- und Konfigurationsabweichungen in Ihren importierten Daten

Die folgende Liste enthält einige Beispiele für Konfigurationsrichtlinien, die für Microsoft Azure Cloud-Ressourcen ausgewertet wurden, um die nicht konformen Ressourcen zu identifizieren:

- Überprüfen Sie, ob die Zugriffsebene für Blob Storage auf „Privat“ festgelegt ist.
- Überprüfen Sie, ob Blob Storage für kritische Daten verschlüsselt ist.
- Stellen Sie sicher, dass die Speicherzugriffsschlüssel regelmäßig neu generiert werden.
- Überprüfen Sie, ob Endpunktschutz für alle virtuellen Computer (VM) installiert ist.
- Überprüfen Sie, ob der Standardzugriff für Speicherkonten auf „Verweigern“ festgelegt ist.
- Überprüfen Sie, ob „SSL-Verbindung erzwingen“ für Standard-MySQL-Datenbankserver auf „Aktiviert“ festgelegt ist.

## Richtlinien und Benchmark-Standards

In der sind ungefähr 123 Richtlinien definiert Microsoft Azure. . 56 dieser Richtlinien oder Empfehlungen sind standardmäßig in der CSPM-Anwendung enthalten.

### Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für Microsoft Azure

Die für diese Integration erforderlichen Anwendungen sind im ServiceNow® Store verfügbar und unter dem Link „Abhängigkeiten und Lizenzierung anzeigen“ auf der Seite mit der App-Liste aufgeführt. Einige Anwendungen weisen Abhängigkeiten auf, die Sie separat herunterladen und installieren müssen.

**Vorbereitungen**
Erforderliche Rolle: admin für Download, Installation und Aktivierung aller Anwendungen.

Der Administrator weist die in Schritt 5 aufgeführten Rollen Now Platform zu. Diese Rollen Now Platform® sind für die Anwendung erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

### Prozedur

1. Klicken Sie auf den Link in der erhaltenen E-Mail, um auf die Anwendungen für diese Integration in der ServiceNow Storezuzugreifen.

   Um die Abhängigkeiten für eine Anwendung anzuzeigen, klicken Sie auf der Anwendungsseite in ServiceNow Storeauf **Abhängigkeiten und Lizenzierungsanforderungen anzeigen** unter „Abhängigkeiten und Lizenzierung“.

   **Hinweis:**
   Die Anwendung Cloud Security Posture Management für Microsoft Azure befindet sich unter dem Link „ **Innovation Lab** “ von ServiceNow Store. Die anderen Anwendungen finden Sie unter **Apps und Lösungen**.

2. Installieren Sie die Anwendungen in der in der folgenden Tabelle aufgeführten Reihenfolge:
3. Nachdem Sie die Anwendungen von ServiceNow Storeheruntergeladen haben, navigieren Sie in Ihrer Instanz von Now Platform zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**. Suchen Sie die Anwendungen, und aktivieren Sie sie in der in der Tabelle angegebenen Reihenfolge.
4. Klicken Sie auf **Installieren**, um sie zu aktivieren.

   **Hinweis:**
   Die Installation dieser Anwendungen kann 2 bis 3 Stunden dauern.

| Anwendung | Installieren Sie die App-Version und die Abhängigkeits-Plugins |
|---|---|
| Plattformversion | San Diego, Tokio |
| Vulnerability Response (Abhängigkeiten) | Plugin-ID: com.snc.vul_dep |
| Configuration Compliance (Abhängigkeiten) | Plugin-ID: com.snc.vulc_dep |
| CMDB CI Class Models | Installieren Sie CMDB CI Class Models: com.sn_cmdb_ci_class - 1.39.0 |
| Security Support Common | Plugin-ID: com.snc.security_support.common – 13.3.3 |
| Security Integration Framework | Plugin-ID: com.snc.sec.int.framework – 13.2.2 |
| Security Support Orchestration | Plugin-ID: com.snc.secops.orchestration – 12.3.0 |
| Vulnerability Response (Kernanwendung) | Plugin-ID: sn_vul – 17.0.2 |
| Configuration Compliance (Kernanwendung) | Plugin-ID: sn_vulc – 14.4.4 |
| Performance Analytics for Vulnerability Response | Plugin-ID: com.snc.vulnerability.analytics – 12.4.4 |
| ServiceNow IntegrationHub Enterprise Pack-Installationsprogramm | Plugin-ID: com.glide.hub.integrations.enterprise |
| Cloud Provisioning and Governance Core | Plugin-ID: com.snc.cloud.core |
| Cloud-Aktionsbibliothek | Plugin-ID: com.sn.itom.cal – 1.3.6 |
| Cloud Configuration Governance | Plugin-ID: com.sn.itom.ccg – 1.3.7 |
| CCG-Inhaltspaket | Plugin-ID: com.sn.itom.ccg_cp - 1.3.7 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendung | Installieren Sie die App-Version und die Abhängigkeits-Plugins |
|---|---|
| Cloud Security Posture Management | Plugin-ID: com.snc.secops.condor – 1.1.1 |

Alle abhängigen Anwendungen, die zusammen mit einer Anwendung ebenfalls automatisch installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die Anweisungen.

Vergewissern Sie sich, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind, bevor Sie mit den nächsten Schritten fortfahren.

Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

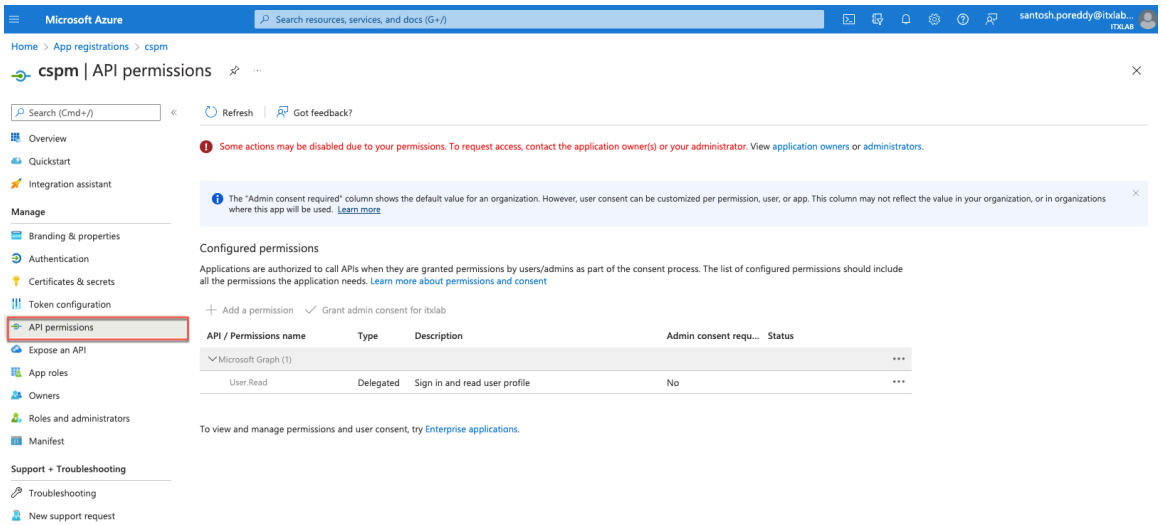
5. Weisen Sie die folgenden Rollen zu, falls sie noch nicht zugewiesen sind:
   Diese Rollen sind für verschiedene Workflow-Aktivitäten in der -Integration erforderlich.
   - discovery_admin oder sn_cmmp.cloud_admin – richtet die Cloud-Servicekonten auf der Now Platform für die entsprechenden Microsoft Azure Servicekonten ein.
   - cspm_security_admin Diese Rolle erbt auch die folgenden Rollen:
     - sn_itom_ccg.governor – erstellt Richtlinien, Richtliniensätze und Sammler. Die Rolle „Kontrolle“ führt die Testrichtlinie aus und erstellt Entitäten, die vom Planungsadministrator verwendet werden.
     - sn_itom_ccg.operator – der Operator Cloud Configuration Governance testet die Richtlinien und überprüft die Ergebnisse. Der Operator korrigiert auch Testergebnisse und Testergebnisgruppen.
     - sn_itom_ccg.scheduling_admin – richtet Cloud Configuration Governance für die Konten Microsoft Azure ein. Erstellt Scan-Konfigurationen und Scan-Zeitplan. Hat Zugriff auf Scan-Ergebnisse, um importierte Entitäten und Richtlinien anzuzeigen.
   - cspm_cloud_account_admin Diese Rolle erbt auch die Rolle sn_itom_ccg.scheduling_admin.
   - mid_server – konfiguriert einen MID-Server.
   - sn_vulc.admin – konfiguriert die Anwendung Configuration Compliance, hat Transparenz für alle Datensätze und kann Eigenschaften ändern. Weist Rollen in der Anwendung Configuration Compliance zu. Weitere Informationen zu Rollen in der Anwendung Configuration Compliance finden Sie unter Mit Configuration Compliance installierte Komponenten.
   - sn_vuln.admin – konfiguriert die Anwendung Performance Analytics for Vulnerability Response.

   Führen Sie die folgenden Schritte aus, damit Sie einen Scan-Datensatz erstellen können, um die Assets in Ihrer Microsoft Azure -Umgebung zu scannen.

6. Konfigurieren Sie in Ihrem Azure-Konto Richtlinien mit der erforderlichen Berechtigungsstufe, um Zugriff auf die Ressourcen Microsoft Azure für Cloud Discovery und Cloud Provisioning and Governance bereitzustellen.
   Verwenden Sie die in der folgenden Abbildung gezeigte Seite, um Ihre Richtlinienberechtigungen zu erstellen. Diese Berechtigungen sind für diese Anwendung erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




In der Anwendung Configuration Compliance sind die in der Anwendung enthaltenen Gruppen- und Zuweisungsregeln standardmäßig deaktiviert. Ein Benutzer mit der Rolle sn_vulc.admin aktiviert diese Regeln.

7. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Gruppenregeln**.
8. Klicken Sie auf die **Zuweisungsgruppe, Testregel**, um den Datensatz zu öffnen und das Feld Aktiv auf **true**zu setzen.

   Diese Regel gruppiert die während des Audits erstellten Testergebnisse. Alle Testergebnisse für eine bestimmte Richtlinie, deren Testergebnis „ falsch “ ist, werden in einer Testergebnisgruppe gruppiert.

   Standardmäßig werden Testergebnisgruppen der CI-Support-Benutzergruppe zugewiesen. Diese Zuweisungsregel ist standardmäßig inaktiv.

9. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Zuweisungsregeln**.
10. Klicken Sie auf den Datensatz An CI-Supportgruppe zuweisen, um ihn zu öffnen, und klicken Sie auf das Kontrollkästchen **Aktiv**, um ihn zu aktivieren.

    Diese Regel weist die Testergebnisgruppen Benutzern in der CI-Supportgruppe zu. Weisen Sie dieser Gruppe Benutzer zu, die an diesen Testergebnissen arbeiten sollen.

    Diese Standardzuweisungsregel ist abhängig von Ihren internen Vorgehensweisen möglicherweise nicht für die Zuweisung von Cloud-Konfigurationsproblemen in Ihrer Organisation geeignet. Möglicherweise möchten Sie stattdessen eine Zuweisungsregel erstellen, die Ihren Anforderungen entspricht. Sie können Cloud-Konto-Metadaten verwenden, indem Sie in der Tabelle „Erkanntes Element“ aus der Tabelle „Testergebnis“ Dot-Walk durchlaufen, um Zuweisungsregeln zu definieren.

    **Hinweis:**

    Weitere Informationen zur Verwendung von Configuration Compliancefinden Sie in der Dokumentation Configuration Compliance auf docs.servicenow.com.

11. Um die Audit-Ergebnisse in den Performance Analytics for Vulnerability Response -Dashboards anzuzeigen, aktiviert ein Benutzer mit der Rolle „sn_vuln.admin“ die Anwendung und die Datensammler.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Navigieren zu **Performance Analytics** > **Datenerfasser** > **Aufträge** und suchen Sie die täglichen Sammleraufträge, um sicherzustellen, dass sie aktiviert sind.
Sie haben das Setup für die Integration abgeschlossen. Sie sind bereit, Ihre Azure-Umgebung mit der CSPM-Anwendung zu scannen.

### Cloud-Konten werden mit der CSPM-Anwendung ServiceNow gescannt

In diesem Abschnitt wird beschrieben, wie Sie Sicherheitsprüfungen für Ihre Cloud-Konten konfigurieren, um die Compliance Ihrer Ressourcen mit Benchmark-Frameworks zu überprüfen. Eine Beispielrichtlinie wird verwendet, um Ihnen diesen Prozess zu zeigen.

#### Vorbereitungen

Setup erforderlich: Dieses Beispiel beginnt mit der Erstellung eines Scan-Datensatzes. Wenn Sie die Informationen in Ihren Servicekonten für Microsoft Azureeinrichten oder überprüfen möchten, sehen Sie sich die Setup-Schritte in Installieren und aktivieren Sie die Anwendung CSPM Innovation Lab für Microsoft Azurean.

Erforderliche Rolle: sn_vul.cspm_cloud_account_admin

#### Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Administration** > **Cloud-Account-Scans** , um einen Scan-Konfigurationsdatensatz in der CSPM-Anwendung zu erstellen.
Die Seite „Cloud-Konto-Scan“ wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.
   a. Geben Sie einen eindeutigen Namen für die Scan-Konfiguration ein.
   b. Geben Sie eine Kurzbeschreibung ein, damit Sie den Datensatz später finden können.
   c. Wählen Sie **Cloud-Servicekonten** und dann die gewünschten Zielservicekonten aus.
   Sie haben diese Datensätze für Ihre Microsoft Azure -Konten erstellt und in Cloud Configuration Governance] eingegeben.
4. Klicken Sie auf das Kontrollkästchen **Hintergrundscan**.
Dadurch wird der Scan stündlich ausgeführt. Wenn das Kontrollkästchen nicht aktiviert ist, müssen Sie den Scan bei Bedarf starten.
5. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisse** > **Alle**.
Die Liste der Testergebnisgruppen (CTR#), die aus dem Richtlinienaudit erstellt wurden, wird angezeigt.

   Testergebnisdatensätze für Ihre nicht konformen Cloud-Ressourcen werden erstellt. Wenn Verstöße behoben werden, werden Testergebnisdatensätze geschlossen.

6. Öffnen Sie einen Datensatz, um die folgenden Daten anzuzeigen:

   **Testfeld**

   In diesem Feld wird die 1:1-Zuordnung zwischen der für das Audit verwendeten Richtlinie und dem Audit-Testdatensatz in Configuration Complianceangezeigt. Klicken Sie, um eine Vorschau anzuzeigen, den Testdatensatz zu öffnen und die Bezugsvermerke anzuzeigen, d. h. die autorisierende Quelle. In diesem Beispiel ist die autoritative Quelle Microsoft Azure (CIS Microsoft Azure Foundations Benchmark, Version 1.4.0), und der angegebene Abschnitt, d. h. die Richtlinie, lautet 3.1.2. Stellen Sie sicher, dass „Mindest-TLS-Version“ auf „Version 1.2“ festgelegt ist. (Automatisiert) .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jede Richtliniengruppe, zu der diese Richtlinie gehört, wird angezeigt. Eine Richtlinie kann sich in mehr als einer Richtliniengruppe befinden. Außerdem wird die Anzahl der durch das Audit generierten Testergebnisse angezeigt.

**Feld „Konfigurationselement“**

Diese Daten beziehen sich auf eine Ressource in Microsoft Azure.

**Feld „Erkanntes Element“**

Ein erkanntes Element in Now Platform ist der Ressource Microsoft Azure zugeordnet. Alle Cloud-Metadaten, die über die Ressource Microsoft Azure importiert wurden, z. B. Region, Cloud-Konto und Ressourcentyp, werden im Datensatz „Erkanntes Element“ gespeichert.

**Registerkarte „Testergebnisgruppen“.**

Standardmäßig gruppiert die Anwendung Configuration Compliance die Testergebnisse basierend auf einer falschen Rückgabe des Audits in Testergebnisgruppen. Für eine Ressource wird nur ein Datensatz pro Testergebnis erstellt und nach Datenimporten aktualisiert. Wenn die Konfigurationseinstellung für eine Ressource in Ihrer Microsoft Azure -Umgebung zwischen Scans geändert wird, wird der Datensatz in Ihrer Now Platform -Instanz aktualisiert.

7. Um importierte Daten zu überprüfen, können Sie zum Benutzerkonto Microsoft Azure zurückkehren.

In diesem Beispiel gibt eine Prüfung für diesen Account an, dass die minimale TLS-Version 1.0 ist. Dieser Status stimmt mit den Sicherheitsdaten überein, die über die Ressourcen und Ressourcengruppen aus der Cloud importiert wurden. Nachdem Sie die Einstellung geändert haben und die Ressource konform ist, werden Ihre Änderungen im nächsten Datenimport berücksichtigt. Im folgenden Beispiel muss die minimale TLS-Version für diese Ressource aktualisiert werden, bevor der Testergebnisdatensatz geschlossen wird.

### Zeigen Sie Azure CSPM-Auditdaten in den Performance Analytics für Vulnerability Response-Dashboards an

Diese Integration umfasst Dashboards in der Anwendung Performance Analytics for Vulnerability Response.

#### Vorbereitungen

Erforderliche Rolle: pa_viewer

#### Prozedur

1. Um das Dashboard anzuzeigen, navigieren Sie zu **Configuration Compliance** > **Übersicht**.

Daten für die Dashboards werden täglich erfasst. Um die Einstellungen zu ändern, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.

**Hinweis:**
Wenn Sie andere Schwachstellenintegrationen von Drittanbietern ausführen, werden alle Ihre Schwachstellendaten und Audit-Ergebnisdaten zusammen in den Dashboard-Visualisierungen angezeigt. Sie können Ihre Filter so festlegen, dass Sie die CSPM-Daten herausfiltern können.

Das Dashboard enthält drei Registerkarten:

- Asset-Kategorie
- Korrektur
- Genehmigungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Klicken Sie auf eine Registerkarte, um die Daten anzuzeigen.
3. Die in den Daten enthaltenen autorisierenden Quellen werden unter den Datenvisualisierungen aufgelistet.

### Erstellen Sie eine benutzerdefinierte Richtlinie für Azure in CSPM

Erstellen Sie eine Richtlinie, um Ihre benutzerdefinierten Compliance-Standards zu implementieren.

#### Vorbereitungen

Erforderliche Rolle: sn_sec_cspm.cspm_security_admin

#### Prozedur

1. Navigieren zu **Alle** > **Cloud Security Posture Management** > **Konfigurationsrichtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular zur Erstellung benutzerdefinierter CSPM-Richtlinien**

| Feld | Beschreibung | | |
|---|---|---|---|
| Richtlinienname | Eindeutiger Name der Richtlinie. | | |
| Beschreibung | Details der Richtlinie. | | |
| Ressourcentyp | | | |
| Cloud-Provider | Cloud-Bereitstellungsplattform für die Richtlinie. | | |
| Ressourcentyp | Typ der Ressource in der Cloud-Umgebung. Wenn der Ressourcentyp nicht vorhanden ist, erstellen Sie einen Ressourcentyp mithilfe der AWS- oder Azure-Konventionen. | | |
| Policenbedingung | | | |
| Typ | | | |
| Bedingung | Bedingung zum Erstellen eines Testergebnisses. Betrachten Sie die folgenden Szenarien. | | |
| | Konfigurationsschlüssel vorhanden? | Ressourcentyp vorhanden? | Nächste Schritte |
| | Ja | Ja, Ressourcentyp und die Flows zum Abrufen der Metadaten sind vorhanden. Beispiel für einen Subflow: CSPM: Azure Subscription Resource Collector. | Geben Sie die Bedingungen für die Richtlinie an. |
| | Nein | Ja | **a.** Erstellen Sie einen Konfigurationsschlüssel. **b.** Erstellen Sie einen Ressourcensammler. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

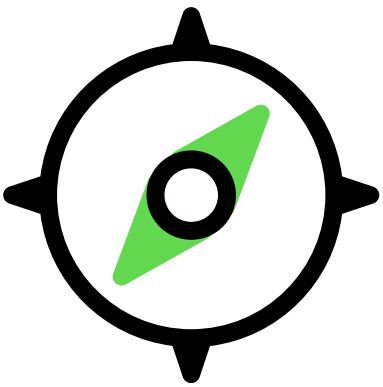
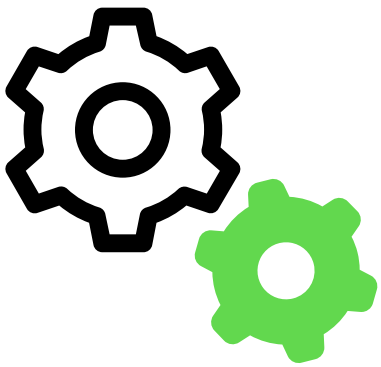
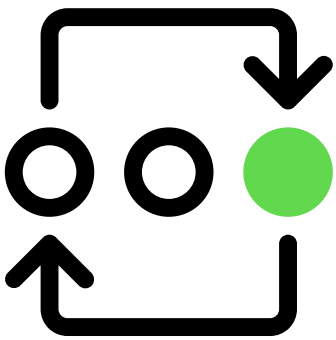
| Feld | Beschreibung | | |
|---|---|---|---|
| | | | **c.** Erstellen Sie einen Konfigurationssammler. **d.** Geben Sie die Bedingungen für die Richtlinie an. |
| Schweregrad | Schweregrad der Richtlinie. | | |

**4.** Wählen Sie **Absenden** aus, um die benutzerdefinierte Richtlinie zu erstellen.

## Vulnerability Response

Die National Vulnerability Database (NVD) und andere Quellen sammeln Informationen über bekannte Schwachstellen. Zu diesen Schwachstellen können Schwachstellen in Software, Betriebssystemen, die von Malware ausgenutzt werden können, und andere Angriffe gehören. Die Anwendung ServiceNow® Vulnerability Response hilft Ihnen bei der Nachverfolgung, Priorisierung und Behebung dieser Schwachstellen.

**Vulnerability Response**

| Erkunden | Einrichten und konfigurieren | integrieren |
|---|---|---|
|  |  |  |
| Erfahren Sie mehr über die Funktionen von Vulnerability Response | Installieren und richten Sie Ihre Vulnerability Response-Anwendung ein | Erweitern Sie Vulnerability Response durch die Integration mit anderen Anwendungen |



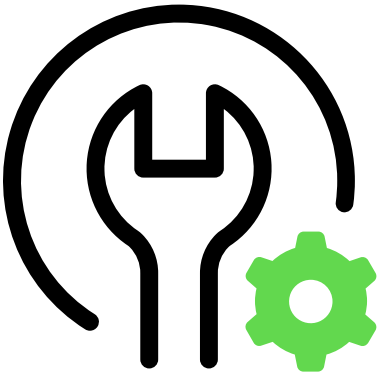
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vulnerability Response (Fortsetzung)

### Erkunden und verwenden Sie die Vulnerability Response-Arbeitsbereiche

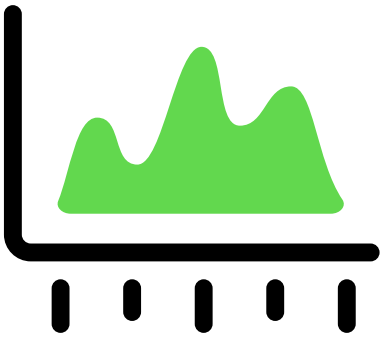
Erfahren Sie, wie Sie Vulnerability Manager und IT Remediation Workspaces verwenden

### Beheben



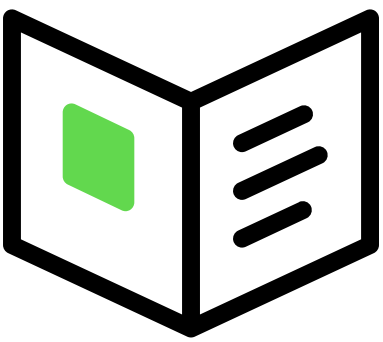
Verwenden Sie die Funktionen von Vulnerability Response, um Ihre Schwachstellen zu beheben und Ihre Assets zu schützen

### Analytik und Berichterstellung



Überwachen Sie den Fortschritt der Korrektur

### Referenz



Erhalten Sie weitere Details zu Versionshinweisen zu Vulnerability Response, Komponenten und Referenzinformationen zu Feldern, Tabellen und Eigenschaften

Automatische Übersetzung

## Die Anwendung Vulnerability Response erkunden

Die Anwendung ServiceNow® Vulnerability Response importiert und gruppiert angreifbare Elemente automatisch gemäß den Regeln, mit denen Sie Schwachstellen schnell

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beheben können. Schwachstellendaten werden aus externen Quellen wie der National Vulnerability Database (NVD) und Integrationen von Drittanbietern abgerufen und mit von ServiceNow®entwickelten Anwendungen verarbeitet.

Sehen Sie sich eine Übersicht über Vulnerability Response an, in der angreifbare Elemente, Korrekturaufgaben und ihre Lebenszyklen definiert werden.

Übersicht über die typische Reaktion auf Schwachstellen innerhalb eines Unternehmens im Vergleich zur Reaktion auf Schwachstellen mit ServiceNow und Definition von angreifbaren Elementen, Schwachstellengruppen und deren Lebenszyklen.

## Vulnerability Response und Ihrer Unternehmensumgebung

Normalerweise verwenden Unternehmen in einer Unternehmensumgebung Schwachstellenscanner und Bewertungstools, um die Risiken zu identifizieren und zu verwalten, die Schwachstellen für ihre Assets darstellen. Von diesen Tools identifizierte Schwachstellen stellen Risiken für die Sicherheits- und IT-Teams dar, die für die Wartung und Sicherung der Assets einer Organisation verantwortlich sind. Einige Risiken umfassen unter anderem die folgenden Arten von identifizierten Schwachstellen:

- Abhängigkeit von veralteter Software oder falsch konfigurierten Systemen
- Ungesicherte Netzwerkprotokolle
- Abhängigkeit von fehlerhaften Softwarebibliotheken von Drittanbietern
- Schlechte oder inkonsistente Systemadministrationshygiene
- Baseline-System-Images, die nicht gesichert sind

Da diese potenziellen Risiken exponiert sind, stehen Sicherheits- und IT-Teams häufig vor Herausforderungen bei der Verarbeitung und Handhabung der Menge an Schwachstelleninformationen, die von ihren Scan- und Bewertungstools generiert werden. Insbesondere sind diese Teams überfordert, wenn sie ein hohes Volumen an identifizierten Schwachstellen verwalten und umsetzbare Reaktionsmaßnahmen zur Minderung der potenziellen Risiken für ihre Organisationen entwickeln.

Sie können diese Herausforderungen für Ihre eigene Sicherheitslage identifizieren, indem Sie die folgenden Fragen stellen:

- Welche identifizierten Schwachstellen sollten zuerst überprüft werden?
- Was bedeuten diese identifizierten Schwachstellen für unsere Organisation?
- Wer sollte für identifizierte Risiken verantwortlich sein und besitzen?
- Wer sollte an der Lösung/Minderung dieser Risiken arbeiten?
- Wie können wir erkannte Schwachstellen mit den verfügbaren Ressourcen effektiv mindern?
- Was sind die potenziellen unbeabsichtigten Ergebnisse der Reduzierung der identifizierten Schwachstellen?
- Welchen Prozess verfolgen wir, um Schwachstellen zu beheben, die unternommenen Schritte nachzuverfolgen und nachzufassen, um sicherzustellen, dass unsere Aktionen funktioniert haben?
- Woher wissen wir, ob wir bei der Reduzierung unserer Gesamtrisikosituation Fortschritte machen?



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vulnerability Response und Now Platform®

Vulnerability Response ist ein Mitglied der Anwendungssuite Security Operations. Zusammen stellen diese Anwendungen die Verbindung zwischen Sicherheit und IT-Abteilung her, erhöhen die Geschwindigkeit und Effizienz Ihrer Reaktion und geben Ihnen einen definitiven Überblick über Ihre Sicherheitslage.

### Übersicht über Security Operations

Die Anwendung ServiceNow Vulnerability Response verfolgt zwei Hauptziele:

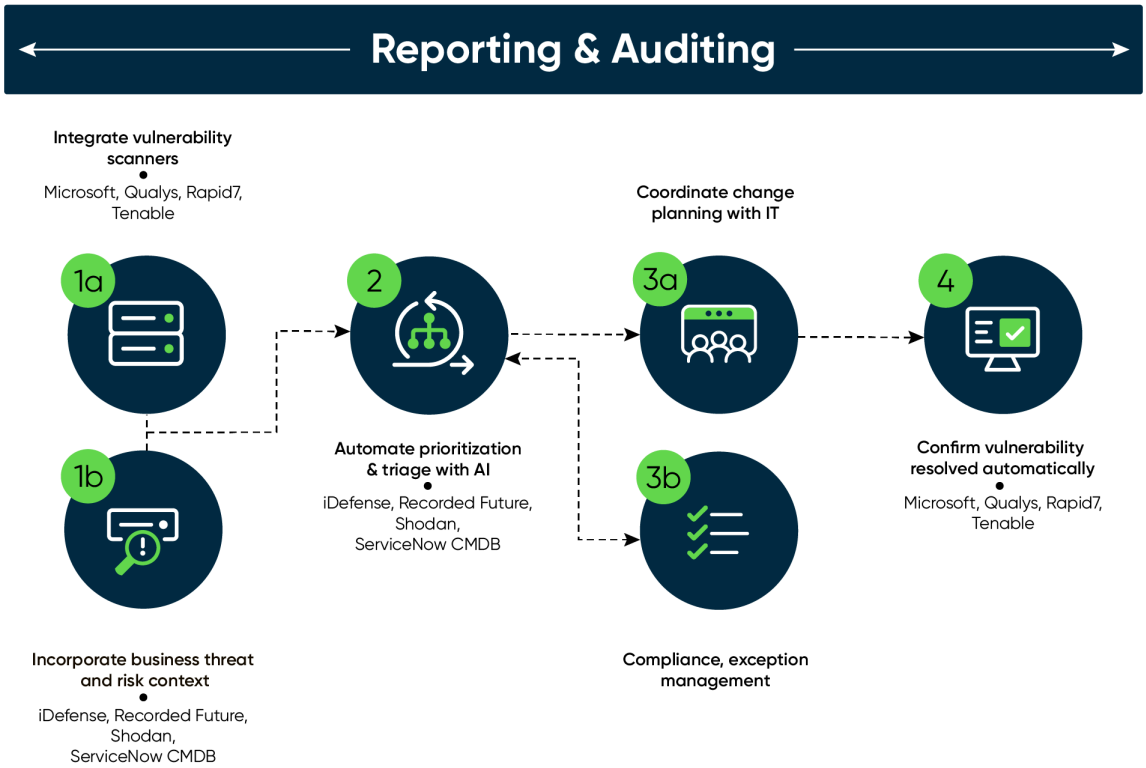
- Helfen Sie den Sicherheitsteams, die mit großen Mengen an Schwachstellendaten konfrontiert sind.
- Unterstützen Sie die Betriebsteams, die mit der Behebung von Schwachstellen beauftragt sind.

Auf diese Weise können Sie die Anwendung Vulnerability Response verwenden, um den Informationsfluss von der Integration über die Untersuchung bis hin zur Lösung zu automatisieren.

Der Schwachstellenmanagementprozess in Now Platform® kann Prozesse, Daten, Berichterstellung und Automatisierung mit CMDBumfassen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- Integrieren Sie Scanner und ServiceNow® -Anwendungen von Drittanbietern mit der Anwendung Vulnerability Response, um bekannte Schwachstellendaten zu erfassen.
- Verbessern Sie Ihre erfassten Schwachstellendaten mit Exploit, Threat Intelligence, Risiko und Geschäftskontext. Verwenden Sie diese Daten als Unterstützung bei Patch- und Korrekturstrategien.
- Importierte Schwachstellen aus dem NVD und Erkennungsdaten aus Drittanbieterprodukten werden mit den Assets in Ihrer CMDB abgeglichen. Die Selektierung kann Folgendes umfassen: Erstellung von Korrekturaufgaben, die aus mehreren angreifbaren Elementen bestehen, d. h. Assets, bei denen Schwachstellen ermittelt wurden, Gruppierung dieser Aufgaben nach Kategorie, Priorisierung und Zuweisung zu Teams.
- Verwenden Sie ein koordiniertes Change- und Ausnahmemanagement, um Schwachstellen zu beheben, die möglicherweise zusätzliche manuelle Eingriffe, mehr Zeit für die Lösung oder umfangreiche Untersuchungen erfordern.
- Vergewissern Sie sich, dass Schwachstellen durch Erkennungen Ihrer Scanner-Produkte automatisch behoben und aktualisiert werden.

## Wer könnte Vulnerability Response in Ihrer Organisation verwenden?

Vulnerability Response -Benutzer fallen im Allgemeinen in zwei Rollen.

- Schwachstellenanalyst
- Verantwortlicher für Korrektur

Die Persona des Schwachstellenanalysten befindet sich normalerweise in den Bereichen Sicherheit, Risiko und Compliance oder Management. Diese Benutzer überwachen Schwachstellen und bestimmen, wann die Korrekturprozesse initiiert werden sollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellenanalysten verwenden hauptsächlich Arbeitsbereich des Schwachstellenmanagers und, um Korrekturaufgaben zu überwachen und zu erstellen.

Die Persona des Korrekturbesitzers ist normalerweise Teil der Bereiche IT Operations, DevOps/Engineering oder Service Owner. Diese Benutzer führen die Korrekturaufgaben durch, die zum Beheben von Schwachstellen erforderlich sind. Sie können Ausnahme- oder Change-Anforderungen übermitteln, wenn kontrollierte Prozesse für die Wartung oder Entfernung von Assets erforderlich sind. Der Korrekturbesitzer arbeitet hauptsächlich an Korrekturaufgaben im Arbeitsbereich des IT-Korrekturbesitzers.

## Application Vulnerability Response

Mit der Funktion Application Vulnerability Response (AVR) der Anwendung ServiceNow® Vulnerability Response werden angreifbare Anwendungselemente (AVITs) importiert. Gemäß den Regeln können Sie Anwendungsschwachstellen beheben. Sie ist über ein separates Abonnement verfügbar. Die Dokumentation zu [ Application Vulnerability Response finden Sie unter Application Vulnerability Response erkunden.

## Verfügbare Versionen

Ein Glossar mit Begriffen und weitere Referenzen, die Links, Fehlerbehebung, Wissensartikel sowie Felddaten in den Formularen und Datensätzen in Vulnerability Responseenthalten, finden Sie unter Vulnerability Response Referenzinformationen.

| Release-Version | Releasehinweise |
| --- | --- |
| Vulnerability Response v21.0<br>Vulnerability Response v20.0<br>Vulnerability Response v19.0<br>Vulnerability Response v18.2<br>Vulnerability Response v18.0 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Installation von Vulnerability Response und unterstützten Anwendungen

Die Anwendung Vulnerability Response ist über den ServiceNow Storeverfügbar. Die Anwendung unterstützt andere ServiceNow Anwendungen und Integrationen von Drittanbietern, die Sie auch aus dem ServiceNow Storeherunterladen können. Weitere Optionen sind ebenfalls verfügbar, um das Basis-Setup zu erweitern.

## Aufgaben für das grundlegende Setup

Die Anwendung Vulnerability Response ist als erster Schritt erforderlich. Weitere Informationen zur Installation von finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response . und Vulnerability Response- Anwendung installieren.

- Nach Abschluss der Installation können Sie Vulnerability Response mit dem Setup-Assistenten konfigurieren.

  Weisen Sie mit dem Setup-Assistenten Benutzer und Gruppen für den Zugriff auf die Anwendung zu, erstellen oder bearbeiten Sie Zuweisungsregeln, Regeln für Korrekturaufgaben und Zieldaten, und richten Sie Risikorechner ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können auch eine oder mehrere unterstützte Drittanbieterintegrationen über den Setup-Assistenten auswählen, installieren und konfigurieren. Diese Integrationen rufen Schwachstellendaten aus externen Systemen und Lieferanten ab. Weitere Informationen zur Funktionsweise von Integrationen und zu den von Vulnerability Responseunterstützten Integrationen finden Sie unter Vulnerability Response-Integrationen.
- Führen Sie vor der Implementierung von Drittanbieterintegrationen die geplante Aufgabe für die NVD-Integration und CWE als Teil der Ersteinrichtung von Vulnerability Responseaus.

  Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern und Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.

- Wählen Sie ggf. eine Analytics-Anwendung aus. Die Anwendung Performance Analytics Content Pack for Vulnerability Response enthält Berichte, die alle Phasen des Lebenszyklus des Schwachstellenmanagements abdecken.

  [Optional] Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA]. Anwendung.

- Wählen Sie ggf. eine Lösungsanwendung aus. Das Lösungsmanagement hilft Ihnen, die Schwachstellen in Ihrer Umgebung mit den Lösungen zu korrelieren, die sie beheben könnten. [Optional] Anwendung Solution Management for Vulnerability Response installieren.

  **Hinweis:**

  - Wenn die Anwendung Vulnerability Solution Management aktiviert ist, können Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten bearbeitet werden.
  - Vulnerability Solution Management erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Vulnerability Solution Management.

- [Optional] Installieren Sie die App ServiceNow Agent und die Vulnerability Response Mobile-App für Mobile Experience für Vulnerability Response.

## Andere Setup-Aufgaben, die Sie ausführen können

Diese zusätzlichen Setup-Aufgaben ergänzen Ihre Basiskonfiguration und unterstützen die Korrektur mit Optionen für Berichterstellung, E-Mail-Benachrichtigungen, native Integrationskonfiguration und Arbeit mit angreifbaren Elementen. Die meisten dieser Aufgaben werden außerhalb des Setup-Assistenten ausgeführt. Weitere Informationen finden Sie unter Zusätzliche Vulnerability Response Setup- und Konfigurationsaufgaben.

## Erweiterte Aufgaben außerhalb des Basis-Setups

Diese optionalen Konfigurationsaufgaben werden außerhalb des Setup-Assistenten ausgeführt und erfordern Codierung oder fortgeschrittene ServiceNow Kenntnisse. Sie werden nicht als Teil der Basiskonfiguration betrachtet. Weitere Informationen finden Sie unter Erweiterte Vulnerability Response Konfigurationsaufgaben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vulnerability Response Personas und granulare Rollen

Bevor Sie Schwachstellen mit der Anwendung Vulnerability Response erfolgreich beheben können, müssen Sie Ihren Benutzern und Gruppen im Setup-Assistenten Personas und Rollen zuweisen.

Einer der ersten erforderlichen Konfigurationsschritte für die Anwendung Vulnerability Response besteht in der Zuweisung von Rollen zu Benutzern und Gruppen. Rollen definieren, was Benutzer und Gruppen in Vulnerability Response, Performance Analytics for Vulnerability Responseund allen Drittanbieterintegrationen mit Vulnerability Responsesehen und tun können.

Sie weisen vorhandenen Benutzern und Gruppen im Setup-Assistenten Persona-Rollen zu. Weitere Informationen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

**Hinweis:**

Wenn Sie Upgrade-Kunde sind, können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Benutzer und Gruppen, denen die Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write zugewiesen wurden, und der Korrekturbesitzer vor v10.3 hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response auf Aufgabenebene tun und anzeigen können, bevorzugen Sie möglicherweise die Verwendung granularer Rollen. Weitere Informationen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Wenn Sie Rollen bereits mit dem Setup-Assistenten zugewiesen haben und granulare Rollenzuweisungen für alle Benutzer und Gruppen aus dem Modul „Benutzeradministration“ verwalten möchten, finden Sie weitere Informationen unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Persona-Rollen und granulare Rollen beginnen

Wichtige Begriffe.

**Rolle**

Rollen definieren, was Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können.

**Gruppe**

Eine Gruppe von Benutzern, die bestimmte Rollen gemeinsam nutzen und ein gemeinsames Ziel verfolgen.

**Persona-Rolle**

Eine vorkonfigurierte Rolle in der Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen „Setup-Assistent“, „Schwachstellenadministrator“, „Schwachstellenanalyst“, „Korrekturbesitzer“, „Konfigurationselement-Manager“ und „Ausnahmemanager“ sind so konzipiert, dass sie den gängigen Berufsbezeichnungen für Manager, Analysten und Serviceverantwortliche in einer IT-Organisation oder Schwachstellenkorrekturgruppe entsprechen.

**Geerbte Rollen**

Ein Begriff, der Rollen beschreibt, die Benutzer automatisch erwerben, wenn ihnen andere Rollen zugewiesen werden. Beispielsweise erben alle Benutzer oder Gruppen, denen die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rolle „sn_vul.remediation_owner“ zugewiesen ist, auch die granularen Rollen „sn_vul.read_assigned“, „sn_vul.write_assigned“.

**Zugriffskontrollliste (ACL)**

Zugriffskontrolllisten schränken den Zugriff auf Daten ein, indem Benutzer eine Reihe von Anforderungen erfüllen müssen, bevor sie mit ihnen interagieren können.

Um Berichte ab Vulnerability Response v16.5 vor der Offenlegung zu schützen, legen **Sie Alle report_view-ACLs** auf `active=true`fest. Diese ACL stellt sicher, dass die geschützten Daten nur für autorisierte Benutzer verfügbar sind.

Sie weisen Gruppen und Benutzern im Setup-Assistenten Persona-Rollen zu.

**Hinweis:**
Im Setup-Assistenten ist die Systemadministratorrolle (admin) für die Aufgaben im ersten Abschnitt erforderlich: Zuweisen von Rollen und Installieren von Integrationen. Nachdem Sie Persona-Rollen im Setup-Assistenten zugewiesen und Integrationen installiert haben, ziehen Sie es möglicherweise vor, einem Benutzer oder einer Gruppe die Rolle „sn_vul.vulnerability_admin“ zuzuweisen, um verbleibende Aufgaben im Setup-Assistenten abzuschließen und die Anwendung Vulnerability Response zu verwalten.

In der folgenden Tabelle sind Vulnerability Response Persona-Rollen aufgelistet, die mit der Anwendung installiert wurden.

| Persona-Rollen für Vulnerability Response | Beschreibung |
|---|---|
| Weisen Sie Benutzern oder Gruppen sn_vul.vulnerability_admin – Schwachstellenadministrator zu. | Benutzer mit dieser Rolle haben vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Benutzer mit dieser Rolle konfigurieren alle VR-Anwendungen und -Regeln und installieren Integrationen von Drittanbietern. |
| Weisen Sie Benutzern und Gruppen sn_vul.vulnerability_analyst – Schwachstellenanalyst zu. | Benutzer und Gruppen mit dieser Rolle können alle Datensätze für die VI-Korrektur anzeigen und aktualisieren. |
| Weisen Sie Benutzern und Gruppen sn_vul.remediation_owner – Korrekturbesitzer zu. | Benutzer und Gruppen mit dieser Rolle beheben Schwachstellen, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. Gruppen oder Benutzer mit dieser Rolle können die Datensätze anzeigen und aktualisieren, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. |
| Weisen Sie Benutzern und Gruppen sn_vul.ci_manager zu. | Benutzer und Gruppen mit dieser Rolle verwalten die Neuklassifizierung von nicht abgeglichenen Konfigurationselementen (CIs), die nicht in der Configuration Management Database (CMDB) gefunden wurden. |
| Weisen Sie Lesezugriff auf bestimmte Bereiche in der Anwendung nach Aufgabe zu. | Weisen Sie beispielsweise sn_vul.read_all zu, damit ein Benutzer alle VR-Datensätze anzeigen kann. Weisen Sie für Lesezugriff zum Anzeigen von Korrekturaufgabenregeln sn_vul.read_group_rules zu. Benutzer und Gruppen mit dieser Rolle aktualisieren keine Datensätze. |

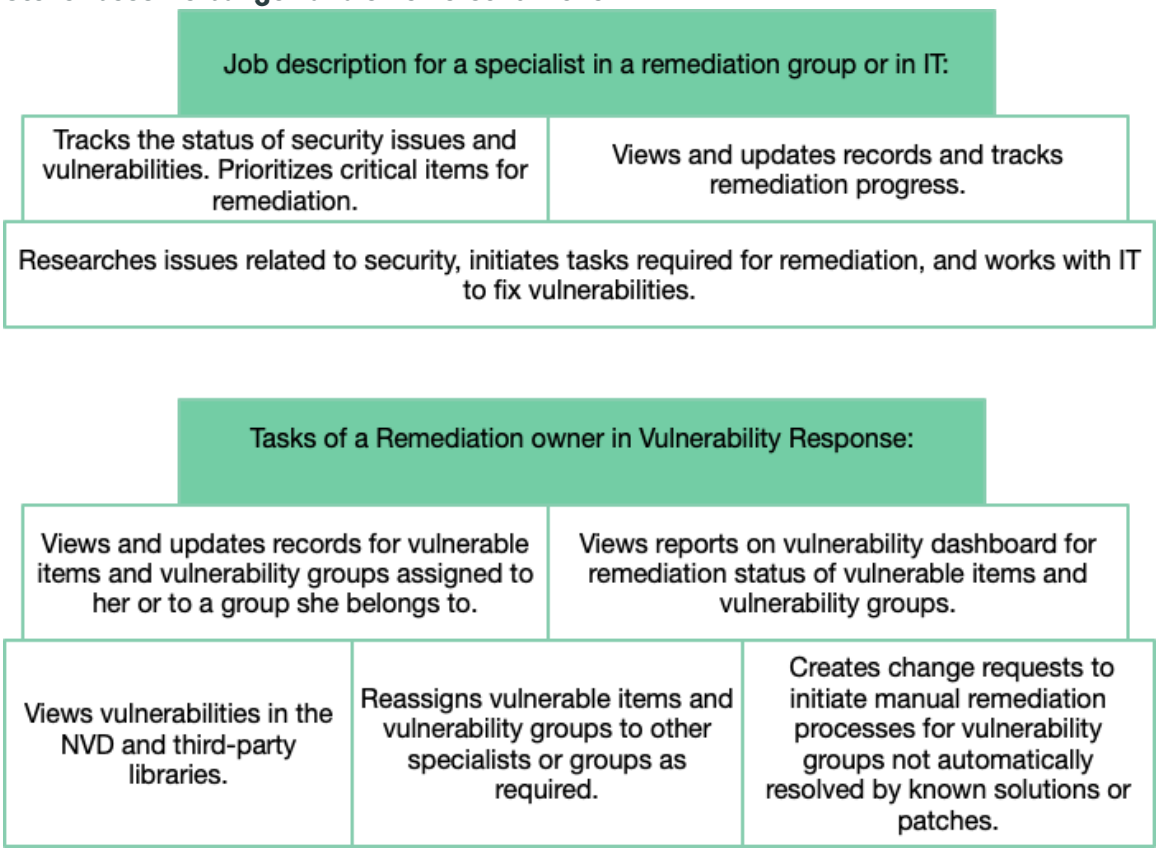


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Granulare Rollen und Persona-Rollen

Eine Möglichkeit, über Persona-Rollen zu denken, besteht darin, zu überlegen, wie sich ihre Beschreibungen auf Stellenbeschreibungen für verschiedene IT- oder Schwachstellenkorrektur-Positionen in Ihrer Organisation beziehen können. Die folgende Abbildung zeigt eine mögliche Stellenbeschreibung für einen Fehlerkorrekturspezialisten in der IT und wie sich die Aufgaben, die dieser Aufgabe zugeordnet sind, auf die Aufgaben einer Persona-Rolle des Korrekturbesitzers in der Anwendung Vulnerability Response beziehen.

**Stellenbeschreibungen und eine Persona-Rolle**




Sowohl die Stellenbeschreibung als auch die Persona-Rolle des Korrekturbesitzers können als eine Reihe von Korrekturaufgaben definiert werden. In der vorherigen Abbildung befinden sich eine Stellenbeschreibung und eine Persona-Rolle in grünen Blöcken über den Aufgaben, die sie beschreiben. In diesem Beispiel entsprechen einige der typischen Jobanforderungen für einen Spezialisten in einer Korrekturgruppe direkt den Aufgaben, aus denen die Persona des Korrekturverantwortlichen in Vulnerability Responsebesteht: Datensätze überprüfen und aktualisieren, den Korrekturstatus von Schwachstellen nachverfolgen, Elemente für die Korrektur priorisieren, und Korrekturen und Patches mit der IT anwenden.

Manchmal entsprechen die Stellen in Ihrer Organisation jedoch nicht direkt den Aufgaben, aus denen eine der fünf Persona-Rollen in der Anwendung Vulnerability Response besteht. Aus verschiedenen Gründen, z. B. zum Schutz vertraulicher Daten oder zur Einhaltung von Vorschriften, müssen Sie den weitreichenden Zugriff beschränken, den einige der Persona-Rollen Ihren Benutzern und Gruppen gewähren. Oder umgekehrt müssen Sie Benutzern und Gruppen mehr Zugriff gewähren, damit sie ihre Aufgaben ausführen können. Mit granularen Rollen können Sie Rollen einfach anpassen und den Zugriff steuern, den Benutzer und Gruppen auf Vulnerability Response, Performance Analytics for Vulnerability Responseund Integrationen von Drittanbietern haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Die granularen Rollen definieren die Aufgaben

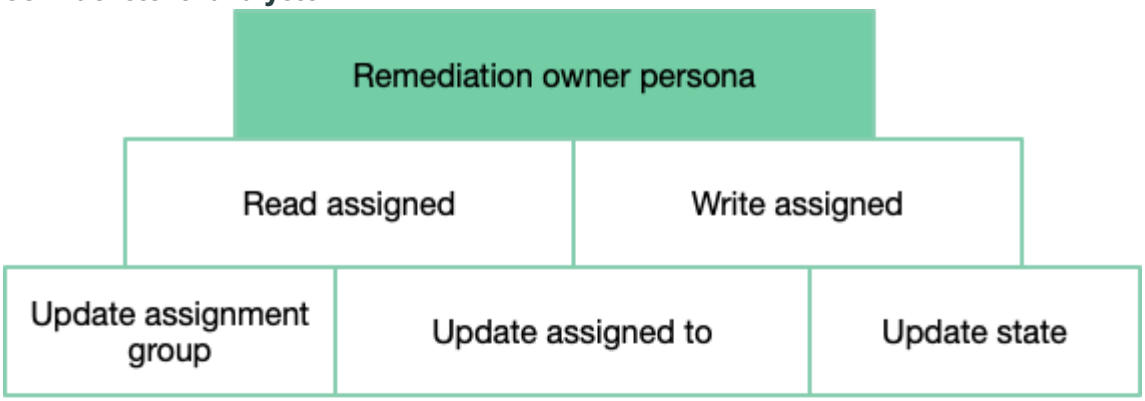
Die Namen für die granularen Rollen in Vulnerability Response beschreiben normalerweise, was Benutzer in der Anwendung Vulnerability Response tun und sehen können. In der vorherigen Abbildung haben Benutzer und Gruppen mit der zugewiesenen Persona „Korrekturbesitzer“ beispielsweise die granularen Rollen „sn_vul.read_assigned“ und „sn_vul.write_assigned“. Mit diesen granularen Rollen können Benutzer oder Gruppen angreifbare Elemente und Korrekturaufgabendatensätze, die ihnen zugewiesen sind, anzeigen und aktualisieren. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie als Benutzer mit der Systemadministratorrolle zu **Benutzeradministration** > **Rollen** und suchen Sie die gewünschte Rolle. Rollen, die automatisch geerbt werden, wenn eine Rolle zugewiesen wird, werden aufgelistet. Wenn eine Rolle von anderen Rollenzuweisungen abhängt, werden auch alle erforderlichen Rollen aufgelistet.

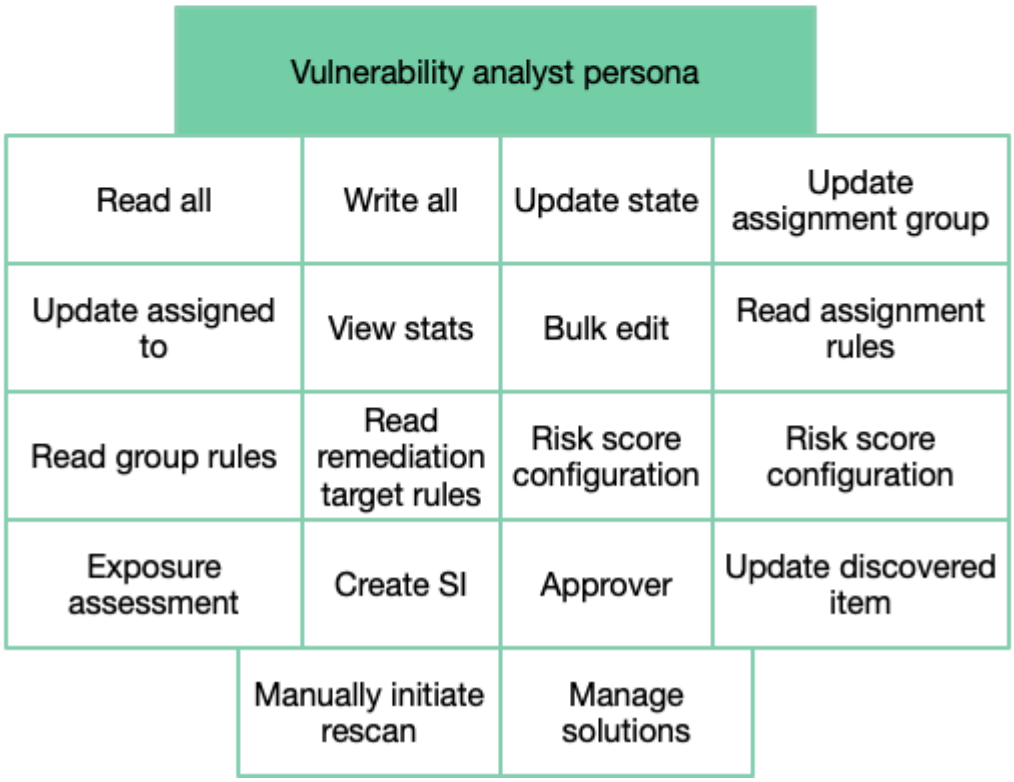
In der folgenden Abbildung sind die granularen Rollen der Persona-Rolle des Korrekturbesitzers und der Persona des Schwachstellenanalysten dargestellt. Beachten Sie, dass die Persona des Korrekturbesitzers nicht die Berechtigungen „read_all“ und „write_all“ der Persona des Schwachstellenanalysten enthält. Die granularen Rollen read_all und write_all sind erforderlich, bevor Benutzer und Gruppen alle Datensätze für angreifbare Elemente und Korrekturaufgaben lesen und bearbeiten können. Um diese Rollen anzupassen, fügen Sie einfach granulare Rollen hinzu oder entfernen sie, um den Zugriff zu erweitern oder einzuschränken.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Granulare Rollen und die Personas des Korrekturverantwortlichen und des Schwachstellenanalysten**






Wenn Sie möchten, dass Ihre Benutzer und Gruppen mehr Zugriff haben, als die Persona-Rollen zulassen, können Sie Benutzern und Gruppen granulare Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Benutzer und Gruppen auf Aufgabenebene beschränken möchten.

**Hinweis:**
Zum Zuweisen und Bearbeiten von granularen Rollen im Benutzerverwaltungsmodul ist die Systemadministratorrolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Granulare Rollen im Modul „Benutzeradministration“.

Ein Beispiel für die Verwaltung granularer Rollen für einen Benutzer oder eine Gruppe finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Informationen zum Zuweisen von Persona-Rollen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

## Vulnerability Response Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Elemente (AEs) automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Die Standardzuweisungsregel **CI-Supportgruppe**zuweisen ist im Basissystem enthalten und weist der CI- **Supportgruppe**angreifbare Elemente zu. Die Regel „Zu CI-Supportgruppe zuweisen“ weist einen VI einer Supportgruppe zu, die für das Configuration Item (CI) festgelegt ist, das dem VI zugeordnet ist.

**Hinweis:**
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.

Zuweisungstyp, ob „ **Manuell** “ oder „ **Regel** “, ist im VI-Formular und in der Listenansicht verfügbar. Jeder VI, der ursprünglich durch eine Regel zugewiesen wurde, aber anschließend manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel.

Verwenden Sie Zuweisungsregel und Zuweisungstypinformationen, um Fälle zu identifizieren, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Sie können die Informationen auch verwenden, um zu ermitteln, welche Regeln die meisten Neuzuweisungen aufwiesen.

Die durch Zuweisungsregeln festgelegten Zuweisungsgruppen werden von Korrekturaufgabenregeln verwendet, um Besitzer Korrekturaufgaben ( **VULs** ) zuzuweisen.

**Hinweis:**
Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset-Listen-Integration vor den anderen Rapid7 InsightVM -Integrationen ausführen.

Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.

## Angreifbare Elemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, angreifbare Elemente mit **Zuweisen mit**zuzuweisen:

- Benutzergruppe : Mit dieser Option können Sie eine der vorhandenen Now Platform® Benutzergruppen auswählen.
- Benutzergruppenfeld : Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:
  - Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
  - Konfigurationselement: Genehmigungsgruppe



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurationselement: Zuweisungsgruppe
- Konfigurationselement: Supportgruppe

- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder fortgeschrittene ServiceNow.

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist oder bei denen ein VI durch die Einhaltung gesetzlicher Vorschriften behandelt werden muss). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um AEs der Gruppe zuzuweisen, die ermittelt, zu welcher Zuweisungsgruppe sie gehören soll. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.

## Bewertungsprozess für Zuweisungsregeln

Zuweisungsregeln werden verwendet, um einen VI zu bewerten und zuzuweisen, wenn ein neuer VI geöffnet, d. h. importiert, manuell erstellt oder erneut geöffnet wird. Sofern Sie die Zuweisungsregeln nicht manuell erneut anwenden, nachdem sich der VI oder sein Status geändert hat, wird ein VI einmal ausgewertet.

Der folgende Prozess wird für jede neue, aktualisierte oder erneut geöffnete AEs verwendet:

- Für jede Schwachstellenzuweisungsregel wird der VI mit dem Zuweisungsfilter verglichen, wobei die Regel der niedrigsten Ordnung zuerst verwendet wird.
- Wenn die Bedingung erfüllt ist, wird dem AE eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung mit allen anderen Regeln finden, wird der VI der Standardzuweisungsgruppe zugewiesen, sofern eine Standardregel vorhanden ist.

  Sobald das angreifbare Element zugewiesen wurde, verwendet die entsprechende Regel für Korrekturaufgaben die Zuweisung als eines der Kriterien, um die angreifbaren Elemente einer Korrekturaufgabe zuzuordnen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Filtern innerhalb Vulnerability Response.

**Hinweis:**
Die Standardregel ist die Regel mit dem höchsten Wert für die Ausführungsreihenfolge. Eine letzte zu verwendende Regel, die ein guter Ausweichkontakt ist, ist active=true. Wenn keine Standardregel vorhanden ist, bleibt der VI nicht zugewiesen, wenn die Korrekturaufgabenregel die Zuweisung vornimmt.

## Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie die Schaltfläche **Änderungen** übernehmen auf der Listenseite „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen AEs mit Ausnahme der manuell zugewiesenen erneut auszuführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Wenn die geplante Aufgabe *`Reapply all vulnerability assignment rules`* vor der ersten Verwendung von **Änderungen anwenden**nicht ausgeführt wurde, werden alle Zuweisungsregeln für alle offenen AEs mit Ausnahme der manuell zugewiesenen AEs ausgeführt. Danach werden bei allen nachfolgenden Verwendungen von **„Änderungen anwenden** “ nur die geänderten Regeln und alle abhängigen Regeln erneut ausgeführt. Änderungen an einer Regel können dazu führen, dass ein VI einer anderen unveränderten Regel entspricht. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Die regelmäßige Aufgabe [*`Reapply all vulnerability assignment rules`*] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen AEs mit Ausnahme der manuell zugewiesenen angewendet. Sie kann **Täglich**, **Wöchentlich**, **Monatlich**, **Regelmäßig**, **Einmal**oder **Bei Bedarf**ausgeführt werden. Je nachdem, wie viele aktive AEs in Ihrer Umgebung vorhanden sind, müssen Sie das Feld **Ausführen** nach der ersten Ausführung entsprechend festlegen, um Auswirkungen auf die Leistung zu vermeiden.

Upgrade-Kunden sollten sich die VR-Versionshinweise ansehen, um Informationen zu den Auswirkungen dieser Funktion auf vorhandene AEs zu erhalten.

Wenn sich eine Zuweisungsgruppe in einer Zuweisungsregel ändert, können die angreifbaren Elemente automatisch neu ausgewertet und neu gruppiert werden, indem die Systemeigenschaft sn_vul.rerun_task_rules und die Geschäftsregel Mit Korrekturaufgaben verknüpfen aktiviert werden.

So aktivieren Sie die Systemeigenschaft:

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Öffnen Sie die Systemeigenschaft sn_vul.rerun_task_rules.
3. **Legen Sie** im Feld Wert den Wert auf true fest.

Wenn die Systemeigenschaft auf „true“ festgelegt ist und die Zuweisungsregeln erneut angewendet werden, wird die Verknüpfung der angreifbaren Elemente mit den Korrekturaufgaben aufgehoben, bei denen die Bedingung nicht mehr übereinstimmt.

**Hinweis:**

Standardmäßig ist die Systemeigenschaft sn_vul.rerun_task_rules auf false festgelegt.

Um die Neugruppierung angreifbarer Elemente zu automatisieren, müssen Sie die Geschäftsregel Korrekturaufgaben verknüpfen aktivieren.

So aktivieren Sie die Geschäftsregel:

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
2. Geschäftsregel Link zu Korrekturaufgaben öffnen.
3. Aktivieren Sie die Checkbox **Aktiv**, um die Business Rule zu aktivieren.

Wenn die Geschäftsregel aktiviert ist, werden die angreifbaren Elemente neu gruppiert, indem sie in die entsprechende Gruppe verschoben oder eine Gruppe erstellt werden, wenn sie nicht unter einer vorhandenen Gruppe gruppiert werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

- Die angreifbaren Elemente werden aus den Gruppen entfernt, ohne die Gruppen zu löschen.
- Es werden nur die Elemente entfernt, die mithilfe von Korrekturaufgabenregeln oder Korrekturaufwand erstellt wurden.
- Die Umgruppierung erfolgt nur automatisch, wenn sich die Zuweisungsgruppe als Teil einer Zuweisungsregel ändert, und nicht, wenn sie manuell geändert wird.

Die Neugruppierung in Arbeitsbereichen wird für Korrekturaufgaben durchgeführt, die aus einer Korrekturmaßnahme erstellt werden.

## Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln

Konfigurieren Sie Korrekturaufgaben (VULs), um Analysten und Korrekturspezialisten bei der Organisation von angreifbaren Elementen (VI) und der Massenanalyse zu unterstützen. Die Kriterien, nach denen Gruppen gebildet werden, sind so konfiguriert, dass Sie angreifbare Elemente nicht manuell Gruppen zuweisen müssen. Mithilfe von Korrekturaufgaben können Sie den Fortschritt überwachen und den Korrekturprozess effizienter gestalten.

## Nachverfolgung der Zurückstellungsanzahl für angreifbare Elemente und Korrekturaufgaben

Verfolgen Sie nach, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Containerelement oder eine Korrekturaufgabe zurückgestellt wurde. Eine regelmäßige Aufgabe, Anzahl der Zurückstellungen **festlegen**, wird täglich ausgeführt, um die Anzahl der Datensätze zu veröffentlichen, die mehr als einmal in der Spalte „Anzahl der Zurückstellungen“ zurückgestellt wurden. Datensätze werden in den Modulen für mehrere Zurückstellungen für VR, AVR und CVR angezeigt.

## Angreifbare Elemente werden automatisch aktualisiert

**Hinweis:**

Die Automatisierung der Aktualisierung angreifbarer Elemente gilt nur für Gruppen, die mit dem Bedingungsfilter oder der Filtergruppe erstellt wurden. Die Automatisierung gilt nicht für VIs, die manuell hinzugefügt oder mithilfe von Regeln für Korrekturaufgaben gruppiert wurden.

Wenn das Kontrollkästchen **Angreifbare Elemente automatisch aktualisieren** aktiviert ist, werden der Aufgabe automatisch neue AEs hinzugefügt, die den Filterkriterien der Korrekturaufgabe entsprechen. Angreifbare Elemente in der Korrekturaufgabe, die den Filterkriterien nicht mehr entsprechen, werden automatisch aus der Aufgabe entfernt.

Standardmäßig wird das Kontrollkästchen deaktiviert, wenn die Korrekturaufgabe den Status „ **Offen** “ verlässt. Wenn Sie möchten, dass angreifbare Elemente der Korrekturaufgabe unabhängig vom Status weiterhin hinzugefügt werden, deaktivieren Sie die Geschäftsregel `Set auto refresh vulnerable items`.

Sie können das Kontrollkästchen im Status Wird untersucht erneut manuell aktivieren. Die**automatische Aktualisierung angreifbarer Elemente** ist nicht deaktiviert, wenn die Korrekturaufgabe in den Status **„Warten auf Implementierung“ verschoben** wird. Sobald sich die Aufgabe im Status „Warten auf Implementierung“ befindet, können der vorhandenen Aufgabe weder neue angreifbare Elemente hinzugefügt noch vorhandene angreifbare Elemente entfernt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn eine Korrekturaufgabe manuell erstellt wird und **AEs** mithilfe des **Bedingungsfilters**oder der Filtergruppe hinzugefügt werden, ist das Kontrollkästchen deaktiviert. Sie haben die Wahl, ob Sie das Kontrollkästchen aktivieren möchten.

## Angreifbare Elemente werden manuell aktualisiert

Wenn Sie bei manuell erstellten Korrekturaufgaben mit einem **Filter fürFiltergruppe** oder **Bedingung** auf der Seite „Korrekturaufgabe“ auf den zugehörigen Link Zugehörige angreifbare Elemente **aktualisieren** klicken, werden alle angreifbaren Elemente hinzugefügt, die den Filterkriterien entsprechen. Elemente, die den Kriterien nicht mehr entsprechen, werden entfernt. Diese Aktion ermöglicht eine sofortige Aktualisierung der Liste der angreifbaren Elemente und wird unabhängig davon verwendet, ob das Kontrollkästchen **Angreifbares Element automatisch** aktualisieren aktiviert ist oder nicht.

Manuell erstellte Korrekturaufgaben mit den Filtertypen **Bedingung** oder **Filtergruppe** werden einmal pro Stunde aktualisiert.

## Grundlegendes zu Regeln für Korrekturaufgaben

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Elemente automatisch gruppiert und zugewiesen werden. Die Standardregel **Vulnerability**(Schwachstelle) ist im Basissystem enthalten und erfasst angreifbare Elemente basierend auf ihren Schwachstellen. Sie können jedoch nach anderen Wertesätzen in Spalten gruppieren, auf die vom AE aus zugegriffen werden kann. Diese Werte können die Supportgruppe für Konfigurationselemente (CI), den Schweregrad der Schwachstelle usw. umfassen.

Sie können eine beliebige Anzahl von Bedingungen erstellen. Sobald Sie eine Gruppieren nach-Auswahl festgelegt haben, wird eine weitere Zeile angezeigt. Sie können bis zu sechs **Gruppieren nach-** Auswahlen haben. Sie können die Gruppenzuweisung auch automatisieren. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben und Filtern innerhalb Vulnerability Response.

**Hinweis:**
Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Korrekturaufgabenregeln verfügbar zu machen, müssen Sie die Asset-Listen-Integration [ Rapid7 InsightVM vor den anderen Rapid7 InsightVM -Integrationen ausführen.

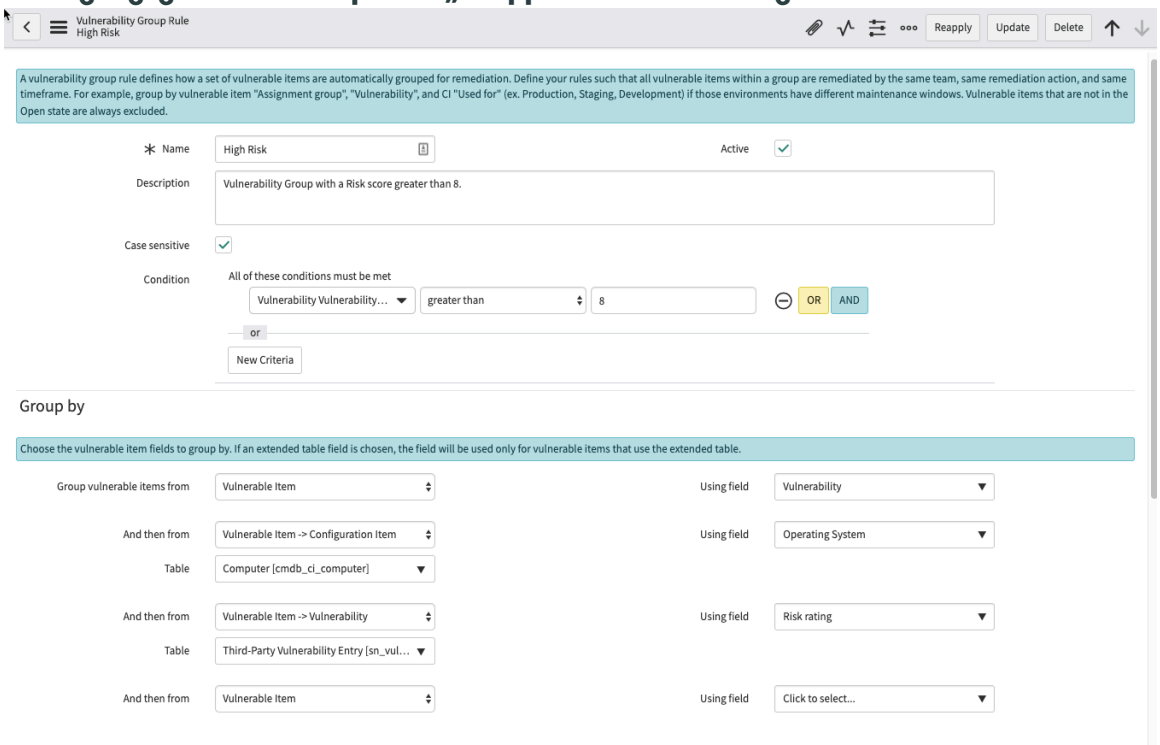
Beispielsweise können Sie angreifbare Elemente nach der Kostenstelle des angreifbaren CI oder nach dem Angriffsvektor der Schwachstelle gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit geringem Schweregrad oder CIs mit geringem Risiko haben. Sie können eine weitere Aufgabenregel für kritische Server und Schwachstellen mit Exploits haben – angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen.

Für angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Korrekturaufgabenregel Gruppieren **nach** Werten angehängt, um die Kurzbeschreibung des neuen Datensatzes zu erstellen. Weitere Informationen zu verfügbaren Feldern finden Sie unter Vulnerability Response-Gruppen erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bedingungsgenerator-Beispiel für „Gruppieren nach“-Einträge**




Wenn ein neues angreifbares Element erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Schwachstellenregeln dafür ausgewertet. Ein VI wird nur einmal automatisch ausgewertet, es sei denn, er wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jeden neuen oder erneut geöffneten VI verwendet:

- Für jede Regel für Korrekturaufgaben wird der AEs mit dem Regelfilter für Korrekturaufgaben verglichen.

- Für jede Regel, bei der die Bedingung der Korrekturaufgabenregel erfüllt ist, ruft die Regel die Daten aus der **Auswahl** Gruppieren nach im VI ab. Es werden ein Gruppenname und ein Feld erstellt. In diesem Fall, **Hohes Risiko: QID-32342:***`Zusammenfassung von QID-3242`* (Name: Schwachstellen-ID: Zusammenfassung der Schwachstelle).

  **Hinweis:**
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel überprüft, ob eine **offene** Korrekturaufgabe vorhanden ist, die derselben Zuweisungsgruppe wie der VI zugewiesen ist.

  - Wenn die Aufgabe gefunden wird, wird der VI der vorhandenen Aufgabe im Status „ **Offen** “ hinzugefügt.
  - Wenn keine Aufgabe im Status „ **Offen** “ gefunden wird, erstellt die Regel eine Aufgabe mit **hohem Risiko: QID-32342**, weist sie derselben Zuweisungsgruppe wie den AE zu und platziert den AE in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Bedingungen der Korrekturaufgabenregel verglichen wird, bevor sie in eine Gruppe eingefügt wird, können zu viele Regeln Auswirkungen auf die Leistung haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig verwenden Korrekturaufgabenregeln die Zuweisungsgruppe, die von den **Zuweisungsregeln** für das angreifbare Element festgelegt wird, wenn die Elemente gruppiert werden, und weisen die Korrekturaufgabe zu, um die angreifbaren Elemente abzugleichen.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln im Modul **„Zuweisungsregeln“** gesteuert. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel aus dem Formular oder der Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle von dieser Regel erstellten **offenen** Aufgaben zu löschen. Nicht **geöffnete** Aufgaben werden ausgeschlossen.

### Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Regel für Korrekturaufgaben ändern möchten, verwenden Sie die **Schaltfläche Erneut anwenden** auf der Seite für Korrekturaufgaben, um die geänderte Regel für alle aktiven **offenen** Korrekturaufgaben erneut auszuführen, die von dieser Regel erstellt wurden. Sie löscht und erstellt Korrekturaufgaben basierend auf der geänderten Regel automatisch neu.

## Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente (VI), ähnlich wie SLAs einen Zeitrahmen für die Korrektur der Schwachstelle selbst bereitstellen. Wenn ein Asset beispielsweise PCI-Daten (Kreditkartendaten) enthält, muss die Schwachstelle in diesem Element gemäß PCI DSS innerhalb von 30 Tagen behoben werden.

Schwachstellenmanager können Korrekturzielregeln erstellen, indem sie Folgendes definieren:

- Das Nachbesserungsziel
- Das Erinnerungsziel
- Die Erinnerungs- und Benachrichtigungsempfänger – Wer benachrichtigt werden soll, wenn die angreifbaren Elemente (AEs) das Erinnerungs- oder Korrekturzieldatum überschritten haben und nicht korrigiert wurden.

Schwachstellenanalysten und -manager können das Korrekturzieldatum im Formular für angreifbare Elemente und in **Listenansichten**anzeigen, solange sich die angreifbaren Elemente nicht im Status „Zurückgestellt“, **„Gelöst“**oder **„Geschlossen** “ befinden.
Korrekturzielregeln werden beim Import ausgeführt und erneut ausgeführt, wenn eine VI erneut geöffnet wird.

Das **Korrekturzieldatum** wird in der VI-Listenansicht wie folgt als Punkte farbcodiert:

- Angreifbare Elemente, deren Benachrichtigungsdatum noch nicht erreicht ist, werden in Grün angezeigt.
- Angreifbare Elemente, die sich dem Korrekturzieldatum nähern, werden in Orange angezeigt.
- Angreifbare Elemente nach dem Korrekturzieldatum werden rot angezeigt.

Gemäß der Korrekturzielregel wird eine Zusammenfassungs-E-Mail gesendet, wenn eine oder mehrere AEs sich ihrem Korrekturzieldatum nähern oder das Korrekturzieldatum verstrichen ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert wird, werden die aktuellen Korrekturzieldaten für die AEs gelöscht, auf die sie angewendet wurde. Wenn ein VI eine aktive Regel erfüllt, wird diese Regel angewendet, andernfalls hat der VI keine Regel oder kein Zieldatum und sein Status ist **Kein Ziel**.

Wenn Regeln gelöscht werden, werden das Korrekturzieldatum und zugehörige Felder für geschlossene, zurückgestellte oder gelöste **AEs** beibehalten. Das Korrekturzieldatum und zugehörige Felder in nicht geschlossenen **AEs** werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

## Szenario der Korrekturzielregel

Wenn mehrere Korrekturzielregeln auf dasselbe angreifbare Element angewendet werden, wird die restriktivste Regel angewendet.

**Hinweis:**
Korrekturziele werden aus dem Datum von „ **Zuletzt geöffnet** “ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.

Ab V17.1 werden Korrekturziele aus dem **Ziel ab (Datum)**berechnet. Der Standardwert bleibt **Zuletzt geöffnet am**.

Beispiel: Wenn ein angreifbares Element die Bedingung für zwei Korrekturzielregeln erfüllt:

Szenario: Angreifbares Element zuletzt geöffnet am 01.03.2018 um 10:00:00.

- Korrekturzielregel 1: Zuletzt geöffnet am 03.07.2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen. Das berechnete Korrekturzieldatum ist der 16.03.2018 10:00:00.
- Korrekturzielregel 2: Zuletzt geöffnet am 10.03.2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen. Das berechnete Korrekturzieldatum ist der 11.03.2018 10:00:00.

In diesem Szenario gilt die Korrekturzielregel 2 für das angreifbare Element, da es das restriktivere Datum hat. 10 Tage seit der ersten Identifizierung des angreifbaren Elements im Vergleich zu 15 Tagen.

**Hinweis:**
Sobald die Korrekturzielregel definiert ist, werden die Korrekturzieldaten von der geplanten Aufgabe *`Evaluate remediation targets`* berechnet.

## Über die geplante Aufgabe „Korrekturziele auswerten“

*`Evaluate remediation targets`* wird einmal täglich um 4:00:00 Uhr ausgeführt.

Sie durchläuft alle aktiven Schwachstellenregeln, beginnend mit den Regeln mit dem frühesten Korrekturzieldatum. Es werden alle angreifbaren Elemente betrachtet, die:

- Sie befinden sich nicht im Status „ **Geschlossen**“, **„Zurückgestellt“**oder **„Gelöst“**.
- Hat kein Korrekturzieldatum.
- Sie haben ein Korrekturzieldatum, das nach dem Datum in der Korrekturzielregel liegt.

*`Evaluate remediation targets`* fügt ein Korrekturzieldatum hinzu, wenn keines vorhanden ist, oder wenn eine Regel zu einem früheren Datum als dem im Datensatz führt,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird das vorhandene Zieldatum aktualisiert. Schließlich werden die Felder **Korrekturziel** und **Korrekturstatus** im Formular für angreifbare Elemente aktualisiert.

Sobald *Evaluate remediation targets* ausgeführt wird, werden verfügbare Benachrichtigungen gesendet.

*Evaluate remediation targets* löscht die Korrekturfelder im VI und beendet das Senden von Benachrichtigungen.

Ab Vulnerability Response v19.0 verhindert die Eigenschaft *sn_sec_cmn.evaluate_targetmissed_records*, wenn sie aktiviert ist, dass die geplante Aufgabe *Remediation Target Rules* verpasste AEs auswertet. Diese Eigenschaft ist standardmäßig aktiviert.

### Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, verwenden Sie die Schaltfläche **Änderungen anwenden** auf der Listenseite „Korrekturzielregeln“, um alle geänderten Regeln für alle aktiven offenen AEs mit Ausnahme derer im Status „ **Geschlossen**“, **„Zurückgestellt“** oder **„Gelöst** “ erneut auszuführen. Je nachdem, wie viele VIs Sie haben, kann dies einige Zeit dauern.

**Hinweis:**

Wenn die geplante Aufgabe *Evaluate remediation targets* ausgeführt wird, können Sie keinen erneuten Anwendungsprozess initiieren. Wenn jedoch bereits ein Prozess zum erneuten Anwenden ausgeführt wird und die geplante Aufgabe, die er ausgelöst hat, ausgeführt wird, werden sie parallel ausgeführt.

Die Prozesse zum erneuten Anwenden in Vulnerability Response und Application Vulnerability Response sind unabhängig und können parallel ausgeführt werden.

**Zugehörige Informationen**

Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

Zeigen Sie den Status des Korrekturziels eines Vulnerability Response angreifbaren Elements an

Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele

## Schwachstellenklassifizierungsgruppen und -regeln

Klassifizierungsgruppen automatisieren die Klassifizierung von Werten einer Tabelle basierend auf den in der Gruppe definierten Klassifizierungsregeln. Die Bedingung für jede Regel wird der Reihe nach ausgewertet, und die erste Übereinstimmungsregel wird verwendet.

Das Vulnerability Response-Basissystem umfasst die folgenden zwei Klassifizierungsgruppen, die erkannte Elemente bzw. Schwachstellen klassifizieren:

- Klassifizierung erkannter Elemente
- Klassifizierung von Schwachstelleneinträgen

Immer wenn Schwachstellen und erkannte Elemente importiert werden, werden die Schwachstellenklassifizierungsregeln in den jeweiligen Gruppen ausgeführt. Basierend auf den in der Regel festgelegten Bedingungen werden die Datensätze in die entsprechende Klassifizierungsgruppe klassifiziert. Sie können diese Regeln erstellen, bearbeiten, löschen oder erneut auf eine vorhandene Schwachstelle anwenden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

- Für eine ausgewählte Tabelle kann es nur eine aktive Klassifizierungsgruppe geben.
- Nachdem Sie eine Gruppe erstellt haben, können Sie sie nicht löschen.

Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie eine Klassifizierungsregel, Wenden Sie eine Regel auf eine vorhandene Schwachstelle an und Deaktivieren oder löschen Sie eine Klassifizierungsregel.

## Lösungen für maschinelles Lernen für Vulnerability Response

Empfehlungen für die Zuweisung von Schwachstellen verwendet ServiceNow® Predictive Intelligence und maschinelles Lernen, um Zuweisungsgruppen für angreifbare Elemente (AEs) und Korrekturaufgaben (VULs oder RTs) zu empfehlen. Sie können die Zeit reduzieren, die Sie für die Identifizierung der Besitzer für nicht oder falsch zugewiesene Schwachstellenergebnisse benötigen. Außerdem sehen Sie eine vom System generierte Konfidenzpunktzahl, die auswertet, ob die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist.

Die Fähigkeiten von Predictive Intelligence werden in Vulnerability Response verwendet, um eine bessere Arbeits-Experience zu bieten, indem ein Lösungsdefinitionsmodell erstellt und trainiert wird, das die Zuweisungsgruppe basierend auf vorhandenen Daten vorhersagen kann.

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

## Empfehlungen für die Zuweisung von Schwachstellen

Mit der Anwendung Empfehlungen für die Zuweisung von Schwachstellen (com.snc.vulnerability.recom) kann das System Empfehlungen in Vulnerability Response mit ServiceNow Predictive Intelligencezuweisen. Dieses Plugin erfordert:

- Vulnerability Response (com.snc.vulnerability)
- Predictive Intelligence (com.glide.platform_ml)

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

## Vertrauensbewertungen

Verwenden Sie die Anwendung Empfehlungen für die Zuweisung von Schwachstellen, um die Konfidenzpunktzahl zu generieren, die das Konfidenzniveau der empfohlenen Zuweisungsgruppen für die ausgewählten RTs oder VIs angibt. Die Konfidenzpunktzahl wertet aus, ob das System davon ausgeht, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Es werden bis zu 10 Empfehlungen angezeigt. Diese Empfehlungen basieren auf der höchsten Wahrscheinlichkeit für erfolgreiche Zuweisungen. Die erste Empfehlung in der Liste bedeutet, dass das System die höchste Konfidenz hat, dass es sich um die richtige Zuweisungsgruppe handelt.

Zum Beispiel gibt die Konfidenzpunktzahl auf einer Skala von 0 bis 100 für jede Zuweisungsgruppe die Wahrscheinlichkeit an, dass ein VI oder RT zu dieser bestimmten Gruppe gehört.

**Zugehörige Informationen**

Predictive Intelligence

Klassifizierungslösung erstellen und trainieren



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Ähnlichkeitslösung erstellen und trainieren

Clustering-Lösung erstellen und trainieren

Erweiterte Einstellungen für ML-Lösungen konfigurieren

## CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln werden verwendet, um Konfigurationselemente (CIs) zu identifizieren und dem Datensatz für angreifbare Elemente hinzuzufügen, um die Korrektur zu unterstützen.

Navigieren Sie ab Version 19.0 zu **Security Operations** > **CMDB** > **Suchregeln** , um die Liste in Ihrer Instanz zu finden.

Beim Importieren von Assets wird zuerst in der Liste „ **Erkannte Elemente** “ anhand von Drittpartei-IDs gesucht, um Übereinstimmungen mit Konfigurationselementen (CIs) aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Host-ID gefunden wird, wird sie als Feld **Konfigurationselement** im Datensatz des angreifbaren Elements verwendet.

Sie können mithilfe der Liste „ **Erkannte** Elemente“ sehen, wie importierte Assets CIs zugeordnet werden. Wenn keine Übereinstimmung gefunden wird oder das Feld „Host-ID“ leer ist, verwenden die Regeln die anderen Hostinformationen, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als Nicht **abgeglichenes CI**gekennzeichnet. Weitere Informationen zum Umgang mit diesen CIs finden Sie unter Nicht abgeglichene CIs.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Jede Quelle kann mehrere Bereitstellungen haben.

**Hinweis:**
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenquellenintegration gemeinsam genutzt. Wenn eine Regel gelöscht oder geändert wird, wirkt sich die Löschung oder Änderung auf alle Bereitstellungen der Schwachstellenintegration aus.

Wenn Sie eine Übereinstimmung versuchen, ist der erste Schritt eine Lieferanten-ID-Suche nach einer genauen Übereinstimmung für Quelle, source_instance und Lieferanten-ID. Dann werden Suchregeln der Reihe nach ausgeführt, von der niedrigsten zur höchsten, und angehalten, wenn eine Regel nur ein einzelnes CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

**Hinweis:**
Um eine Übereinstimmung mit Low-Level-Netzwerkelementen zu vermeiden, wird das übergeordnete CI zurückgegeben, wenn ein übereinstimmendes CI `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`oder `cmdb_ci_ip_address`ist.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist beim Upgrade nicht verfügbar. Informationen zum Upgrade und Anweisungen zum Festlegen der Eigenschaft finden Sie unter CI-Klassen ignorieren.

Um die Suche nach Übereinstimmungsproblemen zu erleichtern, wird die CI-Suchregel, anhand derer eine Übereinstimmung gefunden wird, dem Datensatz „Erkanntes Element“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im Feld „ **CI** -Übereinstimmungsregel“ hinzugefügt. Suchregeln werden zuerst nach dem niedrigsten Wert für die **Reihenfolge** ausgewertet.

Diese Qualys CI-Suchregeln werden mit dem Basissystem geliefert.

- QUALYS-HOST-ID
- FQDN
- NetBIOS
- DNS
- IP

Diese Rapid7 CI-Suchregeln werden mit dem Basissystem geliefert.

- MAC-Adresse
- FQDN
- HostName
- IP

Diese Tenable.io-CI-Suchregeln werden mit dem Basissystem geliefert.

- FQDN
- NETBIOS
- HOSTNAME
- MAC-Adresse
- DNS

Diese Tenable.sc-CI-Suchregeln werden mit dem Basissystem geliefert.

- MAC-Adresse
- FQDN
- NETBIOS

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie, wenn Sie neue Regeln erstellen.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Abgleichen innerhalb von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie benutzerdefinierte CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Schritte zum Verhindern doppelter oder verwaister Datensätze nach dem Ausführen von Vulnerability Response CI-Suchregeln finden Sie weitere Informationen zum Verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

**Hinweis:**
Weitere Informationen zur CI-Übereinstimmung finden Sie unter KB0998706 .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf der Listenseite „CI-Suchregeln“ auf **Änderungen** übernehmen, um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Keine Übereinstimmung mit einer Regel

Wenn sich das Konfigurationselement (CI) nach der erneuten Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die betroffenen Erkennungen und angreifbaren Elemente werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter CI-Suchregeln auf ausgewählte erkannte Elemente erneut anwenden.

### Nicht klassifizierte Hardware

Wenn ein Asset keine Übereinstimmung in den Suchregeln Configuration Management Database (CMDB) nach CI findet, wird das Asset als nicht klassifizierte Hardware bezeichnet.

Wenn Daten aus mit ServiceNow erstellten Integrationen importiert werden, verwendet Vulnerability Response automatisch Hostdaten, um nach Übereinstimmungen in CMDBzu suchen. Die CI-Suchregeln werden verwendet, um Konfigurationselemente (CIs) zu identifizieren und dem Datensatz für angreifbare Elemente hinzuzufügen, um die Korrektur zu unterstützen. Wenn die Assets nicht in CMDBgefunden werden, führt die Identification and Reconciliation Engine (IRE) ihre eigenen Identifizierungsregeln aus, die für die Hardwareklasse und alle ihre untergeordneten Elemente definiert sind, und erstellt ein CI unter einer nicht klassifizierten Hardwareklasse. Wenn Discovery dieses Asset findet, wird ein CI erstellt, anstatt die vorhandene nicht klassifizierte Hardware neu zu klassifizieren. Dies liegt daran, dass die Identifizierungsregel auf dem Namen des Hardware-CI basiert.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

Die folgenden Auszüge zeigen die IRE-Nutzlast für die Erstellung von CI in nicht klassifizierter Hardware über Vulnerability Response bzw. Discovery.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
      "name": "asset01.company.com",//from NetBios,
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123"
   }

"settings": {
      "updateWithoutSwitch": true
   }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
      "name": "asset01",
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123",
      "os_domain": "company"
   }
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"settings": {
      "updateWithoutSwitch": false
   }
```

In diesem Fall wird das vorhandene nicht klassifizierte Hardware-CI nicht auf Windows-Server neu klassifiziert, sondern es wird ein neues CI unter Windows-Server erstellt. Der Grund dafür ist, dass die Identifizierungsregel vom Namen des Hardware-CI abhängt. Wenn Sie die Nutzlasten bemerken, ist der Name in der Nutzlast von Vulnerability Response mit dem FQDN/NETBIOS identisch, es ist jedoch nur der Hostname für die Nutzlast von Discovery.

**Zugehörige Informationen**

Nicht klassifizierte Hardware neu klassifizieren

### Nicht abgeglichene CIs

Konfigurationselemente (CIs) werden beim Import automatisch mit CIs in Configuration Management Database (CMDB) abgeglichen. Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet diese Konfigurationselemente ohne Übereinstimmung auf.

Wenn Sie der Meinung sind, dass ein nicht abgeglichenes CI zu einer vorhandenen Klasse in der CMDB gehört, überprüfen Sie Ihre CI-Suchregeln. Andernfalls sollten Sie das Konfigurationselement neu klassifizieren.

**Hinweis:**
Der Standardfilter für diese Liste ist auf **Nicht abgeglichen**festgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

**Zugehörige Informationen**

Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren

Nicht übereinstimmende erkannte Elemente abstimmen

Schritte zum Verhindern doppelter oder verwaister Datensätze nach dem Ausführen von Vulnerability Response CI-Suchregeln

Vorhandene Konfigurationselemente werden dedupliziert

## Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.

Sie können Konfigurationselemente (CIs) in Configuration Management Database (CMDB) mithilfe der IRE-API (Identification and Reconciliation Engine) erstellen. Wenn Sie die IRE-API zum Erstellen von CIs verwenden, können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in CMDBschreiben.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB enthält Basissystemklassen, in denen Daten zu CIs gespeichert werden.

### IRE zur CI-Erstellung verwenden

Wenn vor Vulnerability Response v12.2, ein übereinstimmendes CI weder in der Liste „Erkannte Elemente“ noch in CMDBgefunden wurde, wird ein CI in der Klasse „Nicht abgeglichene



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs“ (sn_sec_cmn_unmatched_ci) erstellt. Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

Ab Vulnerability Response v12.2 bis 18.0 werden, wenn bei Anwendung der CI-Suchregeln keine Übereinstimmung gefunden wird, die Asset-Informationen an IRE gesendet und ein CI in einer der Klassen *„Nicht klassifizierte Hardware“* und „ *Unvollständige IP – Identifiziertes Gerät* “ erstellt. Ab Vulnerability Response v18.0 ist die neue Klasse „ *Cloud-Ressource* “ ebenfalls enthalten. Weitere Informationen zum Konfigurieren der Kategorisierung nicht abgeglichener Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

## CMDB CI-Klassen

**Hinweis:**
Um die neuen Klassen zu verwenden, aktivieren Sie das Plugin CMDB CI Class Models. Andernfalls werden CIs in der CI-Klasse Nicht abgeglichen erstellt.

Wenn der Host, den Sie von einem Drittanbieter-Scanner importiert haben, nicht in der Liste „Erkannte Elemente“ oder in CMDBgefunden wird, wird er erstellt in einer der folgenden neuen CMDB CI-Klassen.

### CMDB CI-Klassen

| CMDB CI-Klasse | Beschreibung |
|---|---|
| Unvollständige IP-Identifizierung des Geräts (*cmdb_ci_incomplete_ip*) | CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen nur die IP-Adresse verfügbar ist. |
| Nicht klassifizierte Hardware (*cmdb_ci_unclassed_hardware*) | CI wird in dieser Tabelle erstellt, wenn eine der folgenden Informationen in den vom Scanner empfangenen Hostinformationen verfügbar ist:<br>• Hostname<br>• IP-Adresse<br>• DNS<br>• NETBIOS<br>• MAC-Adresse<br>**Hinweis:**<br>Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und dem nicht klassifizierten Hardware-CI zugeordnet. Wenn sowohl die IP- als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adress-CI erstellt und dem nicht klassifizierten Hardware-CI zugeordnet. |
| Cloud-Ressource (*cmdb_ci_cmp_resource*) | CI wird in dieser Tabelle erstellt, wenn *Cloud Resource ID* in den vom Scanner empfangenen Hostinformationen verfügbar ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CMDB CI-Klassen (Fortsetzung)**

| CMDB CI-Klasse | Beschreibung |
|---|---|
| | **Hinweis:** Wenn der Asset-Typ einer Scanner-Integration *Hybrid* und die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* auf „false“ festgelegt ist, werden die CIs in der Klasse „Nicht *klassifizierte Hardware“*, aber nicht in der Klasse „ *Cloud-Ressource* “ erstellt. |

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

Das System verwendet automatisch eine nicht abgeglichene CI-Klasse, wenn einer der folgenden Fälle auftritt:

- Das CI-Klassen-Plugin CMDB ist nicht aktiviert.
- IRE löst beim Erstellen eines CI eine Ausnahme aus.

  Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

**Zugehörige Informationen**

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

### CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert

Ab Vulnerability Response v20.0 können Sie die nicht abgeglichenen Cloud-Assets aus den Scannern Qualys, Rapid7 und Tenable mithilfe der Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* in *nicht klassifizierte Hardware kategorisieren*.

Diese Systemeigenschaft mit dem Standardwert „ false “ ist im Lieferumfang des Basissystems enthalten. Sie klassifiziert die nicht abgeglichenen Cloud-Assets in eine Klasse für *nicht klassifizierte Hardware* (*cmdb_ci_unclassed_hardware*) oder *Cloud-Ressource* (*cmdb_ci_cmp_resource*) für die Integrationen, die sowohl Infrastruktur- als auch Cloud-Assets einbeziehen.

Ab Vulnerability Response v20.0 wird die Spalte „Asset-Typ“ in der Tabelle „Drittpartei-Integrationen“ (sn_sec_int_integration) hinzugefügt, um die Integrationen zu identifizieren, die sowohl Infrastruktur- als auch Cloud-Assets unterstützen. Die Spalte „Asset-Typ“ hat den Wert *Hybrid* für die Scanner, die sowohl Infrastruktur- als auch Cloud-Assets einbeziehen. Beispiel: Qualys, Rapid7- und Tenable-Integrationen haben den Wert *Hybrid* in der Spalte „Asset-Typ“.

- Bei der Neuinstallation von Vulnerability Response v20.0 und höher werden alle nicht abgeglichenen Cloud-Assets wie folgt kategorisiert:
  - Standardmäßig*nicht klassifizierte Hardwareklasse*.
  - Klasse*Cloud-Ressourcen*, wenn Sie die Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* in trueändern.
- Für Upgrades auf Vulnerability Response v20.0:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn sich in der *Cloud-Ressourcenklasse* Assets befinden, wird die Systemeigenschaft „ *sn_sec_cmn.unmatched_cloud_resource_enabled* “ auf „true“ festgelegt, sodass die nicht abgeglichenen Cloud-Assets weiterhin der *Cloud-Ressourcenklasse* (*cmdb_ci_cmp_resource*) hinzugefügt werden.
- Andernfalls wird die Systemeigenschaft „ *sn_sec_cmn.unmatched_cloud_resource_enabled* “ auf „false“ festgelegt, sodass die nicht abgeglichenen Cloud-Assets in die Klasse *„Nicht klassifizierte Hardware“* kategorisiert werden.

**Hinweis:**
Wenn Sie den Wert der Systemeigenschaft *sn_sec_cmn.unmatched_cloud_resource_enabled* ändern, stellen Sie sicher, dass nicht abgeglichene Konfigurationselemente in der zuvor anvisierten CI-Klasse gelöscht werden, und wenden Sie die Suchregeln erneut an. Weitere Informationen zum Löschen vorhandener CIs und zum erneuten Anwenden von CI-Suchregeln, damit die neuen CIs in der richtigen Klasse erstellt werden, finden Sie unter KB1533376 .

## Erkannte Elemente

Assets werden automatisch mit Konfigurationselementen (CIs) in Configuration Management Database (CMDB) abgeglichen, wenn sie mit **CI-Suchregeln**importiert werden. Erkannte Elemente geben Ihnen Einblick, wie die Asset-Identifizierung CIs in der CMDBzugeordnet wird.

Erkannte Elemente werden als **abgeglichen**, nicht **abgeglichen**oder **neu klassifiziert**betrachtet. Identifizierte CIs befinden sich im Status **Abgestimmt**.

Um die Suche nach potenziellen Übereinstimmungsproblemen zu erleichtern, wird die CI-Suchregel, die mit dem **CI übereinstimmt,** im Feld CI-Übereinstimmungsregel angezeigt.

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet nicht abgeglichene Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in erkannten Elementen finden Sie unter Felder des Formulars „Erkannte Elemente“.. Weitere Informationen zum Abgleichen nicht abgeglichener erkannter Elemente und zum erneuten Anwenden von CI-Suchregeln auf ausgewählte erkannte Elemente finden Sie unter Nicht übereinstimmende erkannte Elemente abstimmen bzw. Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente an.

### CI-Änderungen für erkannte Elemente

Wenn sich ein Configuration Item (CI) für ein erkanntes Element (DI) ändert, werden die betroffenen Erkennungen und angreifbaren Elemente (AEs) aktualisiert. Die Risikopunktzahl, Zuweisungsregeln, Gruppenregeln und Korrekturzielregel werden neu ausgewertet.

Wenn eine VI mit derselben Schwachstelle und demselben CI vorhanden ist, werden die Erkennungen mit der vorhandenen VI aktualisiert, und die aktuelle VI wird mit dem Substatus „InvalidCI“ geschlossen. Arbeitsnotizen werden aus folgenden Gründen hinzugefügt:

- Wenn Erkennungen von einem VI in einen anderen verschoben werden.
- Wenn ein doppeltes VI geschlossen wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie das CI für die vorhandene VI nicht aktualisieren möchten, legen Sie die Eigenschaft sn_sec_cmn.update_on_ci_change auf falsefest. Wenn sich dann ein CI ändert, wird ein neuer VI erstellt und der vorhandene als ungültigesCI geschlossen.

Der Standardwert der Eigenschaft sn_sec_cmn.update_on_ci_change ist true.

### Erkannte Elemente werden erneut ausgewertet

Wenn neue Daten zu einem erkannten Element empfangen werden, wird das erkannte Element nicht sofort neu ausgewertet. Beim Empfang neuer Daten wird die Option *reevaluate_citrue* standardmäßig auf [] festgelegt.

Die regelmäßige Aufgabe *Re-apply CI Lookup Rules on the Changed Discovered items* wertet alle erkannten Elemente aus, deren Quelldaten vom Scanner geändert werden. Sie verarbeitet die erkannten Elemente erneut und aktualisiert die angreifbaren Elemente, die sich auf das erkannte Element beziehen, dessen Quelldaten geändert wurden. Der Wert dieser regelmäßigen Aufgabe ist standardmäßig *On Demand*.

**Hinweis:**
Sie können diese regelmäßige Aufgabe auch täglich ausführen.

## Vulnerability Response Status von Korrekturaufgaben und angreifbaren Elementen

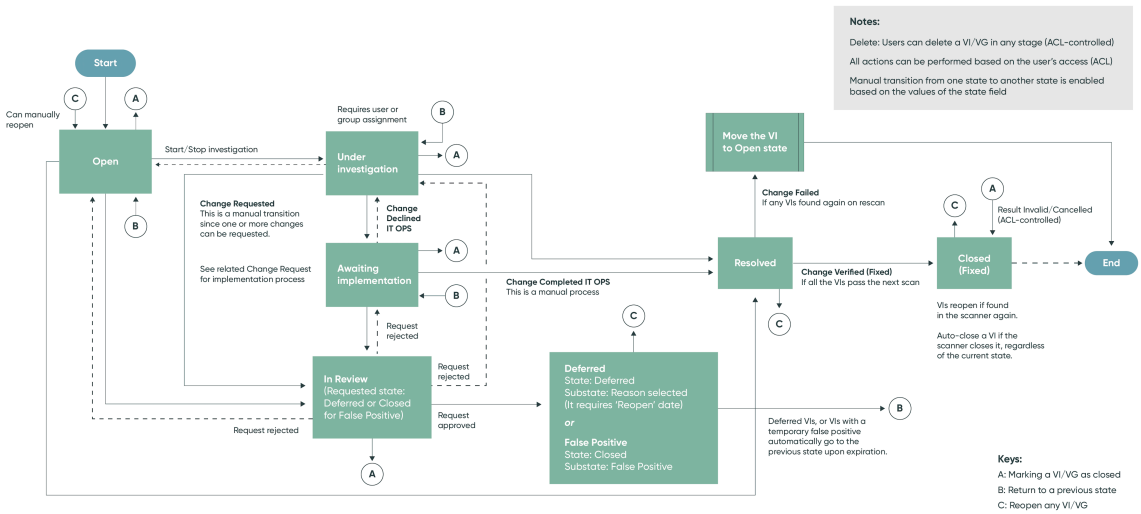
Mit der Anwendung Vulnerability Response können Sie das Statusmodell verwenden, um den Status einer Korrekturaufgabe jederzeit anzuzeigen. Wenn Sie wissen, wie die einzelnen Status miteinander verknüpft sind und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie angreifbare Elemente (AEs) korrigiert werden müssen.

## Status der Korrekturaufgabe

Komplexe Anwendungsfälle können manchmal dazu führen, dass sich ein angreifbares Element in einem anderen Status als seine Korrekturaufgabe befindet. Wenn Sie verstehen, wie Status funktionieren, können Sie dieses Verhalten erklären und beim Erstellen von Korrekturaufgaben und beim Erstellen oder Bearbeiten von Regeln für Korrekturaufgaben helfen.

Korrekturaufgaben haben viele mögliche Status, wie im folgenden Diagramm dargestellt.

### Vulnerability Response-Status-Flow






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Jedes Aufgabenformular enthält die Schaltflächen **Verfolgen** und **Aktualisieren**, die für ServiceNow -Aufgaben standardmäßig vorhanden sind.

Weitere Informationen zu Status von Korrekturaufgaben und Aktionen, die Sie in einem bestimmten Status ausführen können, finden Sie unter Vulnerability Response Status der Korrekturaufgabe.

Weitere Informationen zu Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente finden Sie unter Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente.

Weitere Informationen zu Korrekturaufgaben- und VI-Status finden Sie unterStatus von Korrekturaufgaben und angreifbaren Elementen.

Weitere Informationen zum Status von Korrekturaufgaben für AEs in mehreren Gruppen finden Sie unter Status der Korrekturaufgabe für angreifbare Elemente (AEs) in mehreren Gruppen.

### Berechnung und Anzeige des Alters angreifbarer Elemente

Das Alter von angreifbaren Elementen (AEs) wird in der Anwendung Vulnerability Response mit weiteren Details angezeigt.

## Übersicht

Das Alter des angreifbaren Elements (VI) wird im Format Tage/Stunden/Minuten in der Spalte Alter in der Listenansicht „Angreifbare Elemente“ und in den Feldern Alter und Alter geschlossen in VI-Datensätzen (VIT) angezeigt. Das Alter, das in signifikanteren Ziffern angezeigt wird, kann Ihnen helfen, die folgenden Aktivitäten genauer auszuführen:

- Konfigurieren Sie Regeln im Modul „Regeln für automatische Löschung“, um bestimmte AE-Datensätze nach Tagen/Stunden/Minuten zu löschen. Das Entfernen von Datensätzen mit höherer Genauigkeit kann Ihre Leistung steigern, insbesondere wenn Sie eine große Anzahl von VI-Datensätzen in Ihrer Instanz haben.
- Zeigen Sie Berichte mit spezifischeren Details in der Anwendung Performance Analytics für die Vulnerability Response an.
- Erstellen Sie Filter, die nur die gewünschten AEs identifizieren.
- Beschneiden Sie Listenansichten, um nur die gewünschten VIs anzuzeigen.
- Dot-Walk einfacher.

Eine geplante Aufgabe hat das Alter berechnet und alle aktiven AEs aktualisiert. In Instanzen mit einer großen Anzahl von VI-Datensätzen kann dieser Prozess langsam sein und sich negativ auf die Leistung auswirken. Das AE-Alter wird bei Bedarf effizienter berechnet und mit signifikanteren Stellen mit einer erweiterten Altersspalte angezeigt. Die erweiterte Spalte „Alter“ wird automatisch hinzugefügt, wenn Sie die Anwendung Vulnerability Response installieren oder aktualisieren.

**Hinweis:**
Wenn Sie ein Upgrade durchführen und das AE-Alter nicht in der Listenansicht der angreifbaren Elemente und in den Feldern Alter und Alter geschlossen für aktive AE-Datensätze (VIT) im Format Tage/Stunden/Minuten (9 Tage, 18 Stunden, 29 Minuten) angezeigt wird , die Altersspalte ist in Ihrer Instanz nicht aktuell. Weitere Informationen zur Behebung dieses Problems nach einem Upgrade finden Sie unter KB0749231 .

Die Altersspalte und die Felder können nicht bearbeitet werden. Ein Schwachstellenmanager mit der Berechtigung sn_vul.vulnerability_read oder die Schwachstellenadministrator-Persona kann diesen Wert anzeigen, und IT-Korrekturbesitzer



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit der Rolle sn_vul.remediation_owner können ihn für Datensätze anzeigen, die ihnen zugewiesen sind.

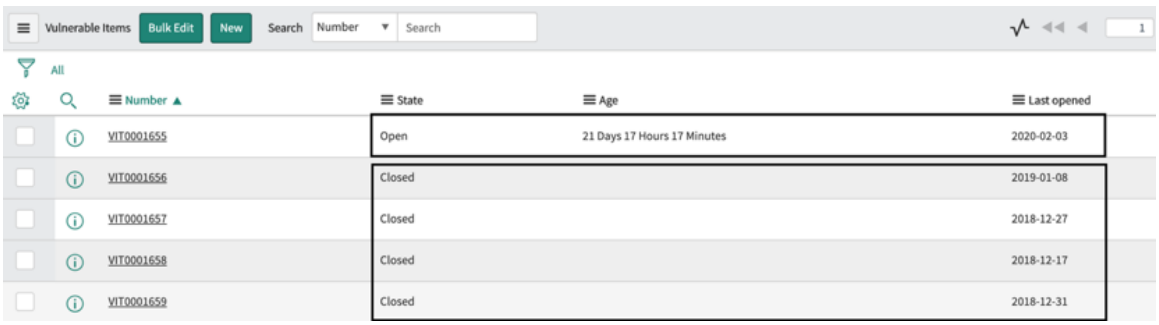
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Das AE-Alter wird wie in den folgenden Abbildungen angezeigt.

## Liste der angreifbaren Elemente

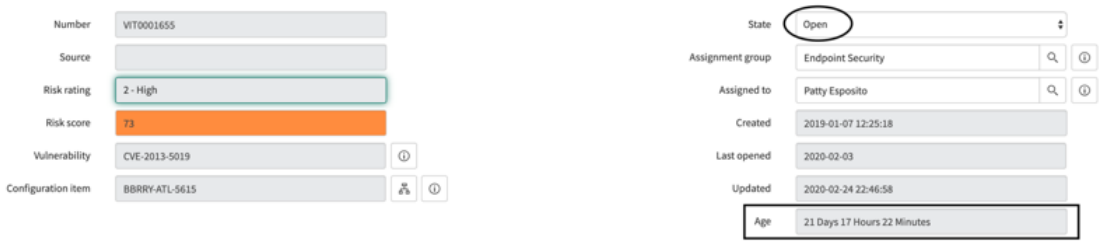
Wie in der folgenden Abbildung dargestellt, wird in der Listenansicht „Angreifbare Elemente“ das Alter in der Spalte Alter nur für aktive AEs in Tagen/Stunden/Minuten (21 Tage 17 Stunden 17 Minuten) angezeigt. Aktive VIs sind VIs in einem anderen Status als „Geschlossen“. Dieser Alterswert stellt die Anzahl der Tage dar, die der VI aktiv war.

Für AEs im Status „Geschlossen“ wird das Alter nicht angezeigt. Bei VIs, die sich zuvor im Status „Geschlossen“ befanden und dann erneut geöffnet wurden, stellt der Wert die Anzahl der Tage dar, die die VI seit dem Datum der letzten Öffnung aktiv war.




## Alter der VI-Datensätze

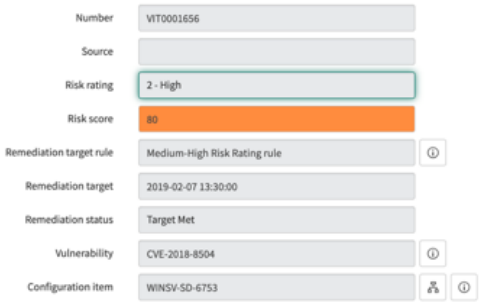
In den VI-Datensätzen ist der Wert der Spalte Alter in der Listenansicht für aktive AEs im Feld Alter sichtbar.

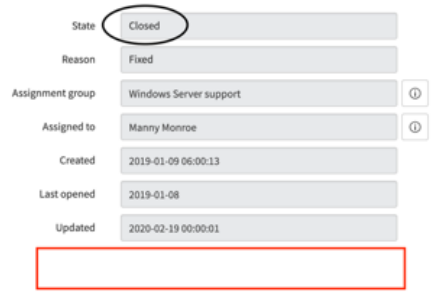



Der Wert der Spalte „Alter“ wird für VI-Datensätze im Status „Geschlossen“ nicht angezeigt.



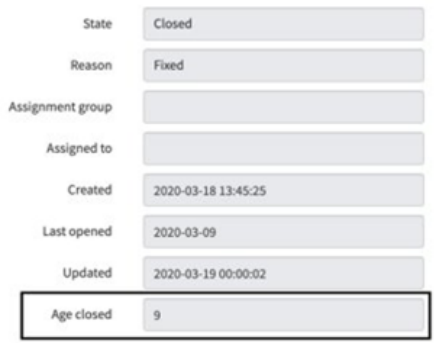
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



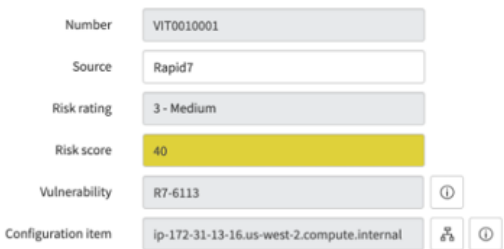



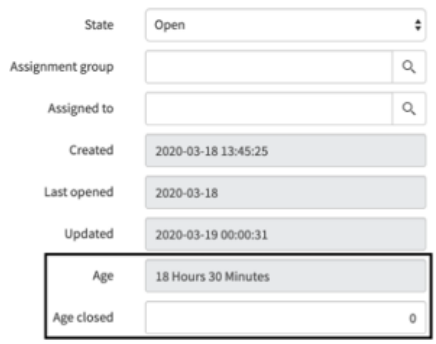

## Alter in der Liste der angreifbaren Elemente und in den AE-Datensätzen, wenn ein AE aktualisiert wird

Wenn sich eine AEs im Status „Geschlossen“ befindet, wird das Feld „Alter“ nicht angezeigt. Wenn der VI in „Geschlossen“ übergeht, wird der Wert in Tagen aus der Spalte „Alter“ im Feld „Alter geschlossen“ (9) angezeigt, wie in der folgenden Abbildung dargestellt. Dieser Wert stellt die Anzahl der Tage dar, die der VI aktiv war, bevor er in den Status „Geschlossen“ überging. In der folgenden Abbildung war dieser VI beispielsweise 9 Tage, 18 Stunden und 29 Minuten lang aktiv, aber im Datensatz „Geschlossen“ wird nur die Anzahl der Tage (9) angezeigt.




Wenn diese VI erneut geöffnet wird und der VI-Status wieder in „Offen“ übergeht, wird das Feld „Alter geschlossen“ auf 0 zurückgesetzt. Da die VI wieder aktiv ist, wird das Alter in Tagen/Stunden/Minuten in der Listenansicht im Alter angezeigt -Spalte und im Feld Alter der VIT.




## Entfernen von Zuweisungen von angreifbaren Elementen und Korrekturaufgaben

Sie können die Felder **Zugewiesen an** und **Zuweisungsgruppe** für angreifbare Elemente direkt aus den Datensätzen für angreifbare Elemente (VIT) und Korrekturaufgaben löschen,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von denen Sie feststellen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

## Übersicht

Ab **v16.5** können Korrekturbesitzer die Datensätze für die Neuzuweisung mit der Schaltfläche Zuweisung aufheben in den Anwendungen Vulnerability Response und Application Vulnerability Response aktualisieren.

## Anwendungsfall

Wenn Sie der Meinung sind, dass VIs nicht in Ihrem Bereich der Korrektur liegen, oder wenn Sie der Meinung sind, dass Ihnen oder Ihren Gruppen Datensätze fälschlicherweise zugewiesen wurden, sollten Sie sich oder Ihre Gruppen aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** für angreifbare Elemente entfernen Element- und Korrekturaufgabendatensätze.

## Heben Sie die Zuweisung des Moduls auf

Die **Schaltfläche Zuweisung** aufheben wird für die folgenden Datensätze in einem anderen Status als „Geschlossen“ oder „Gelöst“ angezeigt:

- Korrekturaufgaben (VULs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response Arbeitsbereichen. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, werden die Felder **Zugewiesen an** und **Zuweisungsgruppe** für alle zugehörigen VIs ebenfalls geleert.
- Angreifbare Elemente (VITs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response Arbeitsbereichen.
- Angreifbare Anwendungselemente (AVITs).

Alle Datensätze, die Sie entweder über die UI-Schaltfläche oder manuell aktualisieren, werden im Modul Nicht zugewiesen unter den entsprechenden Modulen angezeigt.

Informationen zum Neuzuweisen von Datensätzen mithilfe der UI-Aktion [ *`Unassigned`* finden Sie unter Entfernen Sie Zuweisungen von angreifbaren Elementen für sich oder Ihre Gruppen.

## Massenbearbeitung

Sie können die Zuweisungsfelder für mehrere AEs in einer Liste löschen. Nachdem Sie die VIs ausgewählt und **Massenbearbeitung**ausgewählt haben, aktivieren Sie im angezeigten Dialogfeld die **Checkbox** Zuweisung aufheben.

## Systemeigenschaft und Benachrichtigungen

Wenn Sie Administrator mit der Rolle „ **sn_vulc.vulnerability_admin** “ sind und auf Zuweisung aufheben für einen Datensatz klicken, löst die Systemeigenschaft *`sn_vul.unassign_vr.approval_required`* standardmäßig den Genehmigungs-Flow aus und erstellt einen Statusänderungsgenehmigungsdatensatz im Überprüfungsstatus, und die Genehmigungsanforderung wird für den Genehmiger ausgelöst wird in der Liste **„Meine Genehmigungen“** angezeigt.

**Hinweis:**
Als Schwachstellenadministrator können Sie die Systemeigenschaft *`sn_vul.unassign_vr.approval_required`* auf „ **false** “ setzen, um den Genehmigungsprozess zu deaktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn der Genehmiger die Anforderung genehmigt, löscht *sn_vul.default_assignment_group* die Felder **Zugewiesen an** und **Zuweisungsgruppe** und füllt das Feld **Zuweisungstyp** mit **Nicht zugewiesen**aus. Als Schwachstellenadministrator können Sie den Wert in der Systemeigenschaft *sn_vul.default_assignment_group* so ändern, dass die Zuweisungsfelder geleert und dann eine bestimmte Gruppe zugewiesen wird. Wenn ein Benutzer beispielsweise für einen Datensatz auf Zuweisung **aufheben** klickt und Sie ihn zur Überprüfung an eine bestimmte Gruppe umleiten möchten, können Sie im Wertfeld der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.

  **Hinweis:**
  Wenn Sie diesen Wert ändern, werden Benachrichtigungen für alle nicht zugewiesenen VIs, AVITs und CVITs an die von Ihnen angegebene Gruppe gesendet.

- Wenn der Genehmiger Ihre Anforderung ablehnt, wird der Grund für die Ablehnung auf der Registerkarte **Notizen** angezeigt.

Alternativ dazu, wenn *sn_vul.default_assignment_group* nicht für eine bestimmte Gruppe konfiguriert ist, werden Benutzer, die Sie der Benutzergruppe „Zuweisung aufheben“ hinzufügen, standardmäßig benachrichtigt, wenn die Zuweisung von Datensätzen aufgehoben wird. Die Systemeigenschaft *sn_vul.default_assignment_group* bestimmt die Benachrichtigungen an diese Gruppe.

Der Zuweisungstyp, entweder „ **Manuell**“, „ **Regel**“ oder „Nicht zugewiesen“, ist in den VI-Datensätzen und der **Listenansicht**verfügbar. Der **Zuweisungstyp Nicht zugewiesen** wird in Datensätzen angezeigt, nachdem die Felder **Zugewiesen an** und **Zuweisungsgruppe** durch die Systemeigenschaft der Funktion gelöscht wurden.

## Überwachen Ihrer Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche regelmäßige Aufgabe zählt die Datensätze, wenn sie in den Zuweisungstyp **Nicht zugewiesen** übergehen. Mit dieser Anzahl können Schwachstellenanalysten Zuweisungsregeln überwachen und anpassen, die aufgrund von Zuweisungsregeln mit einer höheren Anzahl nicht zugewiesener VIs möglicherweise keine gute Leistung erbringen.

Die geplante Aufgabe *Reassignment count for assignment rules* wird täglich ausgeführt und bucht die Gesamtzahl der VIs, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen wurden.

Die von dieser Aufgabe erfassten Anzahlen gelten für die angreifbaren Elemente und die eindeutigen Zuweisungsregeln für Vulnerability Response und Application Vulnerability Response. Die Anzahl wird nach Zuweisungsregel in jeder Zuweisungsregelliste für jedes Modul angezeigt.

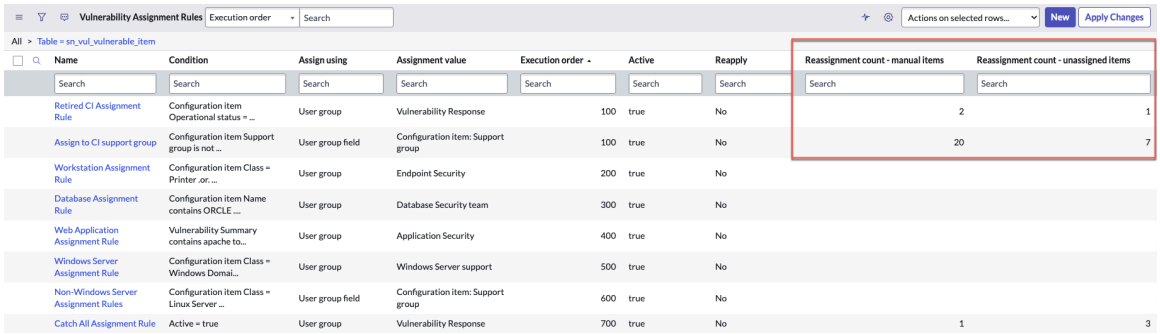
Die Aufgabe zählt auch alle Datensätze, die manuell nicht zugewiesen sind. Sowohl die manuellen Anzahlen als auch die von dieser Funktion erfassten Anzahlen werden in der Liste „Schwachstellenzuweisungsregeln“ in zwei Spalten veröffentlicht: *Reassignment count - manual items* und *Reassignment count - unassigned items*.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Um diese Anzahl anzuzeigen, navigieren Sie als Schwachstellenadministrator zu **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Klicken Sie oben rechts in der Liste auf das Zahnradsymbol, und wählen Sie *Reassignment count - manual items*und *Reassignment count - unassigned items* zur Anzeige aus.
3. Jeder VI, der ursprünglich durch eine Regel zugewiesen wurde, aber anschließend automatisch oder manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel in der Listenansicht.

Das folgende Beispiel zeigt die Anzahl der Neuzuweisungen für zwei Zuweisungsregeln.




| Name | Condition | Assign using | Assignment value | Execution order | Active | Reapply | Reassignment count - manual items | Reassignment count - unassigned items |
|---|---|---|---|---|---|---|---|---|
| Retired CI Assignment Rule | Configuration item Operational status = ... | User group | Vulnerability Response | 100 | true | No | 2 | 1 |
| Assign to CI support group | Configuration item Support group is not ... | User group field | Configuration item: Support group | 100 | true | No | 20 | 7 |
| Workstation Assignment Rule | Configuration item Class = Printer .or. ... | User group | Endpoint Security | 200 | true | No | | |
| Database Assignment Rule | Configuration item Name contains ORCLE .... | User group | Database Security team | 300 | true | No | | |
| Web Application Assignment Rule | Vulnerability Summary contains apache to... | User group | Application Security | 400 | true | No | | |
| Windows Server Assignment Rule | Configuration item Class = Windows Domai... | User group | Windows Server support | 500 | true | No | | |
| Non-Windows Server Assignment Rules | Configuration item Class = Linux Server ... | User group field | Configuration item: Support group | 600 | true | No | | |
| Catch All Assignment Rule | Active = true | User group | Vulnerability Response | 700 | true | No | 1 | 3 |

## Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln

Schwachstellenrechner automatisieren die Berechnung der Anfangswerte für die Felder in angreifbaren Elementen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

### Sicherheitsrisiko-Rechner

Das Vulnerability Response Basissystem enthält zwei Schwachstellenrechner, die die Basis-**Risikopunktzahl** für das angreifbare Element festlegen.

- **Standardrisikorechner**
- **Schwachstellenschweregrad**

Schwachstellenrechner können erstellt werden, um die Auswirkungen angreifbarer Elemente basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle, die Klasse des Konfigurationselements (CI) oder das Alter des angreifbaren Elements handelt, können Sie zusätzliche Schwachstellenrechner erstellen, um andere Felder für angreifbare Elemente festzulegen. Oder Sie können die vorhandenen Schwachstellenrechner anpassen. Ein Rechner kann so geschrieben werden, dass er einen beliebigen Satz von Prioritäten widerspiegelt. Weitere Informationen finden Sie unter Erstellen Sie einen Vulnerability Response -Rechner und Filtern innerhalb Vulnerability Response.

Darüber hinaus können Sie Attribute in „configuration_item“ [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um die Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass CIs, die in Ihrer Organisation nach außen gerichtet sind, angreifbarer sind und möglicherweise eine sofortige Korrektur erfordern, können Sie diesen CIs Attribute wie *Internet Facing* zuweisen. Dieses und andere Attribut sind in den Versionshinweisen zu Common Service Data Model für das Familien-Release Orlando aufgeführt. Aktuelle Informationen und Anleitungen zu CMDBfinden Sie in den folgenden Themen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Common Service Data Model konzeptionelles Modell
- CMDB-Schemamodell

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Der **Schwachstellenschweregrad-** Rechner berechnet die **Risikopunktzahl** für angreifbare Elemente anhand des normalisierten Schwachstellenschweregrads.

**Hinweis:**
Pro Zielfeld (**Risikopunktzahl**) kann jeweils nur ein Rechner aktiv sein. **Schwachstellenschweregrad** ist standardmäßig deaktiviert.

Alle aktivierten Schwachstellenrechner legen die ausgewählten Felder jedes Mal fest, wenn ein angreifbares Element erstellt wird, wenn sich ein zugeordnetes CI oder eine Schwachstelle ändert oder wenn der zugehörige Link **Risikopunktzahl berechnen** in einem angreifbaren Element verwendet wird. Beispiel: Die Risikopunktzahl wird in Datensätzen für angreifbare Elemente automatisch aktualisiert, wenn der Schweregradwert für eine importierte Schwachstelle aktualisiert wird. Nachdem ein Schwachstellenimport eine Schwachstellenpunktzahl aktualisiert hat, wird die Kennzeichnung für die Neuberechnung für diese Schwachstelle aktiviert. Die Risikopunktzahlen für die angreifbaren Elemente, bei denen die Kennzeichnung „Neu berechnen“ für diese Schwachstelle aktiviert (wahr) ist, werden neu berechnet.

Wenn Sie in einem vorhandenen angreifbaren Element auf den zugehörigen Link **Risikopunktzahl** berechnen klicken und einer der Rechner aktiviert ist, wird das Feld **Risikopunktzahl** im angreifbaren Element aktualisiert.

**Hinweis:**
Der zugehörige Link **Risikopunktzahl** berechnen ist nur sichtbar, wenn mindestens ein Schwachstellenrechner aktiviert ist.

## Regeln zum Schwachstellenrechner

Der **Standardrisikorechner** des Basissystems enthält die **Standardrisikoregel**, eine spezialisierte Schwachstellenrechnerregel, die als **Risikoregel**bezeichnet wird. Sie berechnet die **Risikopunktzahl** basierend auf mehreren Werten:

- Schwachstellenschweregrad
- Exploit-Informationen
- Relevanz
- Externe Gefährdung des CI mit der Schwachstelle
- EPSS-Punktzahlen

Sie können die in der **Standardrisikoregel** zu verwendenden Werte anpassen und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis- **Risikopunktzahl**zählt.

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel dafür, wie Risikopunktzahlen für Risikoregelrechner bestimmt werden, finden Sie unter Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response.

Zuweisen eines Gewichtungsprozentsatzes

Sie können auch einen Gewichtungsprozentsatz (0-100) auf Feldwertebene zuweisen, z. B. können Sie jeder Schweregradebene (Keine bis Kritisch) einen Gewichtungsprozentsatz zuweisen.

Wenn die Schweregradgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für den Schweregrad zugewiesen werden:

| Schwachstellenschweregrad | Risikopunktzahl |
|---|---|
| Kritisch | 100 |
| Hoch | 50 |
| Mittel | 20 |
| Keine | 0 |

Wenn der Schweregrad „Kritisch“ ist, beträgt die entsprechende Gewichtung 50. Bei einem hohen Schweregrad beträgt die entsprechende Gewichtung 25, bei einem mittleren Schweregrad beträgt die entsprechende Gewichtung 10. Wenn der Schweregrad Keine lautet, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie unter Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response.

Einstellungen für Schwachstellenrechner-Regeln

Jede Regel hat eine Einstellung für **Reihenfolge**. Die erste Übereinstimmung mit den Bedingungen aktualisiert jedoch das Feld **Risikopunktzahl** im angreifbaren Element. Weitere Informationen zu Regeleinstellungen für Schwachstellenrechner finden Sie unter Erstellen Sie einen Vulnerability Response -Rechner. Nicht geskriptete Rechnerregeln haben in der Regel weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

Der Basissystem- **Schwachstellenschweregradrechner** enthält Rechnerregeln, die jeder Schweregradstufe (Keine bis Kritisch) basierend auf dem Schweregrad einen Wert (0 bis 100) für die **Risikopunktzahl** zuweisen. Dem**Schweregrad „Unbekannt“** wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, und wie **beim Standardrisikorechner**können neue Rechnerregeln oder neue Risikoregeln erstellt werden.

## Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen werden eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Exploit-Informationen usw. zugewiesen. Die Geschäftsregel `Update Risk Rating from Risk Score` in der Tabelle „Angreifbares Element“ ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert war.

| Wert (Risikobewertung) | Gewichtung (Risikopunktzahl) |
|---|---|
| 1 | 90–100 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wert (Risikobewertung) | Gewichtung (Risikopunktzahl) |
|---|---|
| 2 | 70–89 |
| 3 | 40–69 |
| 4 | 1–39 |
| 5 | 0 |

Ab Version 18.0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als vr_risk_rating bereitgestellt. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wurde so geändert, dass Sie die Einträge in den Werten der Tabelle „Risikopunktzahlgewichtungen“ für die Risikobewertungsberechnung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Gewichtungen der Risikopunktzahl“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (CI) von „Nicht mit Internetzugriff“ in „Mit Internetzugriff“ ändert.
- Wenn die zugeordneten Common Vulnerabilities and Exposures (CVEs) oder Drittanbietereinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer CVE Known Exploit Vulnerability (KEV) verknüpft sind

## Integration von Tenable Vulnerability und die Tenable-Risikoregel

Die Tenable-Risikoregel ist mit Tenable Vulnerability Integrationverfügbar. Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable Risk-Regel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten.

## Vulnerability Response Erkennung angreifbarer Elemente aus Drittanbieterintegrationen

Zeigen Sie alle Informationen an, die von Drittanbieter-Scans in Ihrer Now Platform® -Instanz erfasst werden. Zeigen Sie die zurückgegebenen Ergebnisse der Scans bei Erkennung und Datensätze für angreifbare Elemente (VI) in Ihrer Instanz an, während diese Ergebnisse auf den Scannern angezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Übersicht

Die Anwendung Vulnerability Response unterstützt Integrationen von Drittparteien, die Daten zu angreifbaren Elementen aus Ihrer Unternehmensumgebung abrufen. Detaillierte Daten zu Erkennungen, also einzelne, eindeutige Vorkommen von Schwachstellen, die von den Scannern Ihrer Drittanbieterintegrationen gemeldet werden, werden importiert und sowohl im Erkennungs- als auch im Datensatz für angreifbare Elemente in Ihrer Now Platform-Instanz angezeigt.

Drittanbieter-Integrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden. Erkennungsdaten werden mit angreifbaren Elementen kombiniert, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn keine VI gefunden wird, wird eine neue erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

In früheren Versionen von Vulnerability Responsehat die Beziehung zwischen einem CI (Asset) in Ihrer Umgebung und einer importierten Schwachstelle von einem Drittanbieter-Scanner durch Erkennung angreifbarer Elemente ein eindeutiges angreifbares Element in Ihrer Now Platform-Instanz erstellt.

Die Granularität der ursprünglichen vom Scanner bereitgestellten Daten bleibt erhalten. Bei Erkennungen werden die Erkennungsdaten mit angreifbaren Elementen kombiniert. Wenn während einer Erfassung kein angreifbares Element gefunden wird, wird eine neue AEs erstellt.

Ab Version 21.0 von Vulnerability Responsewird die Systemeigenschaft *sn_vul.show_last_open_detection* im Basissystem bereitgestellt. Standardmäßig ist der Wert dieser Eigenschaft auf „false“ festgelegt, und das aktuelle Verhalten der Zusammenfassung der Werte von der ersten Erkennung bis zum VI bleibt unverändert. Wenn sie jedoch auf „true“ festgelegt ist, wird ein AEs automatisch mit der letzten offenen Erkennung nach einer Erfassung aktualisiert. Die Felder wie IP-Adresse, SSL, Port, Protokoll, NetBIOS und Nachweis werden für die VI-Erkennungen aktualisiert. Bei Bedarf können Sie die Erkennungsfelder anpassen, die aktualisiert werden sollen, indem Sie das DetectionBase -Skript ändern.

Um die Werte für die letzte offene Erkennung anzuzeigen, navigieren Sie in der VI-Formularansicht zur Registerkarte **Letzte offene Erkennung**. Um alle im vergangenen Jahr geöffneten AEs mit den letzten offenen Erkennungswerten zu aktualisieren, können Sie die regelmäßige Aufgabe *Update Last Open Detection Value To VITs* bei Bedarf ausführen. Diese regelmäßige Aufgabe wird auch im Basissystem bereitgestellt.

**Hinweis:**
Wenn sich ein Configuration Item (CI) für ein erkanntes Element ändert, werden die entsprechenden Updates auch in den Erkennungen angezeigt. Daher können die Erkennungen von einem VI in einen anderen verschoben werden. Basierend auf dieser Änderung und dem Wert der Eigenschaft *sn_vul.show_last_open_detection* wird für die Werte der Erkennungen ein Rollup zu den Quell- und Ziel-VIs durchgeführt.

## Unterstützte Versionen von Vulnerability Response

Weitere Informationen zum Installieren oder Aktualisieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Unterstützte Integrationen von Drittparteien

Für die Erkennung angreifbarer Elemente ist eine unterstützte Drittanbieterintegration mit Ihrer Anwendung Vulnerability Response erforderlich. Die folgenden Drittanbieterintegrationen werden von der Anwendung Vulnerability Response für Erkennungen angreifbarer Elemente unterstützt:

- Integration der Qualys-Hosterkennung
- Rapid7-Data Warehouse:
  - Integration von angreifbaren Elementen
  - Integration der Lösung angreifbarer Elemente
- Rapid7 Integration von angreifbaren Elementen (InsightVM)
  - Insight VM-Integration
  - Integration von angreifbaren Elementen – API
- Tenable Vulnerability Integration
- Microsoft Defender Threat and Vulnerability Management

Diese Drittanbieterintegrationen sind mit einem separaten Abonnement aus dem ServiceNow Storeverfügbar. Weitere Informationen zu diesen Integrationen finden Sie unter Vulnerability Response-Integrationen und Security Operations und ServiceNow Store, um Berechtigungen zu erhalten.

Informationen zum Überprüfen, ob Ihr Drittanbieter-Scanner für den Import konfiguriert ist, finden Sie unter Installieren und Konfigurieren der Anwendung Rapid7 Integration for Security Operations und Qualys Vulnerability Integration installieren.

## Wichtige Begriffe für Erkennungen angreifbarer Elemente

**Schwachstelle**

Daten über Schwachstellen in Software, Betriebssystemen und Assets, die aus internen und externen Quellen importiert werden. Diese Daten werden importiert und mit vorhandenen Assets (Konfigurationselemente, CIs) verglichen, die in der CMDB aufgeführt sind.

**Angreifbares Element**

Ein angreifbares Element wird erstellt oder aktualisiert, wenn eine importierte Schwachstelle mit einem CI in der CMDB übereinstimmt.

**Erkennung**

Ein einzelnes, eindeutiges Vorkommen einer Schwachstelle, wie von einem Scanner gemeldet, der in der Now Platform -Umgebung als Erkennung angreifbarer Elemente bezeichnet wird. Eine Erkennung enthält angereicherte Daten zu einer Schwachstelle und den entsprechenden angreifbaren Elementen. Diese Daten werden im Erkennungsdatensatz (VID#) und in der Listenansicht der angreifbaren Elemente angezeigt, die die folgenden Details enthält:

- Zuerst gefunden (Daten)
- Zuletzt gefunden (Datum)
- DNS-Name
- NET-BIOS-Name
- IP-Adresse
- Port



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Protokoll
- Nachweis
- SSL
- Anzahl Ermittlungen

**Hinweis:**
Das Hinzufügen einer Geschäftsregel zur Erkennungstabelle wirkt sich auf die Leistung der Erfassung aus.

**Erkennungsschlüssel**

Eine Hash-Kombination von Feldern, die eine Möglichkeit bietet, eine Erkennung zu identifizieren und an ein angreifbares Element zu binden. Erkennungsschlüssel sind integrationsspezifisch.

**Erkennungsschlüsselkonfigurationen**

| Scanner | Schwachste | Port | Protokoll | Asset-ID | Nachweis | NIC |
|---|---|---|---|---|---|---|
| Qualys-IDs | Ja | Ja | Ja | Ja | Nein | NA |
| Tenable | Ja | Ja | Ja | Ja | Nein | NA |
| Rapid7 | Ja | Ja | Ja | Ja | Ja (Groß-/ Kleinschreibung wird nicht beachtet) | Ja |

**Hinweis:**

- Wenn der Erkennungsschlüssel nicht angegeben ist oder für Versionen vor Vulnerability Response 14.0, ist der Erkennungsschlüssel eine Kombination aus Schwachstelleneintrag, Port, Protokoll, Asset-ID und Nachweis.
- Ab v19.0 von Vulnerability Responsewird eine neue Erkennungsschlüssel-NIC für Rapid7 InsightVMhinzugefügt, die standardmäßig aktiviert ist. Vorhandene Erkennungen ohne NIC werden mit der ersten eingehenden NIC in der Nutzlast von Rapid7aktualisiert. Der Erkennungsschlüssel wird bei der Erkennung einschließlich der NIC neu berechnet und ausgefüllt. Neue Erkennungen werden erstellt, wenn ähnliche Erkennungen mit unterschiedlichen NIC-Werten erkannt werden. Für diese Daten wird kein Rollup in der Tabelle „Angreifbares Element“ durchgeführt. Der NIC-Wert wird in einer neuen Spalte in der Tabelle „sn_vul_detection_key_config“ und „sn_vul_detection“ gespeichert.

**De dup**

Der von der Anwendung Vulnerability Response verwendete Prozess zum Reduzieren einzelner Erkennungen in einen einzigen VI, wenn die Daten bestimmte hartcodierte Kriterien erfüllen.

**Externe VI-ID**

Der im Feld Externe ID der VI-Tabelle gespeicherte Wert. Dieser Wert ist ein Hash, der sich aus der Kombination von Schlüsseln innerhalb eines VI zusammensetzt und darstellt, was ihn in der Anwendung eindeutig macht. Sie besteht aus einem CI und einem angreifbaren Eintrag.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Öffnen Sie aufgelöste angreifbare Elemente erneut

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf **Gelöst** gesetzt wurden, aber nicht durch die nachfolgenden Integrationsläufe auf **Geschlossen/** Behoben gesetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Geschlossene **AEs** mit dem **Substatus** „Korrigiert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die AEs mit der neuen Schwachstelle abgeglichen werden können.

Gemäß Skripteinbindung `DetectionBase`, Methode `_shouldReOpenVI()`wird die VIT, wenn sie zuvor mit dem **Substatus** „ **Fixed**“, „ **Stale**“ oder „ **CI Decommissioned**“ (CI außer Betrieb genommen) geschlossen wurde, erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Angenommen, das Abschlussdatum einer VIT liegt nach dem Datum „last_found“ einer Erkennung. Sie würden erwarten, dass diese VIT-Datensätze geschlossen bleiben. Wenn jedoch eine zuvor geschlossene VIT erneut geöffnet wird, bedeutet dies, dass die VIT durch eine frühere Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die der geschlossenen VIT entspricht, die dieselbe Schwachstelle im Konfigurationselement der VIT aufweist, wird die VIT erneut geöffnet.

Für Erkennungen von Rapid7 ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um aufgelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden AEs, die auf **„Gelöst** “ gesetzt sind, aber dann nicht durch nachfolgende Scans in „ **Geschlossen/Korrigiert** “ geändert wurden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder in „ **Offen** “ zurückgesetzt.

Wenn der Scanner bei Erkennungen von Qualys weiterhin AEs findet, die auf „ **Gelöst** “ gesetzt wurden, dann aber durch nachfolgende Scans nicht in „ **Geschlossen”/** „Korrigiert“ geändert wurden, werden diese AEs zurück in den Status „ **Offen** “ verschoben, wenn das Datum des letzten Funds nach dem Datum „Gelöst“ liegt.

## Zeigen Sie Erkennungsdaten an

Sie zeigen die Daten, die aus Erkennungen angreifbarer Elemente importiert wurden, im VI-Datensatz an. Weitere Informationen finden Sie unter Zeigen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente an und Überprüfen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente in Datensätzen der Integrationsausführung (VINTRUN)..

## Vulnerability Solution Management

Korrelieren Sie die Schwachstellen in Ihrer Umgebung automatisch mit den Lösungen, die sie beheben könnten. Identifizieren Sie die Korrekturmaßnahmen, die für Ihre Schwachstellen gelten, und priorisieren Sie sie nach der größten Reduzierung des Schwachstellenrisikos.

## Vulnerability Solution Management

Sicherheits- und IT-Teams wenden häufig viel Zeit auf, um Schwachstellenfunde zu untersuchen, um die effektivsten Behandlungen für ihre Umgebung zu identifizieren. Angesichts des Umfangs und der Komplexität von Schwachstellen in großen Organisationen ist die Übersetzung von Schwachstellenergebnissen in Korrekturaufgaben ein manueller, langwieriger und fehleranfälliger Prozess.

Mit Vulnerability Solution Managementkönnen Sie Ihre Schwachstellenergebnisse automatisch mit den Lösungen korrelieren, die sie beheben. Identifizieren Sie die Softwarepatches,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsupdates und andere Steuerungen, die ohne manuellen Overhead die größten Auswirkungen auf Ihre Organisation haben.

## Vulnerability Solution Management-Anforderungen

Vulnerability Solution Management ist eine Funktion, die in der Anwendung Vulnerability Response verfügbar ist. Vulnerability Solution Management erfordert ein separates Abonnement.

Weitere Informationen zum Abrufen von Berechtigungen für Anwendungen aus ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab. Unter Anwendung Solution Management for Vulnerability Response installieren finden Sie weitere Informationen zur Installation der Anwendung, nachdem Sie sie auf Ihre Instanz heruntergeladen haben.

Nach der Installation bietet Ihnen Vulnerability Solution Management Zugriff auf die Lösungsdaten Microsoft Security Response Center und Red Hat aus Vulnerability Response.

**Hinweis:**

Sie können beide Lösungsanwendungen im Setup-Assistenten konfigurieren. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

Integration der Microsoft Security Response Center-Lösung verstehen Weitere Informationen zu den importierten Lösungen finden Sie unter und Red Hat Solution Integration verstehen.

## Verfügbare Versionen

Stellen Sie für die aktuelle Version von Vulnerability Solution Managementsicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

| Release-Version von Vulnerability Solution Management | Kompatible Versionen von Vulnerability Response | Releasehinweise |
|---|---|---|
| Vulnerability Solution Management v10.3 | Vulnerability Response v18.0 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Lösungen und Ersatz verstehen

Ein abgelöstes Update ist ein vollständiger Ersatz für einen oder mehrere vorherige Releases. Beispielsweise kann ein Hotfix-Update durch ein Service Pack ersetzt werden. Lösungen beziehen sich auf Schwachstellen. Lösungen können sich auch auf andere Lösungen in einer Ersetzungskette beziehen. Lösungen beheben auch Schwachstellen in vorherigen Lösungen, da sie kumulativ sind. Vulnerability Solution Management ordnet Schwachstellen aus vorherigen Lösungen automatisch Ersatzlösungen zu. Wenn eine ältere Schwachstelle gefunden wird, kann sie von einer höheren Ersatzlösung behoben werden. Die höchste Ersatzlösung wird jedoch bevorzugt, da sie am kumulativsten ist.

## Potenzielle und bevorzugte Lösungen

Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben häufig viele mögliche Lösungen. Eine bevorzugte Lösung ist die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einzelne Lösung, die auf die Korrektur einer Schwachstelle oder eines angreifbaren Elements (AE) abzielt. Sie kommuniziert die Absicht und ermöglicht detailliertere Bereitstellungsmetriken.

## Bevorzugte Lösungen

Vulnerability Solution Management legt automatisch die effektivste Lösung (**Bevorzugte Lösung**) für die erkannte Schwachstelle basierend auf der höchsten Ersatzlösung fest, wenn nur eine Lösung mit der höchsten Ersatzlösung vorhanden ist. Wenn für die Schwachstelle mehr als eine höchste Ersetzung vorhanden ist, wird kein Wert festgelegt. In Vulnerability Responseist eine **bevorzugte Lösung** die Lösung Microsoft Security Response Center oder Red Hat mit der höchsten Ersatzlösung, die aus den mit der Schwachstelle verknüpften Lösungen abgeleitet wird.

Werte für „**Bevorzugte Lösung** “ können für das angreifbare Element oder die Schwachstelle festgelegt werden. Wenn diese Option direkt für die Schwachstelle festgelegt wird, erben alle angreifbaren Elemente, die der Schwachstelle zugeordnet sind, diese Lösung. Ändern Sie die Werte für **Bevorzugte Lösung** für mehrere angreifbare Elemente mithilfe der Massenbearbeitungsfunktion. Bei der Massenbearbeitung wird nur die **bevorzugte Lösung** für das angreifbare Element aktualisiert, da durch das Festlegen der **bevorzugten Lösung** auf der Ebene des Schwachstelleneintrags die **bevorzugte Lösung** für alle neuen AEs festgelegt wird. Die Massenbearbeitung gilt nur für aktuell angreifbare Elemente.

**Hinweis:**
Wenn für eine Schwachstelle mehrere Ersatzlösungen mit der höchsten Priorität vorhanden sind, werden die Werte für „ **Bevorzugte Lösung** “ auf der Schwachstellenebene gelöscht, da diese Lösung vom betroffenen Asset abhängt. Wenn für eine Schwachstelle mehrere Lösungen mit der höchsten Ersatzlösung vorhanden sind, legen Sie eine **bevorzugte Lösung** für das angreifbare Element fest. Sie können mithilfe der **Suchliste** im Formular „ **Angreifbares** Element“ eine andere Lösung festlegen.

Alle bevorzugten Lösungen für die angreifbaren Elemente in einer Korrekturaufgabe befinden sich in einer zugehörigen Liste im Datensatz der **Korrekturaufgabe**.

Nicht alle Lösungsimporte führen zu vollständigen Datenaktualisierungen. Der Ersetzungsprozess wird aktualisiert, wenn:

- Ein angreifbares Element wird erstellt.
- Daten haben sich auf einem aktiven AEs geändert.
- Eine neue Zuordnung wird für einen Drittanbietereintrag mit dem CVE erstellt.
- Neue Lösungsdaten wurden seit dem letzten Import veröffentlicht, eine vorhandene Lösung wird aktualisiert oder mit einer manuellen Änderung, die sich auf die Lösungsmetriken auswirkt..

## Was Vulnerability Solution Management tut

- Ordnet neue angreifbare Elemente und Korrekturaufgaben während des Integration der Microsoft Security Response Center-Lösung Imports von und Red Hat Solution Integration automatisch Lösungen zu.

  MSRC -Lösungen sind dem neuesten Bulletin zugeordnet, in dem die Lösung angezeigt wird.

- Ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellendatensätze manuell Lösungen zugeordnet werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf Schwachstellenebene aktualisiert.

- MSRC: Erstellt während des Imports Ersetzungsketten, die Sie in der zugehörigen Liste der Lösung anzeigen können.
- Gibt an, ob eine Lösung die höchste Ersatzlösung ist oder nicht.
- Listet die Lösungsrisikopunktzahl auf, die jeder Lösung zugeordnet ist, um Ihnen die größten Möglichkeiten zur **Risikominderung** zu bieten.

- **Behält den Korrekturstatus** für Lösungen in Datensätzen zu Schwachstelleneinträgen, **Korrekturaufgaben**und **Schwachstellenlösungen**von **Drittanbietern bei**, damit Sie den Korrekturfortschritt nachverfolgen können.

  Sie enthält:

  - Anzahl der angreifbaren Elemente nach behobenem Prozentsatz für AEs mit bevorzugten Lösungen, mit und ohne AEs im Status „Zurückgestellt“.
  - Configuration Item (CI) zählt nach Prozentsatz der Korrektur für die AEs mit bevorzugten Lösungen, mit und ohne AEs im Status „Zurückgestellt“.
  - Anzahl der angreifbaren Elemente nach behobenem Prozentsatz für die AEs mit potenziellen Lösungen, mit und ohne AEs im Status „Zurückgestellt“.
  - Konfigurationselement zählt nach Prozent korrigiert, für die AEs mit bevorzugten Lösungen, mit und ohne AEs im Status „Zurückgestellt“.

## Was Sie mit tun können Vulnerability Solution Management

- Erstellen, aktualisieren, anzeigen oder löschen Sie Lösungen, die Schwachstellen zugeordnet sind, damit Sie Schwachstellenlösungen nachverfolgen können, die nicht durch Lösungsinhalte von Drittanbietern abgedeckt werden. Die Lösungsintegration mit Rapid7 Data Warehouse wird derzeit nicht unterstützt.
- Verknüpfen Sie Schwachstellen von Drittparteien und NVD-Einträge mit einem Lösungsdatensatz.
- Entfernen Sie angreifbare Elemente und Korrekturaufgaben, und ordnen Sie sie einer Lösung neu zu.
- Zeigen Sie die **bevorzugte Lösung** für eine bestimmte Schwachstelle in den Formularen für Schwachstellen und angreifbare Elemente an.
- Zeigen Sie eine zugehörige Liste „ **Bevorzugte Lösungen** “ in Formularen für Korrekturaufgaben an, in der alle Lösungen aufgeführt sind, die von mindestens einem aktiven VI in dieser Gruppe bevorzugt wurden.
- Zeigen Sie die Details zum **Korrekturstatus** für eine Lösung an, die die Risikominderung anzeigen, die mit der Bereitstellung der **bevorzugten Lösung** für Schwachstellen, angreifbare Elemente, Korrekturaufgaben und Lösungsformulare verbunden ist.
- Zeigen Sie im Lösungsformular Schwachstellen an, die für eine bestimmte Lösung gelten.
- MSRC: Zeigen Sie die Ersatzlösungen für eine bestimmte Lösung für eine Schwachstelle an, um das neueste Update zur Bereitstellung oder ein früheres, fokussierteres und effizienteres Update zu finden.
- Zeigen Sie Listen von Lösungen an, die nach verschiedenen Merkmalen sortiert sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle: Lösungen sortiert nach Veröffentlichungsdatum und Nummer.
- MSRC: Höchste Ersetzung: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzlösung**, **Veröffentlichungsdatum**und **Nummer**.
- Mit angreifbaren Elementen: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzlösung** oder **Bevorzugt**, **Risikopunktzahl**und **Nummer**. Wenn bereitgestellt, bieten die obersten Einträge in der Liste die größte Risikominderung für die Assets in Ihrer Umgebung.

### Lösungsdatensatz Risikopunktzahl und Risikobewertung

**Hinweis:**
Die **Risikopunktzahl** und die **Risikobewertung** des Lösungsdatensatzes unterscheiden sich von den Feldern, die für Schwachstellen, angreifbare Elemente und Korrekturaufgaben verwendet werden.

Die Risikopunktzahl des **Lösungsdatensatzes** ist eine gewichtete Berechnung, die auf der Risikopunktzahl des **angreifbaren** Elements und der Anzahl aktiver angreifbarer Elemente mit dieser Lösung als **potenzielle Lösung**basiert. Die Lösungsrisikopunktzahl bietet eine Schätzung der **Risikoreduzierung**, die durch die Lösung erwartet wird.

Die Risikopunktzahl des **Lösungsdatensatzes** wird wie folgt berechnet:

- Es beginnt mit 85 % der höchsten oder maximalen **Risikopunktzahl** eines aktiven angreifbaren Elements mit dieser potenziellen Lösung.
- **Die** Risikopunktzahl des Lösungsdatensatzes tabelliert dann die Gesamtzahl der angreifbaren Elemente mit dieser potenziellen Lösung. Für jeden Bereich der Anzahl angreifbarer Elemente werden einige Punkte hinzugefügt, und es wird eine Gesamtsumme ermittelt.
  - 0–09 angreifbare Elemente fügen keine Punkte hinzu
  - 10–99 angreifbare Elemente fügen 5 Punkte hinzu
  - 100–999 angreifbare Elemente fügen 10 Punkte hinzu
  - 1000 und mehr angreifbare Elemente fügen 15 Punkte hinzu

  Beispiel: Für eine **Risikopunktzahl** des angreifbaren Elements von 80 beginnt die Risikopunktzahl des **Lösungsdatensatzes** bei 68. Wenn es insgesamt 200 aktive angreifbare Elemente mit dieser potenziellen Lösung gäbe, wäre die endgültige **Punktzahl** für das Lösungsrisiko 78.

Die **Risikobewertung** des Lösungsdatensatzes unterteilt die **Risikopunktzahl** des Lösungsdatensatzes in Bereiche von Kritisch bis Keine. **Die Risikobewertung** der Lösung bewertet die Risikominderung für die angreifbaren Elemente, die diese Lösung korrigiert.

Bis VR v16.1 wurde die resultierende Lösungsrisikopunktzahl durch **Risikobewertungen** in die folgenden Bereiche unterteilt:

- 1 – Kritisch (90+ **Lösungsrisikopunktzahl**)
- 2 – Hoch (70–89 Risikopunktzahl des **Lösungsdatensatzes**)
- 3 – Mittel ( **30–69**Risikopunktzahl des Lösungsdatensatzes)
- 4 – Niedrig (1–29 Risikopunktzahl des **Lösungsdatensatzes**)
- 5 – Keine (0 Lösungsdatensatz – **Risikopunktzahl**)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab VR v16.1 wird die resultierende Lösungsrisikopunktzahl durch **Risikobewertungen** in die folgenden Bereiche für Solution Management unterteilt:

- 1 – Kritisch (90+ **Lösungsrisikopunktzahl**)
- 2 – Hoch (70–89 Risikopunktzahl des **Lösungsdatensatzes**)
- 3 – Mittel ( **40–69**Risikopunktzahl des Lösungsdatensatzes)
- 4 – Niedrig (1–39 Risikopunktzahl des **Lösungsdatensatzes**)
- 5 – Keine (0 Lösungsdatensatz – **Risikopunktzahl**)

## Anwendungsfälle

Zeigen Sie den Statusbereitstellungsfortschritt eines aktuellen Patch-Zyklus mit dem höchsten Ersatzmodul an, sortiert nach Datum.

Zeigen Sie Lösungen mit dem höchsten Wert mit dem Modul „Mit angreifbaren Elementen“ an, sortiert nach Risikopunktzahl.

Lösungslisten kommunizieren wichtige Lösungsdetails, Risikopunktzahlen und Bereitstellungsmetriken. Verwenden Sie die Risikopunktzahl und die Anzahl aktiver **AEs** für die Priorisierung. Sehen Sie, welche Lösungen im aktuellen Patch-Zyklus nicht vorankommen, möglicherweise ein Hinweis auf eine verpasste Bereitstellungsvoraussetzung.

**Hinweis:**
Fügen Sie **%VIs remediated(percent_nd_pref_vis_remediated)** aus dem Menü „Listenspalten **personalisieren** “ für den Korrekturfortschritt im Formular „Lösungen für Schwachstellen“ hinzu.

### Integration der Microsoft Security Response Center-Lösung verstehen

Überprüfen und implementieren Sie vorgeschlagene Korrekturlösungen, die von Integration der Microsoft Security Response Center-Lösungbereitgestellt werden.

Integration der Microsoft Security Response Center-Lösung ist in der Funktion Vulnerability Solution Management von Vulnerability Responseenthalten, die über ein separates Abonnement verfügbar ist. Weitere Informationen dazu, wie Vulnerability Solution ManagementVulnerability Response Lösungen integriert, finden Sie unter [].

Microsoft Security Response Center untersucht Berichte über Sicherheitsschwachstellen, die sich auf Microsoft-Produkte und -Services auswirken, und stellt Lösungsinformationen bereit, die bei der Verwaltung von Sicherheitsrisiken helfen. Lösungen sind bekannte Fehlerkorrekturen, die aus dem Produkt Microsoft Security Response Center ] in Ihr Integration der Microsoft Security Response Center-Lösung importiert werden.

Integration der Microsoft Security Response Center-Lösung enthält Einstiegspunkte für das Produkt Microsoft Security Response Center, die als regelmäßige Aufgaben aufgerufen werden. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Geplante Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verfügbare Versionen

Stellen Sie für die aktuelle Version von Vulnerability Solution Management - und Microsoft Security Response Center -Lösungen sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

Weitere Informationen zur Installation und Konfiguration von Vulnerability Solution Management und Lösungsintegrationen finden Sie unter Anwendung Solution Management for Vulnerability Response installieren und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

| Release-Version von Vulnerability Response | Version von Vulnerability Solution Management | Releasehinweise |
|---|---|---|
| Vulnerability Response v15.0 | v10.3 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Rollen

Integration der Microsoft Security Response Center-Lösung -Aufgaben umfassen die folgenden Rollen.

- sn_vul.vulnerability_admin oder sn_vul.admin (veraltet): Kann Datensätze lesen, schreiben und löschen.
- sn_vul.vulnerability_write: Kann Datensätze lesen und schreiben.
- sn_vul.vulnerability.read: Kann Datensätze lesen.
- sn_vul.remediation_owner: Kann interne Notizen zu Datensätzen lesen und schreiben, die der Korrekturspezialistengruppe oder Einzelperson zugewiesen sind. (In der itil-Rolle enthalten.)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Integration der Microsoft Security Response Center-Lösung

Um Integration der Microsoft Security Response Center-Lösunganzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.

Die folgende Integration ist im Basissystem enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Integration der Microsoft Security Response Center-Lösung**

| Integration | Beschreibung |
|---|---|
| Integration der Microsoft Security Response Center-Lösung | Ruft Lösungen und die Zuordnung der National Vulnerability Database (NVD) ab, um Lösungen mit Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zu verknüpfen.<br>**Hinweis:** Integration der Microsoft Security Response Center-Lösung bietet keine Lösungen vor 2016. |

## Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

### Red Hat Solution Integration verstehen

Sie können vorgeschlagene Korrekturlösungen, die von Red Hat Solution Integration bereitgestellt werden, in der Anwendung Vulnerability Response ] überprüfen und implementieren.

Red Hat Solution Integration ist in der Funktion Vulnerability Solution Management von Vulnerability Responseenthalten, die über ein separates Abonnement verfügbar ist. Weitere Informationen dazu, wie Vulnerability Solution ManagementVulnerability Response Lösungen integriert, finden Sie unter [].

Red Hat Solution Integration untersucht Berichte über Sicherheitsschwachstellen, die sich auf Produkte und Services von Red Hat auswirken, und stellt Lösungsinformationen bereit, die beim Management von Sicherheitsrisiken helfen. Lösungen, die als Fehlerkorrekturen bezeichnet werden, werden aus Red Hatin Ihr Red Hat Solution Integration importiert.

Ab Version 21.0 von Vulnerability ResponseRed Hat ] überträgt Nutzlasten im CSAF-Format (Common Security Advisory Framework) und nicht im CVRF-Format (Common Vulnerability Reporting Framework). CSAF, ein XML-basierter Standard, unterscheidet sich in Struktur und Format von CVRF. Um dieser Änderung Rechnung zu tragen, wurde ein neuer CSAF-Parser entwickelt. Dieser Parser interpretiert das CSAF-Format und extrahiert die erforderlichen Felder, um die Tabellen entsprechend auszufüllen.

**Hinweis:**
Standardmäßig erhalten Sie die Nutzlast im CSAF-Format.

Die folgenden Auszüge zeigen das Integrationsskript zum Analysieren der von Red Hat empfangenen Nutzlast im CSAF- bzw. CVRF-Format.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(true);
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
})(integrationProcessGr);
```

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Red Hat Solution Integration enthält Einstiegspunkte für das Red Hat-Produkt, das als regelmäßige Aufgabe aufgerufen wird. Die regelmäßige Aufgabe vereinfacht den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Er wird automatisch ausgeführt. Sie können die geplante Aufgabe auch manuell ausführen.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

## Verfügbare Versionen

Stellen Sie für die aktuelle Version von Vulnerability Solution Management - und Red Hat -Lösungen sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben.

Weitere Informationen zur Installation und Konfiguration von Vulnerability Solution Management und Lösungsintegrationen finden Sie unter Anwendung Solution Management for Vulnerability Response installieren und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

| Release-Version von Vulnerability Response | Version von Vulnerability Solution Management | Releasehinweise |
|---|---|---|
| Vulnerability Response v15.0 | v10.3 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Rollen

Red Hat Solution Integration Aufgaben umfassen die folgende Rolle: sn_vul.configure_rhsa_integration

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Red Hat Solution Integration

Um Red Hat Solution Integrationanzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen**.

Die folgende Integration ist im Basissystem enthalten.

### Red Hat-Integration

| Integration | Beschreibung |
|---|---|
| Red Hat Solution Integration | Ruft Lösungen und die Zuordnung der National Vulnerability Database (NVD) ab, um Lösungen mit Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zu verknüpfen. |

## Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

### Rapid7 Lösungsmanagement

Lösungen sind bekannte Fehlerkorrekturen, die entweder aus Rapid7 Data Warehouse oder Rapid7 InsightVM Rapid7 in Ihr Rapid7 Vulnerability Integration importiert werden. Data Warehouse importiert sowohl Lösungen als auch Ersatzlösungen. Mit Rapid7 InsightVMerhalten Sie Lösungen als Teil der Rapid7 Integration von angreifbaren Elementen – API.

Ab Version 21.0 von Vulnerability Responseändert sich die Art und Weise, wie Lösungen von Rapid7 InsightVMerstellt werden. Anstatt sich auf die Felder **solution_summary**, **solution_fix**oder **solution_type** zu verlassen, erstellt Rapid7 InsightVM jetzt Lösungen mit der vom Scanner bereitgestellten solution_id. Dies bedeutet, dass auch wenn diese Felder leer sind, eine Lösung erstellt wird, solange eine Lösungs-ID verfügbar ist.

Um importierte Lösungen als Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Lösungen**.

Wenn das Plugin Vulnerability Solution Management aktiviert ist, bietet die neueste Version von Rapid7 Vulnerability Integration die folgenden wichtigen Funktionen in Bezug auf -Lösungen:

- Die Rapid7 -Lösungsverwaltung wird in die Schwachstellen-Lösungsverwaltung verschoben.
- Eine neue Integration von Rapid7 Prerequisite Solution Management für das Data Warehouse wird eingeführt. Die Integration ruft die erforderliche Lösung aus dem Data Warehouse Rapid7 ab.
- Die zugehörige Liste von Rapid7 (Lösung) für Drittparteieinträge (TPE) ist ausgeblendet.
- Die zuvor importierten Daten können im neuen Datenmodell angezeigt werden. Rapid7-Lösungen, Lösungsersetzung und Schwachstellenlösungszuordnung werden erneut importiert, und das Feld „ **Importieren seit** “ wird auf leer gesetzt. Das Feld wird in Solution Management ausgefüllt.
- Die Erkennungen werden aktualisiert, um das Lösungsfeld auszufüllen. Erkennungen zeigen die Lösungen an, da sie Teil von Vulnerability Solution Management sind.
- Rapid7 erhält eine höhere Priorität gegenüber anderen Lösungen, wenn die bevorzugte Lösung auf TPE für Rapid7 Data Warehouse festgelegt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für die Lösungen wird ein Rollup zu angreifbaren Elementen (AEs) aus Erkennungen für Rapid7 InsightVMdurchgeführt .

**Hinweis:**
Wenn Sie das Plugin Vulnerability Solution Management nicht aktiviert haben, funktioniert die Anwendung unverändert.

### Vulnerability Solution Management

Wenn Sie das Plugin Rapid7Vulnerability Solution Management aktiviert haben, werden die Lösungen Rapid7 sowohl für das Data Warehouse von [] als auch für [ Rapid7 InsightVM in die Tabelle „Lösungen für Schwachstellen“ [sn_vul_solution] eingetragen. Wenn Sie jedoch das Plugin Rapid7 Vulnerability IntegrationVulnerability Solution Management nicht aktiviert haben, funktioniert [] unverändert und importiert die Lösungen in die benutzerdefinierte Tabelle [sn_vul_r7_solution].

Um die Tabelle mit den Schwachstellenlösungen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenlösungen** , in der Sie die Lösungen verschiedener Anbieter anzeigen und vergleichen können. Um importierte Lösungen in der benutzerdefinierten Tabelle anzuzeigen, navigieren Sie **Alle** > **Rapid7 Vulnerability Integration** > **Lösungen**.

**Hinweis:**
Nach Quelle gruppieren, um Lösungen basierend auf Lieferanten anzuzeigen.

### Rapid7 Prerequisite Solution Management-Integration

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, wird ein Korrekturskript ausgeführt, das die Reihenfolge der Integrationen ändert. Die neue Rapid7 Prerequisite Solution Integration for Rapid7 Data Warehouse ordnet die Lösungen den erforderlichen Lösungen zu. Die Integrationen werden in der folgenden Reihenfolge ausgeführt:

1. Rapid7 Lösungsintegration
2. Rapid7 Erforderliche Lösung
3. Rapid7 Lösungsintegration ablösen
4. Rapid7 Integration der Schwachstellen-Lösungszuordnung
5. Rapid7 VI-Lösungsintegration (ab v19.0 von Vulnerability Response)

**Hinweis:**
Wenn Sie die Integrationen manuell ausführen, beginnen Sie mit der Rapid7 Lösungsintegration. Ändern Sie die Next Integration-Kette in der Rapid7 -Integration nicht. Die Sequenz wird in der Spalte Nächste Integration definiert.

### Zugehörige Liste Rapid7 (Lösungen) in TPE

Wenn Sie das Plugin Vulnerability Solution Management aktiviert haben, können Sie Folgendes tun:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können die TPEs anzeigen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Drittpartei**.
- Sie können die zugehörige Liste Lösungen (Rapid7), die in älteren Releases verfügbar war, nicht sehen.
- Sie können die Rapid7-bezogenen Lösungen in der zugehörigen Liste Lösungen zusammen mit den Lösungen aus anderen Quellen wie RedHat, Microsoft (MSRC) usw. anzeigen.

Wenn Sie das Plugin Vulnerability Solution Management nicht aktiviert haben, geschieht Folgendes:

- Die Funktionalität der zugehörigen Listen bleibt unverändert.
- Sie sehen die zugehörige Liste Lösungen (Rapid7).
- Die zugehörige Liste „Lösungen“ ist ausgeblendet.

### Bevorzugte Lösung für TPE und VIs

Rapid7 ruft die Lösung aus dem Data Warehouse auf der Ebene des Drittparteieintrags (TPE) und für Rapid7 InsightVM auf der Erkennungsebene ab.

Für ein Data Warehouse Rapid7 wird die Lösung folgendermaßen verwaltet:

- Die bevorzugte Lösung wird basierend auf der Schwachstellen- und Lösungszuordnung für das TPE festgelegt.
- Wenn die Schwachstelle von Rapid7 eine einzelne höchste Ersatzlösung von Rapid7hat, wird sie als bevorzugte Lösung festgelegt, unabhängig von anderen Lösungen von Lieferanten, die mit dieser Schwachstelle verbunden sind.
- In allen anderen Fällen bleibt der Flow der bevorzugten Lösung gleich. Weitere Informationen zum Standardverhalten bevorzugter Lösungen finden Sie unter Vulnerability Solution Management.

Für Rapid7 InsightVMwird die Lösung folgendermaßen verwaltet:

- Die bevorzugte Lösung ist ein Rollup von Erkennungen zu AEs.
- Wenn eine einzelne Erkennung und Lösung von Rapid7vorhanden ist, wird für die Lösung ein Rollup zum VI durchgeführt.
- Wenn mehrere Erkennungen vorhanden sind und alle dieselbe Lösung von Rapid7aufweisen, wird für die Lösung ein Rollup bis VI durchgeführt.
- Wenn mehrere Erkennungen mehrere Lösungen von Rapid7haben, wird für die neueste Lösung ein Rollup zum VI durchgeführt.

Ab Version 19.0 von Vulnerability Responsewird die bevorzugte Lösung, die von Rapid7 Data Warehouse generiert wird, direkt in angreifbare Elemente ausgefüllt, indem [] die Notwendigkeit von Vulnerability Solution ManagementRapid7 umgeht. Durch diese Änderung wird sichergestellt, dass jegliche Ungewissheit hinsichtlich möglicher Lösungen für diese angreifbaren Elemente beseitigt wird.

Um diese direkte Auffüllung über Rapid7zu erreichen, werden die folgenden Schritte ausgeführt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine neue Integration, Rapid7 VI Solution Integration, wird eingerichtet und in den vorhandenen Rapid7 Vulnerability Integration-Workflow integriert.
- Eine neue Tabelle [sn_vul_r7_rapid7_vi_solution_import] wird erstellt.
- Eine neue Transformationszuordnung Rapid7 VI-Lösungstransformation wird erstellt.
- Die Skripteinbindung Rapid7AssetsImportProcessor wurde so geändert, dass die Verarbeitung von Lösungen ausgeschlossen wird, die von Rapid7 in Vulnerability Solution Managementgeneriert werden.

Nach der Ausführung der Rapid7 VI-Lösungsintegration werden die unverarbeiteten Daten, die von Rapid7 abgerufen wurden, in der neu erstellten Tabelle gespeichert. Anschließend wird die Rapid7 VI-Lösungstransformation ausgelöst, die diese Daten verarbeitet und die bevorzugte Lösung direkt in die Tabelle „Angreifbares Element“ ausfüllt.

**Hinweis:**
Die Rapid7 VI-Lösungsintegration füllt die bevorzugte Lösung ausschließlich aus, wenn das Plugin Vulnerability Solution Management installiert wurde.

### Aus Rapid7 Data Warehouse importierte Lösungsersetzungskette für eine Schwachstelle

Sie können die Ersatzlösungen für eine Lösung anzeigen, indem Sie auf eine Schwachstellenlösung und dann auf die zugehörige Liste Ersatzlösungen klicken. Sie können die vorherigen Lösungen anzeigen, indem Sie auf die zugehörige Liste „Vorherige Lösungen“ klicken. Wenn Sie eine Lösung an die TPE anhängen, wird die Ersatzlösung dieser Lösung an diese TPE angehängt.

### Ändern Sie die maximale Tiefe der Lösungsersetzungskette im Diagramm nach Systemeigenschaften

Die im Datenmodell Rapid7 empfangene Lösungsersetzungskette ist zu lang, um das Diagramm während der Ausfüllung der bevorzugten Lösung zu erstellen. Um die Tiefe der Kette zu beschränken, wird eine Systemeigenschaft mit dem Namen *sn_vul.max_recursion_depth* mit dem Wert 500 erstellt. Wenn die Kettentiefe mehr als 500 beträgt, wird der Rest der Kette ignoriert. Um die maximale Tiefe der Kette zu ändern, navigieren Sie zur Tabelle [sys_properties], und ändern Sie den Wert der Eigenschaft.

### Die Anwendung Rapid7 wird aktualisiert

Wenn Sie das Plugin [] aktualisieren und das Plugin Rapid7 Vulnerability IntegrationVulnerability Solution Management noch nicht aktiviert haben, funktioniert die Anwendung unverändert.

Unabhängig davon, ob Sie das Plugin Vulnerability Solution Management vor oder nach dem Upgrade der Anwendung Rapid7 ] aktivieren, bleibt das Feld **Importieren seit** für die folgenden Integrationen leer:

- Rapid7 – Integration der ablösenden Lösung
- Integration der Rapid7-Schwachstellen-Lösungszuordnung
- Rapid7-Lösungsintegration

**Hinweis:**
Ab der nächsten Integrationsausführung werden die Daten in die Tabelle der Schwachstellenlösungen eingetragen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Rapid7 InsightVMwerden die Daten auf Erkennungsebene empfangen. Wenn die Rapid7 InsightVM -Integration ausgeführt wird, werden die Lösungen in die Tabelle der Schwachstellenlösungen importiert.

### Generisches Framework zum Erfassen von Daten von einem beliebigen Lösungsanbieter

Das Common Vulnerability Reporting Framework (CVRF) ist eine XML-basierte Sprache, die die gemeinsame Nutzung kritischer sicherheitsbezogener Informationen in einem Standardberichtsformat ermöglicht. Da CVRF den Austausch und die Verarbeitung von Informationen beschleunigt, wird ein generisches Framework für die Integration von Lösungsinformationen bereitgestellt, um Support für Lieferanten zu ermöglichen, die das CVRF-Format unterstützen. Zu diesen wichtigen Lieferanten gehören Oracle, Red Hat, Ciscound Microsoft.

Das von CVRF unterstützte Lösungsmanagement umfasst die folgenden Hauptfunktionen:

- Konfiguration über den Setup-Assistenten
- Unterstützung für den Import von CVRF-Daten durch Dateiimport
- Unterstützung für den Import von CVRF-Daten über die CVRF-URL
- Unterstützung für den Import von CVRF-Daten durch Hinweise
- Zuordnung von Lösungen zu zugehörigen Schwachstellen

Das Vulnerability Response-Plugin sorgt für die Aktualisierung der Metrikstatus der erstellten Lösung.

Weitere Informationen finden Sie unter:

- Konfigurieren Sie Schwachstellen-Lösungsanbieter
- Importieren Sie Common Vulnerability Reporting Framework-Daten durch Dateiimport
- Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen
- Konfigurieren Sie einen anderen Common Vulnerability Reporting Framework-Anbieter als Cisco
- Importieren von Common Vulnerability Reporting Framework-Daten aus Advisories
- Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL
- Importieren von Common Vulnerability Reporting Framework-Daten aus Advisories
- Problembehandlung beim Datenimport von Common Vulnerability Reporting Framework

### Integration der Lösung Common Vulnerability Reporting Framework (CVRF) wird vorbereitet

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das CVRF-Datenformat (Common Vulnerability Reporting Framework) unterstützen.

## Bevor Sie beginnen

Um die Integration mit den Anbietern zu ermöglichen, die die Lösungen bereitstellen, stellen Sie sicher, dass Sie die Aufgaben in der folgenden Prüfliste ausführen. Sie können die Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prüfliste zur Vorbereitung der Integration

| Aufgabe | Beschreibung |
| --- | --- |
| **Abhängige Anwendungen** ☐ | Vergewissern Sie sich, dass die folgenden Anwendungen von ServiceNow Storeinstalliert wurden:<br>• Vulnerability Solution Management: Weitere Informationen zur Installation von Vulnerability Solution Managementfinden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten und Anwendung Solution Management for Vulnerability Response installieren.<br>• Vulnerability Response: Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher. |
| **Anmeldeinformationen für Drittanbieterkonto** ☐ | Vergewissern Sie sich, dass Anmeldeinformationen für Drittparteikonten verfügbar sind. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten. |
| **Lieferantenauthentifizierung** ☐ | Vergewissern Sie sich, dass Sie die Lieferanten für den Import von Lösungen mithilfe der APIs authentifiziert haben. Weitere Informationen zum Authentifizieren von Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen.<br><br>Wenn Sie keinen API-basierten Lieferanten konfigurieren möchten, können Sie diesen Schritt überspringen. |
| **Anpassung von Flow und Flow-Aktion** ☐ | Wenn Sie einen anderen API-basierten Lieferanten als Cisco konfigurieren möchten, müssen Sie den Flow und die Flow-Aktion zum Extrahieren eines eindeutigen Schlüssels und einer CVRF-URL aus der Antwort eines Advisory anpassen.<br><br>**Hinweis:**<br>Die Veröffentlichung der CVRF-URL ist nicht bei allen Lieferanten Standard.<br><br>Informationen zum Anpassen des Flows für andere Lieferanten als Cisco finden Sie unter Konfigurieren Sie einen anderen Common Vulnerability Reporting Framework-Anbieter als Cisco.<br><br>Sie können diesen Schritt überspringen, wenn keine anderen Lieferanten als Cisco konfiguriert werden sollen. Standardmäßig gehört der -Flow für Cisco zum Lieferumfang der -Anwendung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

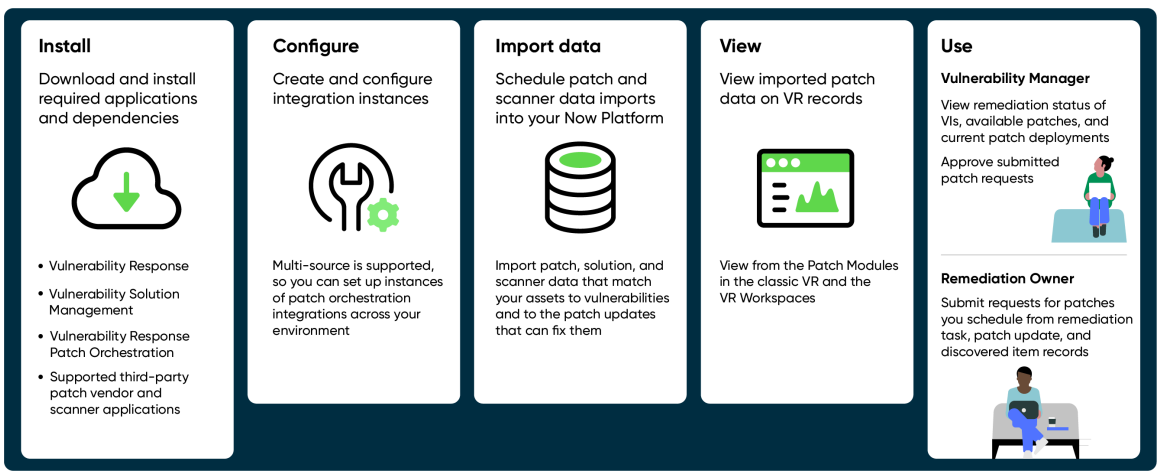
| Aufgabe | Beschreibung |
|---|---|
| **Rollen** ☐ | Stellen Sie sicher, dass Sie eine Administratorgruppe oder einen Benutzer haben, der die Integration verwalten kann. Wenn sie nicht zugewiesen ist, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu. |

## Patch-Orchestration mit Vulnerability Response

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets mit Patch-Orchestration mit Vulnerability Responseverwalten. Vulnerability Response Patch Orchestration und die Patch Orchestration-Integrationen sind im ServiceNow® Storeverfügbar.

## Patch Orchestration mit verstehen Vulnerability Response

Die Patch-Orchestrierung mit Vulnerability Response verwendet Daten aus geplanten Importen aus Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellenscannern. Diese Daten werden in der Anwendung Vulnerability Response korreliert. Mit dieser Organisation der Daten können Sie die Schritte des Korrekturzyklus für Schwachstellen abschließen. Beginnen Sie mit der Identifizierung von Schwachstellen, wenden Sie dann Patches und Updates an, und schließen Sie schließlich angreifbare Elemente mithilfe von Scannerdaten von Drittanbietern, alles in Ihrer Now Platform® -Instanz.




Die Patch-Orchestration mit Vulnerability Response wird sowohl in der klassischen -Umgebung als auch in den Arbeitsbereichen von Vulnerability Response unterstützt.

Weitere Informationen zur Patch-Orchestrierung in den Arbeitsbereichen finden Sie unter Patchen Sie die Orchestration mit den Vulnerability Response -Arbeitsbereichen.

Mit der Patch-Orchestration in Vulnerability Responsekönnen Schwachstellenmanager, Analysten und IT-Korrekturspezialisten die folgenden Korrekturaufgaben ausführen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weiteren Kontext und Informationen zu den Arten von Patches und Lieferanten anzeigen, aus denen ihre Lösungen bestehen (Patches).
- Zeigen und überwachen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in Vulnerability Response Arbeitsbereichen oder in der klassischen Umgebung.
- Stellen Sie Patches, die von Drittpartei-Lösungsanbietern unterstützt werden, für Windows, CentOS, macOS, Oracleund andere Assets in regelmäßigen, geplanten Intervallen bereit. Sie können Patches außerhalb der Geschäftszeiten planen, um Konflikte mit Personen bei der Arbeit zu vermeiden.
- Identifizieren Sie mithilfe importierter Erkennungsdaten, die von Scannern von Drittanbietern bereitgestellt werden, Assets, die Schwachstellen aufweisen und nicht gepatcht oder durch geplante Patches nicht erfolgreich aktualisiert werden.
- Initiieren und planen Sie verfügbare Patches für Assets, die Updates aus Datensätzen für Patch-Updates, Korrekturaufgaben und erkannte Elemente in der Anwendung Vulnerability Response erfordern.
- Überwachen Sie Patch-Bereitstellungen mit einem optionalen Genehmigungsprozess für Patch-Anforderungen, die von Ihren Fehlerkorrektur-Spezialisten übermittelt werden.

## Wichtige Begriffe

**Konfigurationselement (Configuration Item, CI)**

CIs sind die vorhandenen Assets, die in Ihrer Configuration Management Database (CMDB) aufgeführt sind.

**Angreifbares Element (AE)**

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht. Angreifbare Elemente (VITs) werden in Korrekturaufgaben oder Listen gemäß bestimmten Kriterien gruppiert, die Korrekturaktionen für VIs angeben.

**Instanz**

Bezieht sich auf einen eindeutigen Account einer Lösungsanbieteranwendung. Beispielsweise kann jeder Benutzeraccount eine Instanz in der Anwendung HCL BigFix sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Now Platform® -Instanz.

**Lösung**

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: „Potenziell“ und „Bevorzugt“. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben häufig viele mögliche Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

**Patch**

Software-Updates, die Schwachstellen beheben. Patch-Anbieter verwenden ihre eigenen Namen für Patches, z. B. In der Anwendung HCL BigFix werden Patches als Fixlets bezeichnet.

**Bevorzugter Patch**

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Nach der Bereitstellung werden Patches den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie beheben.

**Bereitstellung**

Die Bereitstellung für die Zwecke dieser Integration bezieht sich auf das Anwenden, Initiieren oder Planen eines Patches auf einem Computer.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Eine einzelne vorhandene Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen eines Scanners einer Drittpartei oder eine Lösungsanbieterintegration in Ihrer Umgebung haben.

## Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

- Die Vulnerability Response -Anwendung und die Abhängigkeits-Plugins Security Support Common und Security Support Orchestration.
- Vulnerability Solution Managementan.
- Vulnerability Response Patch Orchestration-Anwendung verfügbar im ServiceNow® Store.
- Eine unterstützte Patch-Anbieter-Anwendung einer Drittpartei, z. B. „The Vulnerability Response Patch Orchestration Integration with HCL BigFix“ oder „ The Vulnerability Response Patch Orchestration Integration with Microsoft SCCM“.
- Unterstützte Scanner-Integrationen von Drittparteien mit Vulnerability Response.

## Erforderliche Rollen

Benutzer benötigen Rollen, die für die von Ihnen verwendete Patch-Orchestration-Integration spezifisch sind, um Daten anzuzeigen und Patches aus der Anwendung Vulnerability Response zu planen. Weitere Informationen finden Sie in den Konfigurationsinformationen für die unterstützten Integrationen, die Sie verwenden.

- Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Response und Vulnerability Response Patch Orchestration Integration with Microsoft SCCM.
- In den Vulnerability Response -Arbeitsbereichen und der klassischen Umgebung wird die Rolle sn_vul_patch_orch.read_patch, mit der Benutzer Daten anzeigen, aber nicht bearbeiten können, mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt.

  Die Rollen, die Sie zuweisen müssen, um die Verbindungen zu den Patch-Anbietern zu konfigurieren und Patches zu planen, sind integrationsspezifisch. Weitere Informationen finden Sie unter Konfigurieren Sie die Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix und Vulnerability Response Patch Orchestration mit MS SCCM konfigurieren.

Es gibt einen Übermittlungs- und Genehmigungsprozess für Patch-Anforderungen, die in den -Anwendungen enthalten sind. Standardmäßig ist eine Systemeigenschaft [**sn_vul_patch_orch.patch_approval_required**] in der Anwendung Vulnerability Response Patch Orchestration in Ihrer Instanz Now Platform aktiviert.

Diese Systemeigenschaft ist aktiviert, damit Patch-Bereitstellungen, wenn sie geplant sind, zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind. Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen können, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen. Wenn Sie die Genehmigungssystemeigenschaft deaktivieren, kann jeder Benutzer mit der Rolle „sn_vul_patch_orch.configure_patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen und Informationen zum Deaktivieren dieser Systemeigenschaft finden Sie im Konfigurationsthema für Ihre unterstützte Integration.

- Konfigurieren Sie die Patch-Orchestration-Integration Vulnerability Response mit HCL BigFixan.
- Konfigurieren Sie die Integration von Vulnerability Patch Orchestration mit Microsoft SCCMan.

### Planen Sie Patches aus Vulnerability Response Datensätzen

Korrekturspezialisten können Patch-Updates planen, um angreifbare Elemente zu beheben, und den Korrekturfortschritt anhand von Datensätzen in der Anwendung Vulnerability Response überwachen.

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update
- Korrekturaufgabe
- Erkanntes Element

### Datensätze, für die ein Rollup der Anzahl aktiver AEs in durchgeführt wird Vulnerability Response

Um potenzielle Leistungsprobleme beim Rollup aller Patches für alle Schwachstellen zu vermeiden, ändert die geplante Aufgabe, die Änderungen aufnimmt, nur die aktive VI-Anzahl. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup zu den folgenden Datensätzen in der Anwendung Vulnerability Response durchgeführt:

- VIT (angreifbares Element)
- RT (Korrekturaufgabe)
- Schwachstellenlösung
- Patch-Update

Weitere Informationen zum Anzeigen von Patch-Daten und zum Rollup von Patch-Daten zu Datensätzen sowie zum Anzeigen von Patches ohne Lösungen finden Sie in den folgenden Themen.

- Rollup für Patch-Daten und -Status für Patch-Orchestration in Vulnerability Responsean.
- Anzeigen von Patch-Daten und Planen von Patches in Vulnerability Response.
- Zeigen Sie Patches ohne Lösungen in an Vulnerability Responsean.

### Massenbearbeitung von angreifbaren Elementen mit Patches

Sie können angreifbare Elemente in der klassischen Umgebung, die Patches aus der klassischen Umgebung enthalten, in großen Mengen bearbeiten. Weitere Informationen zur Massenbearbeitung finden Sie unter Bearbeiten Sie angreifbare Elemente im Massenvorgang in Vulnerability Response. Die bevorzugten Patches für alle für die Massenbearbeitung ausgewählten VIs. Diese Option zum Bearbeiten funktioniert nur, wenn allen ausgewählten VIs bevorzugte Patches zugeordnet sind.

### Exception Management – Übersicht

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann, können Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie behoben werden kann.

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen der Nichtbehebung der Schwachstelle anerkennen und akzeptieren.

## Lebenszyklus einer Ausnahme

**Definition einer Ausnahme**

Eine Ausnahme ist eine Anforderung, die Korrektur eines VI oder RT für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

**Eine Ausnahme wird angefordert**

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für einen VI oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird der VI oder RT in den Status „ **Zurückgestellt“** versetzt.

**Eine Ausnahmeanforderung wird genehmigt**

VIs oder RTs, die nicht sofort korrigiert werden können, werden von Schwachstellenanalysten überprüft, auf Risiko bewertet und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Die Genehmigung einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

### Hinweis:

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

Sobald eine Ausnahmeanforderung für einen VI oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen
- Aktualisieren Sie die Felder **Zuweisung an** oder **Zuweisungsgruppen**

**Nachverfolgung einer Ausnahmeanforderung**

Nach dem Auslösen der Ausnahme können Sie ihren Status mithilfe der Registerkarte „ **Statusänderungsgenehmigungen** “ von VI oder RT nachverfolgen. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen AEs in dieser RT nicht nachverfolgen.

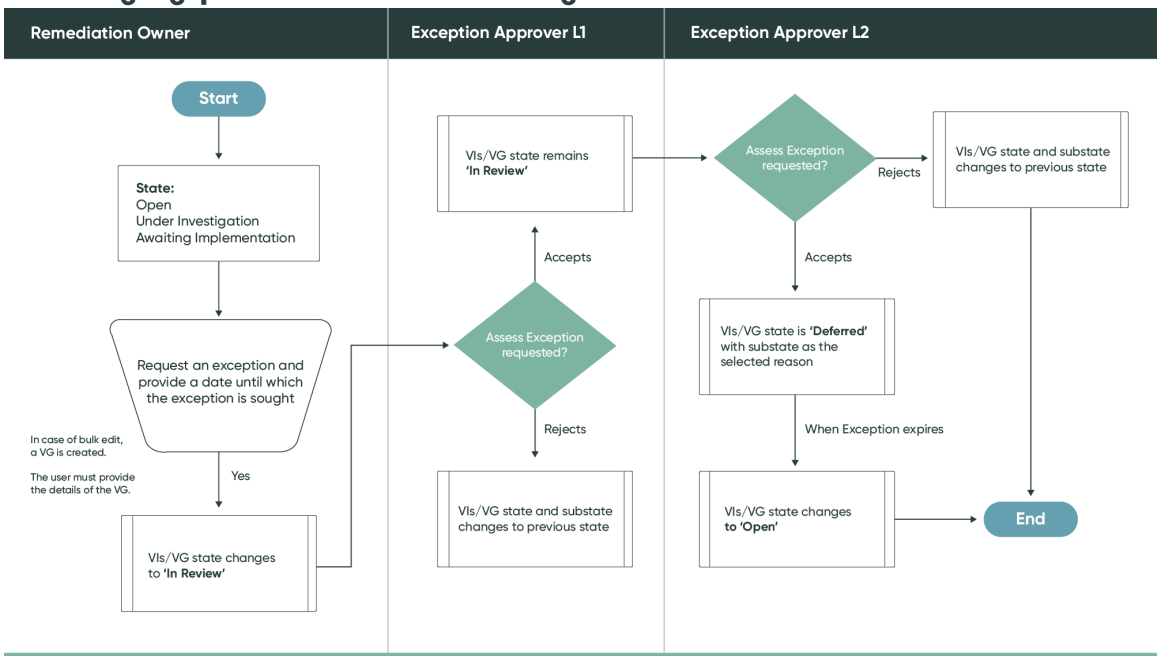
**Ablauf einer Ausnahmeanforderung**

Wenn eine Ausnahmeanforderung für eine bestimmte VI oder RT abläuft, wird die betroffene VI oder RT in den Status „ **Offen** “ zurückgesetzt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Genehmigungsprozess für Ausnahmemanagement vor VR v15.0**




Wenn ein einzelner VI oder alle VIs in einer RT beim nächsten Scan erfolgreich sind, ändern sich die VIs und ggf. das Feld RT-Status in **Geschlossen** mit dem **SubstatusFest**.

## Übersicht über Ausnahmeregeln

Mit Ausnahmeregeln für Vulnerability Response können Sie den Zurückstellungsprozess für angreifbare Elemente (AEs) automatisieren. Fordern Sie eine Ausnahme für die angreifbaren Elemente (VIs) an, die nicht sofort korrigiert oder zurückgestellt werden können, indem Sie die betroffenen Schwachstellen, Konfigurationselemente (CIs) oder VIs identifizieren. Übereinstimmende AEs basierend auf der Regel zurückstellen, wenn das System sie identifiziert, indem der AEs-Zurückstellungsprozess automatisiert wird.

### Verwenden von Ausnahmeregeln in Ihrer Organisation

Verwenden Sie Ausnahmeregeln, um neue und vorhandene AEs automatisch für einen bestimmten Zeitraum zurückzustellen, wenn sie der genehmigten Regelbedingung entsprechen. Die Automatisierung minimiert das Risiko fehlender Servicelevel-Vereinbarungen und erleichtert die Verwaltung mehrerer Elemente, da manuelle Eingriffe entfallen.

Zurückstellungsregeln unterstützen die Reihenfolge, d. h. die Regel mit der höchsten Priorität wird zuerst ausgeführt. Wenn eine Regel mit hoher Priorität auf einen AE angewendet wird, werden keine nachfolgenden Regeln darauf angewendet, auch wenn die Bedingung mit dem AE übereinstimmt.

### Hinweis:

- Sie können Regeln nur erstellen, wenn Sie Vulnerability Response in der Ausnahmeverwaltungskonfiguration auswählen. Details finden Sie unter Konfigurieren Sie Exception Management für Vulnerability Response.
- Wenn VIs durch eine Ausnahmeregel zurückgestellt werden, werden sie in die erstellte Zurückstellungs-Schwachstellengruppe (SG) kopiert. Die AEs sind weiterhin Teil der SGs, denen sie zuvor angehörten.

Der Lebenszyklus einer Ausnahmeregel lautet wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen einer Ausnahmeregel
- Eine Ausnahmeregelanforderung wird genehmigt
- Ausnahmeregel aktivieren
- Zurückstellen einer Ausnahmeregel
- Ablauf einer Ausnahmeregel

### Erstellen einer Ausnahmeregel

Sie können eine Ausnahmeregel erstellen, um die AEs, die den definierten Bedingungen entsprechen, automatisch für den angegebenen Zeitraum zurückzustellen. Nachdem Sie eine Ausnahmeregel erstellt haben, übermitteln Sie sie zur Genehmigung.

### Eine Ausnahmeregelanforderung wird genehmigt

Die Genehmigung einer Ausnahmeregelanforderung ist ein zweistufiger Prozess. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahmeregel durch eine einzige Genehmigung bewertet und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann die Genehmigung einer Ausnahmeregel nicht genehmigt werden. Nachdem die Regel genehmigt wurde, wird eine Korrekturaufgabe (Remediation Task, RT) erstellt. Weitere Informationen finden Sie unter Antrag auf Ausnahmeregel genehmigen.

**Hinweis:**

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

Nachdem eine Ausnahmeregelanforderung genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Abbrechen
- Löschen

### Ausnahmeregel aktivieren

Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird die Ausnahmeregel für alle erstellten AEs und auch für AEs ausgeführt, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden.

**Hinweis:**

Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten am „Gültig ab“-Datum ausgeführt.

### Zurückstellen einer Ausnahmeregel

Sie können AEs, die den in dieser Ausnahmeregel definierten Bedingungen entsprechen, bis zu dem für die Regel definierten Datum „Zurückgestellt bis“ zurückstellen. An diesem Datum wird die Korrekturaufgabe, die Sie für die Ausnahmeregel erstellt haben, geschlossen, und alle AEs in dieser Gruppe werden wieder in den Status „Offen“ versetzt.



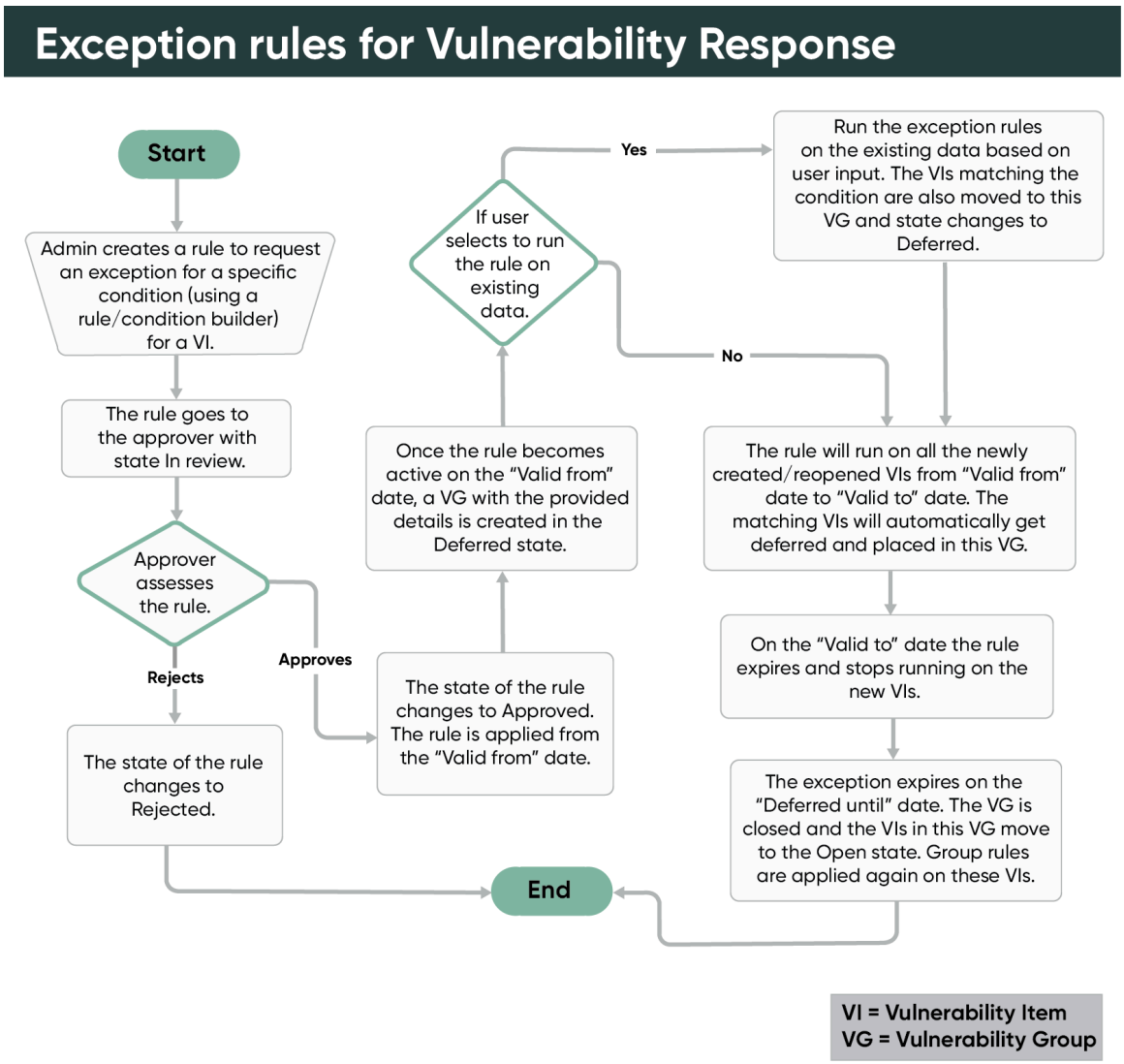
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppenregeln werden erneut auf sie angewendet, um sie den erforderlichen RTs zuzuordnen.

**Ablauf einer Ausnahmeregel**

Nach Ablauf der Ausnahmeregel wird sie nicht mehr für neue oder erneut geöffnete AEs ausgeführt. Die zugeordnete RT bleibt bis zum Datum „Zurückgestellt bis“ im Status „Zurückgestellt“.

**Ausnahmeregel-Workflow vor v15.0**




## Falsch positive Ergebnisse – Übersicht

Ein falsch positives Ergebnis ist eine Bedingung, bei der der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, aber tatsächlich keine Schwachstelle vorhanden ist. Es kann mehrere Gründe geben, z. B. falsche Klassifizierung, falsche Logik oder falscher Algorithmus im Scanner. Der Korrekturbesitzer kann angreifbare Elemente (AEs) oder Korrekturaufgaben (RTs) als falsch positive Meldungen kennzeichnen.

## Lebenszyklus eines falsch positiven Ergebnisses

**Bedeutung von falsch positiven Werten**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Scanner gibt manchmal eine Warnung aus, wenn in Wirklichkeit keine Schwachstelle vorliegt. Beispiel: Wenn ein Konfigurationselement außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit verbundenes Problem auslöst, markieren Sie es als falsch positiv.

**Kennzeichnung als falsch positiv**

Weitere Informationen zum Markieren eines VI oder RT als falsch positiv finden Sie unter Als falsch positiv markieren.

**Arbeiten mit dem falsch positiven Ergebnis**

Sobald ein VI oder RT als falsch positiv markiert ist, wird der Status in „Geschlossen“ aktualisiert und der Substatus in „Falsch positiv“ geändert. Die folgenden Aktionen können ausgeführt werden:

- Erneut öffnen
- Löschen
- Aktualisieren Sie das Datum im Feld **Bis**. Dieses Datum wird dann als Ablaufdatum für das falsch positive Ergebnis verwendet.

**Hinweis:**
Wenn sie nicht genehmigt wird, wird der VI oder RT in seinen vorherigen Status zurückgesetzt.

**Falsch positives Ergebnis wird genehmigt**

Der Genehmiger kann das falsch positive Ergebnis aus seinem Genehmigungs-Workflow genehmigen.

**Hinweis:**

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

**Falsch positives Ergebnis wird erneut geöffnet**

Ein VI oder RT in einem falsch positiven Substatus kann jederzeit erneut geöffnet werden.

**Nachverfolgung eines falsch positiven Ergebnisses**

Verwenden Sie den Abschnitt **Statusänderungsgenehmigungen**, um den Status des falsch positiven Ergebnisses nachzuverfolgen. Nach der Genehmigung wird der Status des VI oder RT auf „Geschlossen“ aktualisiert, und der Grund ist „Falsch positiv“.

**Ablauf eines falsch positiven Ergebnisses**

Nur der falsch positive Genehmiger kann ein Bis-Datum für das falsch positive Ergebnis festlegen, bis der VI oder RT abläuft. Außerdem können nur Falschmeldungen ablaufen, für die der Genehmiger ein Bis-Datum angegeben hat. Dieses Datum kann angegeben werden, nachdem das falsch positive Ergebnis genehmigt wurde.

Ein falsch positives Ergebnis ohne Bis-Datum ist ein dauerhaftes falsch positives Ergebnis. Nach Ablauf der Falschmeldung wird der Status des VI oder der VR zurück in „Offen“ gesetzt.

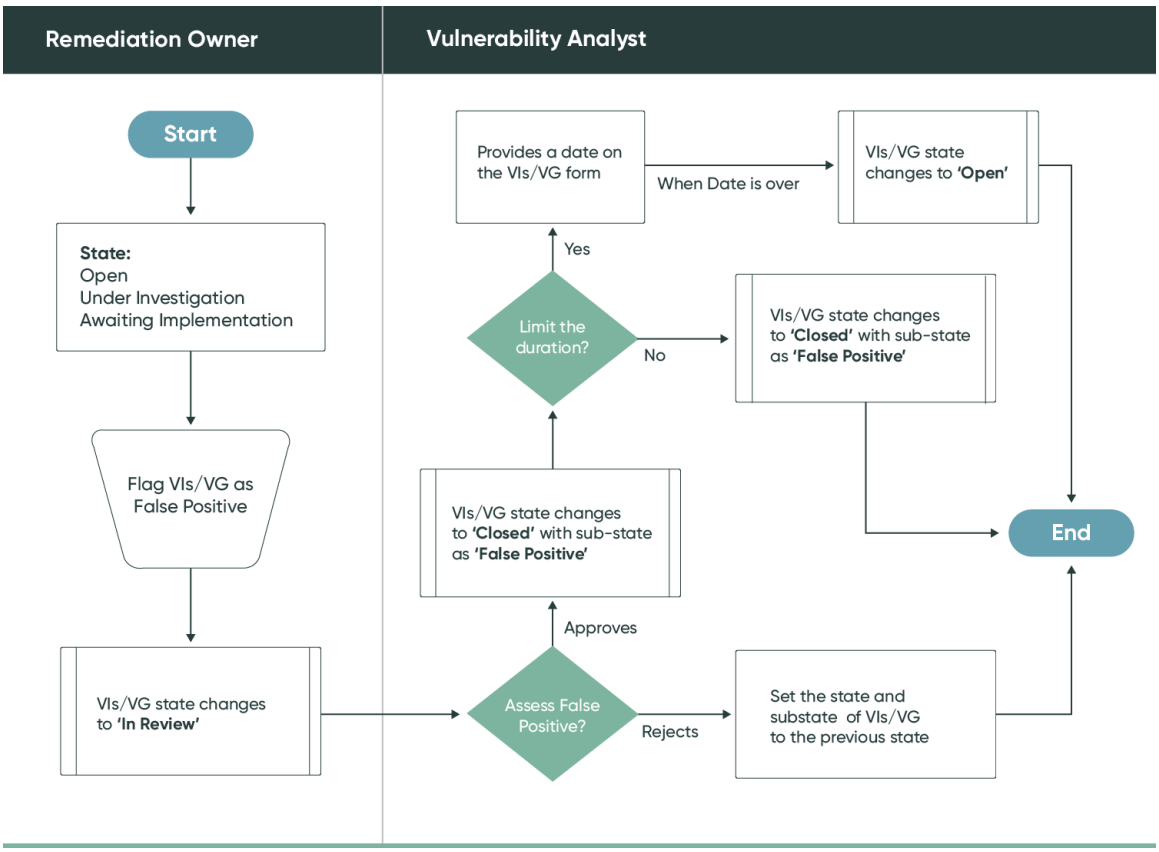


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

**Falsch positiver Genehmigungsprozess vor v15.0**




Automatische Übersetzung

Der Genehmigungsprozess erfolgt automatisch, wenn alle VIs den nächsten Scan bestehen. Die AEs werden unabhängig vom aktuellen Status automatisch geschlossen. Die Felder „AE“ oder „RT-Status“ ändern sich in „ **Geschlossen** “ mit dem **Substatus** „ **Fest“.**

Weitere Informationen finden Sie unter Falsch positive Meldungen markieren und genehmigen.

## Watchdog für Vulnerability Response

Der Watchdog wird verwendet, um Tabellen basierend auf den von Ihnen angegebenen Bedingungen nachzuverfolgen. Beispielsweise kann sie verwendet werden, um Details zu Integrationsausführungsfehlern in Vulnerability Responsezu protokollieren.

Sie können über diese Fehler benachrichtigt werden. Basierend auf dieser Benachrichtigung können Sie die Fehlerkorrektur planen. Die Standard-Watchdogs sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Integrationsausführung fehlgeschlagen: Wenn der Status der Integrationsausführung auf Abgeschlossen und Substatus auf Fehlgeschlagen festgelegt ist, werden Benutzer und Benutzergruppen benachrichtigt, wenn die Bedingung eine Anzahl größer als 0 zurückgibt, d. h. die Integrationsausführung schlägt fehl.
- Integrationen mit langer Ausführungszeit: Skript, um zu überprüfen, ob die Integrationsausführung die festgelegte Zeit überschreitet. Dieser Watchdog benachrichtigt Sie proaktiv, wenn sich der Abschluss der Integrationsausführung verzögert.

### Überwachungsprotokoll

Der Watchdog verfügt über ein Überwachungsprotokoll, das angibt, wie oft die Bedingung erfüllt wurde.

### Übersichts-Dashboard

Verwenden Sie das Übersichts-Dashboard, um den Watchdog für die letzten 30 Tage zu überwachen. Sie können mehrere Widgets erstellen, um andere von Ihnen überwachte Watchdog-Themen nachzuverfolgen.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

**Bericht**

| Name | Beschreibung |
|---|---|
| WatchDog-Fehler der letzten 30 Tage | Alle in den letzten 30 Tagen erfüllten Bedingungen. |

Weitere Informationen finden Sie unter Konfigurieren Sie Watchdog und Fehlerbehandlung für Erkennungen.

## Change Management für Vulnerability Response

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Korrekturaufgaben (RT) in der Anwendung Vulnerability Response erstellen und verwalten. Change-Anforderungen helfen Ihnen, Change-Aktivitäten für Ihre Assets zu initiieren und nachzuverfolgen, damit Sie Ihre Korrekturaufgaben und die entsprechenden angreifbaren Elemente korrigieren können.

### Change-Anforderungen und der Schwachstellen-Workflow

Wenn Sie mit der Anwendung Vulnerability Response nicht vertraut sind, finden Sie weitere Informationen unter Die Anwendung Vulnerability Response erkunden.

Die folgende Abbildung zeigt den Informationsfluss für Vulnerability Response, von der Einrichtung der Integration (Scanner) über die automatisierte Selektierung bis hin zur Untersuchung.

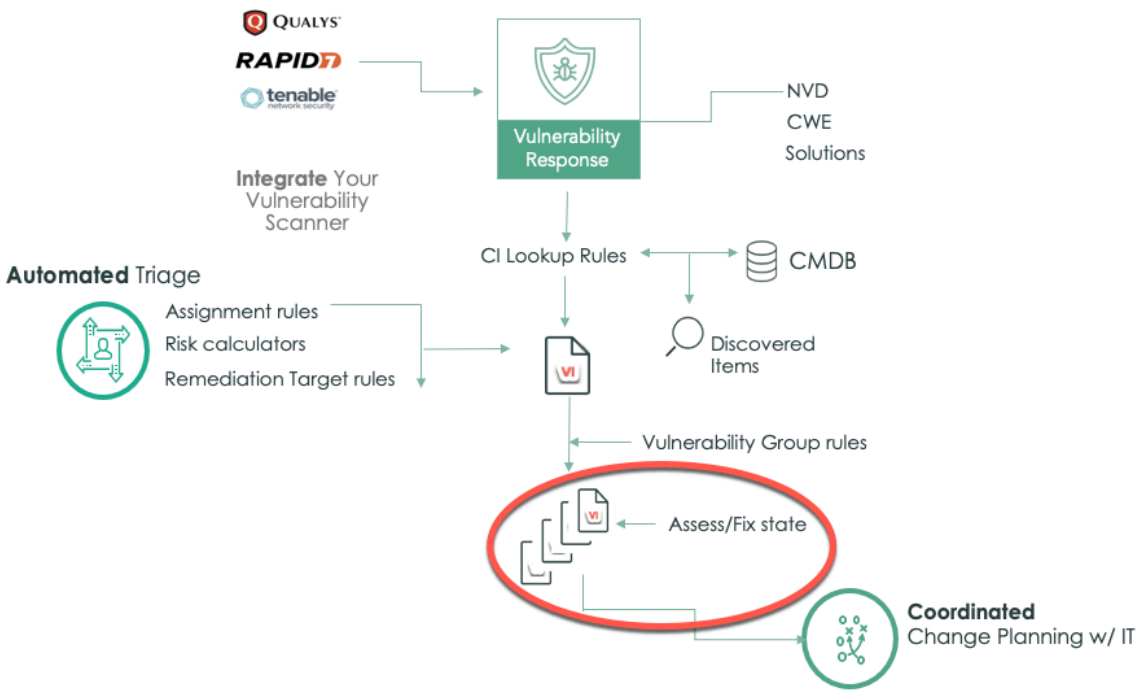
Change-Anforderungen und Change-Management sind Teil des Korrekturprozesses (Status „Bewerten/Korrektur“) im Workflow Vulnerability Response, wie in der folgenden Abbildung dargestellt. Während dieser Phase können Sie Change-Anforderungen verwenden,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um die Behebung von Schwachstellen zu initiieren und nachzuverfolgen. Sie können Change-Anforderungen direkt aus der Korrekturaufgabe erstellen und verwalten und Untersuchungs- und Korrekturaufgaben auflisten, die Lösungen für betroffene Assets für die Konfigurationselemente (CI) in Ihrer CMDB enthalten.

**Change-Anforderungen in Vulnerability Response**




## Wann Change-Anforderungen in Vulnerability Response verwendet werden sollen

Als IT-Korrekturbesitzer können Sie Change-Anforderungen aus einer Korrekturaufgabe erstellen, wenn ein manueller und kontrollierter Prozess jeglicher Art für die Änderung oder Entfernung unterstützter Konfigurationselemente (CIs) in Ihrer CMDB erforderlich ist. Das Erstellen und Verwalten von Change-Anforderungen direkt aus einem Korrekturaufgaben-Datensatz hilft Ihnen, Schwachstellen schnell zu untersuchen und zu beheben. Die VIs einer gelösten Korrekturaufgabe können beim nächsten geplanten Scan in Ihrer Now Platform gescannt und überprüft und an die automatisierte Selektierung des Vulnerability Response -Workflows zurückgegeben werden. Zu den manuellen Eingriffen, für die möglicherweise Change-Anforderungen erforderlich sind, gehören die folgenden Beispiele:

- Ein Software-Patch, eine Korrektur oder eine andere Aufgabe der IT, die für angreifbare Elemente vor der RT-Lösung erforderlich ist.
- Sie stellen fest, dass eine Teilmenge der angreifbaren Elemente in einer Korrekturaufgabe weitere Untersuchungen oder die Neuzuweisung an eine andere Abteilung erfordert.
- Sie legen fest, dass eine Teilmenge angreifbarer Elemente in einer RT mit einer großen Menge angreifbarer Elemente in eine neue Korrekturaufgabe verschoben werden kann.
- Sie können eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuordnen, um eine Duplizierung von Korrekturaufgaben zu vermeiden.

## Typen von Change-Anforderungen für eine RT

Die Anwendung Vulnerability Response verwendet die drei Arten von Serviceänderungen, die vom Produkt ITSM Change-Management in Ihrer Instanz von Now Platform® unterstützt werden – Standard, Notfall und normal. Die Art des Change, den Sie auswählen, bestimmt, welches



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Statusmodell aufgerufen wird und welcher Change-Prozess befolgt werden muss. Change-Anforderungen erfassen die detaillierten Informationen über den Change, z. B. den Grund des Change, die Priorität, das Risiko, den Typ des Change und die Change-Kategorie. Siehe Change-Typen .

Als Vulnerability Response IT-Korrekturbesitzer haben Sie die folgenden Optionen zum Erstellen von normalen, standardmäßigen und Notfall-Change-Anforderungen direkt aus einer Korrekturaufgabe:

- Sie können Change-Anforderungen erstellen, die vorab ausgefüllte Informationen aus der Korrekturaufgabe enthalten, um den Prozess zu optimieren und Zeit zu sparen.
- Sie können eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuordnen, um die Erstellung doppelter Change-Anforderungen zu vermeiden, die ähnliche Informationen und angreifbare Elemente gemeinsam nutzen.
- Mithilfe einer Reihe von Bedingungen können Sie eine Teilmenge der angreifbaren Elemente herausfiltern und eine Korrekturaufgabe aufteilen. Die von Ihnen ausgewählten Elemente werden automatisch in ein neues RT verschoben.

Sie können angreifbare Elemente anhand von Werten aus beliebigen Feldern einer Korrekturaufgabe filtern und die Change-Anforderung nur auf die Elemente anwenden, die Ihren Filterkriterien entsprechen.

**Zugehörige Informationen**

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Teilen Sie eine Korrekturaufgabe auf

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

## Bewertung des Software-Gefahrenpotenzials mit Software Asset Management (SAM)

Verwenden Sie die Anwendung ServiceNow® Risikobewertung, um die Gesamtanzahl der installierten Software für ein bestimmtes Softwarepaket für Ihre Assets zu bestimmen. Bewerten Sie bei Verwendung mit der Anwendung ServiceNow® ITSM Software Asset Management Ihr Gefährdungspotenzial, erstellen Sie angreifbare Elemente, und verwalten Sie die Korrektur für die erkannte angreifbare Software.

Bestimmen Sie Ihr Risiko für angreifbare Software, indem Sie die Informationen zu angreifbarer Software (Herausgeber, Produkt, Edition und Version) angeben, ohne die Datenbank für häufige Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVE) zu verwenden. Bewerten Sie Fälle von Zero-Day-Schwachstellen (aktueller Tag) in Software für die folgenden Fälle:

- Wenn Produkte noch keine CVE-Daten haben.
- Wenn eine Verzögerung zwischen dem Zeitpunkt besteht, zu dem eine Schwachstelle öffentlich bekannt wird, und der Aktualisierung der CVE-Daten mit der Schwachstelle im NVD.
- Wenn Sie zwischen den geplanten Scans Ihres Schwachstellenscanners mehr über die Schwachstelle erfahren.

Wenn Sie mit der Anwendung „Risikobewertung“ den Herausgeber und das Produkt der angreifbaren Software kennen, können Sie anhand der Datensätze, die die von der SAM-Anwendung erstellte installierte Software in Ihrem Netzwerk auflisten, Ihre Gefährdung durch potenziell schädliche Softwarepakete bei Bedarf bewerten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie das Ausmaß Ihrer Gefährdung durch diese Art von Schwachstelle kennen, können Sie proaktiv reagieren, indem Sie eine rote Warnung implementieren und die Software deinstallieren oder Ihr Security Operations Center (SOC) informieren, um nach einem bestimmten Patch zu suchen. Sie können angreifbare Elemente erstellen und dem Korrekturspezialisten Aufgaben zur weiteren Untersuchung der Korrektur zuweisen. Zeigen Sie eine Liste der Korrekturaufgaben (VUL) an, um sicherzustellen, dass die gewünschten angreifbaren Elemente erstellt und der VUL korrekt zugeordnet wurden.

**Zugehörige Informationen**

Konfigurieren Sie die Risikobewertung

Bewerten Sie Ihre Gefährdung durch angreifbare Software

## Schwachstellen-Krisenmanagement

Erstellen und verfolgen Sie kritische Schwachstellen-Ereignisse über den Vulnerability Crisis Management-Workflow. Erstellen Sie Schwachstellenbewertungsdatensätze, erfassen Sie Schlüsselattribute der Schwachstelle, um das Risiko zu berechnen, führen Sie eine Bewertung durch, um das Gefährdungsniveau zu ermitteln, und beziehen Sie Stakeholder ein, um eine koordinierte und schnelle Reaktion auf Schwachstellen zu erhalten.

## Verwalten von Schwachstellen-Krisenevents

Vulnerability Crisis Management ist ein vollständiger Workflow zur Behandlung von Schwachstellen-Krisenereignissen mit den folgenden Funktionen.

- Identifizieren Sie angreifbare Konfigurationselemente effizient, indem Sie kritische Schwachstellen mit dem Softwareinstallationsbestand aus Software Asset Management und Software Bill of Materials (SBOM), vom Scanner gemeldeten Schwachstellen und Configuration Management Database (CMDB)korrelieren.
- Konvertieren Sie Bewertungsergebnisse in angreifbare Elemente zur Korrektur.
- Initiieren Sie einen schwerwiegenden Security Incident, um eine schnelle und koordinierte Reaktion auf die Bedrohung sicherzustellen.
- Arbeiten Sie mit Teams im gesamten Unternehmen zusammen, um eine einheitliche Reaktion auf Schwachstellen zu ermöglichen.
- Stellen Sie funktionsübergreifenden Stakeholdern und beteiligten Teams regelmäßige Statusberichte bereit, um während der Krise Transparenz und Kommunikation zu gewährleisten.

## Vulnerability Crisis Management mit dem Arbeitsbereich für Schwachstellenbewertungen

Bei der Identifizierung einer relevanten Schwachstelle erstellt der Schwachstellen-Ereignismanager einen Schwachstellenbewertungsdatensatz mit Informationen zur Threat Intelligence-Quelle, den Schwachstellenmerkmalen und den betroffenen Produkten. Diese Informationen werden für weitere Auswirkungs- und Gefährdungsanalysen verwendet.

Nachdem der Datensatz für eine relevante Schwachstelle erstellt wurde, wird eine Risikobewertung durchgeführt. Diese Bewertung umfasst die strukturierte Risikobewertung, die Überprüfung des Datensatzes und die Beobachtungen des Analysten, der die Aufgabe ausführt. Die anfängliche Risikopunktzahl für eine relevante Schwachstelle wird anhand der Attribute berechnet, die zum Zeitpunkt der Event-Erstellung verfügbar sind. Die Risikopunktzahl für die Bewertung kann sich ändern, wenn zusätzliche Informationen verfügbar werden. Verwenden Sie die Risikopunktzahl, um die potenziellen Auswirkungen der Ausnutzung zu bestimmen und Antwortprioritäten festzulegen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem die Bewertung für eine Schwachstelle von Interesse erstellt und festgestellt wurde, dass sie ein Risiko für die Infrastruktur der Organisation darstellt, können Sie die Bedrohung weiter analysieren, indem Sie die Risikobewertung mit einer eingehenden Risikobewertung mit dem Softwareinstallationsbestand von Software Asset Management, Software Bill of Materials aktualisieren. (SBOM)-Bestand, vom Scanner gemeldete Schwachstellen und Configuration Management Database (CMDB). Betroffene Konfigurationselemente und Anwendungen werden automatisch durch eine Bewertung identifiziert. Zusätzliche betroffene Elemente können manuell hinzugefügt werden.

Sobald die Bewertung abgeschlossen ist, können angreifbare Elemente oder angreifbare Anwendungselemente für die Gefährdungsergebnisse erstellt werden, denen noch kein angreifbares Element zugeordnet ist. Der Risikopunktzahl-Rechner für angreifbare Elemente kann genutzt/konfiguriert werden, um die Risikopunktzahl für angreifbare Elemente anzupassen, die mit Schwachstellenbewertungsdatensätzen verknüpft sind. Dem Schwachstellenbewertungsdatensatz können eine Gefährdungsstufe und eine Ereignispriorität zugewiesen werden. Basierend auf der Event-Priorität kann der Manager für Schwachstellenereignisse die Schwachstellenbewertung mit einem schwerwiegenden Security Incident vorschlagen, heraufstufen oder verknüpfen.

Verwenden Sie Management schwerwiegender Sicherheits-Incidents, um Korrekturaktivitäten nachzuverfolgen und zu verwalten, laufende Security Incidents zu verknüpfen, Ad-hoc-Aufgaben zu erstellen, betroffene Teams einzubeziehen, Statusberichte zu senden und mithilfe der in Management schwerwiegender Sicherheits-Incidentsverfügbaren Zusammenarbeitsintegrationen zusammenzuarbeiten.

## ServiceNow® Software Asset Management und Software Bill of Materials (SBOM) Bewertungsverarbeitungslogik

Unter Verwendung der Daten Software Asset Management werden die CPEs aus NVD für das CVE und dann die Erkennungsmodelle mithilfe der Zeichenfolgenabgleichslogik abgerufen. Nach dem Abrufen der Discovery-Modelle wird ein Scan nach zugehörigen Installationen ausgeführt, die zugehörigen Konfigurationselemente werden abgerufen und die Tabelle „Betroffene Konfigurationselemente“ wird ausgefüllt. Sie können weitere Details wie Herausgeber, Produkt, Version und Edition angeben. Darauf aufbauend werden alle übereinstimmenden Discovery-Modelle und die Softwareinstallationen für den Datensatz abgerufen. Anschließend werden die zugehörigen Konfigurationselemente abgerufen und die Tabelle „Betroffene Konfigurationselemente“ wird erneut ausgefüllt.

Für SBOMwird die zugehörige Software für das CVE aus der zugehörigen Tabelle (m2m) (zwischen CVE und Software) abgerufen. Nach dem Abrufen der Softwaredetails werden die zugehörigen SBOM-Komponenten identifiziert, indem das Produkt und die Version aus der SBOM-Komponente mit dem Produkt und der Version der identifizierten Software abgeglichen werden.

Nachdem die zugeordneten Komponenten gefunden wurden, werden die mit den Komponenten verbundenen Entitäten abgerufen. Das Produktmodell aus den Entitäten und das zugehörige CI (falls gefunden) werden abgerufen, und das Konfigurationselement wird in der Tabelle „Betroffene Konfigurationselemente“ gespeichert. Wenn das Konfigurationselement keine angreifbaren Elemente enthält, können Sie es zum Erstellen des angreifbaren Elements verwenden. Wenn kein Konfigurationselement gefunden wird, wird das Produktmodell in der Tabelle „Betroffenes Softwaremodell“ gespeichert und kann zum Erstellen von angreifbaren Anwendungselementen verwendet werden.

Weitere Informationen zur Verwendung des Vulnerability Crisis Management-Workflows finden Sie unter Arbeitsbereich„Schwachstellenbewertung“ verwenden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zugehörige Informationen**

Erkunden der Schwachstellenbewertung

Erkunden Sie den Arbeitsbereich „Schwachstellenbewertung“.

Registerkarte „Bewertung“

## Domain Separation und Vulnerability Response

Die Domänentrennung wird in Vulnerability Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

## Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

## So funktioniert Domain Separation in Vulnerability Response

Mit der Domänentrennung können Sie VR-Verfahren (Vulnerability Response) für den gesamten Kundenstamm standardisieren, den Sie bedienen, mit geringeren Betriebskosten und einer höheren Servicequalität.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt und niemals für andere Clients verfügbar sind.

### Unterstützung der Domänentrennung in Vulnerability Response nach Versionsveröffentlichungen

| Release | Support-Stufe | Notizen |
|---|---|---|
| Orlando | Standard | |
| Paris | Standard | |
| Quebec | Standard | |
| Rome | Standard | |
| San Diego | Standard | |
| Tokio | Standard | |
| Utah | Standard | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Unterstützung der Domänentrennung in Vulnerability Response nach Versionsveröffentlichungen (Fortsetzung)**

| Release | Support-Stufe | Notizen |
|---|---|---|
| Vancouver | Standard | |
| Washington DC | Standard | |

Die Domänentrennung für die Anwendung Vulnerability Response umfasst die folgenden Produktfunktionen:

- Erfasst die angreifbaren Elemente von Scannern von Drittanbietern (z. B. Qualys, Rapid 7 oder Tenable) in der richtigen Domäne. Die Daten werden in derselben Domäne wie der Integrationsbenutzer erfasst, dessen Anmeldeinformationen für die Integration verwendet werden.
- Scannt bestimmte Assets von Vulnerability Response in der Domäne, von der sie angefordert wurden, erneut.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen von den Scannern mit den CIs in der CMDB der Domäne des Integrationsanwenders übereinstimmen.
- Berechnet Risikopunktzahlen auf der Ebene des angreifbaren Elements gemäß dem Risikopunktzahl-Rechner, der in derselben Domäne wie die des Integrationsbenutzers definiert ist.
- Korrekturzielregeln werden für angreifbare Elemente gemäß den Korrekturzielregeln ausgeführt, die in derselben Domäne wie die des Integrationsbenutzers definiert sind.
- Regel für Korrekturaufgaben kann definiert werden und in derselben Domäne wie die Domäne des Integrationsbenutzers bleiben.
- Korrekturaufgaben, die mithilfe der Regeln für Korrekturaufgaben erstellt werden, bleiben in derselben Domäne wie die Gruppenregeln.
- Der Zurückstellungs-Workflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.
- Berichte und Dashboards zeigen die Status angreifbarer Elemente an, z. B. Alter des angreifbaren Elements, offene angreifbare Elemente nach CI, Schwachstellen nach Auswirkung und Status des Korrekturzieldatums in der Domäne, zu der es gehört.
- Wissen von Scannern von Drittanbietern oder der National Vulnerability Database (NVD) kann in der globalen Domäne erfasst werden, und Daten können über mehrere Clients hinweg gemeinsam genutzt werden.

**Hinweis:**
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz bei der Trennung getrennter Domänen in der NOW-Plattform.

Weitere Informationen zum Erstellen und Unterstützen von domänengetrennten Importen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration und Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge.

## Anwendungsfälle

Die Anwendung Vulnerability Response verwaltet den Lebenszyklus eines angreifbaren Elements End-to-End. Die folgenden Anwendungsfälle sind für die Domänentrennung geeignet:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Erfassen** Sie angreifbare Elemente (Schwachstellen in Asset) aus Ihrer Drittanbieterintegration.
  - Daten aus mehreren Instanzen erfassen
  - Deduplizieren Sie das angreifbare Element
  - Mit CMDB-CI abgleichen
- **Anreicherung** von angreifbaren Elementen mit Risikopunktzahlen und Korrekturzieldaten
  - Asset-Ergänzung (CMDB)
  - Ergänzung der Risikopunktzahl und des Korrekturzieldatums
- **Gruppieren** Sie angreifbare Elemente, und weisen Sie die Korrekturaufgabe zu
  - Gruppieren Sie die angreifbaren Elemente automatisch
  - Weisen Sie die Korrekturaufgabe automatisch zu
- **Beheben**
  - Korrekturaufgaben
  - Umfassender Lebenszyklus der Korrektur
  - Zurückstellungs-Workflow
- **Messen Sie** die Sicherheitslage der Organisation und das Schwachstellenmanagementprogramm
  - Schwachstellentrend, angreifbarstes Asset, Schwachstelle nach Alter
  - Korrekturstatus nach Korrekturzieldatum

## Setup

Das Einrichten der Domänentrennung für Vulnerability Response erfordert keine zusätzlichen Schritte. Alle Vulnerability Response -Tabellen erfassen die Domänenspalte, nachdem die Instanz domänengetrennt wurde. Sie können Importdaten der Schwachstellenintegration in bestimmte Domänen leiten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

## Domänengetrennte Daten

Daten können domänengetrennt sein, was bedeutet:

- Angreifbare Elemente, die von Scannern von Drittanbietern erfasst werden, verbleiben in derselben Domäne wie die Domäne des Integrationsanwenders und sind von keiner anderen Domäne aus zugänglich.
- Schwachstellen, angreifbare Elemente (Instanzen) oder Assets in einer Domäne können nicht aus anderen Domänen angezeigt werden.
- Der Risikobewertungsalgorithmus, die Korrekturaufgabenregeln und die Korrekturzielregeln können von niemandem außerhalb der Domäne angezeigt werden.
- Schwachstelleninformationen aus dem NVD können in der globalen Domäne vorhanden und für alle Kunden freigegeben werden.
- Korrekturaufgaben in einer Domäne können nicht von einer anderen Domäne aus angezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zurückstellungs-Workflows, die in einer Domäne erstellt wurden, sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen sind in der Domäne enthalten, zu der sie gehören.

### Wie Schwachstellenanalysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen ihre eigene Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen und CI-Suchregeln.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können ihre eigenen Zurückstellungs- und Change-Management-Workflows erstellen.
- Analysten können ihre eigenen Korrekturaufgabenregeln und Risikobewertungslogik erstellen, um Schwachstellen genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenbenutzer erstellen ein manuelles angreifbares Element und schließen das Element.

### Geschäftslogik und Prozesse, die nach Instanzbesitzern domänengetrennt werden können

- Vulnerability Response -Benutzer und -Gruppen
- Vulnerability Response-Integrationen
- Vollständige Setup-Konfiguration (Benutzer- und Gruppenverwaltung, Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen, CI-Suchregeln, Korrekturaufgabenregeln, Risikorechner, Korrekturzielregeln usw.)
- Vollständiger Korrekturlebenszyklus einschließlich Zurückstellung
- Regelmäßige Aufgaben

**Zugehörige Informationen**

Domänentrennung für Service Provider

## Vulnerability Response – Implementierung

Führen Sie die in den folgenden Abbildungen dargestellten Schritte aus, um die Anwendung Vulnerability Response aus dem ServiceNow Storeherunterzuladen, in Ihrer Instanz von Now Platform® ] zu installieren und mit dem Setup-Assistenten zu konfigurieren.

Die folgenden Abbildungen zeigen ein Installations- und Konfigurationsbeispiel für die Installation des Basissystems, der Anwendung Vulnerability Response, und einer Scanner-Anwendung einer Drittpartei, der Anwendung Qualys. Erforderliche Rollen und obligatorische Aufgaben sowie optionale Schritte werden ebenfalls aufgelistet.

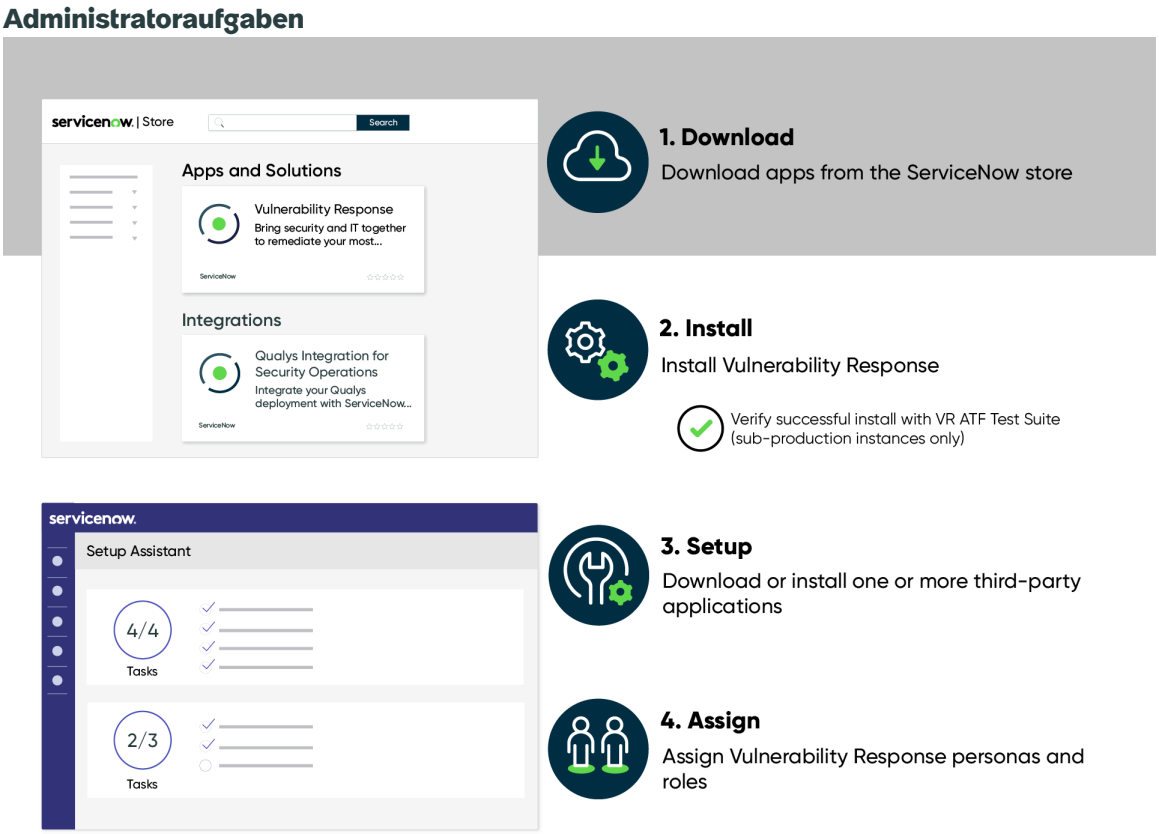
- Weitere Informationen zu den einzelnen Schritten, die in den folgenden Abbildungen dargestellt werden, und eine Prüfliste mit Links zu unterstützender Dokumentation finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response ..
- Sie können die in diesem Beispiel vorgestellten Konzepte und die Reihenfolge der Schritte auf die Installation und Konfiguration anderer unterstützter Anwendungen für Vulnerability



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Responseerweitern. Eine Liste der Support-Anwendungen finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen.

- Die Administratorrolle ist erforderlich, um die Anwendung Vulnerability Response und die Anwendung Qualys Vulnerability, die für dieses Beispiel verwendet werden, herunterzuladen und zu installieren.
- Die Administratorrolle weist Benutzern und Gruppen auch die Persona „Schwachstellenadministrator“ [sn_vul.vulnerability_admin] und andere Persona-Rollen Vulnerability Response zu.




Die Rolle „sn_vul.vulnerability_admin“ konfiguriert die Anwendungen Vulnerability Response und Qualys im Setup-Assistenten und überprüft die erwarteten Ergebnisse.

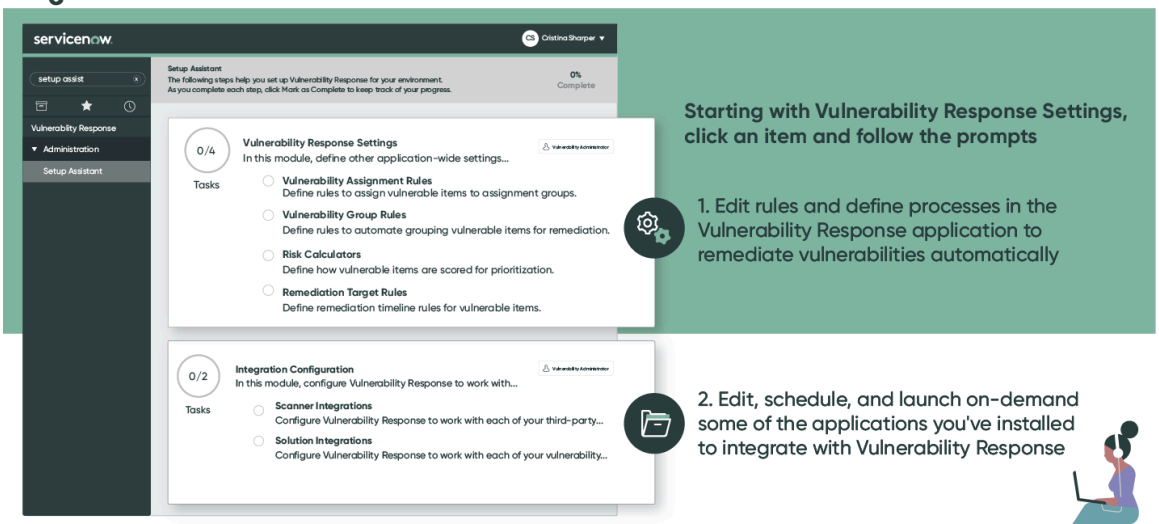
Befolgen Sie die Schritte und Eingabeaufforderungen im Setup-Assistenten, beginnend mit dem Abschnitt Vulnerability Response-Einstellungen, um mit der Installation und Konfiguration fortzufahren. Die Überprüfung dieser Einstellungen hilft Ihnen, die Prozesse von Vulnerability Response zu verstehen und zu überprüfen, während Sie mit der Einrichtung Ihrer Umgebung fortfahren.

Erforderliche Rolle: sn_vul.vulnerability_admin oder alternativ admin.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Aufgaben des Schwachstellenadministrators**




**Roles required:** sn_vul.vulnerability_admin or admin

Überprüfen Sie die Beschreibungen, Standardeinstellungen und Demodaten, die Sie mit den -Anwendungen in den folgenden Abschnitten installiert haben:

- Zuweisungsregeln für Schwachstellen – weisen angreifbare Elemente (VIs) automatisch der entsprechenden Zuweisungsgruppe zu.
- Regeln für Korrekturaufgaben – Gruppieren angreifbare Elemente (VIs) automatisch, wenn sie basierend auf bestimmten Bedingungen importiert werden.
- Risikorechner: Der Risikorechner ist standardmäßig aktiviert.
- Korrekturzielregeln: Definieren Sie Korrekturzeitachsen für VIs und Korrekturaufgaben (RTs).
- Überprüfen und bearbeiten Sie die Einstellungen für die von Ihnen installierten Anwendungen von Drittanbietern und installierten Lösungen, und definieren Sie Bedingungen für Ihre Datenimporte. Geben Sie Ihre Drittpartei-Kontoinformationen ein, und konfigurieren Sie Importeinstellungen und Zeitpläne, Suchregeln für Konfigurationselemente (Configuration Items, CI) sowie andere Einstellungen.

Weitere Informationen finden Sie unter Implementierungsprüfliste für die Anwendung Vulnerability Response ..

Weitere Informationen zum Anpassen oder Implementieren der Anwendung Vulnerability Response finden Sie unter KB1000704 .

## Vulnerability Response installieren

Bevor Sie die Anwendung Vulnerability Response in Ihrer Instanz von Now Platform ausführen, müssen Sie die Berechtigung erhalten und die Anwendung aus dem ServiceNow Storeherunterladen, in Ihrer Instanz von Now Platform ] installieren und einige Installationsschritte im Setup-Assistenten ausführen.

### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

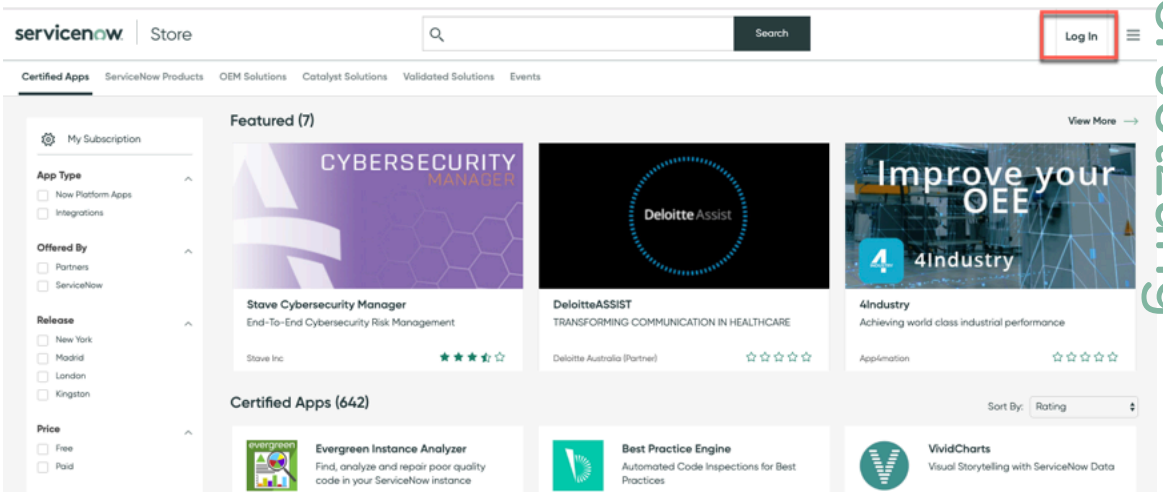
| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Ihnen die erforderlichen Rollen ServiceNow für Ihre Instanz zugewiesen sind. | Die Administratorrolle ist für die Installation erforderlich.<br><br>Wenn nicht bereits zugewiesen, weist der Systemadministrator [admin] auch die Rolle „Schwachstellenadministrator“, „sn_vul.vulnerability_admin“ oder „sn_vul.admin (veraltet)“ zu. |

Erforderliche Rolle: admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Prozedur

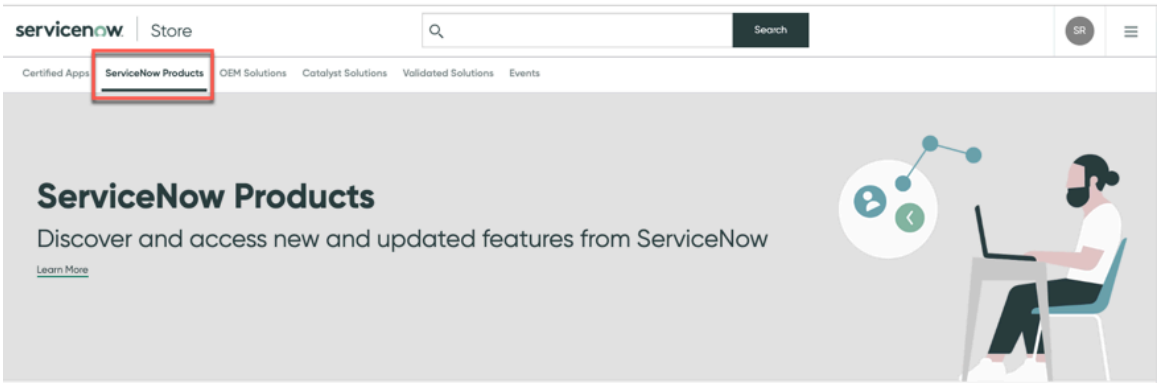
1. Um die -Berechtigung zu erhalten und die Kernanwendung Vulnerability Response herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Anmelden**.



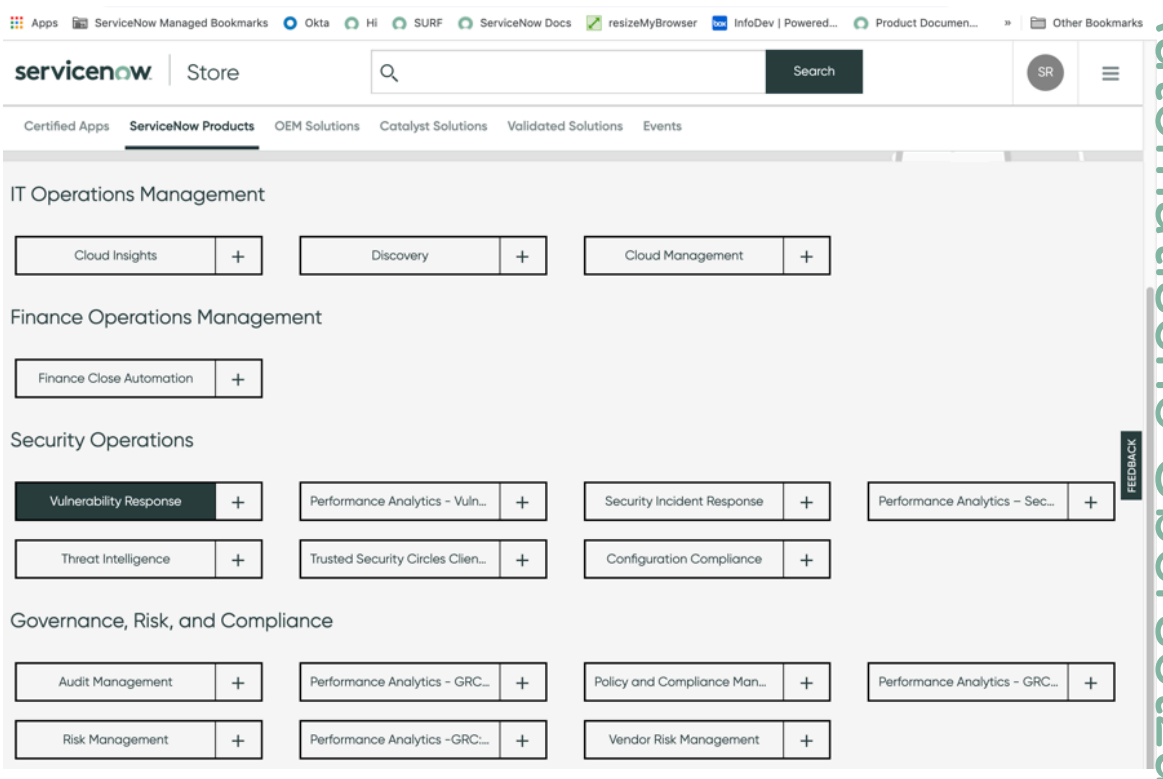

3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
4. Wenn diese Option nicht ausgewählt ist, klicken Sie auf der angezeigten Seite auf die Registerkarte **ServiceNow-Produkte**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



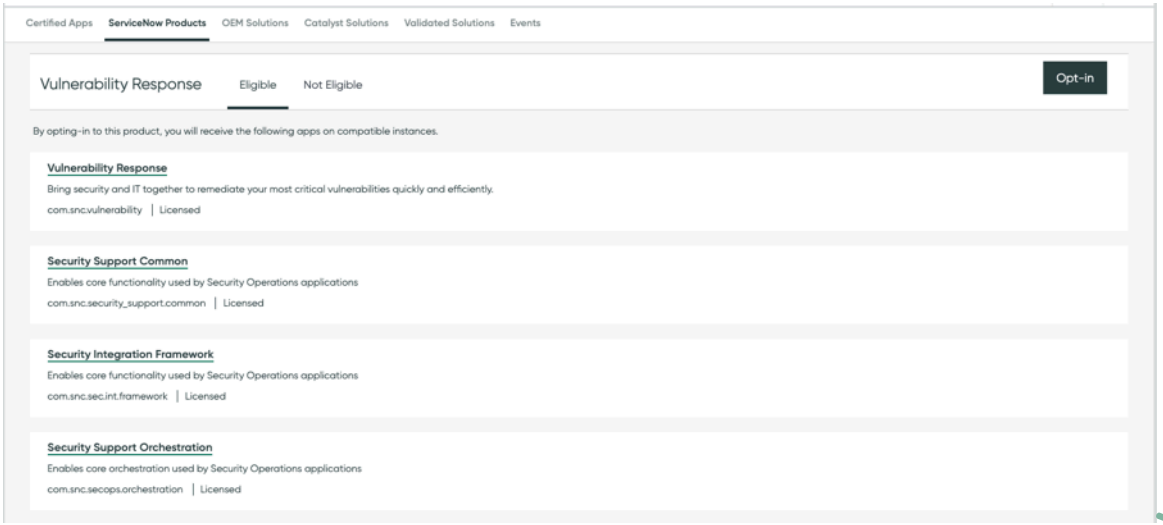

**5.** Um die zugeordneten Anwendungen anzuzeigen, für die Sie mit der Anwendung Vulnerability Response berechtigt sind, klicken Sie auf der Produktlistenseite auf das Produkt **Vulnerability Response**.



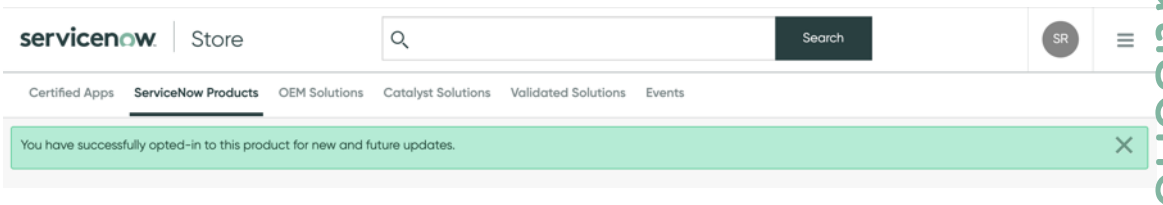

Auf der Registerkarte Berechtigt werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Um weitere Informationen zu einer Anwendung zu erhalten, klicken Sie auf einen Link.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Opt-in**, um die Kernanwendung Vulnerability Response zu erhalten.
7. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
   Eine Nachricht wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung entschieden haben.




Wenn die Registerkarte ServiceNow Produkte ausgewählt und angezeigt wird, ersetzt ein grünes Häkchen das Pluszeichen rechts neben der Anwendung Vulnerability Response, wie in der folgenden Abbildung dargestellt.

Nachdem Sie die Nutzungsbedingungen und verwalteten Berechtigungen für eine der Anwendungen auf der Registerkarte „ **ServiceNow-Produkte** “ akzeptiert haben, können Sie auf der Seite „Produktliste“ auf das Pluszeichen (+) klicken, um die Berechtigung zu erhalten und sich für die anderen Anwendungen in diesem zu entscheiden Seite mit einem einzigen Klick.

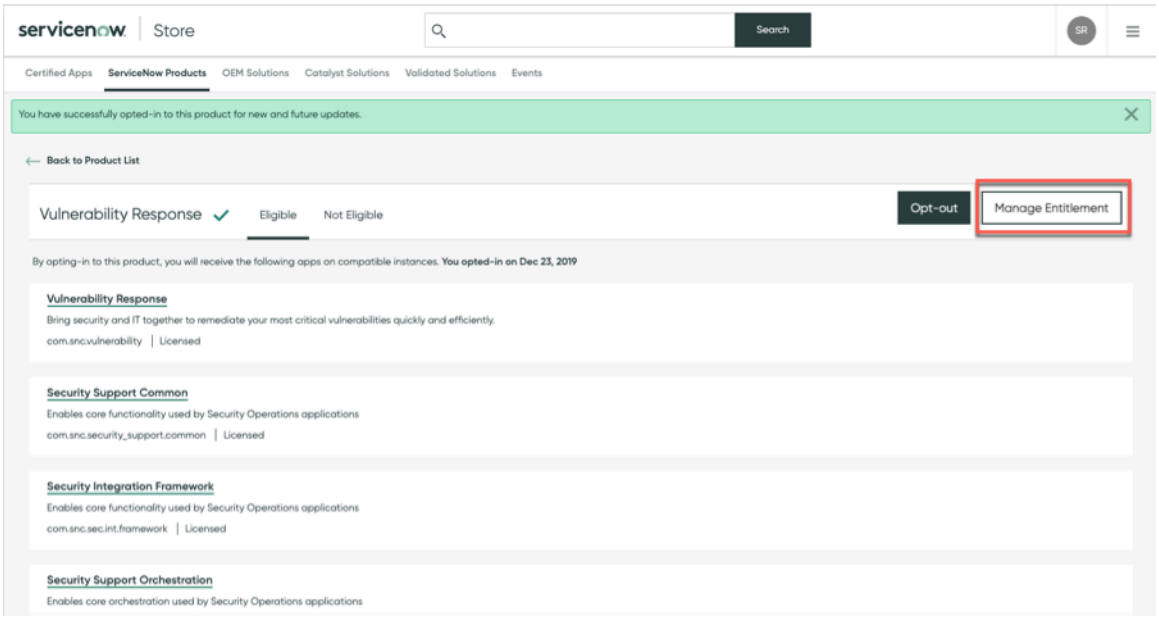
8. Fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Now Platform -Instanz zu installieren.
9. **Wahlweise:** Alternativ führen Sie die folgenden Schritte aus, um Ihre Berechtigung für die Anwendung Vulnerability Response in anderen Instanzen von Now Platform zu verwalten.

   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung Vulnerability Response, um sie anzuzeigen.

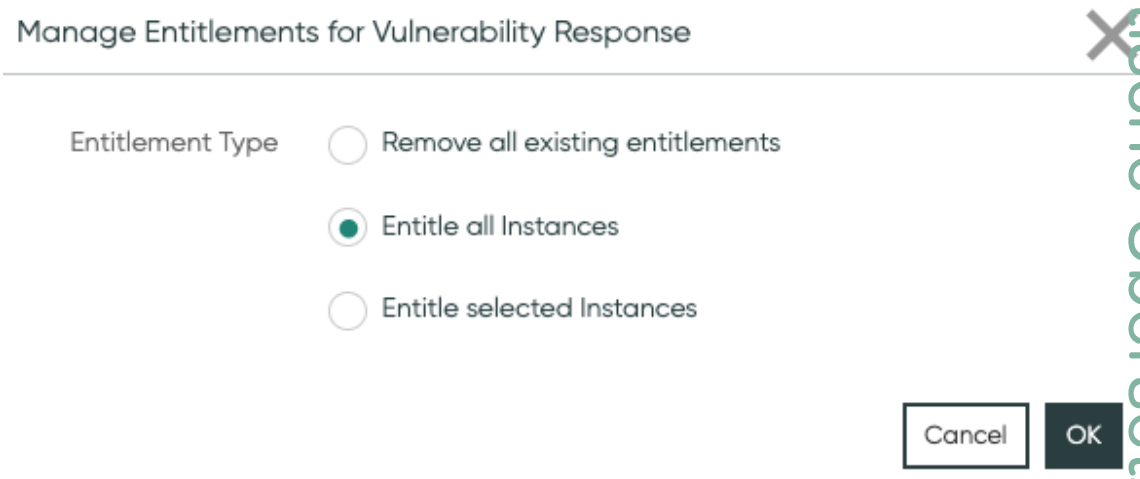
   b. Klicken Sie bei ausgewählter Registerkarte Berechtigt auf **Berechtigung verwalten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**c.** Wählen Sie im angezeigten Dialogfeld „Berechtigungen für Vulnerability Response verwalten“ eine der folgenden Optionen aus:



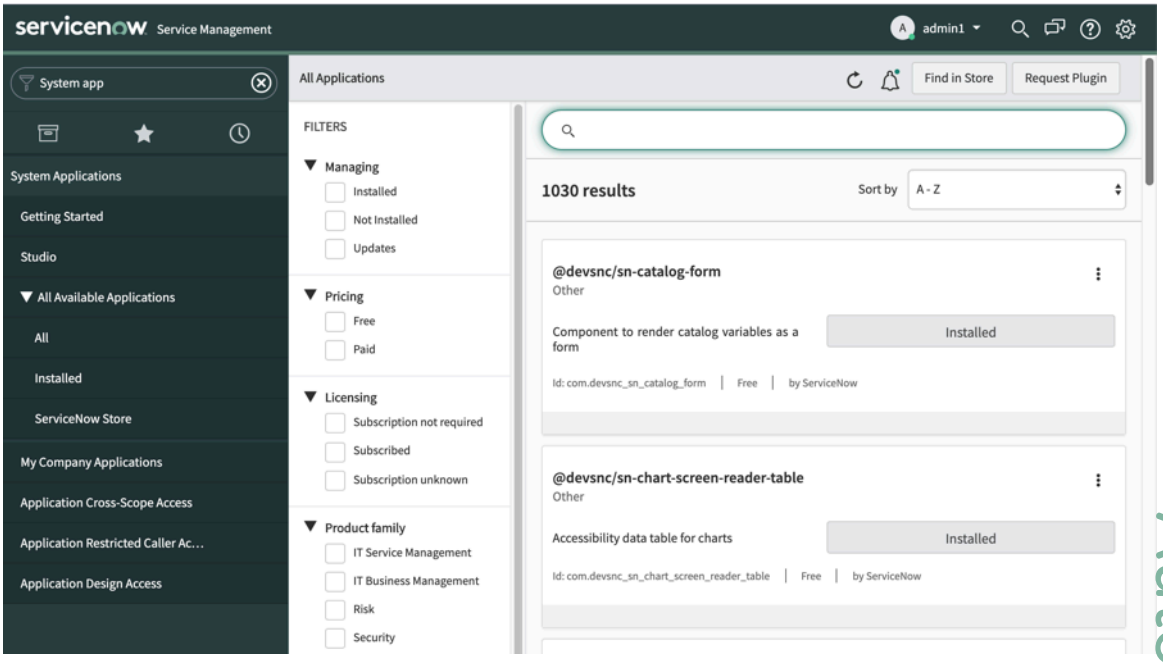

**d.** Klicken Sie auf **OK** oder **Abbrechen**, um fortzufahren.
Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihren Now Platform Instanzen zu installieren.

**10.** Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Response installieren möchten.

**11.** Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

Automatische Übersetzung

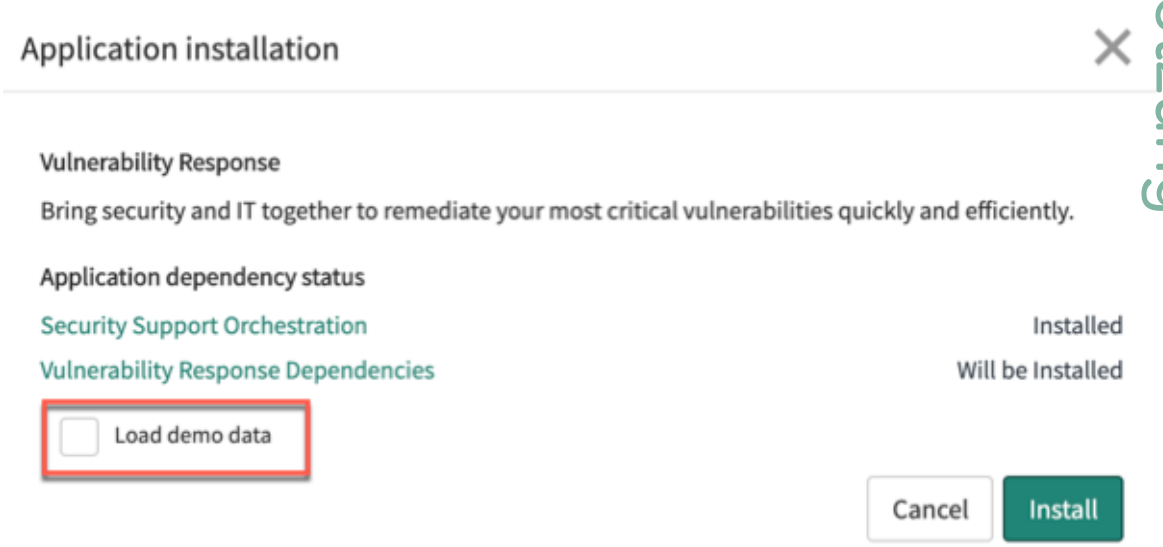
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




12. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Vulnerability Response (sn_vul), wählen Sie eine Version aus der Auswahlliste aus, und klicken Sie auf **Installieren**.
Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle zu installierenden Abhängigkeiten werden angezeigt.
13. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren**.

### Hinweis:

Wenn Sie das Kontrollkästchen Demodaten laden nicht aktivieren, können die **Demodaten** nachträglich nicht über den **Anwendungsmanager** installiert werden. Weitere Informationen dazu, wie Sie Demodaten nach der Erstinstallation installieren oder erneut installieren, finden Sie im Artikel Workaround to install demo data if application is opened (Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist) [KB0722909] in der Knowledge Base von Now Support.

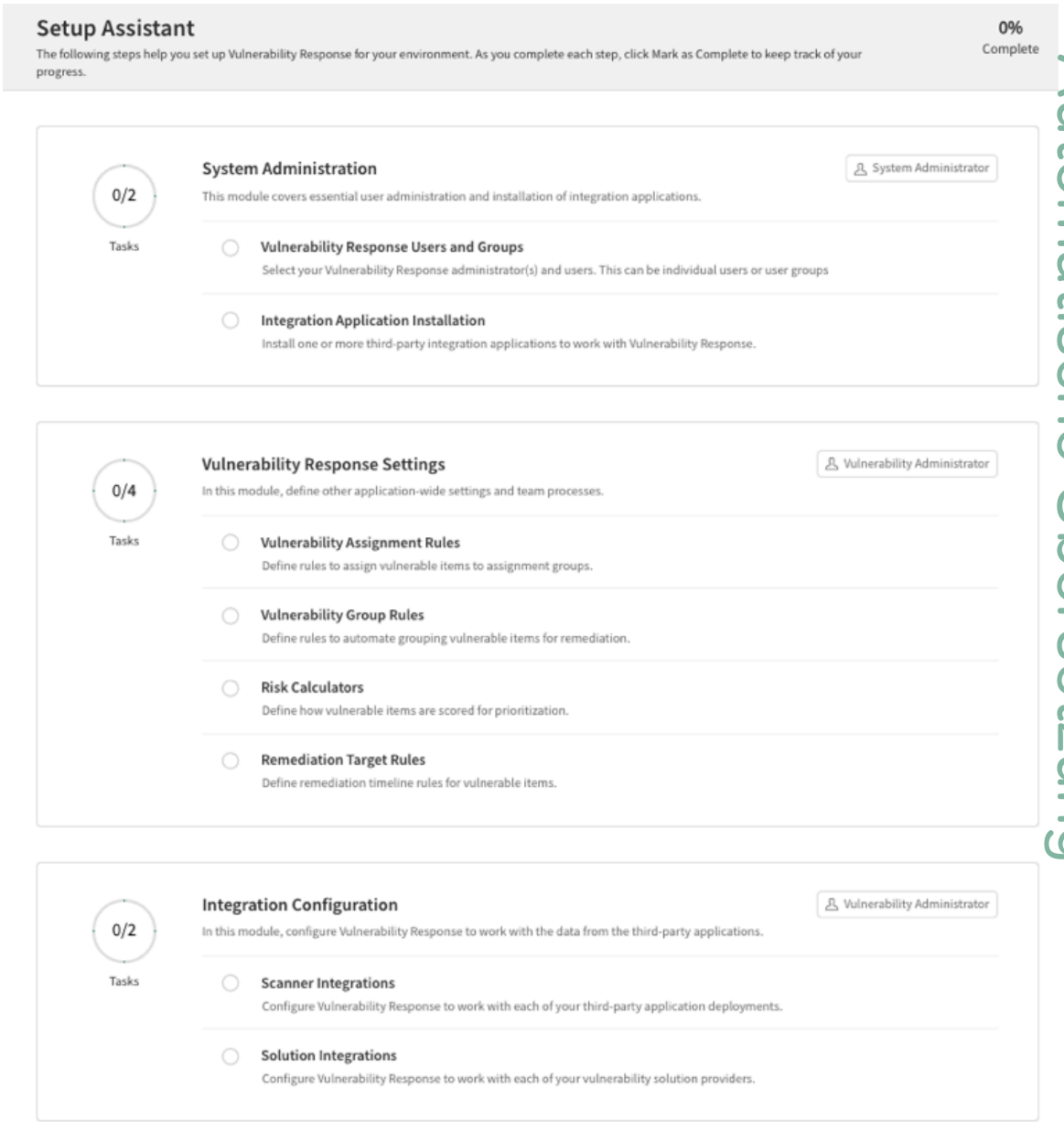



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.

14. Klicken Sie auf **Schließen**.
15. Nachdem die Installation erfolgreich abgeschlossen wurde, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.




16. Befolgen Sie die Anweisungen in den Formularen in den einzelnen Abschnitten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Weitere Informationen zu den Einstellungen von Vulnerability Response, zur Installation von Anwendungen, zur Konfiguration, zu Integrationen, Gruppenregeln, Risikorechnern und Korrekturzielregeln finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

### Mit Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

## Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Anwendungsdateien-Tabelle, sodass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert sein, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Befolgen Sie diese Schritte, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im **Filternavigator sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **UND**und dann **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

## Installierte Rollen

**Hinweis:**
Rollen, geplante Aufgaben und Tabellen für Application Vulnerability Response finden Sie unter Mit Application Vulnerability Response installierte Komponenten.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| sn_vul_cisa.configure_intelligence_integration | Konfiguriert Intelligence-Integrationen. | |
| Schwachstellenmanager und leitende Analysten<br><br>[sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)] | Aktualisiert Eigenschaften und Schwachstellenintegrationen. Die Rolle „sn_vul.vulnerability_admin“ oder „sn_vul.admin“ (veraltet) ist für die Verwaltung von Vulnerability Response erforderlich, einschließlich Schwachstellenintegrationen, Regeln für Korrekturaufgaben, Rechner, Regeln und Aufgaben für Korrekturziele, Berichte und Konfigurationen für die Integration von Drittparteien. | • sn_vul.vulnerability_write<br>• sn_vul.ciso_write<br>• sn_sec_cmn.admin<br>• sn_vul_qualys.admin (wenn Qual Vulnerability Integration installie ist.)<br>• sn_vul_r7.admin (wenn die Rapic Vulnerability Integration installie ist.) |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | | • sn_vul_shodan.admin (wenn die Shodan Exploit-Integration insta ist.)<br>• sn_vul.configure_nvd_integration (wenn die NVD-Integrationen installiert sind)<br>• treemap_admin (wenn die Performance Analytics-Anwendu installiert ist.) |
| Patch-Orchestration | Konfiguriert unterstützte Patch-Lieferanten-Integrationen von Drittparteien. Patch-Daten und Patch-Datensätze anzeigen und anwenden | • sn_vul_patch_orch.configure_pa<br>Konfigurieren Sie Patches, und wenden Sie sie an.<br>• sn_vul_patch_orch.read_patch<br>Kann Patch-Datensätze und -Da anzeigen.<br>• sn_vul_bigfix.configure_integrati<br>Konfiguriert die Anwendung „Big Patch Orchestration Integration" Diese Rolle enthält die granulare Rollen sn_vul_bigfix.read_integra und connection_admin, mit dene Benutzer eine Verbindung zur Bi Konsole herstellen kann.<br>• sn_vul_sccm.configure_integrati<br>Diese Rolle enthält die granulare Rollen sn_vul_sccm.read_integra und connection_admin, mit dene der Benutzer eine Verbindung zu SCCM-Konsole herstellen kann.<br>• sn_vul_bigfix.read_integration<br>Benutzer mit dieser Rolle könne die Datensätze der Anwendung „Vulnerability Response" und der Anwendung „BigFix Patch Orchestration Integration" sowie Patch-Orchestration-Daten anze (schreibgeschützt).<br>• sn_vul_sccm.read_integration<br>Benutzer mit dieser Rolle könne die Datensätze der Anwendung „Vulnerability Response" und de Anwendung „Microsoft SCCM P |

Automatisch übersetzt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | | Orchestration Integration“ sowie Patch-Orchestration-Daten anze (schreibgeschützt). |
| Schwachstellenanalysten<br><br>[sn_vul.vulnerability_write] | Die Rolle sn_vul.vulnerability_write ist für die Verwaltung von Schwachstellengruppen und angreifbaren Elementen und die Überwachung des Fortschritts der Fehlerkorrektur erforderlich. | • sn_vul.vulnerability_read<br>• sn_sc_cmn.write<br>• sn_vul_qualys.user (wenn Qualys Vulnerability Integration installier ist.)<br>• sn_vul_shodan.write (wenn die Shodan Exploit-Integration insta ist.) |
| V19.0: Vulnerability Event Manager<br><br>[sn_vul_analyst.vul_event_manager] | Die Rolle „sn_vul_analyst.vul_event_manager“ wird verwendet, um die Auswirkungen einer neuen Schwachstelle oder Software zu bewerten oder eine Zero-Day-Schwachstelle hinzuzufügen, um die betroffenen Assets zu identifizieren und angreifbare Elemente (AEs) zu erstellen. | • sn_sec_cmn.read<br>• canvas_user<br>• sn_vul_analyst.emergency_respo<br>• sn_vul.manage_exposure_assess |
| Andere<br><br>[sn_vul.read_all]<br><br>Die Rolle sn_vul.vulnerability_read ist veraltet. | Die Rolle sn_vul.read_all ist für alle erforderlich, die Einblick in das Schwachstellenmanagement benötigen. Zum Beispiel IT- und Sicherheitsverantwortliche oder jemand, der Detailinformationen von Dashboards auf hoher Ebene zu den Elementen anzeigen möchte, aus denen die Dashboard-Visualisierungen bestehen. | • sn_sec_cmn.read<br>• sn_vul_qualys.read (wenn Qualys Vulnerability Integration installier ist).<br>• sn_vul_shodan.read (wenn die Shodan Exploit-Integration insta ist.)<br>• pa_viewer (wenn die Performanc Analytics-Anwendung installiert<br>• sn_vul_tenable.read_integration (wenn Tenable Vulnerability Integration installiert ist.) |
| VR-Systemimportadministrator<br><br>[sn_vul.vr_import_admin] | Vom System ausgeführter Benutzer. Führt geplante Aufgaben aus.<br><br>**Hinweis:** Dieser Benutzer ist der Standard-Ausführungsbenutzer für jeden Integrationsdatensatz. Nicht ändern. | • import_admin<br>• sn_vul.vulnerability_write |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| Korrekturbesitzer<br><br>[sn_vul.remediation_owner] | Zeigen Sie die Berechtigung für angreifbare Elemente und Korrekturaufgaben an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie. Kann alle Schwachstellen und Lösungen anzeigen. Hat Schreibzugriff auf das**Feld Interne Notizen** im Lösungsdatensatz. | Enthalten in der itil-Rolle. |
| CISOs und Schwachstellenverantwortliche<br><br>[sn_vul.vulnerability_ciso] | Zeigen Sie das CISO-Dashboard in Performance Analytics für Vulnerability Response an. | • sn_vul.ciso_read<br>• sn_vul.read_all |

## Installierte Scheduled Jobs

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Füllen Sie gespeicherte OOTB-Filter für Host- und App-Modul aus | Migriert Module im Zusammenhang mit dem Host- und App-Modul. |
| Füllen Sie gespeicherte OOTB-Filter für das CC-Modul aus | Migriert Module, die sich auf das CC-Modul beziehen. |
| Füllen Sie gespeicherte OOTB-Filter für das Containermodul aus | Migriert Module, die sich auf das Containermodul beziehen. |
| Aktualisieren Sie die hostbezogenen gespeicherten Filter | Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des Hostmoduls beziehen. |
| CC-bezogene gespeicherte Filter aktualisieren | Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des CC-Moduls beziehen. |
| Aktualisieren Sie die gespeicherten Container-bezogenen Filter | Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des Containermoduls beziehen. |
| Aktualisieren Sie die App-bezogenen gespeicherten Filter | Aktualisiert alle Zusammenfassungsdaten, die sich auf gespeicherte Filter des App-Moduls beziehen. |
| Löst die Erstellung und Ausführung der Zusammenfassung für den gespeicherten Filter aus | Erstellt, aktualisiert, führt die Zusammenfassungen aus, die sich auf den gespeicherten Filter beziehen. |
| Version 19.0 von Vulnerability Response und v4.0 von Veracode Vulnerability Integration | Die Veracode-CWE-Integration ruft Veracode spezifische CWE-Daten (Common Weakness Enumeration) für Bedrohungsinformationen und Korrekturempfehlungen ab.<br><br>Die Veracode SBOM-Integration erfasst Release-, Versions- und Schwachstelleninformationen aus Veracode zu den Komponenten in Ihren Softwareprojekten. Die Integration generiert SBOMs im JSON-Format „CycloneDx“ und lädt sie in Ihre Instanz<br><br>Die Integration von Veracode-Kategorien ruft erweiterte Kategoriendaten aus Veracodeab. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| | Mit der Veracode DevOps-Integration können DevOps-Benutzer Zusammenfassungsdetails für Schwachstellenprüfungen von Drittanbietern ohne SecOps-Lizenz anzeigen.<br><br>JSON-basierte APIs für die folgenden Veracode-Integrationen: Angreifbares Anwendungselement, Scan-Zusammenfassung, Anwendungsliste. Die XML-basierten API-Versionen dieser Integrationen sind veraltet. |
| Ordnen Sie vorhandene VIs der automatischen Ausnahmeregel zu | Ordnet die automatische Ausnahmeregel automatisch vorhandenen VIs zu. |
| Erkennung von Schwachstellen automatisch schließen | Schließt automatisch die veralteten angreifbaren Erkennungen basierend auf der in der Tabelle „sn_vul_auto_close_config“ definierten Konfiguration. |
| Version 16.1:<br><br>HCL BigFix-Sammlung, Fixlet und Aktionsintegrationen. | Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit Patches aus dem Produkt HCL BigFix. |
| Zugehörige Anzahlen für alle Lösungen berechnen | Standardmäßig deaktiviert. Verarbeitet Lösungsdaten einmal pro Nacht anstatt kontinuierlich. |
| Berechnet die zugehörigen VI-Anzahlen für Schwachstelle und Korrekturaufgabe | Erfasst manuelle und VI-Importänderungen für den Tag. Gleicht Schwachstellen- und Lösungsbeziehungen ab und berechnet die Summen neu.<br><br>Lösungsdaten werden in die Warteschlange gestellt und separat von der geplanten Aufgabe „Warteschlange für Lösungsmetriken für **Schwachstellen** verarbeiten“ verarbeitet. |
| Aktivieren Sie die Zeitüberschreitung für Mid-Server | Pingt den MID-Server an und meldet nach 30 Sekunden Fehler. |
| V19.0: Überprüfen Sie das potenzielle Schwachstellenrisiko | Verarbeitet die Delta-CVEs, -Software und -Installationen, um das Risiko zu erhalten. |
| Überprüfen Sie den Ausführungsstatus WaitComplete | Markiert eine Integrationsausführung als abgeschlossen, sobald sie als vollständig abgeschlossen verifiziert wurde. |
| Überprüfen Sie das Ablaufdatum für angreifbare Elemente und Gruppen | Sendet Benachrichtigungen, wenn angreifbare Elemente oder Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen).<br><br>Überprüft, ob eine Ausnahmeregel für einen zurückgestellten VI gilt, und aktualisiert die Felder **Grund** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| | und **Bis** gemäß der Ausnahmeregel. Der Status des AEs bleibt bis zum letzten Ablaufdatum zurückgestellt. |
| Schließen Sie VITs ab, denen kein CI zugeordnet ist | Schließt automatisch angreifbare Elemente, denen kein Konfigurationselement (CI) zugeordnet ist und die seit drei Tagen nicht aktualisiert wurden. Der Status wird auf „Geschlossen/Abgebrochen“ gesetzt. |
| VI beim Löschen des Exp.-Datensatzes schließen | Schließt eine VI, wenn sie gelöscht wird. |
| Integration von Compliance-Ergebnissen | Importiert Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerken mit autorisierenden Quellen zur Verarbeitung in der Anwendung Configuration Compliance. |
| Integration von Compliance-Ergebnisauffüllung | Als Teil einer verketteten Integrationsausführung mit Tenable.io Assets Integration importiert Konfigurationsbewertungsdaten für ignorierte Assets, die erkannt werden (importiert durch Assets-Integration). |
| CR-Statussynchronisierung | Das Skript passt alle vorhandenen Korrekturaufgaben in CHG-Beziehungen nach, sodass sie synchronisiert werden. Aktiviert die zukünftige Synchronisierung. |
| Version 15.0 Integration von Anmeldeinformationen | Importiert und speichert vorübergehend Tenable.io Anmeldeinformationen, die für den Zugriff auf den Scanner für erneute Scans bei Bedarf verwendet werden. |
| CWE Comprehensive 2000-Integration | Schwachstellenintegration, die Schwachstelleninformationen aus dem CWE-Datensatz (Common Weakness Enumeration) abruft, der von MITRE erstellt wurde. |
| V18.0: Veraltete Split-Aktionsdatensätze löschen | Täglicher Auftrag zum Bereinigen veralteter Datensätze in Zwischentabellen für aufgeteilte Aufgaben. |
| Deaktivieren Sie VR-Lösungen, wenn die Lösungsanwendung nicht aktiv ist | Deaktiviert und blendet die Funktion Vulnerability Solution Management aus, wenn die Anwendung Solution Management for Vulnerability Response nicht installiert ist. |
| Bewerten Sie die Korrekturziele | Legt Korrekturzieldaten für alle angreifbaren Elemente fest oder aktualisiert sie. Bestimmt den Status der Korrekturzieldaten anhand von Regeln. |
| • Die Erkennungen für einen aktualisierten Schlüssel für Rapid7 werden korrigiert<br>• Die Erkennungen für aktualisierten Schlüssel für Qualys werden korrigiert<br>• Die Erkennungen für einen aktualisierten Schlüssel für Tenable werden korrigiert | Bereinigt Erkennungsdaten automatisch durch eine integrationsspezifische geplante Aufgabe, die nach dem Upgrade auf Vulnerability Responseausgelöst wird. |
| Version 16.1: Generieren eines Fehlerkorrektur-Digest | Dieser Auftrag generiert automatisch eine E-Mail-Zusammenfassung für alle Benutzer in der Benutzergruppe „Korrekturbesitzer“. Die Aufgabe ist standardmäßig aktiviert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| V19.0: Von CISA ausgenutztes CVE in Risikokonfiguration einfügen | Fügt CISA-CVEs in die Risikokonfigurationstabelle ein, um das Risiko zu berechnen. |
| V18.0: Fügen Sie klassische Korrekturaufgaben in eine einheitliche Korrekturaufgabe ein | Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Benutzeroberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_remediation_task). |
| Integration der Microsoft Security Response Center-Lösung | Vulnerability Solution Management -Integration, die Lösungen aus dem Microsoft Security Response Centerabruft. |
| Version 16.1: Microsoft SCCM-Integrationen für Sammlung, Patch-Update und Bereitstellungen | Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit Microsoft SCCM-Patches. |
| Gedrosselten Integrationsprozess aufnehmen | Erstellt den Integrationsprozess für Shodan Exploit Integration. |
| Füllen Sie den Text der betroffenen Produkte aus | Behandelt nach dem Upgrade vorhandene Lösungen, um den Text der betroffenen Produkte auszufüllen. Dieser Auftrag wird nur einmal ausgeführt. |
| Füllen Sie die neue CR-Anzahlspalte aus | Füllt die neue CR-Anzahlspalte für Kunden automatisch mit vorhandenen Daten in der Tabelle „Korrekturaufgabe“ [sn_vul_vulnerability] aus. |
| Warteschlange für Metriken der Schwachstellenlösung verarbeiten | Stellt Lösungsdaten kontinuierlich in die Warteschlange und verarbeitet sie, wenn sie importiert oder manuell aktualisiert werden. |
| Füllen Sie Datensätze in der Zuordnungstabelle für Schwachstellenanbieter aus<br><br>Füllen Sie Datensätze in der Zuordnungstabelle der Schwachstellenanbieter für Rapid7-Schwachstellen aus | Fügt Datensätze in die Zuordnungstabelle der Schwachstellenanbieter für vorhandene Schwachstellen ein. |
| Öffnen Sie zurückgestellte Schwachstellengruppen erneut | Öffnet zurückgestellte Korrekturaufgaben erneut, wenn das Zurückstellungsdatum abgelaufen ist. |
| Wenden Sie alle Schwachstellenzuweisungsregeln erneut an | Wertet Zuweisungsregeln für alle **offenen** AEs neu aus. |
| Version 16.5: Anzahl der Neuzuweisungen für Zuweisungsregeln | Wird täglich ausgeführt und veröffentlicht die Gesamtzahl der VIs und Korrekturaufgaben, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen wurden. |
| Red Hat Solution Integration | Vulnerability Solution Management -Integration, die Lösungen aus dem Red Hat Security Advisoryabruft. |
| V17.1: Doppelte VITs in Korrekturaufgabe aktualisieren und beheben | Sucht nach doppelten angreifbaren Elementen für die Elemente in der Korrekturaufgabe, bei denen „Doppelte VIs automatisch aktualisieren“ aktiv ist. |
| Aktualisieren Sie die zugeordneten angreifbaren Elemente für eine | Aktualisiert die Korrekturaufgabe mit angreifbaren Elementen, die den Kriterien Filtergruppe und Bedingungsgruppen entsprechen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| regelbasierte Korrekturaufgabe ohne Korrekturaufgabe | |
| Reparieren Sie fehlerhafte angreifbare Elemente, die zuletzt geöffnet und geschlossen wurden | Repariert vorhandene UI-Daten, die durch zuvor behobene Fehler beschädigt wurden. |
| Rechner erneut ausführen | Wendet die Rechner erneut auf alle angreifbaren Elemente an, die von der Änderung betroffen sind. Dies löst eine Neuberechnung der kumulativen Risikopunktzahlen ihrer Korrekturaufgabenaus.<br>**Hinweis:**<br>Das erneute Ausführen von Rechnern kann je nach Umgebung sehr lange dauern. |
| Importsätze für abgebrochene Integration wiederholen | Wiederholt abgebrochene Integrations-Importsätze. Versucht 5 Mal, bevor ein Fehler zurückgegeben wird. |
| Integrationsprozesse wiederholen | Versucht Integrationsprozesse. Versucht 5 Mal, bevor ein Fehler zurückgegeben wird. |
| Rollup der Werte für angreifbare Elemente zu Schwachstelle und Gruppe | Berechnet die Risikopunktzahl, die Anzahl der angreifbaren Elemente und den Status des Korrekturziels für Korrekturaufgabenmit dem Rollup-Rechner. |
| Führen Sie den Schweregradrechner nach der Heraufstufung des Schwachstelleneintrags aus | Führt den Schweregradrechner aus, nachdem eine zuvor fehlende Schwachstelle mit ihrer Punktzahl und anderen Daten von einem Drittanbieter aktualisiert wurde, z. B. Qualys Cloud Platform, Rapid7 Nexpose. |
| V19.0: Risikobewertung für konfigurierte CVEs ausführen | Berechnet das Risiko für alle CVE-Datensätze in der Tabelle „Risikokonfiguration“. |
| V19.0: Führen Sie Software-Exposure aus | Berechnet das Risiko für alle Softwaredatensätze in der Tabelle „Risikokonfiguration“. |
| Datenquellenprozessor für geplante Schwachstelle | Überprüft die Importwarteschlange auf zu verarbeitende Einträge und weist basierend auf den verfügbaren Ressourcen einen geplanten Importauftrag zu. |
| Geplante Anhangsbereinigung des Schwachstellenintegrationsprozesses | Entfernt XML-Anhänge für die Integration, sobald sie 14 Tage alt sind. Diese Aufbewahrungszeit ist nicht konfigurierbar. |
| Zeitüberschreitungsprüfung für geplante Schwachstellenintegration | Bricht Integrationsausführungen ab, die mehr als 60 Minuten in Anspruch nehmen. |
| Legen Sie zugehörige CI-Services für VI fest | Sobald der Integrationsimport abgeschlossen ist, werden betroffene Business Services zum angegebenen Zeitpunkt mit CIs verknüpft, die mit angreifbaren Elementen verbunden sind. |
| Legen Sie die Anzahl der Zurückstellungen fest | Erfasst die Anzahl der Zurückstellungen eines angreifbaren Elements, eines angreifbaren Anwendungselements, eines angreifbaren Containerelements oder einer Korrekturaufgabe. |
| Nächste Integration auslösen | Löst die nächste Integration in einer verketteten Integrationsausführung aus. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Vorlagenintegration | Ein einzelner Vorlagendatensatz wird während des erneuten Scannens an Tenable.io gesendet. |
| Aktualisiert nicht gruppierte angreifbare Elemente | Bestimmt, ob sich ein angreifbares Element in der Korrekturaufgabe befindet , und fügt es der Liste der **nicht gruppierten angreifbaren** Elemente hinzu oder entfernt sie daraus.<br>**Hinweis:**<br>Dieser Auftrag wird nach dem Upgrade ausgeführt und kann je nach Datensatz sehr lange dauern. |
| Aktualisieren Sie Schwachstelle auf VG | Aktualisiert das Feld **Schwachstelle** in der Tabelle Schwachstellengruppe (sn_vul_vulnerability) nach dem Upgrade. Dieser Auftrag wird einmal ausgelöst und anschließend deaktiviert. |
| Importvorlage für Schwachstelle | Engine, die die Importwarteschlange verarbeitet. Einer von 10. |
| Vulnerability Response-Alter der Aktualisierung | Aktualisiert die Spalte „Alter geschlossen“ in der VI-Tabelle. |
| CI-Anzahl in Vulnerability Response | Berechnet die Anzahl der CIs, die in den letzten 30 Tagen von Scannern von Drittanbietern gescannt wurden. |
| Vulnerability Response-Risiko- und Remediation-Status-Upgrade | Aktualisiert die Risikobewertung für Daten, wenn Sie ein Upgrade durchführen. |
| v20.0: Überprüfen Sie den Ablauf der Risikoverringerung | Überprüft, ob Ausgleichskontrollen für ein angreifbares Element und eine Korrekturaufgabe abgelaufen sind. Wenn sie abgelaufen sind, wird die Risikopunktzahl auf die ursprüngliche Risikopunktzahl zurückgesetzt und eine E-Mail-Benachrichtigung gesendet, die angibt, dass die Ausgleichskontrollen abgelaufen sind. Sendet auch eine E-Mail-Benachrichtigung, wenn Ausgleichskontrollen so festgelegt sind, dass sie innerhalb von 7 Tagen ablaufen. |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| sn_vul_cmn_ws_saved_filter | Speichert die Daten des gespeicherten Filters. |
| sn_vul_licensing_usage | Enthält das doppelte Asset, das unvollständige IP-Asset, die Gesamtanzahl der Scanner-Assets und die endgültige Verwendung. |
| sn_vul_m2m_entry_compensating_control | Stellt die Zuordnung zwischen Schwachstelleneinträgen und Ausgleichskontrollen dar. |
| v21.0<br>Rapid7-Scan-Engine [sn_vul_r7_scan_engine] | Speichern Sie die Datensätze der importierten Scan Engine-Daten, die für die Erkennung von Assets während eines Scans und deren Überprüfung auf Schwachstellen verantwortlich sind. |
| v21.0<br>Import der Rapid7 Scan Engine [sn_vul_r7_scan_engine_import] | Wird von der Rapid7 Scan Engine-Integration verwendet, um Importdaten vor der Verarbeitung bereitzustellen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Version 19.0:<br><br>[sn_vul_veracode_cwe_import] | Erweitert die Veracode-Kategorietabelle für CWE-Korrekturempfehlungen. |
| Version 19.0:<br><br>[sn_vul_veracode_category_import] | Speichert importierte Kategoriedaten. |
| Version 19.0:<br><br>[sn_vul_veracode_sbom_import] | Speichert importierte SBOM-Daten, die aus Veracode stammen. |
| V17.1: Nachweis zum VI-Schlüssel hinzufügen<br><br>[sn_vul_ Proof_key_vulnerability] | Rapid7-Schwachstellen, für die Nachweise im VI-Schlüssel enthalten sein müssen. |
| Bewertete angreifbare Elemente<br><br>[sn_vul_m2m_exp_sw_vi] | Weist während der Korrekturaufgabenerstellung einer Zuweisungsgruppe eine Korrekturaufgabengruppe zu. |
| Zuweisungsregel<br><br>[sn_vul_vgr_assignment_rule] | Weist während der Korrekturaufgabenerstellung einer Zuweisungsgruppe eine Korrekturaufgabengruppe zu.<br><br>Vor v15.0: Weist einer Zuweisungsgruppe während der Erstellung der Korrekturaufgabe eine [] Korrekturaufgabe zu. |
| Change-Anforderung zuordnen<br><br>[sn_vul_action_associate_cr] | Bereitstellungstabelle, die zur Verarbeitung neuer Zuordnungen zwischen Korrekturaufgabe und CHG verwendet wird.<br><br>Vor v15.0: Bereitstellungstabelle zur Verarbeitung neuer VG-CHG-Zuordnungen. |
| Asynchrone angreifbare Elemente Auftrag<br><br>[sn_vul_async_vi_job] | Enthält Hintergrundaufträge, die angreifbare Elemente verarbeiten. Es wird nur ein Auftragstyp unterstützt. Wird verwendet, um Schwachstellen in Massen zu bearbeiten. |
| Auftragstyp des asynchronen angreifbaren Elements<br><br>[sn_vul_async_vi_job_type] | Enthält die Typen von Hintergrundaufträgen und verweist auf das entsprechende Skript. Hat nur einen Prozessor, den **VulnerabilityBulkEditProcessor** |
| Veraltete Erkennungen automatisch schließen<br><br>[sn_vul_auto_close_config] | Speichert die Konfiguration dafür, wie veraltete Erkennungen automatisch geschlossen werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Granularität angreifbarer Elemente konfigurieren<br>[sn_vul_action_vi_granularity_config] | Speichert das UI-Formular, das zum Aktivieren oder Deaktivieren von „Port einschließen“ auf der Konfigurationsseite im Modul „AE-Granularität konfigurieren“ verwendet wird |
| Change-Anforderungen erstellen<br>[sn_vul_action_create_cr] | Wird verwendet, um Change-Anforderungen aus der Korrekturaufgabe zu erstellen. |
| Angreifbare Elemente erstellen<br>[sn_vul_action_create_vi] | Eine Bereitstellungstabelle, die als Platzhalter für Informationen verwendet wird. In dieser Tabelle werden keine Datensätze gespeichert. |
| Sammlung<br>[sn_vul_patch_orch_collection] | Speichert Sammlungsdaten aus verschiedenen Instanzen. |
| CWE<br>[sn_vul_cwe] | Katalog der CWE-Softwareschwachstellen (Common Weakness and Enumeration). |
| Anwendbare CWE-Plattform<br>[sn_vul_cwe_m2m_cwe_platform] | Enthält die importierten anwendbaren CWE-Plattformdaten |
| CWE-Kategorie<br>[sn_vul_cwe_category] | Enthält die importierten CWE-Kategoriedaten |
| Häufige CWE-Konsequenz<br>[sn_vul_cwe_consequence] | Enthält die importierten allgemeinen CWE-Konsequenzdaten |
| Externe CWE-Referenz<br>[sn_vul_cwe_reference] | Enthält die importierten externen CWE-Referenzdaten |
| Beispiel für CWE-Beobachtung<br>[sn_vul_m2m_cwe_cve] | Enthält die importierten CWE-CVE-Daten |
| CWE-Plattform<br>[sn_vul_cwe_platform] | Enthält die importierten CWE-Plattformdaten |
| Externe CWE-Referenz<br>[sn_vul_cwe_reference] | Enthält die importierten CWE-bezogenen externen Referenzdaten |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| CWE-Beziehung<br>[sn_vul_m2m_cwe_relation] | Enthält die importierten CWE-Beziehungsdaten |
| CWE-Ansicht<br>[sn_vul_cwe_view] | Enthält die importierten CWE-Ansichtsdaten |
| CWE-Schwäche<br>[sn_vul_cwe_weakness] | Enthält die importierten CWE-Schwachstellendaten |
| Version 16.1: Gerätesammlung<br>[sn_vul_patch_orch_m2m_src_ci_collection] | Speichert Sammlungsdaten zu erkannten Elementen. |
| Version 16.1: Geräte-Update<br>[sn_vul_patch_orch_m2m_src_ci_update] | Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden. |
| Übereinstimmung Discovery-Modell verwundbare Softw<br>[sn_vul_discovery_model_software_match] | Ergänzt den Abgleich von angreifbarer Software mit einem Discovery-Modell. |
| Konfiguration für Ausnahmeverwaltung<br>[sn_vul_exception_config] | Speichert die Konfigurationseinstellungen für die Ausnahmeverwaltungsfunktion |
| Ausnahmeregel<br>[sn_vul_auto_exception_rule] | Enthält den für Exception Management ausgewerteten Regelsatz. |
| Exploit<br>[sn_vul_exploit] | Enthält die Definitionen von Exploits: öffentlich verfügbarer Code, der eine Schwachstelle ausnutzt. |
| Exploit-Framework<br>sn_vul_exploit_framework | Enthält die Namen von Exploit-Frameworks: vollständige Softwarepakete, die viele Exploits ausführen können. |
| Verfügbar gemachte Discovery-Modelle<br>[sn_vul_m2m_exp_sw_model] | Speichert die Zuordnung zwischen Discovery-Modell und Risikobewertung. |
| Bewertung des Gefahrenpotenzials<br>[sn_vul_exp_by_sw] | Speichert die Datensätze für die Risikobewertung. |
| V19.0: Risikomanifest<br>sn_vul_analyst_exposure_manifest | Manifesttabelle für die Delta-Verarbeitung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Einträge zum Gefahrenpotenzial von Schwachstellen<br>[sn_vul_m2m_entry_exp] | Speichert die Zuordnung zwischen Schwachstelle (sn_vul_entry) und Risikobewertung. |
| Malware-Kit<br>[sn_vul_malware_kit] | Enthält die Details von Malware-Kits: vorab geschriebene Tools, mit denen ein Exploit oder eine Reihe zugehöriger Exploits ohne zusätzliche Codierungs- oder Konfigurationsarbeit ausgeführt werden kann |
| Fehlende Asset-Tabelle [sn_vul_tenable_missing_asset] | Enthält temporäre Asset-IDs für ignorierte Konfigurations-Compliance-Bewertungsdaten mit nicht abgeglichenen Assets. |
| Update der Microsoft Response Center-Lösung<br>[sn_vul_msrc_update] | Enthält den Zeitpunkt, zu dem die Lösungsdaten zuletzt von Microsoft aktualisiert wurden. Wird zum Vergleich mit dem nächtlichen Import verwendet, um die Delta-Daten für den Download zu bestimmen. |
| Microsoft Security Response Center Lösungsimport<br>[sn_vul_msrc_solution_import] | Wird von der Microsoft Security Response Center-Lösungsintegration verwendet, um Importdaten vor der Verarbeitung bereitzustellen. |
| Integration der Microsoft Security Response Center-Lösung<br>[sn_vul_msrc_integration] | Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für Integration der Microsoft Security Response Center-Lösung. |
| Nationale Verwundbarkeit – Datenbankeintrag<br>[sn_vul_nvd_entry] | Dokumentierte Schwachstelle aus der NIST National Vulnerability Database. |
| NVD-CVSS-Import<br>[sn_vul_nvd_cvss_import] | Enthält Bereitstellungsdaten, die während des NVD-Imports noch nicht in das Schema Vulnerability Response umgewandelt wurden |
| Version 16.1<br>[sn_vul_patch_orch.patch_approval_required] | Wenn Patch-Bereitstellungen aus einer Patch-Integration geplant werden, werden Anforderungen zur Überprüfung und Genehmigung an Benutzer übermittelt, die der Genehmigungsgruppe „Ebene 1 – Patch-Aktualisierung“ zugewiesen sind. Diese Eigenschaft ist standardmäßig aktiviert. |
| Version 16.1: Patch-Bereitstellung<br>[sn_vul_patch_orch_deployment] | Speichert Informationen zu bereitgestellten Patches für Sammlungen und CIs. |
| Version 16.1: Patch-Update<br>[sn_vul_patch_orch_update] | Speichert Informationen zu den Patches, die für verschiedene Instanzen verfügbar sind |
| Version 16.1: Potenzieller Patch<br>[sn_vul_patch_orch_m2m_vuln_patch] | Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können. |
| V19.0: Potenzielles Schwachstellenrisiko | Risikobewertungstabelle für CVE. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| sn_vul_analyst_m2m_pot_exp_sw_model | |
| Produktkategorie<br>[sn_vul_product_category] | Enthält die importierten Produktkategoriedaten |
| Red Hat Security Advisory<br>[sn_vul_rhsa_update] | Vergleicht die Lösungen Red Hat mit dem nächtlichen Job, um die Delta-Daten für den Import zu bestimmen. |
| Red Hat Lösungsimporte<br>[sn_vul_rh_solution_import] | Wird von Red Hat Solution Integration verwendet, um Importdaten vor der Verarbeitung bereitzustellen. |
| Red Hat Solution Integration<br>[sn_vul_rh_integration] | Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für Red Hat Solution Integration. |
| Zugehörige Business Services<br>[sn_vul_m2m_ci_services] | Verknüpft CIs mit Business Services für die Suche nach betroffenen Services. Enthält eine Kennzeichnung, die angibt, ob sie von Service Mapping hinzugefügt wurde. |
| V18.0: Anzahl der Korrekturmaßnahmen<br>[sn_vul_daily_count_re] | Tägliche Anzahl der Korrekturmaßnahmen. Diese Tabelle wird täglich aktualisiert. |
| V18.0: Datensatz der Korrekturmaßnahme<br>[sn_vul_remediation_effort_record] | Verfolgt den Korrekturfortschritt für Korrekturbemühungen (RE) nach. Enthält Verweise auf die REs |
| Korrekturzielregel<br>[sn_vul_ttr_rule] | Definiert den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Elements. Erweitert Anwendungsdatei. |
| V18.0: Korrekturaufgabe<br>[sn_vul_remediation_task] | Speichert alle Korrekturaufgaben für VR, AVR, CVR und Testergebnisgruppen. |
| REST-Integration<br>[sn_vul_rest_integration] | Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_integration] für die REST-basierten Integrationen. |
| SAM-NVD-Schwachstellenerkennung<br>[sn_vul_sam_config] | Enthält, welche CIs und Schwachstellen mit SAM NVD überwacht werden und ob die SAM NVD-Schwachstellenerkennung aktiviert ist oder nicht. |
| Geplanter Importpool<br>[sn_vul_sched_import_pool] | Sammlung von Datensätzen für geplante Importsätze, die verwendet werden, um gleichzeitige Datenquellenimporte zu erleichtern. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Wählen Sie Angreifbares Element aus<br>[sn_vul_action_select_vi] | Basisbereitstellungstabelle, die verwendet wird, um geteilte VGs zu verarbeiten, CHGs zu erstellen und CHGs zuzuordnen |
| Setup-Status<br>[sn_vul_setup_status] | Nur intern: Wird vom Setup-Assistenten verwendet. Immer wenn der Setup-Assistent geöffnet wird, wird der Status der Schritte Abgeschlossen angezeigt, und der Prozentsatz in der rechten oberen Ecke stammt aus dieser Tabelle. |
| Schweregradzuordnung<br>[sn_vul_severity_map] | Enthält die Zuordnungen vom Quellschweregrad zum normalisierten Schweregrad |
| Zuordnung für Lösungsscanner<br>[sn_vul_solution_scanner_mapping] | Ordnet Lieferant, Scanner und Stichwörter für den Ausschluss oder Einschluss zu. |
| Schwachstellengruppe] aufteilen<br>[sn_vul_action_split_vg] | Bereitstellungstabelle, die zum Aufteilen von Korrekturaufgabenverwendet wird. |
| Eintrag für DrittVendor-Sicherheitslücke<br>[sn_vul_ Third_party_entry] | Dokumentierte Schwachstelle aus einer Drittanbieterquelle. |
| [sn_vul_tenable_io_template | Ein Vorlagendatensatz wird an Tenable.io gesendet und dann während des erneuten Scannens für Elemente mit Tenable.io als Quelle importiert. |
| Manifest aktualisieren<br>[sn_vul_update_manifest] | Liste der Korrekturaufgaben, die aktualisiert wurden und eine Neuberechnung durch den Rollup-Rechner erfordern. |
| V17.1: Verwendung nach CI-Klassen<br>[sn_vul_licensing_usage_by_ci_classes] | Enthält die von der CI-Klasse zusammengefasste Verwendungsanzahl |
| Anzahl der VR-Konfigurationselemente<br>[sn_vul_vr_configuration_item_count] | Enthält den gleitenden kumulierten 90-Tage-Durchschnitt der Konfigurationselemente, die aus Drittanbieterintegrationen importiert wurden. |
| Zuweisungsregel für Schwachstellen<br>[sn_vul_assignment_rule] | Enthält den Satz von Regeln, die ausgewertet werden, um die Zuweisungsgruppe für VIs festzulegen. |
| Sicherheitsrisiko-Rechner<br>[sn_vul_calculator_group] | Enthält die Regeln des Schwachstellenrechners Die Reihenfolge der Rechner bestimmt, welcher Rechner zuerst ausgewertet wird, und in jedem Rechner wird höchstens eine Rechnerregel verwendet. |
| Regel zum Schwachstellenrechner<br>[sn_vul_calculator] | Enthält die Regeln für alle Rechner. Für jeden Rechner werden die Rechnerregeln der Reihe nach überprüft. Der erste Rechner, der die Bedingung erfüllt, verwendet die Werte innerhalb dieser Regel. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Schwachstellen-CVEs<br>[sn_vul_m2m_entry_cve] | Verknüpft NVD Common Vulnerability Exposures (CVE)-Daten mit angreifbaren Einträgen. |
| Warteschlangeneintrag Verwundbarkeits-Datenquellen<br>[sn_vul_ds_import_q_entry] | Warteschlange für Anhänge, bevor sie von einer Datenquelle verarbeitet werden. Wird von Schwachstellenintegrationen verwendet. |
| Schwachstelleneintrag<br>[sn_vul_entry] | Dokumentierte Schwachstelle. |
| Schwachstelleneintrags-Scan<br>[sn_vul_entry_scan] | Speichert die Beziehung zwischen einem Scan und einem Schwachstelleneintrag |
| Schwachstellen-Exploit-Framework<br>[sn_vul_m2m_framework_vul] | Enthält die Beziehung zwischen Exploit-Frameworks und Schwachstellen |
| V19.0: Bewertung des Schwachstellenrisikos<br>sn_vul_analyst_sam_config | Konfigurationstabelle für Risikobewertung für CVE. |
| Konfiguration der Schwachstellengranularität<br>[sn_vul_granularity_config] | Speichert und verwaltet den Status des Einschluss- oder Ausschlussports für das Modul „AE-Granularität konfigurieren“. |
| Schwachstellengruppe<br>[sn_vul_vulnerability] | Sammlung von angreifbaren Elementen, die zur Korrektur organisiert wurden. |
| Change-Anforderungen für Schwachstellengruppe<br>[sn_vul_m2m_vg_change_request] | Speichert die Zuordnung von Korrekturaufgaben und CHG-Anforderungen. |
| Element der Schwachstellengruppe<br>[sn_vul_m2m_vul_group_item] | Zuordnung von Korrekturaufgaben und angreifbaren Elementen. |
| Regel für Schwachstellengruppen<br>[sn_vul_grouping_rule] | Enthält die Regeln, die die Kriterien definieren, nach denen Gruppen automatisch für einen Satz angreifbarer Elemente erstellt werden. |
| Integration von Sicherheitslücken<br>[sn_vul_integration] | Planbarer Datensatz zum Importieren von Schwachstellendaten aus einer externen Quelle. Erweitert die geplante Skriptausführung. |
| Datenquelle Sicherheitslückenintegration<br>[sn_vul_int_data_src] | Datenquelle, die mit einer Schwachstellenintegration verwendet werden soll. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Schwachstellenintegrationsprotokoll<br><br>[sn_vul_integration_log] | Zeichnet Protokollinformationen auf, die von Ausführungen der Schwachstellenintegration ausgegeben werden. |
| Integrationsprozess für Schwachstellen<br><br>[sn_vul_integration_process] | Einzelnes Prozessvorkommen für eine Schwachstellenintegration. |
| Warteschlange für Schwachstellenintegration<br><br>[sn_vul_integration_queue] | Ordnet die Importanforderungen für eine Integrationsausführung in die Warteschlange ein, wenn alle Datenquellen verwendet werden. |
| Integrationsausführung für Schwachstellen<br><br>[sn_vul_integration_run] | Aufrufe von Schwachstellenintegrationen<br><br>**Hinweis:**<br>Wenn eine Integration ausgeführt wird, kann sich nur eine Integration im Rückstand im Status „Bereit“ befinden. |
| Statistiken zur Ausführung von Schwachstellenintegrationen<br><br>[sn_vul_integration_stats] | Speichert die Aufgliederung jedes Schritts, z. B. REST-API-Zeit, VI-Erstellungszeit usw. für eine Integrationsausführung |
| Aufgabe für angreifbares Element<br><br>[sn_vul_m2m_item_task] | Angreifbare Elemente, die Problemen, Änderungen und Security Incidents zugeordnet sind. |
| Schwachstellen-Malware-Kit<br><br>[sn_vul_m2m_malware_kit_vul] | Enthält die Beziehungen zwischen Schwachstellen und Malware-Kits |
| Erforderliche Schwachstellenlösung<br><br>[sn_vul_m2m_solution_prerequisite] | Enthält die quellenspezifischen Voraussetzungen für die Anwendung einer Lösung, sofern verfügbar. |
| Grenzwert für Schwachstellenrate<br><br>[sn_vul_rate_limit] | Definiert eine Quotengrenze, die für einen Scanner verwendet werden soll. |
| Verwundbarkeitsreferenz<br><br>[sn_vul_reference] | Externe Referenzen für bekannte Schwachstellen. |
| Schwachstellen-Korrekturstatus<br><br>[sn_vul_m2m_ttr_status] | Status des angreifbaren Elements im Vergleich zur nächsten angewendeten Korrekturzielregel. |
| Regel zum Schwachstellenrisiko<br><br>[sn_vul_calc_risk] | Spezialisierte Rechnerregel, die mit den Risikopunktzahl-Rechnern verwendet wird. Verwendet Gewichtungen, die angeben, welche Werte im Zusammenhang mit einem VI zur Berechnung der Risikopunktzahl verwendet werden sollen. |
| Rechner für Schwachstellen-Rollup | Liste der Rechner für Schwachstellen-Rollups. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| [sn_vul_rollup] | |
| Schwachstellen Scan<br>[sn_vul_scan] | Schwachstellenscan. Enthält, was gescannt werden soll, mit welchem Scanner, und eine Zusammenfassung der Scan-Ergebnisse. |
| Configuration Item für Schwachstellen-Scan<br>[sn_vul_m2m_scan_configuration_item] | Ordnet CMDB-CIs zu, die sich in der Warteschlange zum Scannen befinden. |
| Scan-Warteschlangeneintrag für Schwachstelle<br>[sn_vul_scan_q_entry] | Scan-Datensatz zum Scannen oder Verarbeiten in die Warteschlange gestellt. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen. |
| Quelle des Schwachstellen Scans<br>[sn_vul_m2m_scan_source] | Ordnet Quellen einem Scan-Datensatz zu und kennzeichnet alle Datensätze, die sich in der Warteschlange befinden, um gescannt zu werden. |
| Aufgabe des Schwachstellen Scans<br>[sn_vul_m2m_scan_vulnerability] | Ordnet Schwachstellenaufgaben für die Quellen eines Scan-Datensatzes zu. |
| Schwachstellen-Scanner<br>[sn_vul_scanner] | Definiert Scanner von Drittparteien, die in Scans verwendet werden sollen. |
| Quotengrenze des Schwachstellenscanners<br>[sn_cmn_scanner_rate_limit] | Ordnet einen Scanner einer Quotengrenze zu. |
| Verwundbare Software<br>[sn_vul_m2m_entry_software] | Enthält Zuordnungen zwischen Schwachstellen und angreifbarer Software. |
| Schwachstellenlösung<br>[sn_vul_solution] | Enthält die Beziehungsdaten zwischen der Schwachstelle und den möglichen Lösungen für sie. |
| Schwachstellenlösung<br>[sn_vul_m2m_vulnerability_solution] | Verknüpft die Tabelle „Schwachstelleneintrag“ (sn_vul_entry) mit der Tabelle „Schwachstellenlösung“ (sn_vul_solution). |
| Sicherheitsrisikostatus Change-Genehmigung<br>[sn_vul_change_approval] | Verfolgt den Genehmigungsprozess für Schwachstellen nach. |
| Ersatzlösung für Schwachstelle<br>[sn_vul_m2m_solution_Supersedence] | Enthält die quellenspezifische Beziehung zwischen Lösungen. |
| Schwachstellenupdatemanifest<br>[sn_vul_vuln_update] | Enthält eine Liste von Schwachstellen, deren Rollup-Daten aktualisiert werden müssen, nachdem die angreifbaren Elemente aktualisiert oder geschlossen wurden oder deren Risikopunktzahl geändert wurde. |



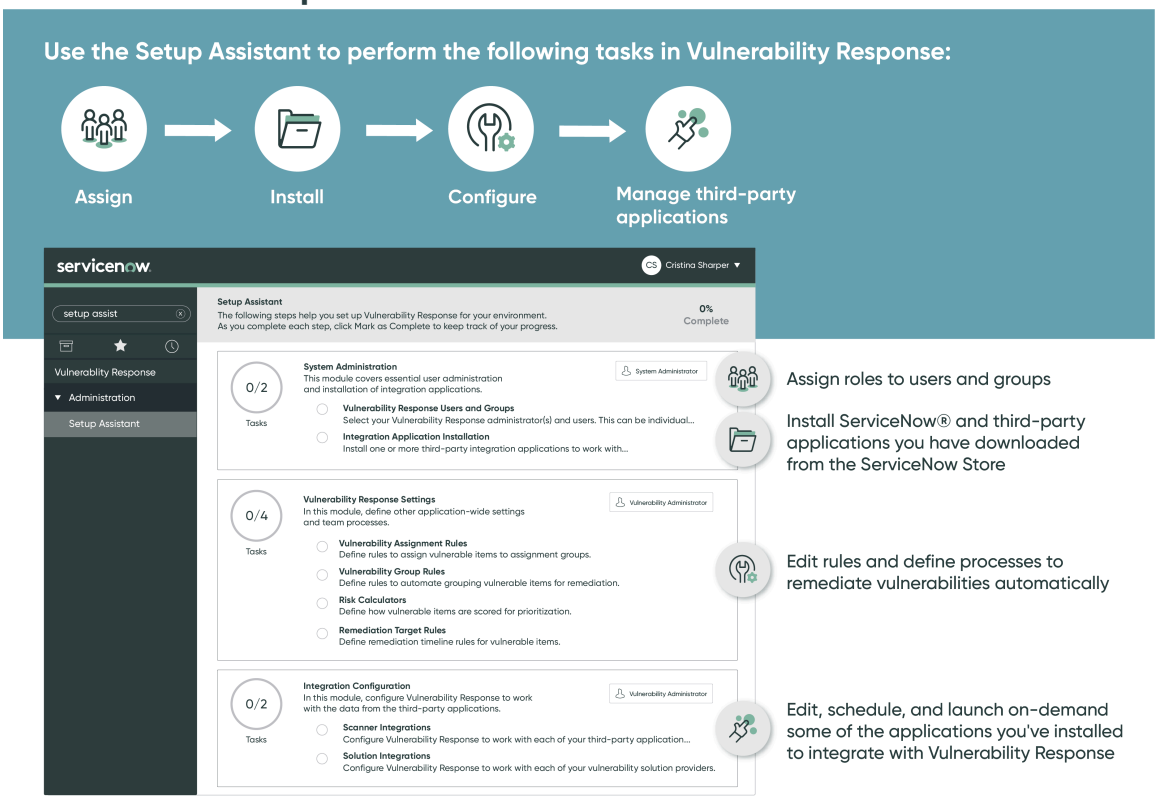
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| Schwachstellenzuordnung für Lieferanten<br>[sun_vul_vulnerability_vendor_mapping] | Enthält eine Liste von Schwachstellen und deren Lieferanten. |
| Angreifbares Element<br>[sn_vul_vulnerable_item] | Enthält das Auftreten einer Schwachstelle in einem Konfigurationselement |
| Erkennung von angreifbarem Element<br>[sn_vul_detection] | Enthält die Erkennungen angreifbarer Elemente aus Drittanbieterintegrationen |
| Software mit Schwachstellen<br>[sn_vul_software] | Software, die bekanntermaßen bestimmte Schwachstellen aufweist. |

## Vulnerability Response mit dem Setup-Assistenten konfigurieren

Der Setup-Assistent führt Sie durch die Einrichtung von Vulnerability Response und bestimmten Drittanbieterintegrationen für Ihre Umgebung. Der Setup-Assistent bietet fast alles, was Sie zum Installieren und Einrichten Ihrer Umgebung benötigen, damit Sie Vulnerability Responseverwenden können.

### Funktionalität des Setup-Assistenten




**Now Platform® roles:** admin and vulnerability admin

Für die Verwendung des Setup-Assistenten sind zwei verschiedene Now Platform® Rollen erforderlich: Administrator und Schwachstellenadministrator.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In den folgenden Abschnitten finden Sie Informationen zu den Anweisungen und Eingabeaufforderungen im Setup-Assistenten.

## Systemadministration – Benutzer und Gruppen zuweisen und Integrationsanwendungen installieren

Erforderliche Rolle: admin

Vor Beginn dieser Aufgaben sollte vom Schwachstellenmanager eine Liste der Benutzer und Integrationen eingeholt werden.

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.
2. Im ersten Abschnitt, Systemadministration, weist der Administrator Benutzern und Gruppen Rollen zu und installiert unterstützte Integrationen.

   Weisen Sie Benutzern und Gruppen im Setup-Assistenten Vulnerability Response Personas und Rollen zu.

   Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

3. Weisen Sie Rollen im Setup-Assistenten zu.
   - Weisen Sie Benutzern oder Gruppen die Rolle „sn_vul.admin“ zu.
   - Weisen Sie die Rolle „sn_vul.admin“ für die Verwaltung und Konfiguration von Vulnerability Response zu, einschließlich Schwachstellenintegrationen, Regeln für Korrekturaufgaben, Rechner und Regeln für die Korrekturzeit.
   - Weisen Sie die Rolle sn_vul_vulnerability_write für die Erstellung und Aktualisierung von Korrekturaufgaben und angreifbaren Elementen zu.

     **Hinweis:**
     Alle anderen Benutzer erhalten automatisch Schreibzugriff nur auf Korrekturaufgaben, die ihnen zugewiesen sind.

   - Weisen Sie die Rolle sn_vul_vulnerability_read zu, um Korrekturaufgaben, angreifbare Elemente und andere Informationen zu Schwachstellen anzuzeigen.

     **Hinweis:**
     Benutzern mit der Rolle „itil“ wird automatisch die Rolle „sn_vul.remediation_owner“ gewährt, mit der sie Korrekturaufgaben und angreifbare Elemente, die ihnen zugewiesen sind, Schwachstelleneinträge und Lösungen in der Anwendung Vulnerability Response in ihrer Instanz und in der Anwendung Mobile Agent anzeigen können. Es ist keine zusätzliche Zuweisung erforderlich.

4. Installieren Sie Integrationsanwendungen von Drittparteien.

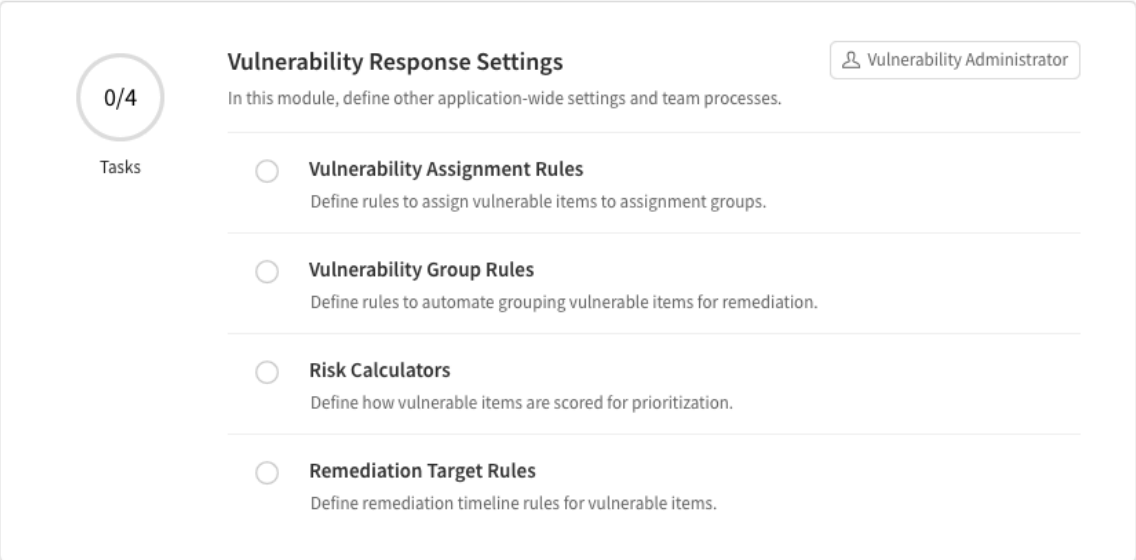


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weitere Informationen zu Anwendungen, die von [] unterstützt werden, finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen und Vulnerability Response-IntegrationenVulnerability Response.
- Weitere Informationen zur Verwendung des Setup-Assistenten zum Installieren unterstützter Apps finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.

## Vulnerability Response-Einstellungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin




In den Vulnerability Response-Einstellungen definiert der Schwachstellenadministrator anwendungsweite Einstellungen und Regeln für Vulnerability Response. Alternativ kann der Administrator diese Aufgaben ausführen.

1. Erstellen Sie Schwachstellenzuweisungsregeln.

   Erstellen Sie Regeln, die die automatische Zuweisung von Korrekturaufgaben zur Lösung definieren. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

   **Hinweis:**

   Die Funktion „Erneut anwenden“ erfordert eine Baselineanwendung der Regeln. Sobald Ihre Regeln erstellt sind, aktivieren Sie die geplante Aufgabe `Reapply all vulnerability assignment rules`, um sie nach Belieben auszuführen. Andernfalls müssen Sie alle Regeln erneut auf alle offenen AEs anwenden, bevor Sie sie ändern.

   Wenn die Aufgabe abgeschlossen ist, legen Sie das Feld **Ausführen** in der geplanten Aufgabe entsprechend Ihrer Umgebung fest. Abhängig von der Anzahl Ihrer aktiven AEs kann die tägliche Auswertung und Aktualisierung nicht unerhebliche Auswirkungen auf die Leistung haben. Erwägen Sie für größere Umgebungen eine Aktualisierung einmal pro Woche oder sogar einmal im Monat.

   Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Erstellen Sie Regeln für Korrekturaufgaben.

   Erstellen Sie Regeln, die die automatische Erstellung von Korrekturaufgaben für die Lösung definieren. Mindestens eine Regel, **Schwachstelle,** wird mit dem Basissystem geliefert. Sie können die Regeln aus dem Formular oder der Listenansicht erneut anwenden.

   - Wenn eine Gruppenregel gelöscht wird, haben Sie im Formular oder in der Listenansicht die Möglichkeit, alle von dieser Regel erstellten **offenen** Gruppen zu löschen. Gruppen, die sich nicht im Status „ **Offen** “ befinden, werden ausgeschlossen.
   - Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.
   - Weitere Informationen zur Verwendung von Vulnerability ResponseDie Anwendung Vulnerability Response erkunden zur Behebung von Schwachstellen finden Sie unter [].

3. Erstellen und aktivieren Sie Risikorechner.

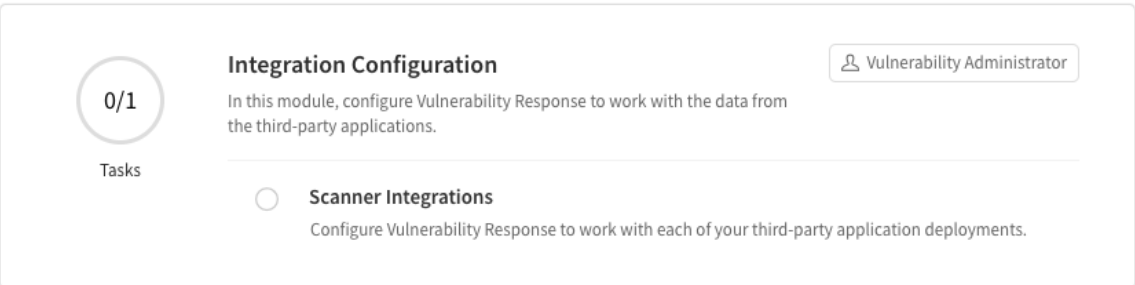
   Aktivieren Sie Risikorechner, die definieren, wie angreifbare Elemente für die Priorisierung bewertet werden. Im Lieferumfang des Basissystems sind mehrere Risikorechner enthalten. Informationen zum Erstellen oder Bearbeiten von Risikorechnern für Ihre Umgebung finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.

4. Erstellen Sie Korrekturzielregeln.

   Erstellen Sie Korrekturzielregeln für Korrekturkategorien. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung finden Sie unter Vulnerability Response Korrekturzielregeln.

## Integrationskonfiguration

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin.




Im Abschnitt „Integrationskonfiguration“ können Sie die folgenden Schwachstellenscanner-Integrationen von Drittanbietern und, wenn die Anwendung Solution Management for Vulnerability Response installiert ist, Lösungsanbieter konfigurieren, planen, bearbeiten und bei Bedarf starten.

- Weitere Informationen zum Konfigurieren von [ Konfigurieren Sie Qualys Vulnerability Integration mit dem Setup-Assistenten finden Sie unter Qualys Vulnerability Integration.
- Die KonfigurationVulnerability Response Integration with Tenable der Anwendung [] wird unterstützt. Siehe Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten.
- Nachdem Sie die Anwendung Vulnerability Solution Management installiert haben, wird die Option **Lösungsintegrationen** unter **Scanner-Integrationen**angezeigt. Klicken Sie auf



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Lösungsintegrationen**, um die installierten Anbieter von Schwachstellenlösungen in diesem Abschnitt des Setup-Assistenten zu konfigurieren. Red Hat Solution Integration und Integration der Microsoft Security Response Center-Lösung werden unterstützt.

Weitere Informationen zu installierten Lösungen finden Sie unter Vulnerability Solution Management. Weitere Informationen zur Installation finden Sie unter Anwendung Solution Management for Vulnerability Response installieren.

Weitere Informationen zum Konfigurieren der installierten Lösungen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.

- Wenn eine Integration aus mehreren Quellen stammt, können Sie mehrere Bereitstellungen derselben Drittpartei-Integration haben.
- Die Einstellungen aus Ihrer ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

**Hinweis:**
Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Daten aus jeder Drittanbieterintegration werden eindeutig identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

**Hinweis:**
Mehrere Schwachstellenintegrationen für Rapid7 InsightVM sind im Setup-Assistenten nicht verfügbar. Informationen zum Konfigurieren und Erstellen mehrerer Rapid7 InsightVMErstellen Sie domänengetrennte Importe für eine Integration -Integrationen finden Sie unter [].

## Zusätzliche Aufgaben

Weitere Informationen zu Setupaufgaben, die nicht im Setup-Assistenten enthalten sind, finden Sie unter Zusätzliche Vulnerability Response Setup- und Konfigurationsaufgaben.

### Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu

Weisen Sie die Persona-Rollen Vulnerability Response Gruppen oder Benutzern mit dem Setup-Assistenten zu.

#### Vorbereitungen

Wenn Sie bereits Persona-Rollen in Vulnerability Response mit dem Setup-Assistenten zugewiesen haben und weitere Informationen zum Bearbeiten und Verwalten Ihrer granularen Rollen und Rollenzuweisungen im Benutzeradministrationsmodul wünschen, finden Sie weitere Informationen unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Wenn Sie Upgrade-Kunde sind, können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Benutzer und Gruppen, denen die Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write sowie die Rollen „Korrekturbesitzer“ zugewiesen wurden, die in früheren Versionen von Vulnerability Response verfügbar waren, hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response auf Aufgabenebene tun und sehen können, bevorzugen Sie möglicherweise die Verwendung von Personas und granularen Rollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Persona-Rolle sn_vul.vulnerability_admin noch nicht mit dem Setup-Assistenten zugewiesen haben, führen Sie die folgenden Schritte aus, um sie zuzuweisen. Nach der Zuweisung hat der Schwachstellenadministrator mit dieser Persona-Rolle die Berechtigung, die Aufgaben des Setup-Assistenten nach dem ersten Abschnitt abzuschließen und Regeln und Drittanbieterintegrationen in der Anwendung Vulnerability Response zu verwalten.

Eine Übersicht über Persona-Rollen und granulare Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen.

Wenn Sie Upgrade-Kunde sind, verwenden Sie die folgende Tabelle als Referenz.

| Vor v10.3 | Ab v10.3 |
|---|---|
| Wenn Sie sn_vul.admin zugewiesen haben | Möglicherweise möchten Sie Benutzern oder Gruppen sn_vul.vulnerability_admin – Schwachstellenadministrator zuweisen.<br><br>Benutzer mit dieser Rolle haben vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Benutzer mit dieser Rolle konfigurieren alle VR-Anwendungen und -Regeln und installieren Integrationen von Drittanbietern. |
| Wenn Sie sn_vulnerability_write für Benutzer und Gruppen zugewiesen haben. | Möglicherweise möchten Sie Benutzern und Gruppen „sn_vul.vulnerability_analyst – Schwachstellenanalyst“ zuweisen.<br><br>Benutzer und Gruppen mit dieser Rolle können alle Datensätze für die VI-Korrektur anzeigen und aktualisieren. |
| Wenn Sie sn_vul.remediation_owner zugewiesen haben | Möglicherweise möchten Sie Anwendern und Gruppen „sn_vul.remediation_owner – Korrekturbesitzer“ zuweisen.<br><br>Benutzer und Gruppen mit dieser Rolle beheben Schwachstellen, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. Gruppen oder Benutzer mit dieser Rolle können die Datensätze anzeigen und aktualisieren, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. |
| Wenn Sie sn_vul.admin für die Verwaltung nicht abgeglichener Konfigurationselemente (CIs) zugewiesen haben | Möglicherweise möchten Sie Benutzern und Gruppen den CI-Manager sn_vul.ci zuweisen.<br><br>Benutzer und Gruppen mit dieser Rolle verwalten nicht abgeglichene Konfigurationselemente (CIs), die in der Configuration Management Database (CMDB) nicht gefunden wurden. Gruppen oder Benutzer mit dieser Rolle aktualisieren erkannte Elemente. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Vor v10.3 | Ab v10.3 |
|---|---|
| Wenn Sie sn_vul.admin für Zurückstellungen und Ausnahmegenehmigungen zugewiesen haben. | Möglicherweise möchten Sie Anwendern und Gruppen „sn_vul.exception_approver – Ausnahmegenehmiger“ zuweisen.<br><br>Benutzer und Gruppen mit dieser Rolle genehmigen Ausnahmen, Zurückstellungen und Abschlüsse von Korrekturaufgaben und angreifbaren Elementen.<br><br>Ab v20.0 wurde die granulare Rolle sn_vul.read_all für diese Rolle entfernt, sodass Sie auf die Ihnen und Ihrer Gruppe zugewiesenen angreifbaren Elemente und Korrekturaufgaben zugreifen können, anstatt auf alle angreifbaren Elemente und Korrekturaufgaben. |
| Wenn Sie sn_vul.vulnerability_read zugewiesen haben, um Einblick in das Schwachstellenmanagement zu erhalten. | Möglicherweise möchten Sie Lesezugriff auf bestimmte Bereiche in der Anwendung nach Aufgabe zuweisen.<br><br>Weisen Sie beispielsweise sn_vul.read_all zu, damit ein Benutzer alle VR-Datensätze anzeigen kann. Weisen Sie für Lesezugriff zum Anzeigen von Korrekturaufgabenregeln sn_vul.read_group_rules zu. Benutzer und Gruppen mit dieser Rolle aktualisieren keine Datensätze. |

Um die granularen Rollen anzuzeigen, die ein Benutzer oder Gruppen mit einer Persona-Rolle standardmäßig erben, navigieren Sie zu **Alle** > **Benutzeradministration** > **Rollen**. Suchen Sie die gewünschte Rolle und klicken Sie darauf, um den Datensatz zu öffnen. Auf der Registerkarte „Enthält Rollen“ werden alle granularen Rollen der Persona-Rolle sowie alle geerbten Rollen aufgelistet.

Möglicherweise möchten Sie überprüfen, ob Sie alle erforderlichen Benutzer und Gruppen erstellt haben, bevor Sie Rollen im Setup-Assistenten zuweisen. Um neue Benutzer und Gruppen aus dem Setup-Assistenten hinzuzufügen, klicken Sie im Formular der folgenden Abbildung auf den Link zum **Modul Benutzeradministration**.

Im folgenden Beispiel wird gezeigt, wie Sie einem Benutzer die Persona des Schwachstellenadministrators zuweisen, um den Zugriff auf die Anwendung Vulnerability Response zu beschränken. Normalerweise ziehen Sie es vor, Gruppen andere Persona-Rollen als „sn_vul.vulnerability_admin“ zuzuweisen.

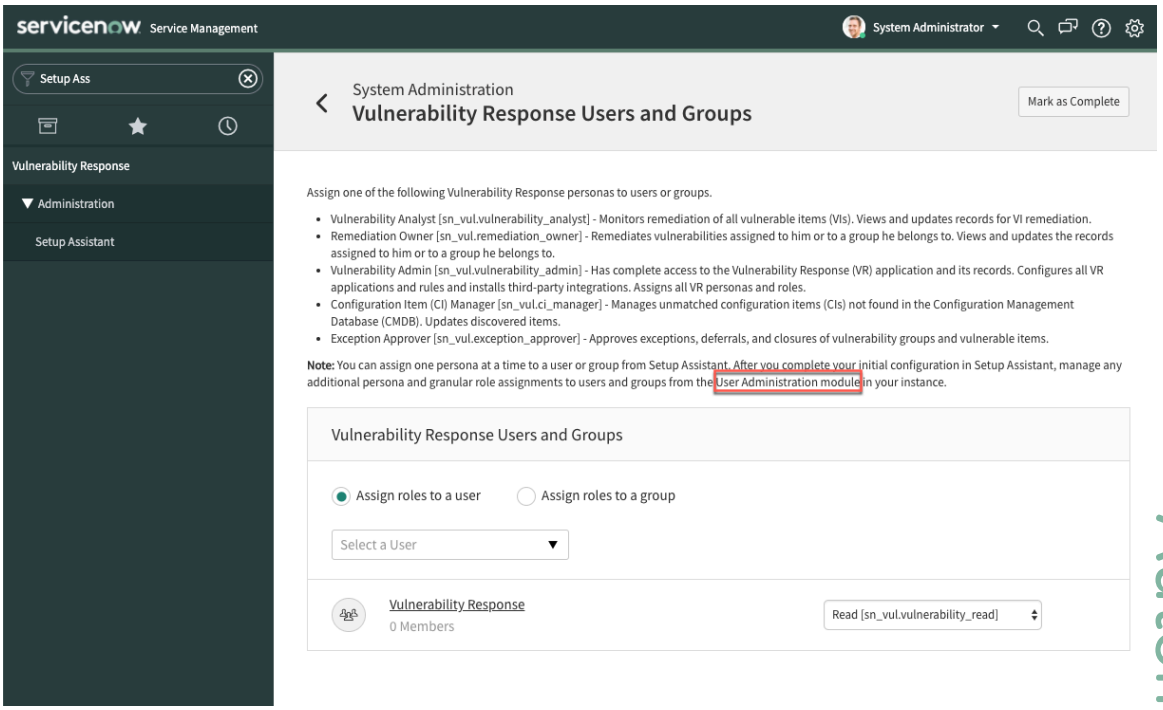
Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration Setup-Assistent**.
   Die Seite „Setup-Assistent“ wird angezeigt.
2. Klicken Sie auf Vulnerability Response Benutzer und Gruppen.
   Die Seite Systemadministration Vulnerability Response-Benutzer und -Gruppen wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Wenn Rollen einem Benutzer zuweisen ausgewählt ist, wählen Sie einen vorhandenen Benutzer aus der Liste aus.

   Sie können einem Benutzer oder einer Gruppe nur eine Persona-Rolle zuweisen.

   Nachdem Sie auf der rechten Seite des Formulars einen Benutzer oder eine Gruppe ausgewählt haben, wird standardmäßig die Standardpersona „Korrekturbesitzer“ [sn_vul.remediation_owner] zugewiesen und in der Liste angezeigt, bis Sie sie ändern.

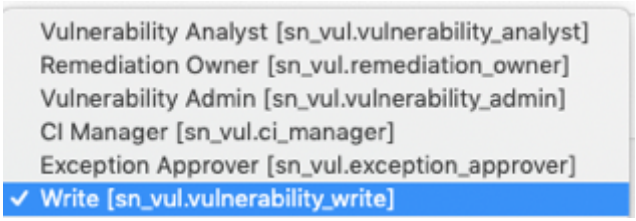
   **Hinweis:**
   Wenn Sie ein Upgrade auf eine neuere Version von Vulnerability Response durchführen und die Rolle „sn_vul.vulnerability_read“ oder „sn_vul.vulnerability_write“ vor dem Upgrade einem Benutzer oder einer Gruppe zugewiesen haben, wird sie zusammen mit den neuen Persona-Rollen angezeigt (siehe folgende Abbildung). .

   Wenn Sie Upgrade-Kunde sind, können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Der Zugriff für Benutzer und Gruppen, denen die Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write zugewiesen wurden, und der Korrekturbesitzer vor v10.3 hat sich nicht geändert.

   Beachten Sie, dass für vorhandene Benutzer oder Gruppen, denen derzeit die Rollen sn_vul.vulnerability_read oder sn_vul.vulnerability_write zugewiesen sind, diese Rollen zusammen mit den Persona-Rollen in der Liste angezeigt werden. Sobald Sie eine Persona-Rolle zugewiesen haben, ist die alte Rolle künftig nicht mehr verfügbar. Beispiel: Wie in der folgenden Abbildung dargestellt, wird die Rolle „Schreiben“ [sn_vul.vulnerability_write] nicht mehr als Option für diesen Benutzer oder diese Gruppe angezeigt, nachdem ihm eine der Persona-Rollen zugewiesen wurde.

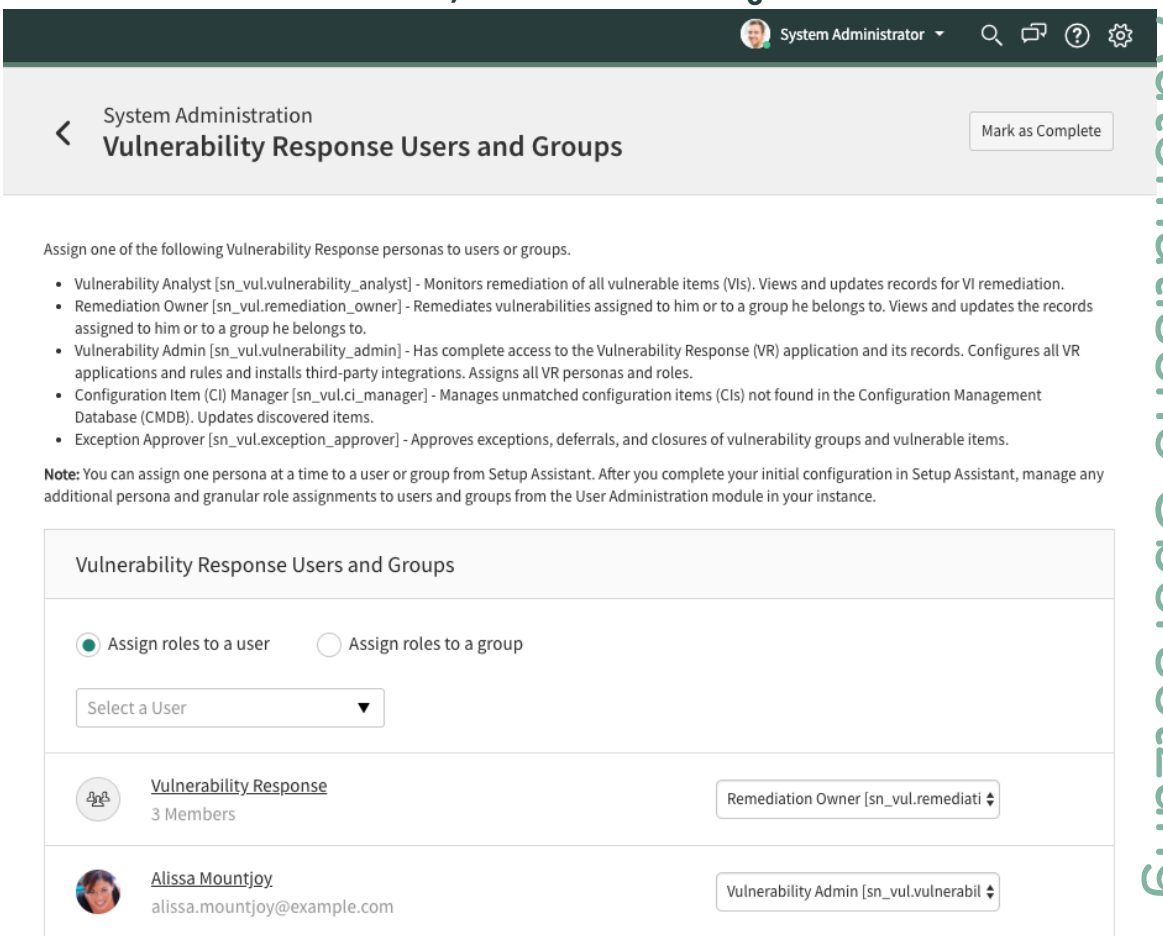
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wählen Sie in der Liste auf der rechten Seite des Formulars die **Option Schwachstellenadministrator [sn_vul.vulnerability_admin] aus**.
   Eine Nachricht wird angezeigt, die angibt, dass die Persona dem Benutzer oder der Gruppe erfolgreich zugewiesen wurde.

**Persona des Korrekturbesitzers, die einer Gruppe zugewiesen ist, und Persona des Schwachstellenadministrators, die einem Benutzer zugewiesen ist**




5. Weisen Sie anhand der Beschreibungen der oben aufgeführten Persona-Rollen alle Benutzer und Gruppen den verbleibenden Persona-Rollen zu: Korrekturbesitzer, Schwachstellenanalyst, CI-Manager und Ausnahmegenehmiger.
   Sie haben die Zuweisung von Persona-Rollen zu Benutzern und Gruppen mit dem Setup-Assistenten erfolgreich abgeschlossen.
6. **Wahlweise:** Führen Sie die folgenden Schritte aus, um die Benutzer in einer Gruppe über den Setup-Assistenten zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn die Gruppe im Formular angezeigt wird, klicken Sie auf den Namen der Gruppe, die Sie bearbeiten möchten.
Der Gruppendatensatz wird angezeigt.

b. Klicken Sie bei ausgewählter Registerkarte Gruppenmitglieder auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt

c. Verwenden Sie den Slushbucket, um Benutzer auszuwählen oder zu entfernen.

d. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern und zum Gruppendatensatz zurückzukehren.

e. Klicken Sie auf **Aktualisieren**, um zum Setup-Assistenten zurückzukehren.

f. Klicken Sie auf der Seite „Setup-Assistent“ auf **Vulnerability Response-Benutzer und -Gruppen**, um mit der Konfiguration im Setup-Assistenten fortzufahren.

### Nächste Maßnahme

Fahren Sie als Systemadministrator mit der Konfiguration von Vulnerability Response im Setup-Assistenten fort. Beachten Sie, dass Sie nach Abschluss des ersten Abschnitts einen Benutzer, dem Sie die Rolle des Schwachstellenadministrators zugewiesen haben, die Aufgaben im Setup-Assistenten ausführen lassen können. Weitere Informationen zum Verwalten granularer Rollen und Beispiele finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Verwalten Sie Personas und granulare Rollen für Vulnerability Response

Nachdem Sie die erste Zuweisung von Persona-Rollen mit dem Setup-Assistenten abgeschlossen haben, verwalten Sie zusätzliche granulare Rollenzuweisungen an Benutzer oder Gruppen über das Benutzeradministrationsmodul in Ihrer Instanz.

### Vorbereitungen

Wenn Sie die Ersteinrichtung und -konfiguration für Vulnerability Response mit dem Setup-Assistenten noch nicht abgeschlossen oder Benutzern und Gruppen keine Persona-Rollen zugewiesen haben, navigieren Sie zu **Vulnerability Response** > **Administration** > **Setup-Assistent**. Weitere Informationen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Wichtige Begriffe und eine Übersicht über Persona-Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen.

Eine Persona-Rolle ist eine vorkonfigurierte Rolle in der Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen „Setup-Assistent“, „Schwachstellenadministrator“, „Schwachstellenanalyst“, „Korrekturbesitzer“, „Konfigurationselement-Manager“ und „Ausnahmemanager“ sind so konzipiert, dass sie den gängigen Berufsbezeichnungen für Manager, Analysten und Serviceverantwortliche in einer IT-Organisation oder Schwachstellenkorrekturgruppe entsprechen.

Wenn Sie möchten, dass Ihre Benutzer und Gruppen mehr Zugriff haben, als eine der Rollen zulässt, können Sie Benutzern und Gruppen granulare Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Benutzer und Gruppen auf Aufgabenebene beschränken möchten. Außerdem können Sie benutzerdefinierte Rollen erstellen, die Ihren Anforderungen entsprechen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin

### Prozedur

1. Um granulare Rollen für Benutzer und Gruppen zu verwalten, wählen Sie eine aus, um fortzufahren.

   Die Namen für die granularen Rollen in Vulnerability Response beschreiben normalerweise, was Benutzer tun und sehen können. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie zu **Alle** > **Benutzeradministration** > **Rollen** und suchen Sie die gewünschte Rolle. Rollenbeschreibung, Rollen, die automatisch geerbt werden, wenn eine Rolle zugewiesen wird, und alle Rollen, die von anderen Rollen abhängen, werden ebenfalls aufgelistet.

2. Führen Sie die folgenden Schritte aus, um eine granulare Rolle für einen Benutzer oder eine Gruppe zuzuweisen oder zu entfernen.
   Angenommen, Sie möchten einem IT-Manager eine Rolle zuweisen, mit der dieser Manager Datensätze anzeigen, aber nicht aktualisieren oder bearbeiten kann. Um Datensätze in Vulnerability Response, Performance Analytics for Vulnerability Responseund für alle Drittanbieterintegrationen anzuzeigen, weisen Sie diesem Benutzer die granulare Rolle sn_vul.read_all zu.

   a. Navigieren zu **Alle** > **Benutzeradministration** > **Anwender**.

   b. Suchen Sie den Benutzer, und klicken Sie in der Spalte Name auf den Datensatz, um ihn zu öffnen.
   Der Datensatz des Benutzers wird angezeigt.

   c. Wenn nicht ausgewählt, wählen Sie die Registerkarte Rollen aus.
   Die dem Benutzer derzeit zugewiesenen Rollen werden angezeigt.

   d. Klicken Sie auf **Bearbeiten**.
   Das Formular „Mitglieder bearbeiten“ wird angezeigt.

   e. Geben Sie im Feld Sammlung des Slushbucket den Namen der Rolle ein, wenn Sie ihn kennen, oder geben Sie `*sn_vul` ein, um nur die für Vulnerability Response verfügbaren granularen Rollen anzuzeigen.

   f. Suchen und verschieben Sie sn_vul.read_all in die Rollenliste.

   **Hinweis:**
   Verwenden Sie den gleichen Vorgang, um bestimmte granulare Rollen von Benutzern im Slushbucket zu entfernen, indem Sie die Rolle aus der Liste „Rollen“ in die Liste „Sammlung“ verschieben.

   g. Klicken Sie auf **Speichern**.
   Der Benutzerdatensatz wird mit der neuen granularen Rolle angezeigt.

   h. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Benutzerliste zurückzukehren.
   Sie haben einem Benutzer die Berechtigung erteilt, Datensätze in Vulnerability Response, Performance Analytics for Vulnerability Responseund für Drittanbieterintegrationen zu lesen, aber nicht zu aktualisieren.

3. Führen Sie die folgenden Schritte aus, um eine Gruppe so zu bearbeiten, dass nur bestimmte Mitglieder erweiterten Zugriff mit granularen Rollen haben.
   Angenommen, Sie möchten bestimmten Benutzern in der Gruppe „Korrekturbesitzer“ (sn_vul.remediation_owner) erlauben, angreifbare Elemente manuell zu erstellen, diese



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigung jedoch nicht auf alle Benutzer in der Gruppe erweitern. Die Berechtigung zum manuellen Erstellen von angreifbaren Elementen wird von der granularen Rolle sn_vul.create_vulnerable_items gewährt. Führen Sie die folgenden Schritte aus, um diese Berechtigung nur für ausgewählte Benutzer aus dieser Gruppe zu erteilen.

**a.** Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.

**b.** Suchen Sie die Gruppe Korrekturbesitzer, und klicken Sie in der Spalte Name auf die Gruppe, um den Datensatz zu öffnen.
Der Gruppendatensatz wird angezeigt.

**c.** Wenn nicht ausgewählt, wählen Sie die Registerkarte Gruppenmitglieder aus.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

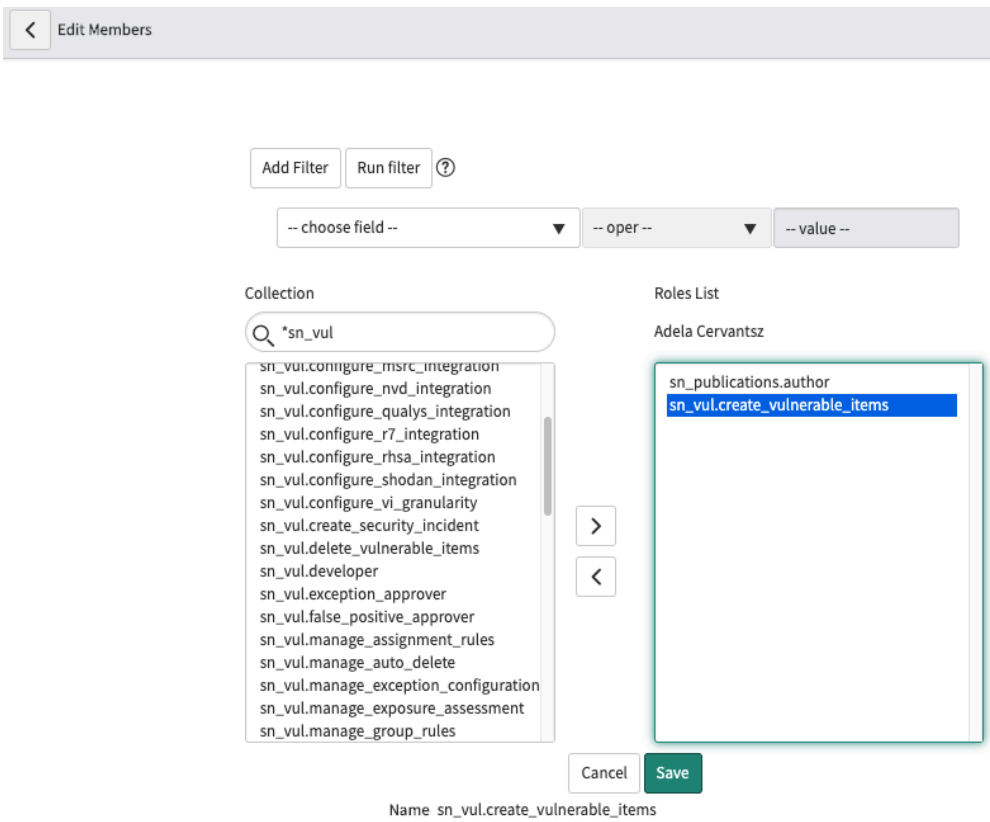
**d.** Klicken Sie in der Liste, der Sie die granulare Rolle zuweisen möchten, auf einen Namen, und öffnen Sie den Datensatz.

**e.** Scrollen Sie im Datensatz zur Registerkarte Rollen, und wählen Sie sie aus.
Die dem Benutzer zugewiesenen Rollen werden angezeigt.

**f.** Klicken Sie auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt.

**g.** Geben Sie im Feld Sammlung den Namen der Rolle ein, wenn Sie ihn kennen, oder geben Sie `*sn_vul` ein, um alle für Vulnerability Response verfügbaren granularen Rollen anzuzeigen.

**h.** Suchen und verschieben Sie sn_vul.create_vulnerable_items in die Rollenliste.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Klicken Sie auf **Speichern**.
Der Benutzerdatensatz wird mit der neuen granularen Rolle angezeigt.

j. Klicken Sie auf den Zurück-Pfeil, um zum Anzeigen der Benutzer im Datensatz für die Gruppe „Korrekturbesitzer“ zurückzukehren

k. Klicken Sie in der Liste, der Sie diese granulare Rolle zuweisen möchten, auf Namen, öffnen Sie deren Datensätze, und verwenden Sie den Slushbucket, um die Rolle zuzuweisen.

l. Nachdem Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.
Sie haben einigen Benutzern in der Gruppe „Korrekturbesitzer“ (sn_vul.remediation_owner) die Berechtigung erteilt, angreifbare Elemente manuell zu erstellen.

4. Führen Sie die folgenden Schritte aus, um eine neue Rolle nur mit den von Ihnen ausgewählten granularen Rollen zu erstellen.
In diesem Beispiel möchten Sie eine Rolle für einen Compliance-Auditor erstellen. Diese Rolle arbeitet eng mit Governance, Risk, and Compliance (GRC) zusammen, und die Aufgabe erfordert die folgenden Berechtigungen und Aufgaben in Vulnerability Response:
   - Verwaltet Korrekturfristen für angreifbare Elemente und Schwachstellengruppen
   - Genehmigt Ausnahmeanforderungen für die Verlängerung von Fristen oder die Zurückstellung der Remediation
   - Verwaltet die Bereinigung älterer angreifbarer Elemente mit automatischer Löschung
   - Definieren Sie Risikopunktzahlen
   - Liest alle Datensätze in Vulnerability Response, darf sie jedoch nicht bearbeiten.

   a. Navigieren zu **Alle** > **Benutzeradministration** > **Rollen**.

   b. Klicken Sie in der Liste „Rollen“ auf **Neu**.

   c. Füllen Sie im Datensatz „Rolle“ die Felder aus.

      Erstellen Sie einen Namen, wählen Sie die Anwendung aus, die diesen Datensatz enthält, und geben Sie eine Kurzbeschreibung für Ihre neue Rolle ein. Weitere Informationen zu den anderen Feldern im Formular finden Sie unter Rollen erstellen

      **Hinweis:**
      Wenn Sie einen Namen für Ihre neue Rolle erstellen, möchten Sie möglicherweise einen Namen verwenden, der in der Rollenliste leicht zu erkennen ist und die Funktionalität der Rolle beschreibt. In diesem Beispiel bevorzugen Sie möglicherweise einen Titel wie „Compliance Auditor – GRC-VR“.

   d. Klicken Sie auf **Absenden**.
   Die Liste „Rollen“ wird angezeigt.

   e. Suchen Sie Ihre neue Rolle, und klicken Sie darauf, um den Datensatz zu öffnen.

   f. Klicken Sie auf **Bearbeiten**.
   Das Formular „Mitglieder bearbeiten“ wird angezeigt.

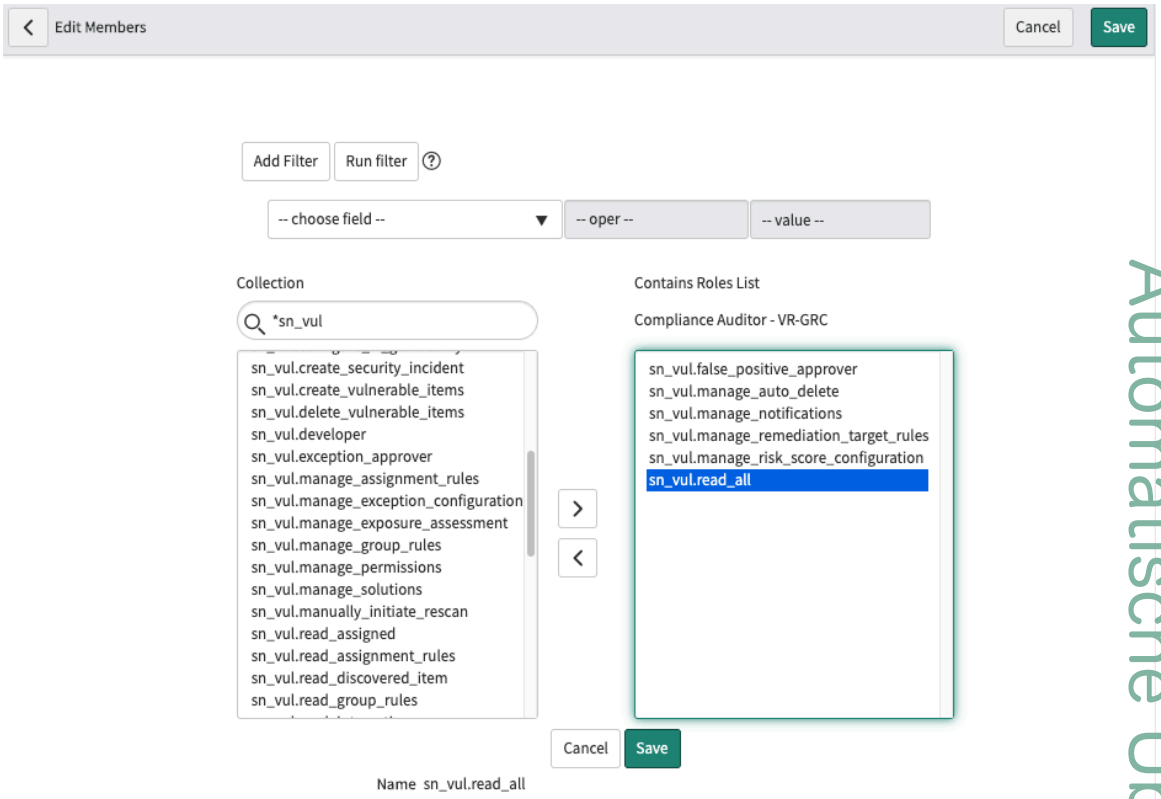


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**g.** Verwenden Sie den Slushbucket, um Ihrer neuen Rolle granulare Rollen hinzuzufügen.

In diesem Beispiel werden die erforderlichen Rollen für diese neue Rolle in der rechten Spalte in der folgenden Abbildung angezeigt.

Um nur die granularen Rollen für Vulnerability Response anzuzeigen, geben Sie im Feld Sammlung *sn_vul ein.




**h.** Klicken Sie auf **Speichern**.
Der Datensatz für Ihre neue Rolle wird angezeigt. Beginnen Sie mit der Registerkarte „Enthält Rollen“ und bearbeiten Sie die Rolle nach Bedarf.

**i.** Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
Ihre neue Rolle wird in der Liste „Rollen“ angezeigt.

## Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten

Installieren Sie mithilfe des Setup-Assistenten die Integrationsanwendungen von Drittanbietern, für die Sie Berechtigungen in Vulnerability Response haben.

### Vorbereitungen

Der Setup-Assistent unterstützt die Installation der meisten Integrationsanwendungen von Drittanbietern mit Vulnerability Response, aber Sie fahren mit der Konfiguration für einige Anwendungen fort, die Sie aus Konfigurationsmodulen in Ihrer Instanz installieren. Unter Vulnerability Response-Integrationen finden Sie eine Liste der Anwendungen, die von Vulnerability Responseunterstützt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

- Nach der Installation erhalten Sie über die Funktion Vulnerability Solution Management von Vulnerability Response Zugriff auf Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten.
- Vulnerability Solution Management ist über ein separates Abonnement verfügbar. Weitere Informationen dazu, wie Vulnerability Solution ManagementVulnerability Response Lösungen integriert, finden Sie unter [].

Bevor Sie Anwendungen von Drittanbietern über den Setup-Assistenten installieren und aktivieren können, führen Sie die folgenden Aufgaben aus, um eine reibungslose Installation zu gewährleisten:

| Setup-Aufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie über gültige ServiceNow Berechtigungen für die Integrationsanwendungen verfügen, die Sie installieren möchten. | Navigieren zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz, um Berechtigungen zu überprüfen. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Weitere Informationen zum Abrufen von Berechtigungen für eine Security Operations -Anwendung von ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab. |
| (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. | Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren und konfigurieren. |
| Wenn noch nicht installiert und aktiviert, müssen Sie Schwachstellendaten mit der geplanten Aufgabe für NVD-Integration und CWE aktivieren und importieren, bevor Sie eine Scanner-Anwendung eines Drittanbieters zum Importieren von Daten ausführen. | Führen Sie die NVD- und CWE-Integrationen als Teil der Ersteinrichtung von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren. Weitere Informationen finden Sie unter Grundlegendes zu den NVD-Integrationen. |
| Vergewissern Sie sich, dass Sie alle Setup-Aufgaben abgeschlossen haben, die für die Drittanbieterintegrationen für Vulnerability Responseerforderlich sind. | Überprüfen Sie alle erforderlichen Setup-Aufgaben für jede Integration, die Sie unter Vulnerability Response-Integrationeninstallieren möchten. |

Erforderliche Rolle: admin

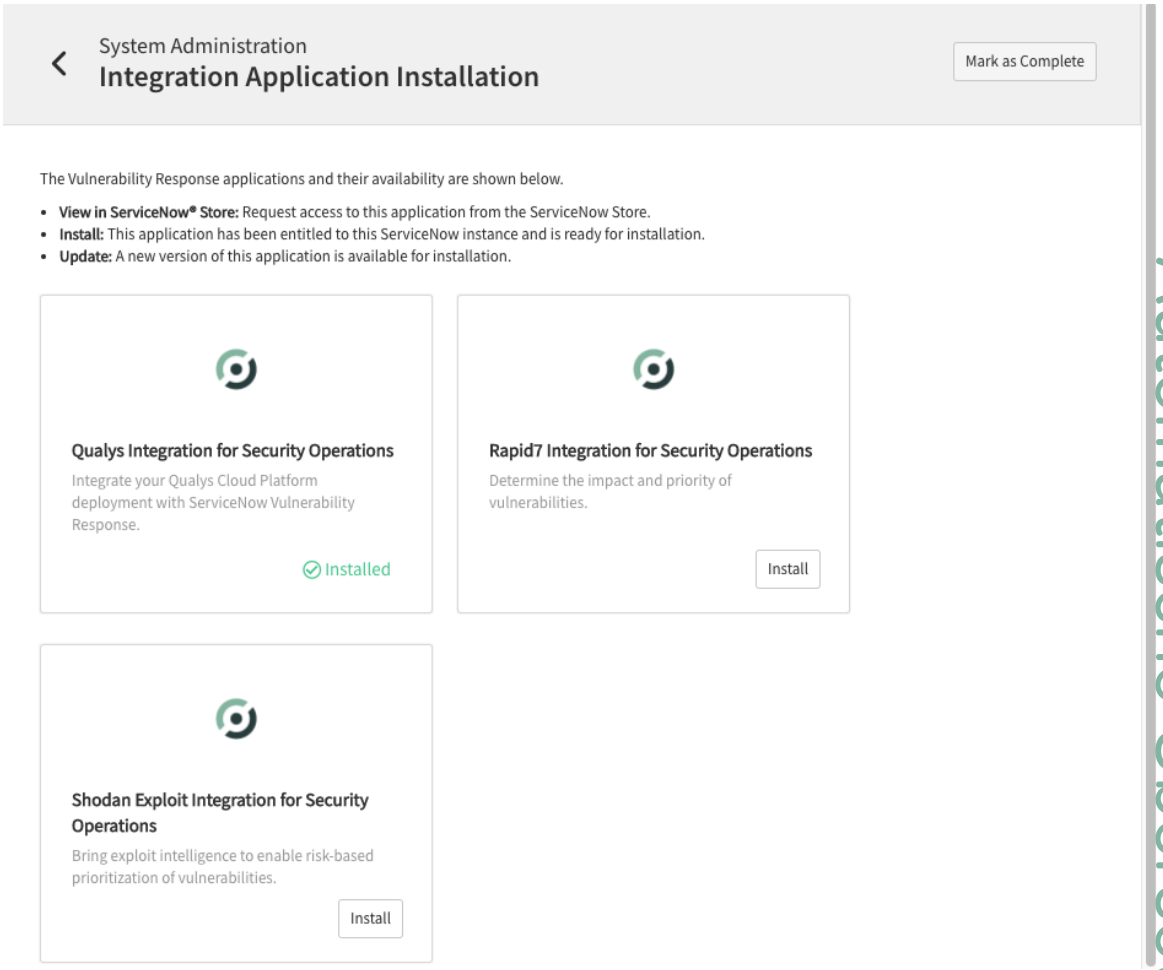


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Systemverwaltung** > **Installation der Integrationsanwendung**.

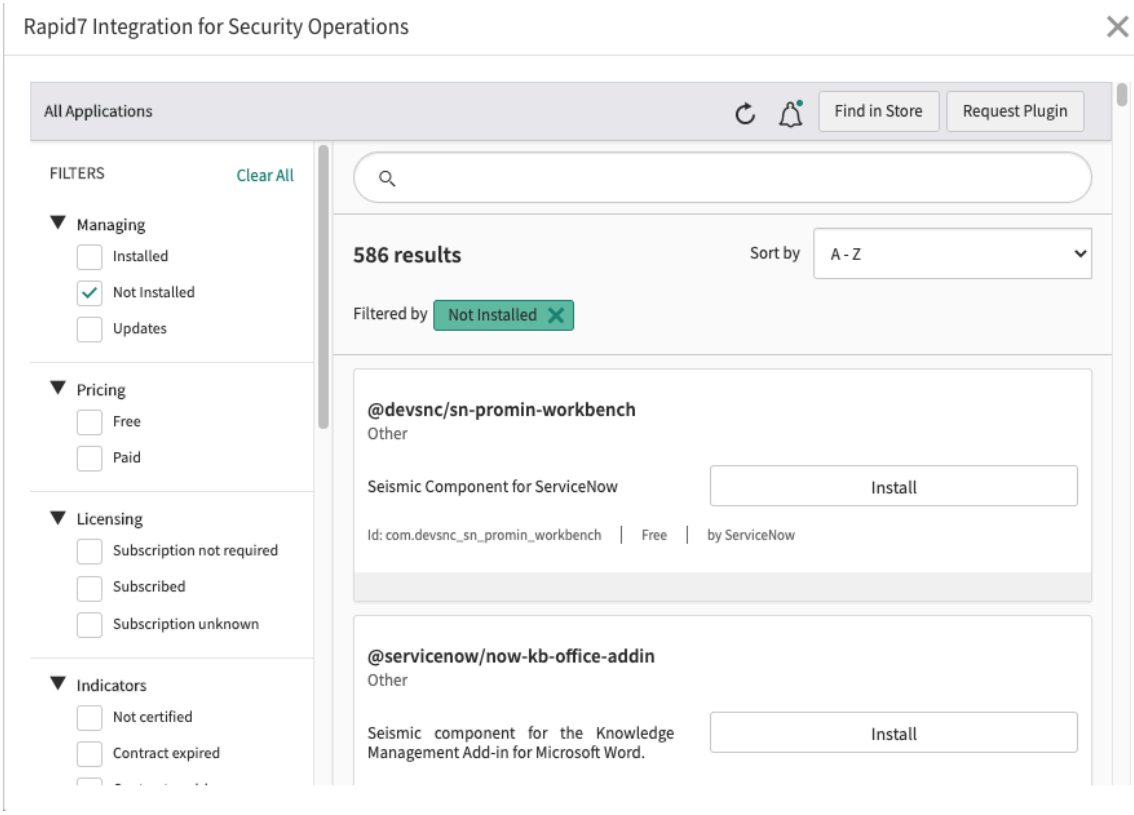
   Nach einigen Minuten werden die Anwendungen angezeigt, für die Sie eine Berechtigung haben und die für die Installation in Ihrer Instanz verfügbar sind.




2. Suchen Sie die Anwendung, die Sie installieren möchten, und klicken Sie auf der Anwendungskachel auf **Installieren**.
   Das Dialogfeld Alle Anwendungen wird mit dem Namen der Anwendungskachel angezeigt, auf die Sie geklickt haben, z. B. Rapid7 Integration for Security Operations, wie in der folgenden Abbildung dargestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

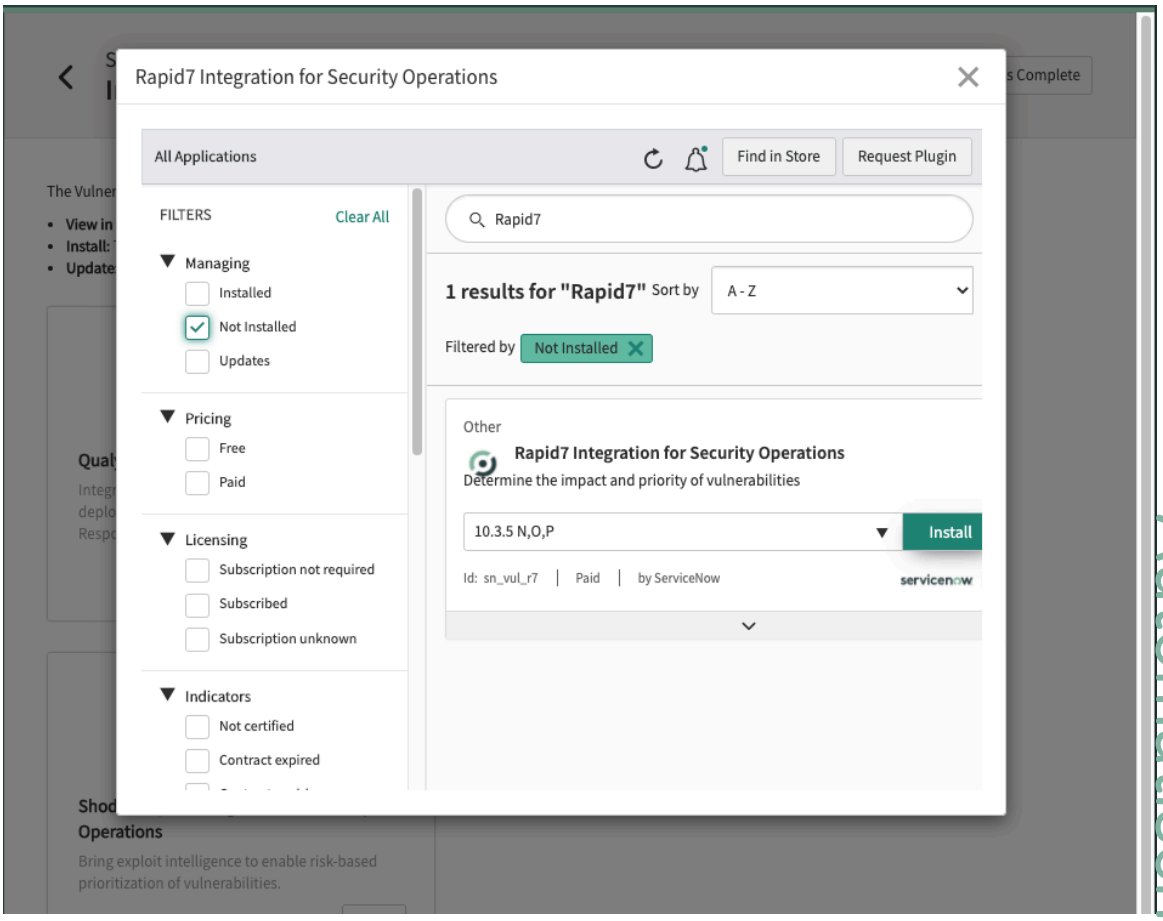



3. Suchen Sie die Anwendung, wählen Sie eine Version aus der Auswahlliste aus, und klicken Sie auf **Installieren**.

   Wenn ein Update für die Anwendung verfügbar ist, wird die Schaltfläche **Aktualisieren** angezeigt.

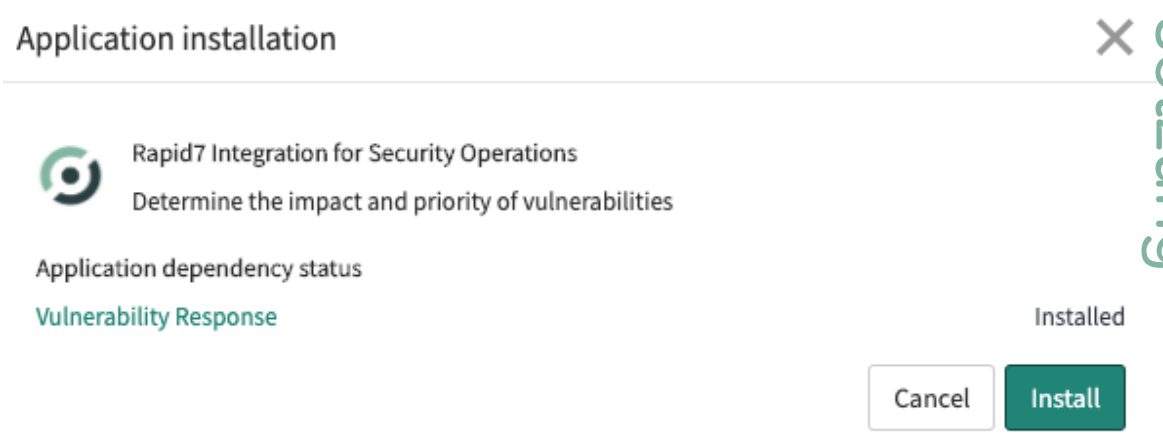
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld „Anwendungsinstallation“ auf **Installieren**.




Im Dialogfeld „Installieren“ wird angezeigt, wenn die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Dialogfeld.
Die Seite Alle Anwendungen wird angezeigt und zeigt an, dass Ihre Anwendung erfolgreich installiert wurde.

Nach der Installation und Aktivierung können Sie die folgenden Anwendungen und installierten Lösungen direkt im Abschnitt „Integrationskonfiguration“ des Setup-Assistenten konfigurieren, planen und starten:

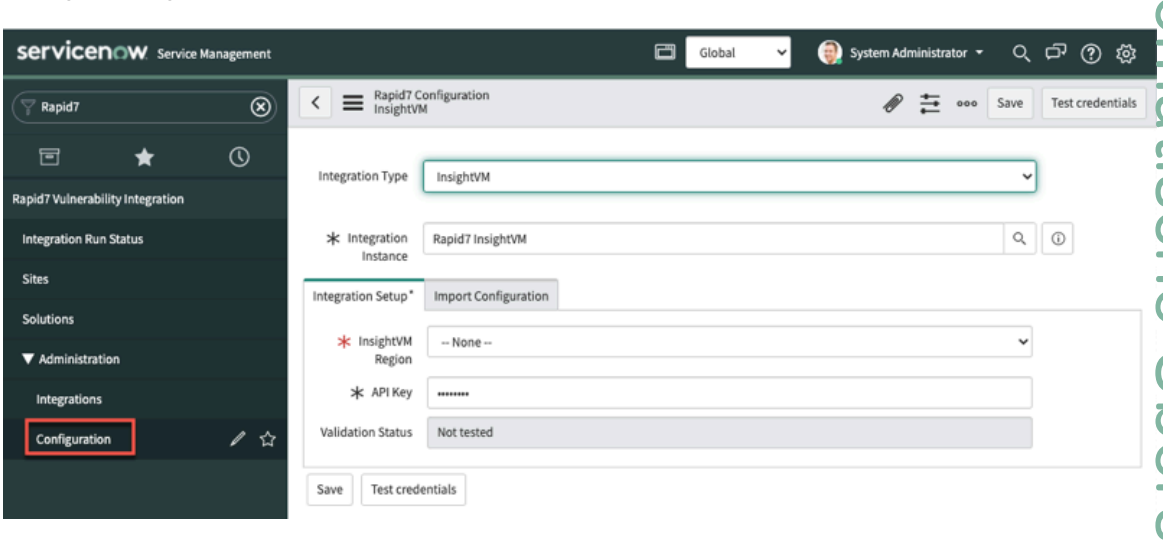
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Qualys Vulnerability Integration
- Vulnerability Response Integration with Tenable.
- Die Integration der Microsoft Security Response Center-Lösung
- Die Red Hat Solution Integration
- Integration der Microsoft Security Response Center-Lösung
- Die Integration von Microsoft Defender Threat and Vulnerability Management .

Navigieren Sie für andere Anwendungen, die oben nicht aufgeführt sind, direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren und die erforderlichen Anmeldeinformationen von Drittanbietern einzugeben. Die folgende Abbildung zeigt beispielsweise den Speicherort der Konfiguration und des Moduls für die Anwendung Rapid7.

Weitere Informationen zum Konfigurieren bestimmter Anwendungen finden Sie in der Installations- und Konfigurationsproduktdokumentation nach Produktnamen, die für jede Anwendung bereitgestellt werden.




**Nächste Maßnahme**
Fahren Sie mit der Konfiguration Ihrer Anwendung im Setup-Assistenten fort, wenn Ihre Anwendung unterstützt wird.

Wenn Ihre Anwendung für die Konfiguration im Setup-Assistenten nicht unterstützt wird, navigieren Sie direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren. Informationen zum Anzeigen unterstützter Anwendungen im Setup-Assistenten finden Sie unter, Installation von Vulnerability Response und unterstützten Anwendungen.

### Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern

Falls noch nicht installiert, laden Sie die NVD-Integration herunter, führen Sie sie aus, und führen Sie die geplante CWE-Aufgabe als Teil der Ersteinrichtung von Vulnerability Response und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt einer Drittpartei aus. Vulnerability Response Integration with NVD ist im ServiceNow Storeverfügbar.

## CWE- und NVD-Daten werden erfasst

Importierte Daten aus den NVD- und CWE-Integrationen werden verwendet, um die Schwachstellendaten in Ihrer Instanz anzureichern und Ihnen bei der Entscheidung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu helfen, ob die Korrektur für eine Schwachstelle, ein angreifbares Element oder eine Korrekturaufgabe eskaliert werden soll. Nach einem ersten Import können Sie Bibliotheksdatensätze bei Bedarf aktualisieren oder eine regelmäßige Aufgabe so konfigurieren, dass die Datensätze regelmäßig aktualisiert werden. Vulnerability Response speichert sie unter **Libraries**.

Das Common Vulnerability Scoring System (CVSS), das in NVD- und Drittanbietereinträgen enthalten ist, erfasst die Hauptmerkmale einer Schwachstelle. Vulnerability Response verwendet CVSS-Daten, um einen normalisierten Wert zu erzeugen, der den Schweregrad der Schwachstelle widerspiegelt. Wenn der Schweregrad berechnet wird, bietet die Schwachstelle ein besseres Verständnis des Risikos, das diese Schwachstelle für Ihre Organisation darstellt. Der Schweregrad hilft Ihnen, die Korrektur von Schwachstellen zu bewerten und zu priorisieren.

Wenn dies Ihre erste Installation von Vulnerability Responseist oder bevor Daten zum ersten Mal mit einem Scanner-Produkt einer Drittpartei erfasst werden:

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000-Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus. Sie führen CWE-Aktualisierungen **bei Bedarf** standardmäßig über den Integrationsdatensatz durch und müssen sie konfigurieren, wenn sie als geplante Aufgabe ausgeführt werden sollen.

   **Hinweis:**
   Planen Sie das CWE-Update so, dass es vor dem Update der NVD-Datenbank ausgeführt wird. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

2. Stellen Sie sicher, dass die Anwendung Vulnerability Response Integration with NVD installiert ist und Daten aus der NIST National Vulnerability Database Integration – API (nur CVE) oder der NIST National Vulnerability Database Integration – API (CVE und CPE) erfolgreich importiert wurden.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nach der Installation wird die Integration der NIST National Vulnerability Database Integration - API (nur CVE) standardmäßig aktiviert. Sie wird täglich ausgeführt. Weitere Informationen finden Sie unter Grundlegendes zu den NVD-Integrationen und Installieren Sie Vulnerability Response Integration with the NIST National Vulnerability Database.

3. Bibliotheken von Drittanbietern werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

## Importierte Schwachstellendaten und angreifbare Elemente anzeigen

Die folgenden Bibliotheken sind verfügbar:

| Bibliotheken | Beschreibung |
|---|---|
| NVD | Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken, einschließlich Exploits. |
| CWE | Liste der von der Community entwickelten Softwareschwachstellentypen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Bibliotheken | Beschreibung |
|---|---|
| | Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur als Referenz. |
| Drittpartei | Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste der zugehörigen Referenzen, angreifbaren Elemente, Exploits und CVEs. |

**Zugehörige Informationen**

Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an

### Anwendung Solution Management for Vulnerability Response installieren

Bevor Sie die Funktion Solution Management for Vulnerability Response von Vulnerability Response in Ihrer Instanz verwenden können, müssen Sie die Installation der Anwendung Vulnerability Solution Management abschließen. Diese Anwendung ist als separates Abonnement im ServiceNow Storeverfügbar.

## Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Führen Sie diese Setup-Aufgaben für eine reibungslose Installation aus.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration sind die Lösungsanwendungen, die nach der Installation von Vulnerability Solution Managementin Solution Management for Vulnerability Response verfügbar sind.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Solution Management for Vulnerability Response erfordert die Anwendung Vulnerability Response.<br><br>Stellen Sie für die aktuelle Version von Vulnerability Solution Managementsicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben. Weitere Informationen finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix und Release Schema Changes .<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Sie über Berechtigungen für die Anwendung verfügen. | Um zu überprüfen, ob Sie über Berechtigungen für die Anwendung Vulnerability Solution Management verfügen, |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| | navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Informationen zum Abrufen der Berechtigung für die Anwendung Vulnerability Solution Management von ServiceNow Store und zum Herunterladen in Ihre Instanz von Now Platform finden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab. |
| Stellen Sie sicher, dass Ihre NVD-Datensätze für die letzten 10 Jahre auf dem neuesten Stand sind. | Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern. |
| Stellen Sie sicher, dass Ihre Drittpartei-Schwachstellen auf dem neuesten Stand sind. | Weitere Informationen zu Schwachstellenintegrationen von Drittparteien finden Sie unter Vulnerability Response-Integrationen. |
| Vergewissern Sie sich, dass Ihnen die erforderlichen Rollen Now Platform für Ihre Instanz zugewiesen sind. | Die folgenden Rollen sind für die Installation und Überprüfung der erwarteten Ergebnisse erforderlich:<br><br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.<br><br>• Der Systemadministrator [admin] installiert die Anwendung. Falls noch nicht zugewiesen, weist der Administrator die Rolle „Schwachstellenadministrator“ [sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)] zu.<br>• Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rollen: admin für die Installation der Anwendung Vulnerability Solution Management und Schwachstellenadministrator für die Konfiguration.

### Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie **auf Anmelden,** und geben Sie Ihre HI-Anmeldeinformationen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die Registerkarte **ServiceNow-Produkte**, um die verfügbaren ServiceNow Produkte anzuzeigen.
4. Klicken Sie auf das Pluszeichen (**+**) neben **Vulnerability Solution Management**, um alle zugehörigen Anwendungen anzuzeigen, für die Sie berechtigt sind.
5. Klicken Sie auf **Opt-in**, um zu bestätigen, dass Sie über die Berechtigung für Vulnerability Solution Management für die Anwendung verfügen.
6. Wenn Sie bereits berechtigt sind, fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Instanz Now Platform zu installieren.
7. Aktivieren Sie das Kontrollkästchen, und klicken Sie bei der Eingabeaufforderung auf **Akzeptieren**, um den Nutzungsbedingungen zuzustimmen.
   Eine Nachricht wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung entschieden haben.
8. **Wahlweise:** Klicken Sie auf Berechtigung verwalten, wenn Sie Ihre Berechtigung für Vulnerability Solution Management in anderen Now Platform Instanzen verwalten möchten.

   **Hinweis:**
   Wenn die Schaltfläche **Berechtigung verwalten** nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung **Vulnerability Solution Management**, um sie anzuzeigen.

   a. Option wählen

   b. Klicken Sie auf **OK** oder **Abbrechen**, um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung in Ihren Instanzen zu installieren.

9. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Solution Management installieren möchten.
10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
11. Suchen Sie die Anwendung Vulnerability Solution Management (sn_vul_solution), und klicken Sie auf **Installieren**.
    Im Dialogfeld „Anwendungsinstallation“ wird der Status des Plugins für Anwendungsabhängigkeiten angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.
12. Klicken Sie auf **Installieren**.
    Diese Installation kann einige Zeit in Anspruch nehmen. Eine Nachricht wird im Dialogfeld „Installieren“ angezeigt, nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden.

    Der Schwachstellenadministrator kann die Anwendung jetzt über den Setup-Assistenten konfigurieren.

13. Klicken Sie auf **Schließen**.

Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration sind die Lösungsanwendungen, die nach der Installation von Vulnerability Solution Managementin Solution Management for Vulnerability Response verfügbar sind.

Zeigen Sie die Schwachstellenlösungen an, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Nachdem Sie die Anwendung und die verfügbaren Lösungen konfiguriert haben, überprüfen Sie mithilfe der Tabelle „Schwachstellenlösung“ [sn_vul_m2m_vulnerability_solution], ob CVEs und Lösungen übereinstimmen.

### Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA].

Bevor Sie die Anwendung Performance Analytics for Vulnerability Response verwenden können, müssen Sie die Berechtigung erwerben und die Anwendung aus dem ServiceNow Storeherunterladen, in Ihrer Instanz von Now Platform® ] installieren und einige Installations- und Konfigurationsschritte ausführen. Die PA-Anwendung wird nicht als Teil der Anwendung Vulnerability Response installiert. Sie ist als separates Abonnement verfügbar.

### Vorbereitungen

Wenn Sie die Anwendung bereits in Ihrer Instanz haben und auf eine neuere Version der Anwendung aktualisieren, fahren Sie mit Schritt 8 in den folgenden Schritten fort, um mit der Aktualisierung und Konfiguration fortzufahren.

Führen Sie für eine Neuinstallation vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Um zu überprüfen, ob Plugins und Anwendungen installiert und aktiviert sind, navigieren Sie zu **Alle** > **Subscription Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass das Plugin „Vulnerability Response Dependencies“ (com.snc.vul_dep) installiert und aktiviert ist. | **Vulnerability Response-Abhängigkeiten**<br>Dieses Plugin enthält alle Abhängigkeits-Plugins, die zur Unterstützung der Anwendung erforderlich sind.<br>Um zu überprüfen, ob das Plugin installiert und aktiviert ist, navigieren Sie in Ihrer Instanz, zu der die Anwendung navigieren soll **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.<br>Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern, und folgen Sie den Anweisungen, um fortzufahren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass die Anwendung ServiceNow Vulnerability Response (sn_vul) installiert und aktiviert ist. | **Vulnerability Response**<br><br>Um zu überprüfen, ob das Plugin installiert und aktiviert ist, navigieren Sie in Ihrer Instanz, zu der die Anwendung navigieren soll **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.<br><br>Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern, und folgen Sie den Anweisungen, um fortzufahren.<br><br>Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Wenden Sie sich an ServiceNow, um Einzelheiten zu erfahren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen.<br><br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br><br>• Der Performance Analytics-Administrator [pa_admin] oder der Systemadministrator [admin] installiert die Anwendung und überprüft die erwarteten Ergebnisse.<br>• Der Schwachstellenadministrator [sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse mit den PA-Dashboards.<br>• Der Korrekturbesitzer [sn_vul.remediation_owner] überwacht Change-Management-Aufgaben und liest und aktualisiert zugewiesene Datensätze. Die Rolle „sn_vul.remediation_owner“ wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle „itil“ zugewiesen wird. |
| Stellen Sie sicher, dass die Anwendungen Performance Analytics und Vulnerability Response kompatibel sind. | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

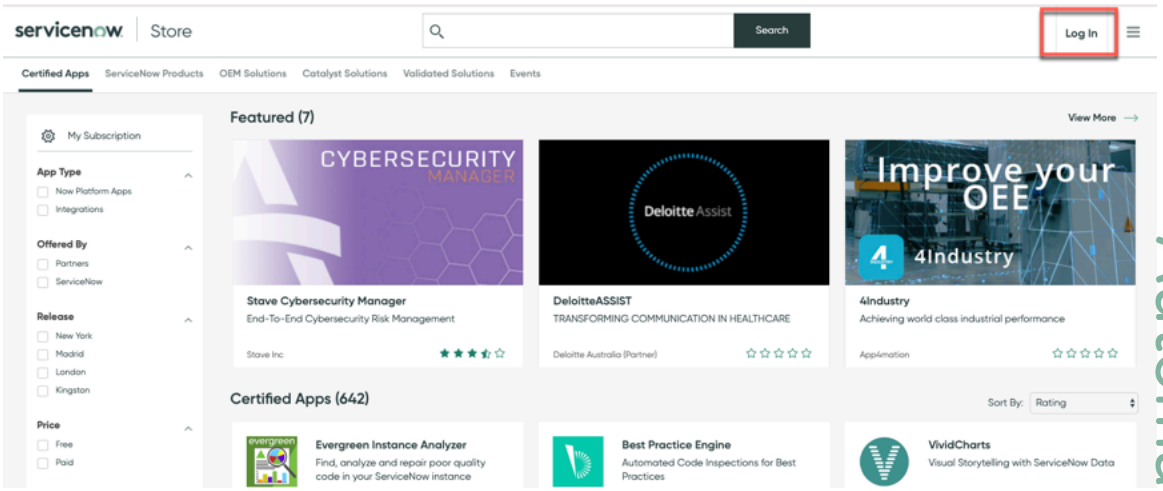


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

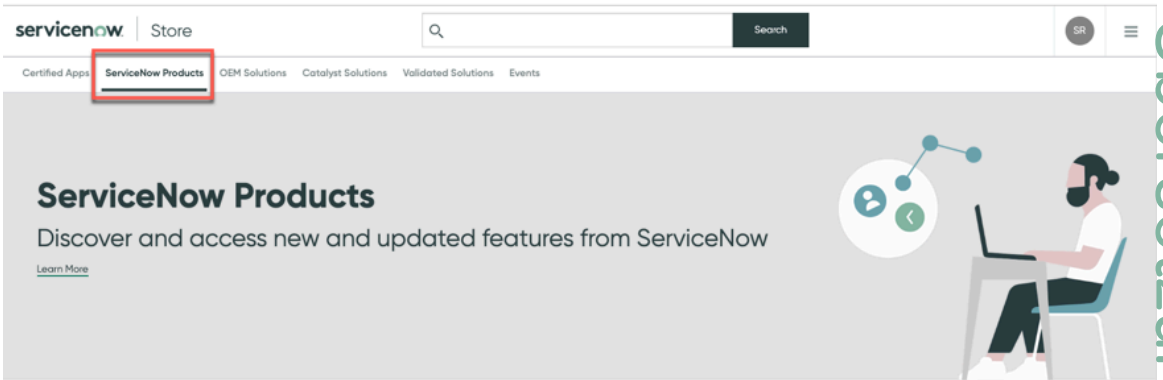
Erforderliche Rolle: admin oder pa_admin

### Prozedur

1. Um die Berechtigung zu erhalten und die Anwendung in Ihrer Instanz Now Platform herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Anmelden**.




3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
4. Wenn diese Option nicht ausgewählt ist, klicken Sie auf der angezeigten Seite auf die Registerkarte **ServiceNow-Produkte**.



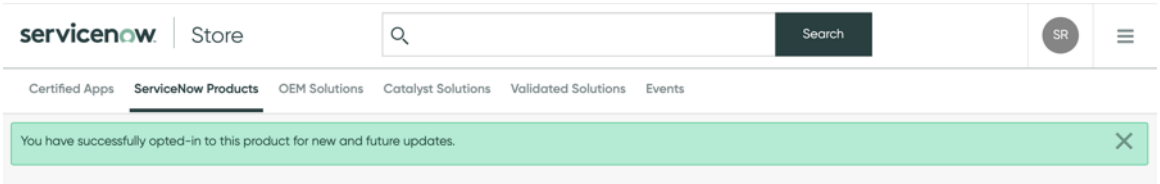

5. Klicken Sie auf der Produktlistenseite auf **Performance Analytics - Vulnerability Response**.

6. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
   Eine Seite mit der Schaltfläche Opt-in wird angezeigt.
7. Klicken Sie auf **Opt-in**, um die Anwendung Performance Analytics for Vulnerability Response zu erhalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.

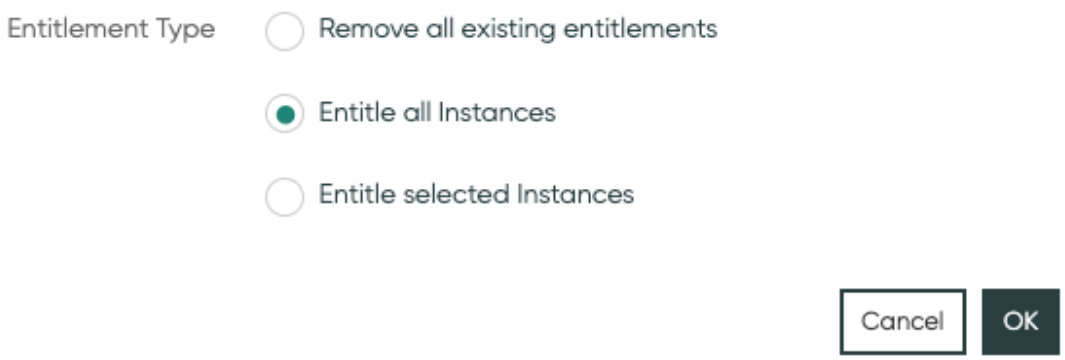



9. **Wahlweise:** Alternativ führen Sie die folgenden Schritte aus, um Ihre Berechtigung für die Anwendung in anderen Now Platform -Instanzen zu verwalten.

   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung Performance Analytics for Vulnerability Response, um sie anzuzeigen.

   b. Klicken Sie bei ausgewählter Registerkarte Berechtigt auf **Berechtigung verwalten**.

   c. Wählen Sie im angezeigten Dialogfeld „Berechtigungen für Vulnerability Response verwalten“ eine der folgenden Optionen aus:

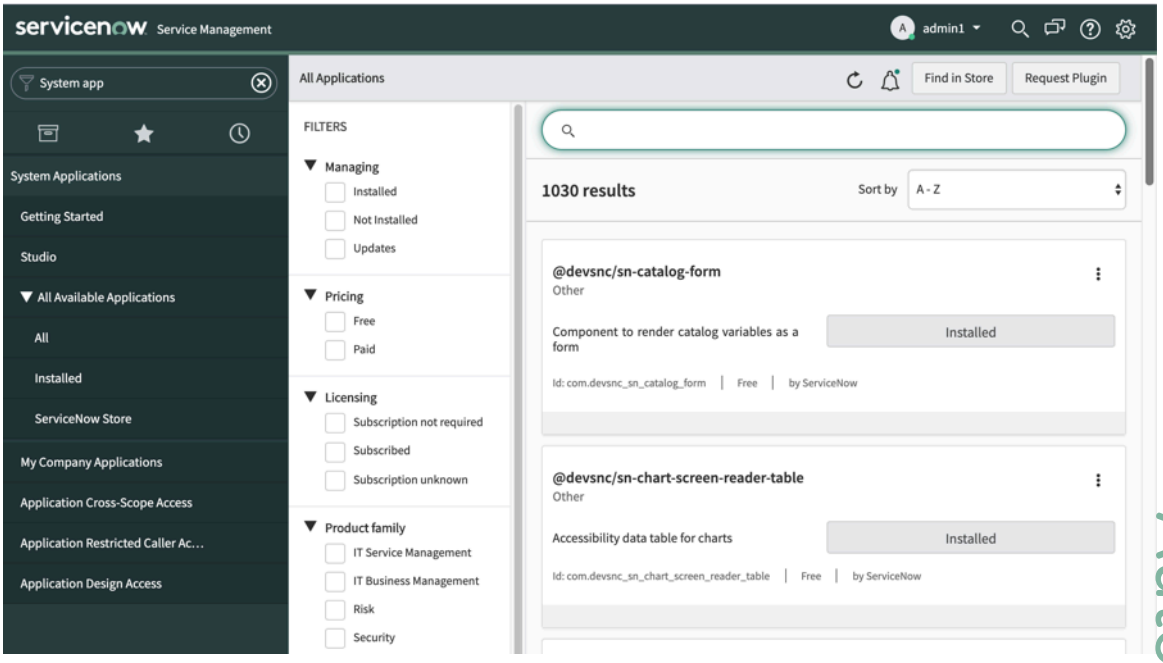



   d. Klicken Sie auf **OK** oder **Abbrechen**, um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihren Now Platform Instanzen zu installieren.

10. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Vulnerability Response installieren möchten.
11. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




12. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Performance Analytics - Content Pack - Vulnerability Response (sn_vul_analytics), und klicken Sie auf **Installieren**.

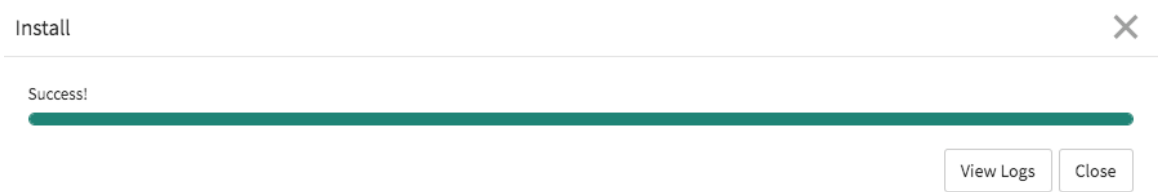
    **Hinweis:**
    Wenn Sie auf eine neue Version aktualisieren, wählen Sie die gewünschte Version aus der Auswahlliste aus.

    und klicken Sie auf **Aktualisieren**.
    Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle Abhängigkeiten, die automatisch mit der Anwendung installiert werden, werden ebenfalls angezeigt.

13. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren**.

    **Hinweis:**
    Wenn Sie das Kontrollkästchen Demodaten laden nicht aktivieren, können die **Demodaten** nachträglich nicht über den **Anwendungsmanager** installiert werden. Weitere Informationen dazu, wie Sie Demodaten nach der Erstinstallation installieren oder erneut installieren, finden Sie im Artikel Workaround to install demo data if application is opened (Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist) [KB0722909] in der Knowledge Base von Now Support.

    Diese Installation kann einige Zeit in Anspruch nehmen. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Meldung angezeigt.




14. Klicken Sie auf **Schließen**.

15. **Wahlweise:** Wenn Sie eine große Anzahl aktiver angreifbarer Elemente in Ihrer Umgebung erwarten, sollten Sie die Standardeinstellung für die maximale Anzahl der erfassten Datensätze ändern, geplante Aufgaben aktivieren und Erfassungszeiten außerhalb der Geschäftszeiten festlegen.

Automatische Übersetzung

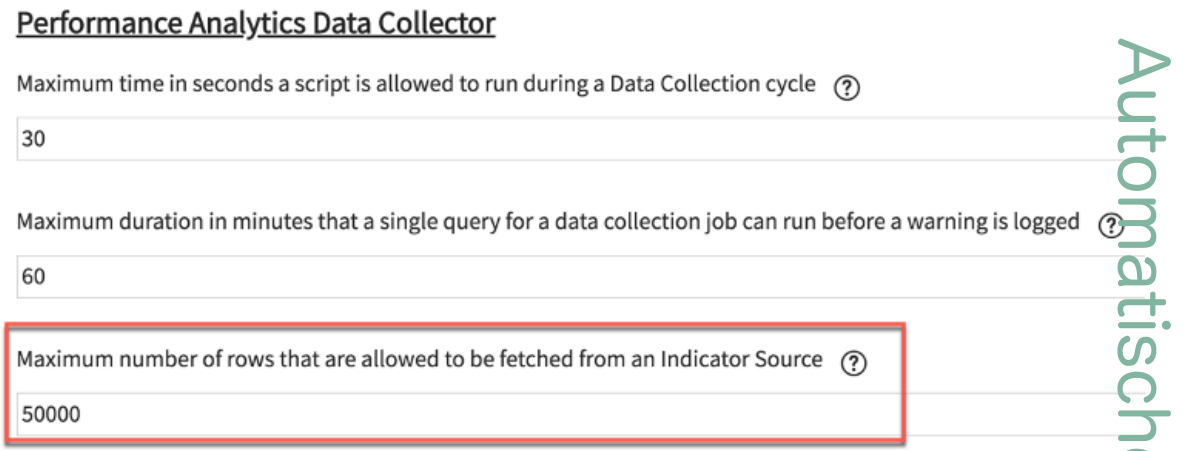
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie die folgenden Schritte aus, um diese und andere Einstellungen für die Anwendung nach der Installation zu ändern.

**a.** Navigieren zu **Alle** > **Performance Analytics** > **Administratorkonsole**.

**b.** Klicken Sie auf der Kachel „Erweiterte Konfiguration“ auf den Link **Performance Analytics-Eigenschaften**.

**c.** Scrollen Sie auf der Seite „Administratorkonsole [Performance Analytics]“ zum Abschnitt „Performance Analytics Data Collector“.
Die Standardeinstellung (50.000 Datensätze) wird für die maximale Anzahl von Zeilen angezeigt, die aus einer Indikatorquelle abgerufen werden dürfen.




**d.** Sie können diese Anzahl auf einen Wert erhöhen, der ungefähr 20 % höher ist als die Gesamtzahl der aktiven angreifbaren Elemente (VIs), die Sie in Ihrer Umgebung erwarten.

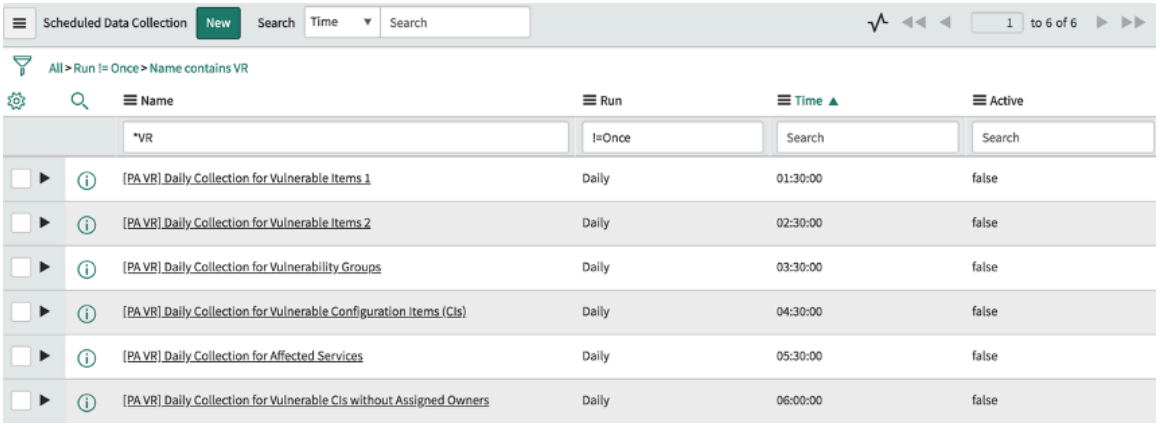
**e.** Klicken Sie auf **Speichern**.

**f.** Um regelmäßige Aufgaben zu aktivieren, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**.
Die Liste Geplante Datensammlung wird angezeigt. In der Spalte Aktiv sind die geplanten Aufgaben, die in der Spalte Anwendung für Performance Analytics - Content Pack - Vulnerability Response aufgeführt sind, standardmäßig deaktiviert (false).

**Hinweis:**
Eine geplante Aufgabe für die Verlaufsdatenerfassung wird nicht in der Liste der Aufgaben angezeigt. Bei großen Datensätzen ziehen Sie es möglicherweise vor, Daten und Trends im Laufe der Zeit zu sammeln, indem Sie Ihre täglichen Aufgaben aktivieren, wenn Sie die Anwendung Performance Analytics für Vulnerability Response einrichten.

Automatische Übersetzung

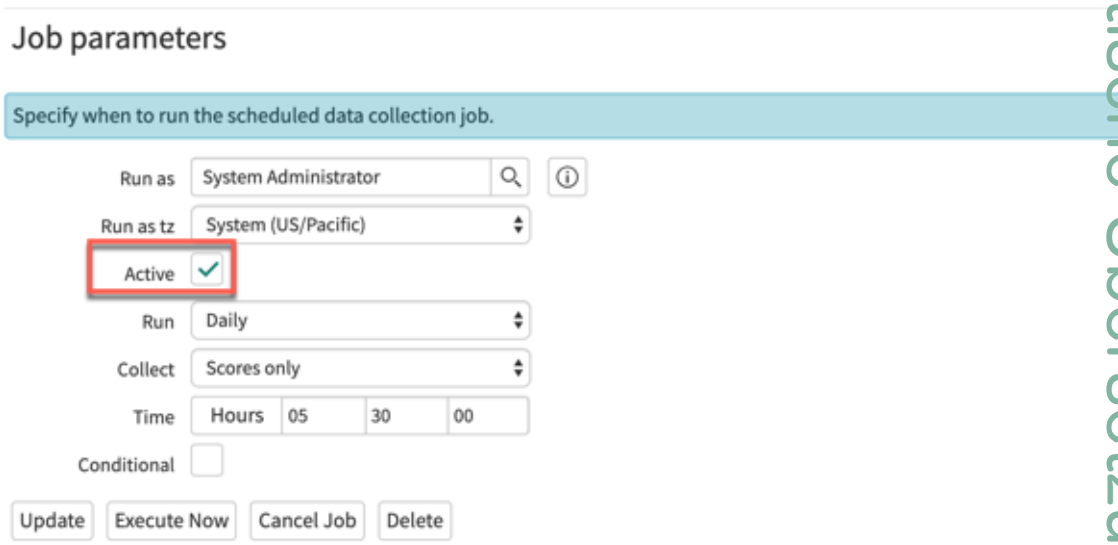
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**g.** Klicken Sie in der Spalte Name auf einen Link, um einen PA_VR-Auftragsdatensatz zu öffnen.

**h.** Wenn Felder nicht bearbeitet werden können, klicken Sie auf den Link **hier**, um sie zu bearbeiten.

**i.** Klicken Sie im Abschnitt „Auftragsparameter“ auf das Kontrollkästchen Aktiv, um einen Auftrag zu planen.
Die Zeitfelder werden angezeigt.




**j.** Geben Sie die Startzeit für die Aufgabe ein.
Wenn Sie mit einem großen Volumen rechnen, ziehen Sie es möglicherweise vor, die Erfassungszeiten außerhalb der Geschäftszeiten festzulegen. Wenn Sie in Ihrer Umgebung mit 10 Millionen aktiven AEs oder mehr rechnen, wenden Sie sich an Ihren ServiceNow® -Implementierungspartner, um weitere Informationen zum Einrichten Ihrer Datenerfassungsumgebung zu erhalten.

Weitere Informationen zu den für die Datenerfassung verwendeten Indikatoren finden Sie unter Indikatoren [ Performance Analytics für Vulnerability Response [PA] anzeigen.

**k.** Nachdem Sie alle gewünschten Aufträge aktiviert haben, klicken Sie auf **Aktualisieren**.
Die Liste Geplante Datensammlung wird angezeigt. Weitere Informationen finden Sie unter Performance Analytics-Eigenschaften .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Navigieren zu **Vulnerability Response** > **Übersicht** , um das Dashboard anzuzeigen.

#### Erstellen oder bearbeiten Sie Vulnerability Response Zuweisungsregeln

Nachdem Sie Ihre erste Bewertung der Zuweisungsregeln mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen angreifbare Elemente zu, wenn sie importiert oder manuell erstellt werden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem enthält die Zuweisungsregel für Schwachstellen, **An CI-Supportgruppe zuweisen**, die angreifbare Elemente derselben Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel kann mithilfe von Filterbedingungen geändert werden, oder Sie können eine neue Regel erstellen. Mit Zuweisungsregeln definieren Sie die Bedingungen der Zuweisung und die Reihenfolge der Ausführung. Sobald ein VI mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Öffnen Sie die Regel **An CI-Supportgruppe zuweisen,** oder klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

#### Zuweisungsregel für Schwachstellen

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppenregel. |
| Aktiv | Gibt an, ob die Zuweisungsregel aktiv ist. |
| Ausführungsbefehl | Reihenfolge, in der die Regeln ausgewertet werden.<br><br>Regeln mit hoher Priorität, Elemente, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist, oder ein VI, die von der Compliance mit gesetzlichen Vorschriften behandelt werden müssen, müssen zuerst ausgeführt werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist oder , und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um AEs der Gruppe zuzuweisen, die ermittelt, zu welcher Zuweisungsgruppe sie gehören soll. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt. |
| Beschreibung | Beschreibung der Zuweisungsregel. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Bedingung | |
| Vorschau | Zeigt an, wie viele Ergebnisse diese Abfrage zurückgibt. |
| Bedingungsfelder | Bedingungen, die erfüllt sein müssen.<br><br>**Hinweis:**<br>Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar zu machen, müssen Sie die Rapid7 InsightVM Asset-Listen-Integration vor den anderen Rapid7 InsightVM -Integrationen ausführen.<br><br>Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt. |
| Neues Kriterium | Fügt weitere Bedingungsfilterfelder hinzu, aus denen Sie auswählen können. |
| Zuweisen mit | Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.<br>○ Benutzergruppe: Wählen Sie eine Benutzergruppe aus der Suchtabelle aus.<br>○ Benutzergruppenfeld: Wählen Sie im Dropdown-Menü ein Benutzergruppenfeld aus.<br>○ Skript: Erstellen oder bearbeiten Sie ein Skript.<br><br>**Hinweis:**<br>Das Erstellen oder Bearbeiten eines Skripts erfordert Kenntnisse von ServiceNow. |

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import bewertet.

**Hinweis:**

Die Funktion „Erneut anwenden“ erfordert eine Baselineanwendung der Regeln. Sobald Ihre Regeln erstellt wurden, aktivieren Sie, falls noch nicht geschehen, die geplante Aufgabe *`Reapply all vulnerability assignment rules`*, um sie nach Belieben auszuführen. Sie wendet alle Regeln auf alle offenen AEs mit Ausnahme der manuell zugewiesenen an. Je nachdem, wie viele aktive AEs in Ihrer Umgebung vorhanden sind, müssen Sie das Feld **Ausführen** nach der ersten Ausführung entsprechend festlegen, um Auswirkungen auf die Leistung zu vermeiden.

Wenn Sie diese regelmäßige Aufgabe nicht ausgeführt haben und versuchen, die Schaltfläche **Änderungen** übernehmen im Formular „Zuweisungsregeln“ zu verwenden, müssen Sie dies nachholen. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

### Erstellen Sie eine Vulnerability Response -Zuweisungsregel mit ML

Verwenden Sie das folgende Skript, um eine Ausweichkontakt-Zuweisungsregel für angreifbare Elemente zu erstellen, die ML-Empfehlungen von Predictive Intelligence verwendet, um sie automatisch zur Korrektur zuzuweisen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Die Anwendung Vulnerability Assignment Recommendations for Vulnerability Response muss installiert und aktiviert sein. Diese Anwendung ist auf der ServiceNow Storeverfügbar.

Eine Klassifizierungslösung muss definiert, aktiv und trainiert sein. Sie verwenden dieses Modell, um die geeignete Zuweisungsgruppe für angreifbare Elemente (AEs) in Fällen vorherzusagen, in denen Ihre Zuweisungsregeln keine richtige Übereinstimmung für die beabsichtigten Empfänger gefunden haben.

Diese Regel kann Ihnen helfen, die Anzahl der nicht zugewiesenen AEs zu reduzieren, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

Weitere Informationen finden Sie unter Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren und Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird

Möglicherweise möchten Sie diese Aufgabe nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung verfügen oder über fundierte Kenntnisse über Now Platform, seine Predictive Intelligence-Funktionen und die Funktionsweise von Zuweisungsregeln verfügen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Zuweisungsregeln.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option **Skript**aus.
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
   /*
   * Catch-all assignment rule using ML recommendation
   * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
   * Classification Solution must be active and trained
   */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
   var ARU = new sn_vul.AssignmentRecommendationUtils();
   ARU.initialize();

   var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
   /*
   *returns object containing array of predictions
   *payload structure:
   *
   {
      "predictions": [
         {
            "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
            "name": "Windows Server support ",
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "confidence_score": "57.54"
        },
        ...
    ],
    "exception": ""
}
*/
var viPredictionArray = viPredictionObj['predictions'];
var topPredictionObj = viPredictionArray.shift();

return topPredictionObj['sys_id'];
}
```

6. Wählen Sie **Absenden**.

### Nächste Maßnahme

Überprüfen Sie Vulnerability Response Übersicht über Zuweisungsregeln auf allgemeinere Informationen zu Zuweisungsregeln und der geplanten Aufgabe *`Reapply all vulnerability assignment rules`*.

## Erstellen Sie eine Vulnerability Response -Zuweisungsregel für den Service-Support

Verwenden Sie das folgende Skript, um eine Regel zu erstellen, die angreifbare Elemente basierend auf den betroffenen Business Services zur Korrektur zuweist.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird

Möglicherweise möchten Sie diese Aufgabe nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung verfügen oder über fundierte Kenntnisse über Now Platform und die Funktionsweise von Zuweisungsregeln verfügen.

Mit dieser Regel werden AEs entsprechend ihrer Übereinstimmung mit den in Ihrer CMDB aufgeführten Business Services zugewiesen. Wenn keine zugehörigen Services, Abteilungen oder Supportgruppen übereinstimmen, werden AEs der Gruppe „Schwachstellenanalyst“ zugewiesen.

Diese Regel kann Ihnen helfen, die Anzahl der falsch zugewiesenen oder nicht zugewiesenen AEs zu reduzieren, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Zuweisungsregeln.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option **Skript**aus.
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
      hasSvc = svc.next();
   }
   if (!hasSvc) {
      // If there are no services it should be assigned to a default assignent group
      return defaultAssignmentGroupID;
   } else {
      var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
      return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
   }
}
```

6. Wählen Sie **Absenden**.

### Nächste Maßnahme

Überprüfen Sie Vulnerability Response Übersicht über Zuweisungsregeln auf allgemeinere Informationen zu Zuweisungsregeln und der geplanten Aufgabe *`Reapply all vulnerability assignment rules`*.

#### Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben

Nachdem Sie Ihre erste Bewertung der Regeln für Korrekturaufgaben mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente basierend auf Filterbedingungen automatisch zu gruppieren. Diese Regeln gruppieren angreifbare Elemente automatisch, wenn sie importiert oder manuell erstellt werden. Verwenden Sie den Filter, um die nach dieser Regel gruppierten angreifbaren Elemente zu begrenzen, z. B. Auswahl aller angreifbaren Elemente mit Exploits.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird
Das Basissystem wird mit der Korrekturaufgabenregel **Schwachstelle**geliefert, die angreifbare Elemente nach Schwachstelle und Zuweisungsgruppe (aus **Zuweisungsregeln**) gruppiert. Sie können die Regeln aus dem Formular oder der Listenansicht erneut anwenden. Für einige Beispieleinträge Vulnerability Response Beispiele für Korrekturaufgabenregeln.

Diese Regel kann wie folgt geändert werden:

Durch Verwenden von Filterbedingungen und Gruppieren nach Auswahlmöglichkeiten.

Standardmäßig verwenden Korrekturaufgaben, sofern verfügbar, **Zuweisungsregeln**als Teil ihrer Filterkriterien.

**Hinweis:**
Wenn keine Zuweisungsregeln vorhanden sind, können Sie eine Gruppe mithilfe des Felds **Benutzergruppe** auswählen.

Ab Version 18.0 von Vulnerability Responseist die Regel für Korrekturaufgaben für **Schwachstellen** in Vulnerability Response für neue Implementierungen deaktiviert.

### Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**.
2. Öffnen Sie die Regel, oder klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

**Regel für Korrekturaufgaben**

| Feld | Beschreibung |
|---|---|
| Name | Name der Aufgabenregel. |
| Aktiv | Gibt an, ob die Aufgabe aktiv ist. |
| Beschreibung | Eine Beschreibung der Regel. |
| Groß-/ Kleinschreibung beachten | Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht.<br>**Hinweis:**<br>Beim Standardwert wird die Groß-/Kleinschreibung beachtet. |
| Bedingung | Optionale Filterbedingungen für die Regel.<br>**Hinweis:**<br>Um Rapid7 InsightVM Asset-Tags für die Verwendung im Bedingungsfilter für Korrekturaufgabenregeln verfügbar zu machen, müssen Sie die Asset-Listen-Integration [ Rapid7 InsightVM vor den anderen Rapid7 InsightVM -Integrationen ausführen.<br>Standardmäßig (Kontrollkästchen „Groß-/Kleinschreibung beachten“ deaktiviert) wird beim**Suchtext**, den Sie im Bedingungsgenerator für Datensätze und Formulare für Aufgabenregeln eingeben, nicht zwischen Groß- und Kleinschreibung unterschieden. Sie |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | haben die Möglichkeit, die Suche nach Groß-/Kleinschreibung in Aufgabendatensätzen und Formularen zu aktivieren. |
| **Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)** | |
| Angreifbare Elemente gruppieren aus | Die Tabelle, die die Regel zum Gruppieren von AEs verwendet. Sie können bis zu sechs Filter haben.<br>Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Angreifbares Element [sn_vul_vulnerable_item]<br>○ Angreifbares Element – Konfigurationselement [cmdb_ci]<br>○ Angreifbares Element → Schwachstelle [sn_vul_thritte_partei_entry]<br>**Hinweis:**<br>Wenn Sie eine erweiterte Tabelle auswählen, wird das **Feld Verwendet** nur für angreifbare Elemente angewendet, die diese erweiterte Tabelle verwenden. |
| Mit Feld | Feld in der Tabelle, das die Regel zum Gruppieren von AEs verwendet. |
| **Zuweisung** | |
| Korrekturaufgaben zuweisen nach | Bei der automatischen Zuweisung **von** Korrekturaufgaben wird die Auswahl Zuweisung zusätzlich zu den Auswahlmöglichkeiten Gruppieren nach verwendet, um die angreifbaren Elemente zu gruppieren. Bei Bedarf werden neue Aufgaben erstellt, um sicherzustellen, dass jedes angreifbare Element in einer Aufgabe mit einem übereinstimmenden Zuweisungsgruppensatz platziert wird.<br>Um die Zuweisung von Aufgaben zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.<br>○ Feld Gruppieren nach: Wenn Sie ein Benutzergruppenfeld aus **Feldwerte** verwenden **im**Abschnitt Gruppieren nach ausgewählt haben, werden diese im Dropdown-Menü angezeigt.<br>○ Benutzergruppe: Verwenden Sie die Nachschlageliste, um eine statische Benutzergruppe auszuwählen. |

**Hinweis:**
Wenn Sie Ihre Meinung zu einer der Gruppieren **nach** -Einstellungen ändern, setzt der zugehörige Link **Gruppieren nach Feldern** löschen die Gruppieren **nach** Felder im Formular zurück.

Wenn eine Gruppenregel gelöscht wird, haben Sie im Formular oder in der Listenansicht die Möglichkeit, alle von dieser Regel erstellten **offenen** Gruppen zu löschen. Gruppen, die sich nicht im Status „ **Offen** “ befinden, werden ausgeschlossen.

Einige Beispieleinträge finden Sie unter Vulnerability Response Beispiele für Korrekturaufgabenregeln.

### Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten verwenden. Durch Auswahl der Felder, die in der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

### Vorbereitungen

Darüber hinaus können Sie Attribute in „configuration_item“ [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um die Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass CIs, die in Ihrer Organisation nach außen gerichtet sind, angreifbarer sind und möglicherweise eine sofortige Korrektur erfordern, können Sie diesen CIs Attribute wie `Internet Facing` zuweisen. Dieses und andere Attribut sind in den Versionshinweisen zu Common Service Data Model für das Familien-Release Orlando aufgeführt. Aktuelle Informationen und Anleitungen zu CMDBfinden Sie in den folgenden Themen:

- Common Service Data Model konzeptionelles Modell
- CMDB-Schemamodell

Erforderliche Rolle: sn_vul.manage_risk_score_configuration

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner**.
2. Klicken Sie auf der Seite „Schwachstellenrechner“ auf **Standardrisikorechner**.
3. Navigieren zu **Seite „Schwachstellenrechner“.** > **Registerkarte „Schwachstellenrechner – Regeln“** > **Standardrisikoregel**.
4. **Wahlweise:** Legen Sie im Abschnitt „Risikorechnerkriterien“ der Seite „Schwachstellenrisikoregel“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung in der Gesamtrisikopunktzahlberechnung fest.
5. Um die Regel zu deaktivieren, müssen Sie das Kontrollkästchen **Aktiv** deaktivieren.
6. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
7. Füllen Sie die Felder des Formulars aus.

**Formular „Risikoregelfeld“.**

| Feld | Beschreibung |
|---|---|
| Referenztabelle auswählen | Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen:<br>○ **Angreifbares**Element: Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus per Dot-Walking zugänglich sind<br>○ **Angreifbares Element – Konfigurationselement**: Fügen Sie Dot-Walkable-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci).<br>○ **Angreifbares Element – Schwachstelle**: Fügen Sie Dot-Walkable-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittparteieintrag. Diese |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Felder sind nicht Teil der Basistabelle „Schwachstelleneintrag“.<br>○ Referenztabelle für angreifbare Elemente: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (**m2m**) sind, oder Tabellen, die einen Verweis auf das angreifbare Element enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar.<br>○ **Konfigurationselement-Referenztabelle**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar.<br>○ **Schwachstellen-Referenztabelle**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vul_entry sind, oder Tabellen, die einen Verweis auf sn_vul_entry enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar.<br>○ **Benutzerdefinierte Bedingungen**: Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der mit dem Internet verbundene Filter, ob ein Configuration Item (CI) extern oder intern ist. |
| Tabelle | Feld, das nur angezeigt wird, wenn eine der folgenden Optionen in der Referenztabelle Wählen ausgewählt wird:<br>○ **Angreifbares Element -> Konfigurationselement**<br>○ **Angreifbares Element -> Schwachstelle**<br>○ **Referenztabelle für angreifbare Elemente**<br>○ **Referenztabelle für Konfigurationselemente**<br>○ **Referenztabelle für Schwachstellen** |
| Feld | Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll. |
| Zusammenfassung | Feld, das nur angezeigt wird, wenn eine Referenztabelle aus Referenztabelle wählen ausgewählt wird. Wählen Sie den minimalen oder maximalen Wert aus, der für Berechnungen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | berücksichtigt werden soll, wenn Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird. |
| Gewichtung | Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein. |
| Definieren Sie die Wertgewichtung | Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). Die Gewichtungen müssen Ganzzahlen zwischen 0 und 100 sein.<br>**Hinweis:**<br>Dieses Feld wird nicht angezeigt, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt ist. |
| Bedingungstabelle | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Wählen Sie eine Bedingung aus der Liste aus. |
| Feldname | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Geben Sie einen Namen für die Risikokriterien ein. |
| Bedingung | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen. |

8. Klicken Sie auf **Absenden**.
9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

**Example:**
Beispiel 1: Quellschweregrad als Kriterium für eine Risikoregel hinzufügen

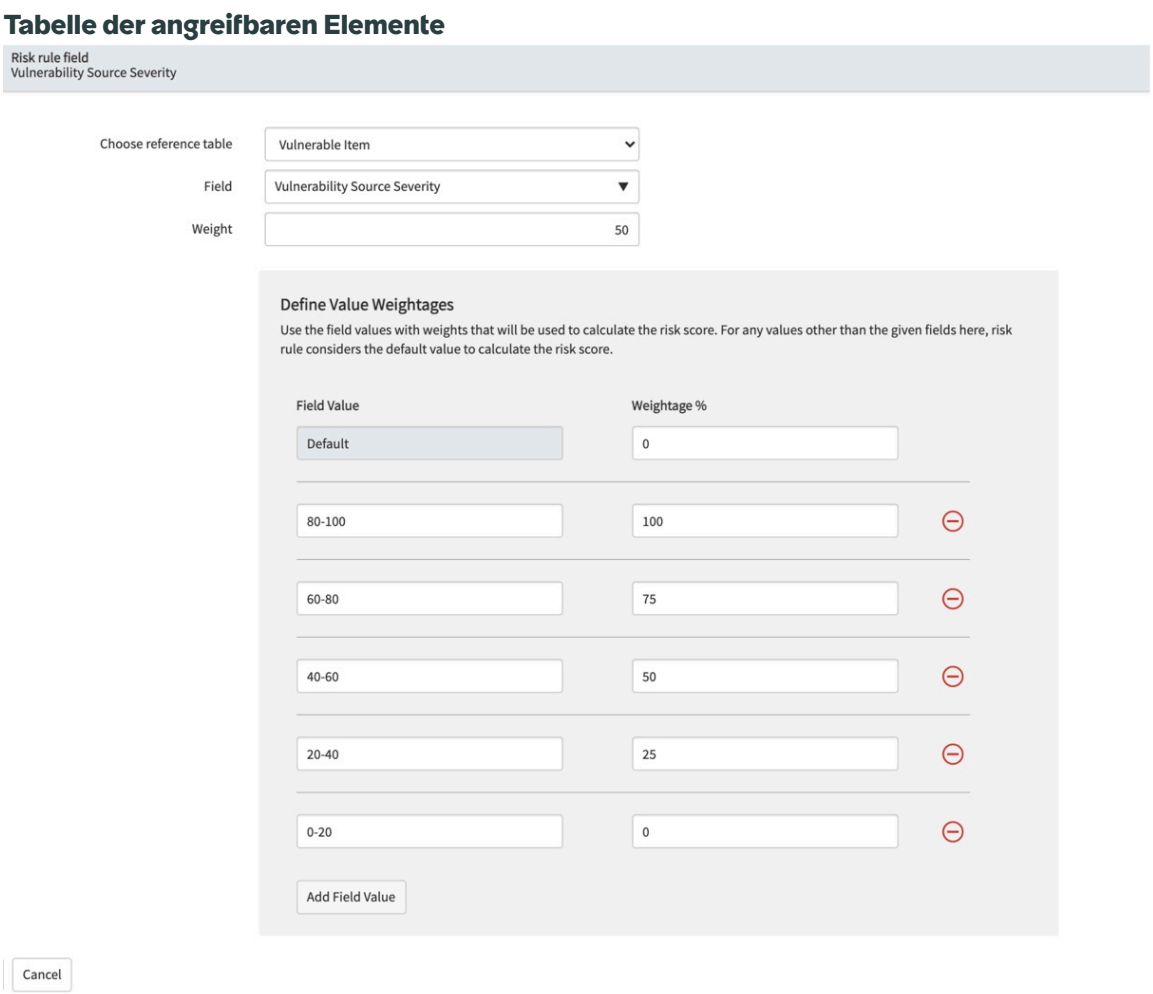
Anwendungsfall: Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden in das Feld Quellenschweregrad in der Tabelle „ **sn_vul_entry** “ eingetragen. Verwenden Sie dieses Feld für Risikopunktzahlberechnungen. Gehen Sie wie folgt vor, um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden:

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
4. Wählen Sie in der Liste Referenztabelle wählen die **Option Angreifbares Element**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der Liste Feld die Option **Vulnerability.Source Schweregrad**aus.
6. **Geben Sie** im Feld Gewichtung die relative Bedeutung dieses Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.




8. Klicken Sie auf **Absenden**.

Beispiel 2: Geschäftsrelevanz als Kriterium für eine Risikoregel hinzufügen.

Anwendungsfall: Angenommen, Ihre Organisation verfügt über viele Geschäftsservices. Das Konfigurationselement (CI) LINUX-SF-6381 wird von den folgenden Services verwendet:

**Relevanz der Business Services**

| Geschäftsservice | Relevanz |
|---|---|
| Cloud-Management | 1 – Am kritischsten |
| E-Commerce | 2 – Einigermaßen kritisch |
| Client-Services | 3: Weniger kritisch |
| Reisekosten und Spesen | 4: Nicht kritisch |

Automatische Übersetzung

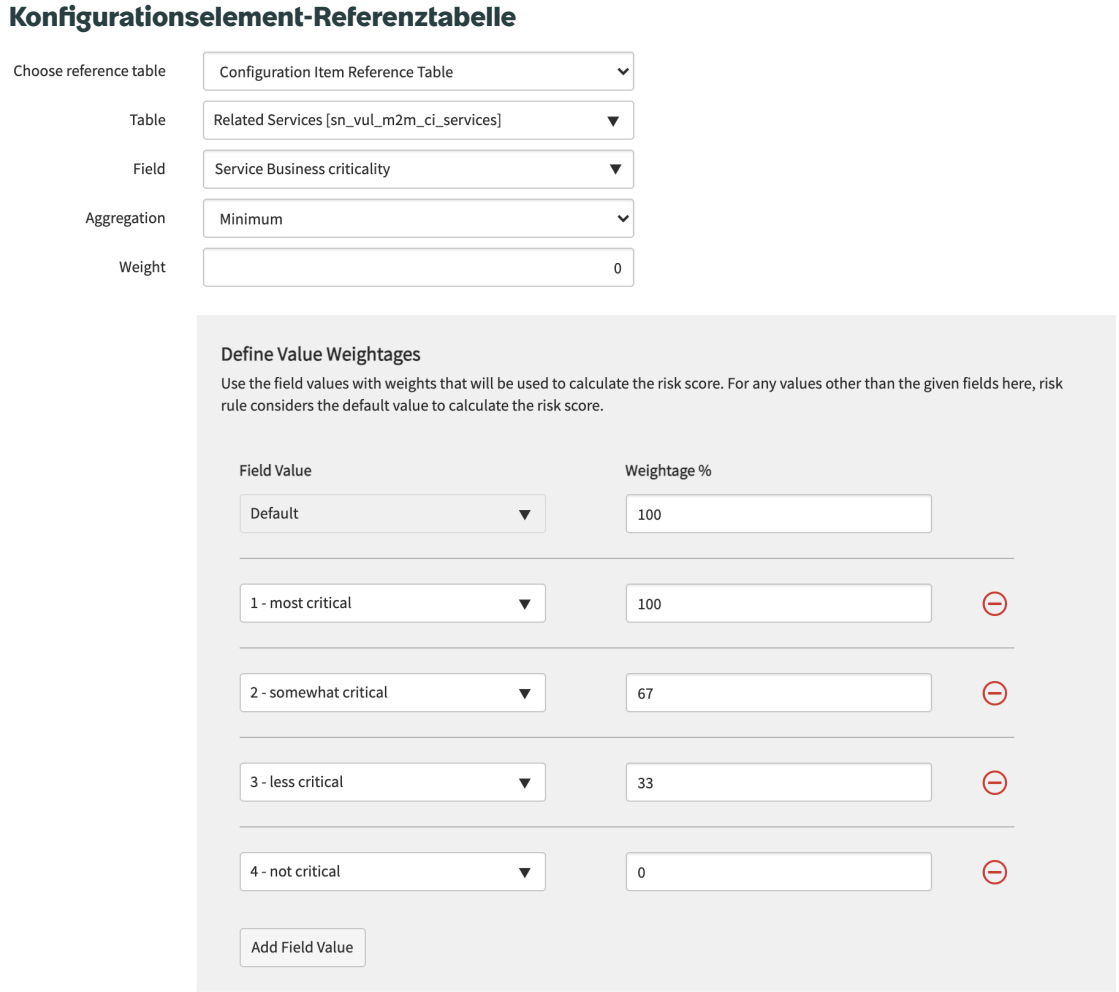
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zuordnung zwischen CI und Services wird in der Tabelle „Zugehörige Services“ [sn_vul_m2m_ci_services] gespeichert. Wenn im Asset LINUX-SF-6381 eine Schwachstelle gefunden wird, wird ein angreifbares Element (VI) erstellt. Sie können den Wert der Geschäftsrelevanz der betroffenen Services verwenden, um die Risikopunktzahl für diesen VI zu berechnen. Gehen Sie wie folgt vor, um den Relevanzwert dieser Services zur Berechnung der Risikopunktzahl zu verwenden:

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
4. Wählen Sie in der Liste Referenztabelle auswählen **Konfigurationselement-Referenztabelle**aus.
5. Wählen Sie in der Liste Tabelle **Zugehörige Services [sn_vul_m2m_ci_services] aus**.
6. Wählen Sie in der Liste Feld die **Option Service.Geschäftsrelevanz**aus.
7. **Wählen** Sie im Feld Zusammenfassung die Option **Minimum** aus, um den kritischsten Service für diesen Anwendungsfall abzurufen (1 –**Am kritischsten** Wert), oder Maximum, um den am wenigsten kritischen Service für diesen Anwendungsfall abzurufen (**4 – Nicht kritischer** Wert).
8. **Geben Sie** im Feld Gewichtung die relative Bedeutung dieses Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
9. Fügen Sie im Abschnitt „Wertgewichtungen definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**10.** Klicken Sie auf **Absenden**.

Beispiel 3: Dem Risikorechner ein bedingtes Kriterium hinzufügen

Angenommen, eine Organisation verfügt über mehrere Konfigurationselemente (CIs), von denen ein externer Benutzer nur auf einige zugreifen kann. Benutzer können Risikopunktzahlgewichtungen für diese nach außen gerichteten CIs hinzufügen.

**Hinweis:**
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „external“.

Gehen Sie wie folgt vor, um der Risikoregel ein bedingtes Kriterium hinzuzufügen:

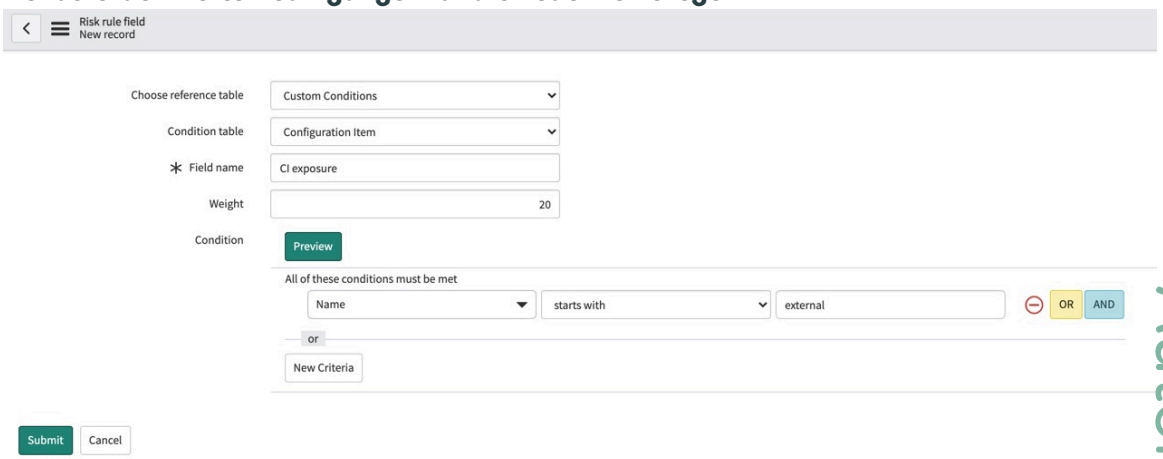
1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
4. Wählen Sie in der Liste Referenztabelle auswählen die **Option Benutzerdefinierte Bedingungen aus**.
5. Wählen Sie in der Liste Bedingungstabelle die Option **Konfigurationselement**aus.
6. Geben Sie im **Feld** Feldname den Namen **CI Exposure**ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Geben Sie** im Feld Gewichtung die relative Bedeutung dieses Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
8. Wählen Sie im Feld **Bedingung** die Option aus **Name** > **beginnt mit**und geben Sie den Wert **external**ein.

**Benutzerdefinierte Bedingungen für die neue Risikoregel**




9. Klicken Sie auf **Absenden**.

**Hinweis:**
Das Hinzufügen von bedingten Kriterien zu Ihrer Risikoregel kann die Leistung beeinträchtigen.

**Zugehörige Informationen**

Vulnerability Response-Rechner und Schwachstellen-Rechnerregeln

Erstellen Sie einen Vulnerability Response-Rechner

Filterung innerhalb von Vulnerability Response

### Vulnerability Response Rollup-Rechner

Verwenden Sie nach der ersten Bewertung der Risikorechner im Setup-Assistenten die Rollup-Rechner für Schwachstellen, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird.

Verwenden Sie die Rollup-Rechner für Schwachstellen, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird. Die folgenden Rollup-Rechner werden mit dem Basissystem geliefert:

- *`Remediation Task Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Elemente in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für die gesamte Gruppe angreifbarer Elemente bereitzustellen.
- *`Patch Update Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Elemente mit demselben Patch-Update zusammen, um eine Gesamtrisikopunktzahl für das Patch-Update bereitzustellen.
- *`Organization Risk Score Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Hostelemente, angreifbaren Anwendungselemente, angreifbaren Containerelemente und Konfigurationsprobleme in einer Organisation zusammen, um eine Gesamtrisikopunktzahl für die gesamte Organisation in einem einheitlichen Dashboard bereitzustellen.
- *`Vulnerable Item Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Hostelemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl der gesamten Organisation für das einheitliche Dashboard beizutragen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *`Vulnerability Entry Rollup`*: Fasst die Risikopunktzahlen für alle angreifbaren Elemente mit demselben Schwachstelleneintrag zusammen, um eine Gesamtrisikopunktzahl für den Schwachstelleneintrag bereitzustellen.
- *`Rollup EPSS Scores from NVD to TPEs`*: Führt einen Rollup der EPSS-Punktzahlen für alle angreifbaren Elemente/CVE durch, die in der NVD-Tabelleaufgeführt sind, zu vorhandenen TPEs, um eine Gesamtwahrscheinlichkeit der Ausnutzung der Schwachstelle bereitzustellen.
- *`Remediation Effort Rollup`*: Fasst die Risikopunktzahlen für alle Datensätze in einer Korrekturmaßnahme zusammen, um eine Gesamtrisikopunktzahl für die Korrekturmaßnahme bereitzustellen.

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Rechner für Schwachstellen-Rollup**.

Konfigurieren Sie den Rollup-Rechner, um anzugeben, wie viel Gewichtung jeder dieser berechneten Werte beim Festlegen der kumulativen Risikopunktzahl haben soll. Je höher die Gewichtung, desto mehr wird dieser Wert verwendet, um die zusammengefasste Risikopunktzahl in den Schwachstellen- oder Korrekturaufgaben zu bestimmen.

**Hinweis:**
Wenn **Zurückgestellte** einbeziehen ausgewählt ist, werden alle zurückgestellten angreifbaren Elemente in die Rollup-Berechnung für die Korrekturaufgaben einbezogen. Stellen Sie sicher, dass Sie die Auswirkungen auf die Gesamtberechnung verstehen, bevor Sie diese Option auswählen.

Rollup-Rechner führen alle 15 Minuten die regelmäßige Aufgabe *`Rollup vulnerable item values to vulnerability and groups`*aus, um Änderungen zu erfassen und die Details und Risikopunktzahlen für Korrekturaufgaben und Schwachstellen zusammenzufassen. Diese regelmäßigen Aufgaben berechnen auch kumulative Werte für die Anzahl der AEs, die maximale Risikopunktzahl, das Korrekturzieldatum und den Status für Korrekturaufgaben.

**Hinweis:**
Berechnete Werte für Schwachstelleneinträge enthalten keine Korrekturzieldaten.

Die Risikopunktzahl wird berechnet, wenn:

- Die Risikopunktzahl, das Korrekturziel, der Korrekturstatus oder die Schwachstelle ändert sich für die angreifbaren Elemente.
- Der Status des angreifbaren Elements ändert sich in „Offen“, „Zurückgestellt“, „Geschlossen“ oder von „Geschlossen“ oder „Zurückgestellt“.
- Angreifbare Elemente werden gelöscht.
- Angreifbare Elemente werden der Korrekturaufgabe hinzugefügt oder daraus entfernt.

Beispiel für den Schwachstellen-Rollup-Rechner: Betrachten Sie die Korrekturaufgabe VUL324567, die die folgenden angreifbaren Elemente aufweist:

- VIT1001 mit Risikopunktzahl 30
- VIT1002 mit Risikopunktzahl 40
- VIT1003 mit Risikopunktzahl 50

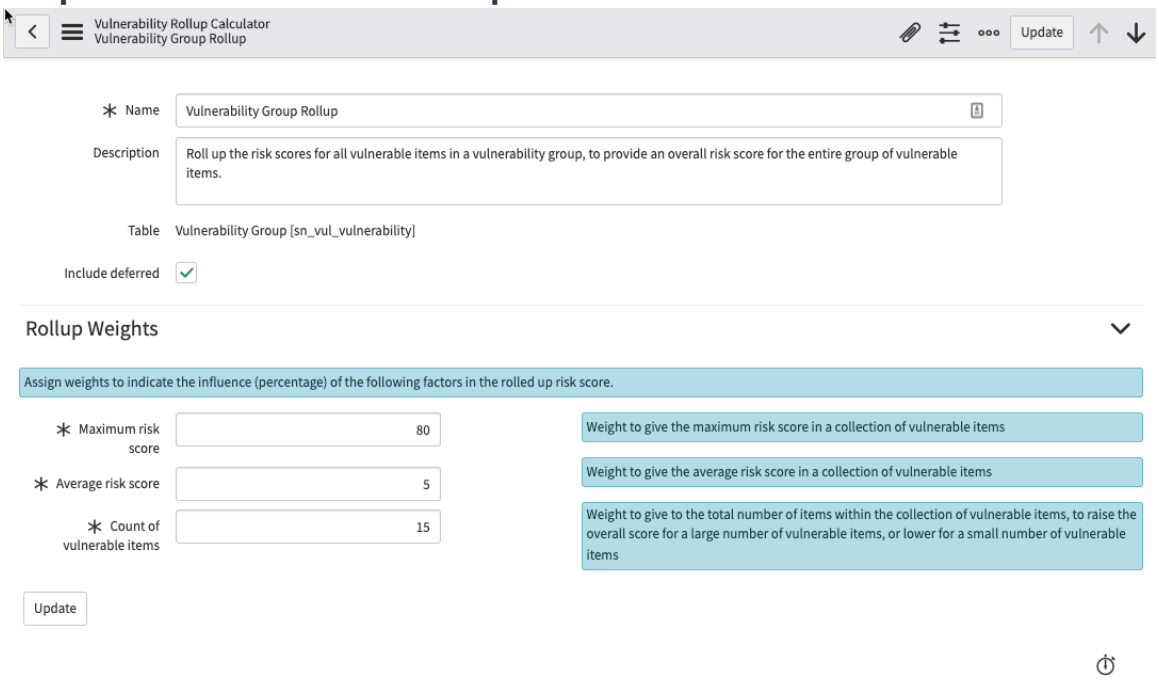
Berücksichtigen Sie auch die folgenden Gewichtungen im Schwachstellen-Rollup-Rechner:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Maximale Risikopunktzahl: 80
- Durchschnittliche Risikopunktzahl: 5
- Anzahl der angreifbaren Elemente: 15

**Beispiel für den Schwachstellen-Rollup-Rechner**




Im Beispiel des Schwachstellen-Rollup-Rechners lautet die Formel zur Bestimmung der **Risikopunktzahl** der Korrekturaufgabe wie folgt:

(**Maximale Risikopunktzahl**/100) * 80 + (**Durchschnittliche Risikopunktzahl** /100) * 5 + (Faktor * 15)

Der Faktor wird wie folgt bestimmt:

| VI-Anzahl | Faktor |
|---|---|
| <10 | 0,2 |
| 10–100 | 0,4 |
| 101–1000 | 0,6 |
| 1001–10.000 | 0,8 |
| > 10.000 | 1 |

Für die Korrekturaufgabe VUL324567 gilt Folgendes:

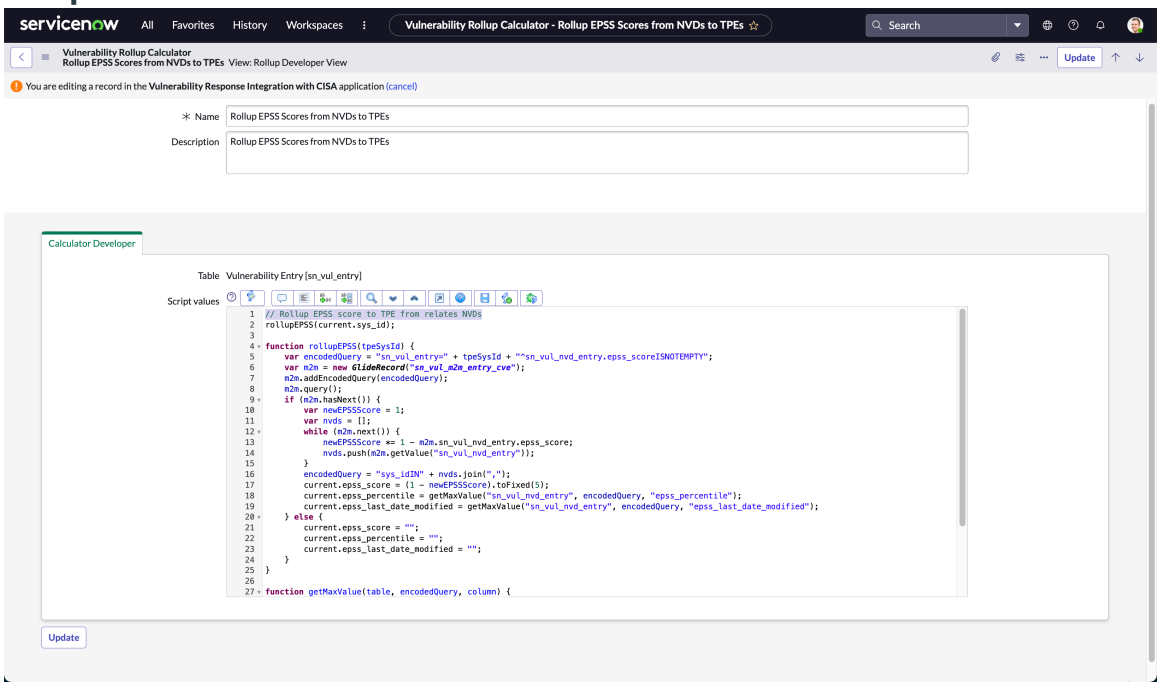
- Die durchschnittliche Risikopunktzahl beträgt 40
- Die maximale Risikopunktzahl beträgt 50
- 50 (Maximale Risikopunktzahl)
- Faktor ist 0,2

Die **Risikopunktzahl** wäre 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45].

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Rollup von EPSS-Punktzahlen von NVDs zu TPEs




## EPSS-Rollup-Rechner – Beispiel

Betrachten Sie beispielsweise eine Organisation mit 100 Schwachstellen mit jeweils einer Wahrscheinlichkeit von 5 %, ausgenutzt zu werden. Die Frage, die für einen Netzwerkverteidiger von großem Interesse ist, könnte sein: Wie hoch ist die Wahrscheinlichkeit, dass mindestens eine dieser Schwachstellen ausgenutzt wird, und was ist daher meine allgemeine Bedrohung? Die Wahrscheinlichkeit, dass mindestens ein Ereignis auftritt, ist einfach das Komplement (das Gegenteil) von keinem Ereignis, d. h.:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Dabei ist die Wahrscheinlichkeit, dass keine Schwachstellen vorhanden sind, das lineare Produkt jeder nicht ausgenutzten Schwachstelle. Da in diesem Beispiel für jede Schwachstelle eine Wahrscheinlichkeit von 5 % besteht, dass sie ausgenutzt wird, beträgt die Wahrscheinlichkeit, dass sie nicht ausgenutzt wird, jeweils 95 %. Und da es 100 davon gibt, können wir dies schreiben als:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

Dies besagt, dass die Wahrscheinlichkeit, dass mindestens eine der Schwachstellen ausgenutzt wird, 99,4 % beträgt.

**Wichtig:**
Um *`Rollup EPSS Scores from NVD to TPEs`*zu ändern, müssen Sie die Kontextmenüansicht des Formulars aus der **Standardansicht** in die **Rollup-Entwickleransicht**ändern.

### Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

Nach der ersten Bewertung der Korrekturzielregeln im Setup-Assistenten können Schwachstellenmanager eine Korrekturzielregel auf der Ebene des angreifbaren Elements einrichten, um die Korrektur von Schwachstellen mit hohem Risiko zeitnah voranzutreiben. Wenn das Korrekturdatum für ein angreifbares Element näher rückt, wird eine Benachrichtigung an die in der Regel angegebenen Benutzer oder Gruppen gesendet.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Nachbesserungszielregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel. |
| Ziel (Tage) | Geben Sie die Anzahl der Tage an, innerhalb derer die angreifbaren Elemente seit dem letzten Öffnen korrigiert werden sollen. |
| V17.1: Ziel ab (Datum) | Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur das Datums- oder das Datums- und Uhrzeittypfeld angeben. Der Standardwert ist Zuletzt geöffnetes Datum. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1185029. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn diese Checkbox deaktiviert ist, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden. |
| Benachrichtigen (Tage vor dem Fälligkeitsdatum) | Anzahl der Tage vor der angestrebten Korrekturzeit für das Senden einer Benachrichtigung. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „In Ausführung“. Wenn das Benachrichtigungsdatum überschritten ist und das Korrekturzieldatum erreicht ist, wird der Status als „Ziel erreicht“ angezeigt.<br>**Hinweis:**<br>Wenn dieses Feld auf 0 festgelegt ist, wird nur eine Benachrichtigung **„Ziel verfehlt** “ gesendet. |
| Beschreibung | Text, der die Korrekturzielregel beschreibt. |
| Bedingung | Wählen Sie mithilfe des Bedingungsfilters die Kriterien für die Anwendung der Regel auf die angreifbaren Elemente aus. Um Auswirkungen auf die Leistung zu vermeiden, testen Sie Ihre Bedingungen im vollständigen Produktionsmaßstab. Mit Tests können Sie bestimmen, wie lange die Ausführung der Aufgabe „ **Korrekturziele evaluieren** “ unter Berücksichtigung der Bedingungen und der Größe Ihres Configuration Management Database (CMDB)dauert.<br>Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt. |
| Benachrichtigungen | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| **Hinweis:** Die in der Benachrichtigungs-E-Mail angezeigte Anzahl enthält keine angreifbaren Elemente im Status „ **Zurückgestellt“**, **„Gelöst“**oder **„Geschlossen** “. | |
| Anwender | Die Personen, die benachrichtigt werden sollen, wenn sich das ausgewählte angreifbare Element seiner angestrebten Korrekturzeit nähert oder diese überschreitet. |
| Gruppe | Die Gruppe, die benachrichtigt werden soll, wenn sich das ausgewählte angreifbare Element der anvisierten Korrekturzielzeit nähert oder diese überschreitet. |
| Update-Verlauf | |
| | Wird für die erstmalige Erstellung einer Regel nicht verwendet. Anschließend werden hier Systemarbeitsnotizen protokolliert. |

4. Klicken Sie auf **Absenden**.
   Diese Regel wird bei der nächsten Ausführung der geplanten Aufgabe `Evaluate remediation targets` oder bei Verwendung der Schaltfläche **Änderungen** übernehmen in der Listenansicht der Korrekturzielregeln wirksam. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Weitere Informationen zur regelmäßigen Aufgabe und zum **Anwenden von Änderungen** finden Sie unter Vulnerability Response Korrekturzielregeln.

### Konfigurieren Sie installierte Drittanbieterintegrationen mit dem Setup-Assistenten

Konfigurieren Sie Vulnerability Response so, dass es mit jeder Ihrer installierten Drittanbieteranwendungsbereitstellungen funktioniert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration**.
2. Wählen Sie **Scanner-Integrationen** aus, um installierte Anwendungsbereitstellungen von Drittanbietern zu konfigurieren.
3. Wenn Solution Management for Vulnerability Response installiert ist, können Sie **Lösungsintegrationen** auswählen, um die Anbieter Ihrer Schwachstellenlösungen zu konfigurieren.

### Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management mit dem Setup-Assistenten

Nachdem Sie die Anwendung Vulnerability Solution Management installiert haben, können Sie die Anbieter Ihrer Schwachstellenlösungen mit dem Setup-Assistenten konfigurieren.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für installierte Lösungsintegrationen für Solution Management for Vulnerability Responsezu ergänzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Sie Vulnerability Solution Management und die gewünschten Lösungsintegrationen bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.
- Vergewissern Sie sich, dass Anmeldeinformationen für Drittparteikonten verfügbar sind. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.
- Weitere Informationen finden Sie unter Anwendung Solution Management for Vulnerability Response installieren, bevor Sie installierte Lösungen konfigurieren.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**.

   Der Integration der Microsoft Security Response Center-Lösung erfordert einen API-Schlüssel und eine URL aus dem Microsoft Security Response Center, um ihn zu konfigurieren.

   **Hinweis:**
   Die Eingabe des API-Schlüssels ist für MSRCoptional. Um den Schlüssel MSRC zu erhalten, benötigen Sie eine Microsoft-ID aus einem live.com-, outlook.com- oder Microsoft.com-E-Mail-Konto, eine bei Microsoft registrierte Telefonnummer oder eine Anmeldung bei einem Benutzernamensportal.

2. Geben Sie die URL ein.
   Die URL im Setup-Assistenten für MSRC lautet https://api.msrc.microsoft.com.
3. Klicken Sie auf **Fertigstellen**.
4. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf der Konfigurationsseite auf **Jetzt** ausführen klicken, nachdem Sie Ihre Anmeldeinformationen eingegeben haben.
5. Red Hat Solution Integration ist ebenfalls verfügbar.
   Es ist kein API-Schlüssel erforderlich.
6. Klicken Sie im Setup-Assistenten rechts neben Red Hat Solution Integrationauf **Bearbeiten**.
7. Vergewissern Sie sich, dass die URL im Setup-Assistenten für RHSIhttps://access.redhat.com/hydra/restlautet
8. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf der Konfigurationsseite auf **Jetzt** ausführen klicken.
9. **Klicken** Sie auf **Fertigstellen und anschließend auf Als** abgeschlossen markieren, um die Konfiguration abzuschließen.
   Wenn Sie die Konfiguration abgeschlossen haben, wird im Setup-Assistenten für Lösungsintegrationen ein Häkchen angezeigt.

#### Konfigurieren Sie die MS TVM-Schwachstellenintegration mit dem Setup-Assistenten

Konfigurieren Sie die Anwendung Vulnerability Response integration with Microsoft Threat and Vulnerability Management (MS TVM), nachdem Sie sie mit dem Setup-Assistenten installiert haben.

### Vorbereitungen

Zusätzlich zu den Anweisungen und Aufforderungen, die im Setup-Assistenten für die Integration von Vulnerability Response mit Microsoft Threat and Vulnerability Management bereitgestellt werden, führen Sie die folgenden Aktionen aus:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.
- Weitere Informationen finden Sie unter Vorbereitung auf die Microsoft Threat and Vulnerability Management-Schwachstellenintegration, bevor Sie die Microsoft Threat and Vulnerability Management-Integration für Vulnerability Responsekonfigurieren.
- Vergewissern Sie sich, dass die Anmeldeinformationen für das MS TVM-Konto verfügbar sind. Informationen zum Abrufen dieser Anmeldeinformationen finden Sie unter Richten Sie Microsoft Azure für die MS TVM-Integration ein.

Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_msft_tvm.configure_integration) für die Konfiguration

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.

   Die Kachel „Microsoft Threat & Vulnerability Management“ wird angezeigt.

   MS TVM ist eine Integration mit mehreren Quellen, was bedeutet, dass Sie mehrere Bereitstellungen derselben Drittpartei-Integration haben können. Die Einstellungen aus Ihrer ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

   **Hinweis:**
   Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

   Daten aus jeder Drittanbieterintegration werden eindeutig identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

2. Um die Microsoft Threat and Vulnerability Management-Integration zu konfigurieren, klicken Sie auf **Bearbeiten**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Account-Anmeldeinformationen“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Instanz. |
| TVM-Region | Region in der Nähe Ihres Serverstandorts. Verwenden Sie den Server, der Ihrem Standort am nächsten liegt, um eine optimale Leistung der API zu erzielen. |
| Authentifizierungstyp | Methode zum Überprüfen der Identität. Die Benutzerauthentifizierung steuert die Sichtbarkeit bestimmter Assets für bestimmte Benutzer. MS TVM exportiert die Gerätegruppen, die für diesen Benutzer berechtigt sind. Der Standardwert ist Anwendung. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Mandanten-ID | Mandantenidentität Ihrer Organisation. |
| Client-ID | Clientidentität, die nach der Registrierung von MS TVM in Microsoft Azure generiert wird. |
| Benutzername | Benutzer, der Zugriff auf die vollständige Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn Benutzer unter Authentifizierungstyp ausgewählt wird. |
| Passwort | Passwort für den Benutzernamen, der Zugriff auf die vollständige Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn Benutzer unter Authentifizierungstyp ausgewählt wird. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel, der nach der Registrierung der MS TVM-Anwendung generiert wird. Dieses Feld wird nur angezeigt, wenn unter Authentifizierungstyp die Option Anwendung ausgewählt wird. |

4. Um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren, klicken Sie auf **Weiter**.
   Das Formular „Importkonfiguration für Schwachstellen“ wird angezeigt.
5. Aktivieren oder deaktivieren Sie den Import von Schwachstellen, bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten, und planen Sie, wann der Import von MS TVM-Schwachstellen ausgeführt werden soll.
   Wenn Sie alle Schwachstellen importieren möchten, lassen Sie das anfängliche Startdatum leer.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Schwachstellen jetzt**importieren.
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.
6. Um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren, klicken Sie auf **Weiter**.
   Das Formular „Empfehlungen – Konfiguration importieren“ wird angezeigt.
7. Aktivieren oder deaktivieren Sie den Import von Empfehlungen, und legen Sie den Zeitplan fest, wann der Import von MS TVM-Schwachstellen ausgeführt werden soll.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Empfehlungen jetzt**importieren.
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.
8. Um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren, klicken Sie auf **Weiter**.
   Das Formular „Computer-Importkonfiguration“ wird angezeigt.
9. Aktivieren oder deaktivieren Sie den Computerimport, legen Sie das anfängliche Startdatum für die Computer fest, die Sie importieren möchten, und planen Sie, wann der Import von MS TVM-Computern ausgeführt werden soll.
   Wenn Sie alle Computer importieren möchten, lassen Sie das anfängliche Startdatum leer.

**Hinweis:**
Computer-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der in der MS TVM-Umgebung aufgelisteten Computer verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **CI-Suchregeln**, um die standardmäßigen Suchregeln für Configuration Items (CIs) anzuzeigen. CI-Suchregeln definieren, wie Maschinendaten aus Drittanbieterquellen zum Identifizieren von Konfigurationselementen (CIs) in Now Platform CMDBverwendet werden. Sie haben die Möglichkeit, Suchregeln hinzuzufügen oder die standardmäßigen CI-Suchregeln auf dieser Seite zu ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

b. Um Daten bei Bedarf zu importieren, klicken Sie auf **Computer jetzt**importieren.

**Hinweis:**
Computer mit dem Status „Onboarding“ in MS TVM werden von der ServiceNow-Anwendung abgerufen.

c. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen**.

10. Um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln, klicken Sie auf **Weiter**. Das Formular „Importkonfiguration für Computer-Schwachstellen“ wird angezeigt.

11. Aktivieren Sie die folgenden Integrationen, und bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten.

**Formular „Importkonfiguration für Computer-Schwachstellen“**

| Integration | Beschreibung |
|---|---|
| Delta-Import von Microsoft TVM-Computer-Schwachstellen | Ruft Schwachstellen ab, die während des vollständigen Imports von Schwachstellen aktualisiert wurden, einschließlich neuer, behobener und aktualisierter Schwachstellen. Sie können nur Delta-Daten für die letzten 14 Tage importieren. |
| Vollständiger Import von Microsoft TVM-Computer-Schwachstellen | Ruft alle offenen Schwachstellen ab. Aufgrund des hohen Datenimportvolumens können Sie eine wöchentliche Ausführung planen. |

**Hinweis:**

Führen Sie den Computerimport vor der Integration von Computer-Schwachstellen aus. Andernfalls werden für die fehlenden Computer keine AEs erstellt.

12. Um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen, klicken Sie auf **Fertig stellen**.

### Nächste Maßnahme

Wenn Sie eine Gruppierung angreifbarer Elemente in der klassischen Umgebung aktivieren möchten, navigieren Sie zu > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben** > **Microsoft TVM-Empfehlung**.

Wählen Sie im angezeigten Formular die Option **Aktiv** aus, um sie zu aktivieren. Alternativ können Sie **Neu** wählen, um eine neue Regel zu erstellen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie Qualys Vulnerability Integration mit dem Setup-Assistenten

Nachdem Sie die Anwendung Qualys installiert haben, konfigurieren Sie sie mit dem Setup-Assistenten.

## Vorbereitungen

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für die Konfiguration von Qualys Vulnerability Integrationzu ergänzen.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.
- Weitere Informationen finden Sie unter [ wird vorbereitet Qualys Vulnerability Integration, bevor Sie Qualys Vulnerability Integrationkonfigurieren.
- Vergewissern Sie sich, dass Anmeldeinformationen für Drittparteikonten verfügbar sind. Sie sind erforderlich, um einige Anwendungen von Drittanbietern zu bearbeiten.

Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) für die Konfiguration.

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
   Die installierten Integrationen werden angezeigt.
2. Klicken Sie rechts neben Qualys Vulnerability Integration, das Sie konfigurieren möchten, auf **Bearbeiten**.
3. Geben Sie im Formular „Kontoanmeldeinformationen“ Ihre Qualys Cloud Platform -Anmeldeinformationen ein.
   Für die Konfiguration sind Ihre Anmeldeinformationen erforderlich.
4. Verwenden Sie die folgenden Hinweise als Leitfaden, wenn Sie mit der Konfiguration fortfahren.
   - Der Link **Erweiterte Einstellungen** verweist auf den Integrationsdatensatz Qualys. Sie können Parameter hinzufügen, die vom Produkt Qualys für Ihre geplanten Abfragen unterstützt werden, um die importierten Schwachstellendaten zu filtern. Weitere Informationen finden Sie unter Legen Sie zusätzliche Filterparameter für Qualys Importe fest.
   - Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Response mit einer bereits konfigurierten Version von Qualys Vulnerability Integration durchgeführt haben, ist diese Version mit beibehaltenen Konfigurationseinstellungen weiterhin verfügbar.

     Unter Importeinstellungen in Hosterkennungskonfiguration für Qualys Vulnerability Integrationgibt es eine Option zum Anzeigen von Datensätzen zur Erkennung von Qualys korrigierten Schwachstellen. Wenn diese Option aktiviert ist, können Sie angreifbare Elemente aus Erkennungsdatensätzen mit einem festen Status (Status =**Repariert**) erstellen. Weitere Informationen zu Erkennungen angreifbarer Elemente finden Sie unter Vulnerability Response Erkennung angreifbarer Elemente aus Drittanbieterintegrationen.

     Sie können das Kontrollkästchen Nach Netzwerkpartition suchen auf der Seite „ **Hosterkennungskonfiguration** “ aktivieren, um den Bezeichner der Netzwerkpartition in die IP-Adresssuche einzubeziehen. Weitere Informationen finden Sie unter Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Qualys Vulnerability Integration.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Host-Tags werden als Teil der Qualys Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Zuweisungs- und Korrekturaufgabenregeln verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

**Hinweis:**
Die Qualys -Hostlisten-Integration sollte vor dem Erstellen von Zuweisungs- oder Korrekturaufgabenregeln in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

Qualys **Asset-Tags** werden im Modul „Host-Tags“ unter Qualys Vulnerability Integrationgespeichert.

- Qualys Vulnerability Integration unterstützt mehrere Quellen. Sie können mehrere Bereitstellungen derselben Drittanbieterintegration haben. Um eine weitere Integration hinzuzufügen, klicken **Sie**auf der Seite „Scanner-Integrationen“ auf Integration hinzufügen.

  Die Einstellungen aus Ihrer ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

  **Hinweis:**
  Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

  Daten aus jeder Drittanbieterintegration werden eindeutig identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

- Sie können Importe bei Bedarf ausführen, indem Sie auf einer Konfigurationsseite auf **Jetzt** ausführen klicken.

5. **Klicken** Sie auf Fertigstellen, um die Konfiguration im Setup-Assistenten abzuschließen.

### Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten

Nachdem Sie die Anwendung Vulnerability Response Integration with Tenable installiert haben, konfigurieren Sie sie mit dem Setup-Assistenten.

**Vorbereitungen**
Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Eingabeaufforderungen im Setup-Assistenten für die Vulnerability Response Integration with Tenable -Integration zu ergänzen.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.
- Weitere Informationen finden Sie unter [ Vorbereitung auf die Tenable Vulnerability-Integration, bevor Sie Tenable for Vulnerability Responsekonfigurieren.
- Vergewissern Sie sich, dass Anmeldeinformationen für Drittparteikonten verfügbar sind. Sie sind erforderlich, um einige Anwendungen von Drittanbietern zu bearbeiten.

Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_tenable.configure_integrations) für die Konfiguration.

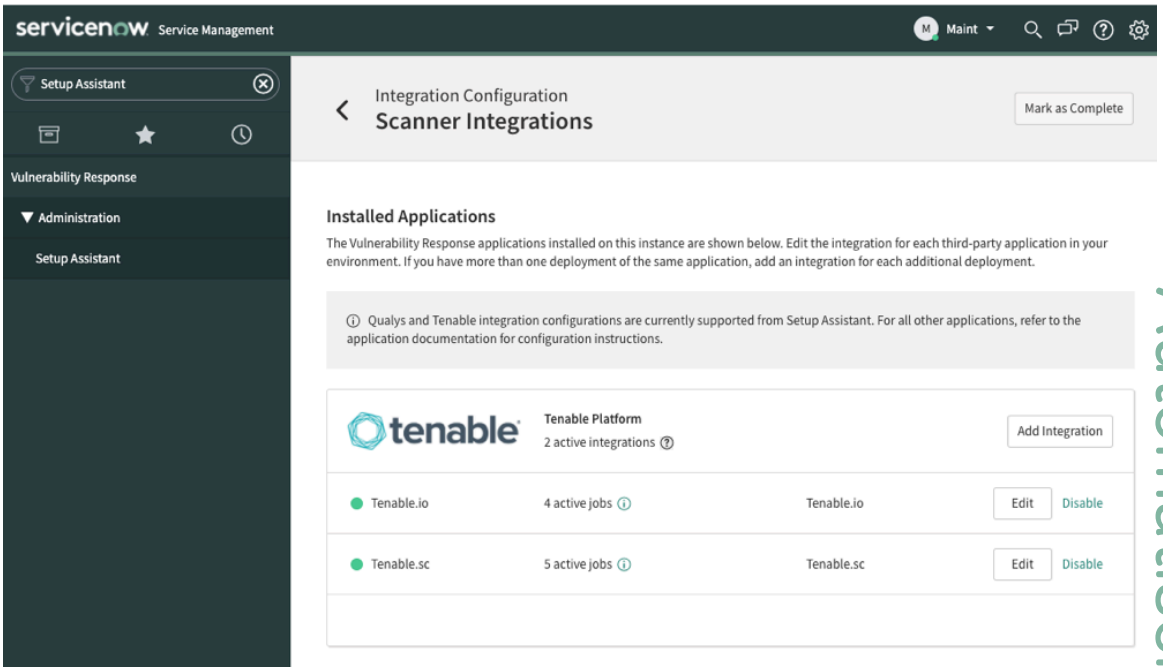


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn nicht angezeigt, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.

   Die Integrationen Tenable.io und Tenable.sc werden angezeigt.




   Tenable ist eine Integration mit mehreren Quellen, und Sie können mehrere Bereitstellungen derselben Drittpartei-Integration haben. Die Einstellungen aus Ihrer ursprünglichen Drittanbieterintegration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

   **Hinweis:**
   Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Ziehen Sie in Betracht, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

   Daten aus jeder Drittanbieterintegration werden eindeutig identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

2. Klicken Sie rechts neben der Tenable-Integration, die Sie konfigurieren möchten, auf **Bearbeiten**.
3. Füllen Sie die Felder im Formular „Kontoanmeldeinformationen“ aus.

   - Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64.

     **Hinweis:**
     Ab Version 3.8 von Vulnerability Response Integration with Tenable sind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Basisbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen.

   - Tenable.sc erfordert Zugriff durch Sicherheitsanalysten oder -manager.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

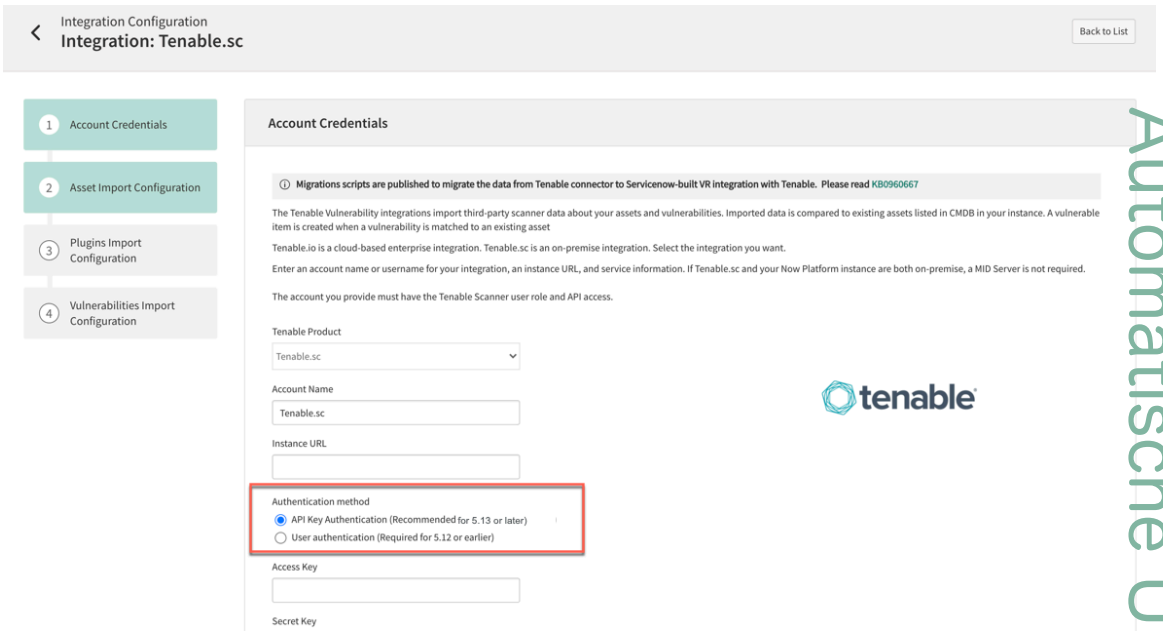
**a.** Wählen Sie Ihr Tenable-Produkt aus.

**b.** Geben Sie Ihren Tenable-Kontonamen ein.

**c.** Geben Sie im Feld Instanz-URL die URL für Ihre Tenable-Plattform ein.

**d.** Wählen Sie eine Authentifizierungsmethode aus.

Basierend auf Ihrer Version von Tenable.schaben Sie zwei Optionen für die Authentifizierung:




**i.** Wählen Sie ab Version 5.13 von Tenable.sc**API-Schlüsselauthentifizierung**aus. Geben Sie Ihren Tenable-Zugriff und Ihre geheimen Schlüssel ein.

**ii.** Vor v5.13 wird die Benutzerauthentifizierung von Ihrer Now Platform® -Instanz unterstützt und ist erforderlich. Geben Sie Ihren Now Platform -Benutzernamen und Ihr Passwort ein.

Für Tenable.scwird nur die API-Schlüsselauthentifizierung unterstützt. Geben Sie Ihren Tenable-Zugriff und Ihre geheimen Schlüssel ein.

**e. Wahlweise:** Wählen Sie einen MID Server aus.

(Optional) Wenn sich Ihre Now Platform -Instanz und Ihre Tenable.sc -Anwendung nicht am selben Speicherort befinden, wählen Sie einen konfigurierten MID Server aus der Auswahlliste aus. Weitere Informationen finden Sie unter MID Server .

- Ab Version 15.0 von Vulnerability Response und Version 3.0 von Tenable Vulnerability Integrationhaben Sie die Möglichkeit, den Parameter `Async_request` wie in Datenabrufeinstellungen für die Tenable Vulnerability-Integrationbeschrieben zu aktivieren. Einige Konfigurationen mit Tenable sind erforderlich, wenn Sie synchrone Aufrufe durchführen möchten. Wenden Sie sich an das Tenable-Produkt, um Hilfe zu erhalten. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und es gibt eine Zeitüberschreitung von 30 Sekunden. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

- (Optional) Für Bestandskunden ist ein Korrekturskript verfügbar, wenn Sie asynchrone Aufrufe verwenden.

Wenn Ihre Now Platform -Instanz und Ihre Tenable.sc -Anwendung beide lokal vorhanden sind, aber nicht erforderlich sind, haben Sie die Möglichkeit, einen konfigurierten MID Server aus der Auswahlliste auszuwählen.

**Hinweis:**
Unabhängig davon, ob Sie einen MID Server verwenden oder nicht, läuft die Integration nach fünf Minuten ab, und eine Meldung wird angezeigt, wenn keine Antwort vom Server eingeht.

(Optional) Wenn ein Zeitüberschreitungsfehler angezeigt wird, überprüfen Sie im Setup-Assistenten, ob Sie die richtigen Anmeldeinformationen und die richtige URL eingegeben haben.

4. Klicken Sie auf **Weiter**, um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
Das Formular „Asset-Importkonfiguration“ wird angezeigt.

5. Aktivieren oder deaktivieren Sie in diesem Formular die Asset-Importintegration, legen Sie das anfängliche Startdatum für die Assets fest, die Sie importieren möchten, und planen Sie, wann der Tenable-Asset-Import ausgeführt werden soll.

   Für Tenable.io

   - Assets Integration kann mit Tenable.io Compliance-Ergebnissen und Compliance-Ergebnisauffüllungsintegration verwendet werden, um sichere Konfigurationsbewertungsdaten zu Ihren Assets in die Anwendung Configuration Compliance zu importieren.
   - Version 12.2 der Anwendung Configuration Compliance ist in Ihrer Instanz erforderlich, wenn Sie diese sicheren Konfigurationsbewertungsdaten importieren und anzeigen möchten.

     Unter Configuration Compliance importierte Daten finden Sie weitere Informationen darüber, welche Daten mit diesen Integrationen importiert werden und wo sie veröffentlicht werden.

   - Die Tenable.io Compliance-Ergebnisse und Compliance-Ergebnisauffüllungs-Integrationen sind standardmäßig nicht aktiviert. Wenn Sie sie aktivieren, möchten Sie möglicherweise die bereitgestellten Standardzeitplaneinstellungen verwenden. In den unten aufgeführten Schritten erfahren Sie, wie Sie Integrationen für Tenable Vulnerability Integrationsuchen und aktivieren.
   - Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Tenable.io in Ihrer Instanz initiieren. Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen vor dem Initiieren von erneuten Scans aktiviert werden.

   Standardmäßig sind diese Integrationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io -Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

   a. Navigieren zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.

   b. Suchen Sie in der angezeigten Liste die gewünschten Tenable.io Integrationsdatensätze.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**c.** Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.

**d.** Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

**e.** Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

- Für die Tenable.io -Integration haben Sie auch die Möglichkeit, den Import von Asset-Tags zu aktivieren und zu deaktivieren. Asset-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der in Ihrer CMDB in der Umgebung Tenable.io aufgeführten Assets verwendet.
- Wenn Sie für die Produkte Tenable.io und Tenable.sc die **Option Suche nach Netzwerkpartition aktivieren** unter Suche nach Netzwerkpartition aktivieren, können Sie mit der Engine Identification and Reconciliation (IRE) einzelne CIs für Ihre Assets erstellen, die dieselbe IP-Adresse aufweisen. Weitere Informationen finden Sie unter Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Tenable Vulnerability Integration und Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“..
- Klicken Sie oben auf dem Bildschirm neben dem Link Asset-Import auf den Link **CI-Suchregeln**, um die standardmäßigen Suchregeln für Configuration Items (CIs) anzuzeigen. CI-Suchregeln definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Konfigurationselementen (CIs) in der Now Platform CMDB verwendet werden. Sie haben die Möglichkeit, Suchregeln hinzuzufügen oder die standardmäßigen CI-Suchregeln auf dieser Seite zu ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.
- Klicken Sie auf **Assets jetzt** importieren, um Daten bei Bedarf zu importieren.
- Der Link **Erweiterte Einstellungen** verweist auf den Datensatz „Asset-Integration“. Ab v3.3 können Sie Parameter hinzufügen, die vom Produkt Tenable.io für Ihre geplanten Abfragen unterstützt werden, um die Schwachstellendaten zu filtern, die Sie mit den Assets von Tenable.io sowie den Integrationen von festen und offenen Schwachstellen importieren. Weitere Informationen finden Sie unter Legen Sie zusätzliche Filterparameter für Tenable.io Importe fest.

**6.** Klicken Sie auf **Weiter**, um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren. Das Formular „Plugins-Importkonfiguration“ wird angezeigt.

**7.** Aktivieren oder deaktivieren Sie in diesem Formular den Import von Plugins (Schwachstelleneinträge von Drittparteien), bestimmen Sie das anfängliche Startdatum für die Plugins, die Sie importieren möchten, und planen Sie, wann der Import der Tenable-Plugins ausgeführt werden soll.

Wenn Sie alle Plugins, Schwachstellen und Assets importieren möchten, lassen Sie das anfängliche Startdatum leer.

- Klicken Sie auf **Plugins jetzt** importieren, um Daten bei Bedarf zu importieren.
- Der Link **Erweiterte Einstellungen** verweist auf den Plugin-Integrationsdatensatz.
- Für den Import von Schwachstellen können Sie Schweregrade für Tenable.io für die Schwachstellen planen und festlegen, die erfasst werden sollen. Legen Sie ein Datum fest, damit nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.
- Für die Tenable.sc -Integration können Sie einen Abfragefilter und ein Datum festlegen, sodass nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Weiter**, um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren. Das Formular „Importkonfiguration für Schwachstellen“ wird angezeigt. Aktivieren oder deaktivieren Sie die Integration, und legen Sie das anfängliche Startdatum für die Schwachstellen fest, die Sie importieren möchten.

   Für das Produkt Tenable.io :

   - Importieren Sie nur die Schwachstellen und zugehörigen AEs, die den Bedingungen entsprechen, die Sie mit dem Schweregradfilter auswählen.
   - Für die Tenable.io Asset-Integration wird `Last Scan Time` nur für Assets mit Schwachstellen importiert und aktualisiert.
   - Aktivieren Sie die Option Behobene **Schwachstellen**, um AEs für feste Erkennungsdatensätze anzuzeigen. Wenn diese Kennzeichnung im Setup-Assistenten aktiviert ist, werden neue VIs für Erkennungen im Status „ **Festgelegt** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind. Wenn diese Funktion aktiviert ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.
   - Der Link **Erweiterte Einstellungen** neben „Importfilter“ verweist auf den Datensatz „Integration von Schwachstellen“.
   - Klicken Sie oben auf den Link **Zeitpläne** importieren, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und aktivieren Sie die Integration.

   Für das Produkt Tenable.sc :

   - Importieren Sie nur die Schwachstellen und zugehörigen VIs, die den Bedingungsfiltern entsprechen, die von einer Tenable-Abfrage in der Tenable-Plattform festgelegt werden. Weitere Informationen zu Tenable-Abfragen finden Sie in der Tenable-Dokumentation.

     Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets-Integration. Es werden nur die Assets mit den Schwachstellen importiert, die den Bedingungen des Abfragefilters entsprechen.

   - Aktivieren Sie die Option Behobene **Schwachstellen**, um AEs für feste Erkennungsdatensätze anzuzeigen. Wenn diese Kennzeichnung im Setup-Assistenten aktiv ist, werden neue AEs für Erkennungen im Status „ **Festgelegt** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind. Wenn diese Funktion aktiv ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.
   - Um den Netzwerkpartitionsbezeichner in die IP-Adresssuche einzubeziehen, wählen Sie **Suche nach Netzwerkpartition aktivieren** Checkbox aus dem **Suche nach Netzwerkpartition** Abschnitt. Weitere Informationen finden Sie unter Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Tenable Vulnerability Integration.
   - Klicken Sie oben auf **Zeitpläne** importieren, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und aktivieren Sie die Integration.
   - Der Link **Erweiterte Einstellungen** neben „Importfilter“ verweist auf den Datensatz „Integration von Schwachstellen“.
   - Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen wird automatisch im Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen von Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen) konfigurieren.

     Diese Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Produkt Tenable.sc in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren zu **Vertretbare Schwachstellenintegration** > **Integrationen** > **Tenable.sc-Integration von Scan-Anmeldeinformationen** , um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen.

9. **Klicken** Sie auf Fertigstellen, um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen.

### Nächste Maßnahme

(Optional) Navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner** > **Standardrisikorechner** > **Tenable-Risiko-Regel** , um die Tenable Risk-Regel zu aktivieren.

Aktivieren Sie im angezeigten Formular „Schwachstellenrechner-Regel“ das Kontrollkästchen Aktiv, um sie zu aktivieren.

Die Tenable Risk-Regel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Responseinstalliert. Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit dem neuen Standardrisikorechner verwendet wird. Diese Risikoregel ist standardmäßig deaktiviert. Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Die Aktivierung dieser Tenable Risk Calculator-Regel kann Auswirkungen auf die Leistung der Datenerfassung haben.

Siehe Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln

#### Konfigurieren Sie Schwachstellen-Lösungsanbieter

Nachdem Sie die Anwendung Vulnerability Solution Management installiert haben, konfigurieren Sie die Anbieter der Schwachstellenlösungen mithilfe des Setup-Assistenten.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration**.
2. Klicken Sie **auf Lösungsintegrationen**.
3. Rufen Sie im Abschnitt „Common Vulnerability Response Framework“ Daten mithilfe einer URL, einer API oder eines Imports ab.
   - Um Daten mithilfe einer URL oder API abzurufen, klicken Sie auf **Integration hinzufügen**.
   - Klicken Sie auf **Datei**importieren, um Daten durch Hochladen einer CVRF-Datei (Common Vulnerability Response Framework) abzurufen.

### Nächste Maßnahme

Je nachdem, wie Sie die CVRF-Daten importieren möchten, können Sie eine der folgenden Aufgaben ausführen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Informationen zum Importieren einer CVRF-Datei finden Sie unter Importieren Sie Common Vulnerability Reporting Framework-Daten durch Dateiimport.
- Informationen zum Importieren von CVRF-Daten mithilfe der APIs finden Sie unter Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL.
- Wenn Sie CVRF-Daten über Hinweise importieren möchten, finden Sie weitere Informationen unter Importieren von Common Vulnerability Reporting Framework-Daten aus Advisories.

### Importieren Sie Common Vulnerability Reporting Framework-Daten durch Dateiimport

Importieren Sie eine CVRF-Datei, um Daten im CVRF-Format anzuzeigen. Der Import ist eine einmalige Aktivität.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin.

#### Warum und wann dieser Vorgang ausgeführt wird

Nach dem Import wird ein Warteschlangeneintrag mit einem Anhang erstellt, der bei der Verarbeitung des Eintrags analysiert wird. Die Daten werden dann in die entsprechenden Tabellen eingetragen. Vor dem Analysieren der CVRF-Daten wird basierend auf der Konfiguration ein Scanner-Zuordnungsdatensatz erstellt. Anschließend werden die Scanner-Zuordnungsdaten in Lieferantenzuordnungsdaten umgewandelt.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken Sie **auf Datei importieren**.

   **Hinweis:**
   Sie können jeweils nur eine XML-Datei mit einer maximalen Dateigröße von 1 GB hochladen.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die Integration ein.
   Der Planer wird mit diesem Namen erstellt.
4. **Geben Sie** im Feld Lieferant den Namen des Lieferanten ein.
   Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt.
5. Klicken Sie auf **Fertigstellen**.

#### Ergebnisse

Eine Importwarteschlange wird erstellt. Klicken Sie auf den Link in der Infoleiste, um die Warteschlangeneinträge für den Lieferanten zusammen mit der zugehörigen Liste anzuzeigen. Sie können auch den Status des Auftrags anzeigen.

Nachdem die Daten in das CVRF-Format importiert wurden, werden die Daten wie folgt verarbeitet:

1. Wenn die Warteschlange verarbeitet wird, wird die Datei mit einer dedizierten Datenquelle analysiert.
2. Nach Abschluss der Verarbeitung wird das Anwendungsprotokoll aktualisiert.
3. Sobald die CVRF-XML-Datei analysiert wurde, füllt sie die folgenden Tabellen in der Anwendung ServiceNow® Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_solution
- sn_vul_m2m_vulnerability_solution
- sn_vul_nvd_entry
- sn_vul_software
- sn_vul_product_category

Sie können die detaillierten Informationen zu Fehlern oder Ausnahmen in den Anwendungsprotokollen anzeigen.

### Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen, um Lieferanten zu authentifizieren. Bei der beratenden Analyse werden Drittanbieter authentifiziert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

#### Prozedur

1. Erstellen Sie eine OAuth-Authentifizierung.
   Weitere Informationen finden Sie unter Erstellen eines Endpunkts für Clients für den Zugriff auf die Instanz .
2. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.
   Siehe Aliasse für Verbindungen und Anmeldeinformationen erstellen .
3. Erstellen Sie eine Verbindung.
   a. Klicken Sie auf den Namen des neu erstellten Alias für Verbindungen und Anmeldeinformationen.
   b. Klicken Sie auf der Registerkarte **Verbindungen** auf **Neu**.
   c. Wenn der Authentifizierungstyp OAuth ist, wählen Sie das in Schritt 1 erstellte Anwendungsregistrierungsprofil als **OAuth-Entitätsprofil**aus.
   d. Erstellen Sie einen Datensatz in Verbindungen aus der zugehörigen Liste des Datensatzes.
   e. Wählen Sie im Feld **Credential** (Anmeldeinformationen) den in Schritt 3d erstellten Anmeldeinformationsdatensatz aus.
   f. Geben Sie im Feld **Verbindungs-URL** die URL des Lieferanten ein.
   g. Klicken Sie auf **Absenden**.

### Konfigurieren Sie einen anderen Common Vulnerability Reporting Framework-Anbieter als Cisco

Konfigurieren Sie einen anderen CVRF-Anbieter (Common Vulnerability Reporting Framework) als Cisco mit API-Support.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder admin

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen Datensatz mit dem vom Lieferanten unterstützten Authentifizierungstyp.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Authentifizieren eines Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen.

3. Navigieren zu **Alle** > **Vulnerability Response** > **Flow Designer**.
4. Duplizieren Sie den Flow mit der Bezeichnung „Advisory Parsing“.

   **Hinweis:**
   - Wenn eine der Aktionen geändert werden muss, kopieren Sie die Aktion, und verwenden Sie sie im neuen Flow.
   - Aktualisieren Sie die paginierungsbezogene Logik gemäß dem Lieferanten

5. Wenn die Logik des Datumsbereichsparameters nicht mit der von Cisco identisch ist, kopieren Sie die Aktion **Paginierungsparameter aktualisieren**, und nehmen Sie die für den Lieferanten erforderlichen Änderungen vor.
6. Navigieren zu **Alle** > **Vulnerability Response** > **Ergänzungsdatenzuordnungen**.
7. Erstellen Sie einen Datensatz gemäß Cisco, indem Sie den **Eigenschaftsschlüsselwert** gemäß dem Lieferanten ändern.
   Diese Logik dient der Zuordnung erforderlicher Felder aus einer beratenden Nutzlast zu einer Tabelle ServiceNow.
8. Ordnen Sie die folgenden API-Tags aus der API-Nutzlast zu.
   Diese Tags müssen Details zugeordnet werden, die in der Tabelle „Ergänzungsdatenzuordnung“ ausgefüllt werden sollen. Standardmäßig wird die Cisco-spezifische Zuordnung ausgeliefert.

   **Hinweis:**
   Sie müssen einen Datensatz erstellen, wenn Sie mehrere Lieferanten konfigurieren müssen, die Empfehlungen veröffentlichen.

| Beratendes Payload-Tag | Spalte aus der Tabelle „sn_vul_cvrf_solution_integratio | Beschreibung |
|---|---|---|
| CVRF-URL | cvrf_url | Tag-Name, der die CVRF-URL enthält. |
| Beratende ID (eindeutiger Schlüssel für Antwort) | ID | Tag-Name, der einen eindeutigen Bezeichner enthält. |
| Datum der letzten Änderung | last_modified_date | Tag-Name, der das Datum enthält, an dem der Datensatz zuletzt aktualisiert wurde. |

9. Ändern Sie basierend auf dem Antwortformat die Analyselogik, indem Sie die Aktion **Liste** abrufen aus dem Flow der beratenden Analyse kopieren.

### Importieren von Common Vulnerability Reporting Framework-Daten aus Advisories

Importieren Sie CVRF-Daten aus Hinweisen, indem Sie die Lieferanten-URL mit dem Importtyp als API konfigurieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

#### Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden die Hinweise abgerufen. Die CVRF-URL und die Empfehlungs-ID werden aus der Nutzlast extrahiert. Die REST-API-Aufrufe werden



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für jede CVRF-URL ausgeführt, und die Daten werden analysiert und in der Tabelle sn_vul_solution gespeichert.

### Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken **Sie auf Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Lösungshinweise importieren“.**

| Feld | Beschreibung |
|---|---|
| Importtyp | Option zum Auswählen des Importtyps. Wählen Sie **API aus**. |
| Name | Eindeutiger Name für die Integration. |
| Lieferant | Name des Lieferanten.<br>**Hinweis:**<br>Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt. |
| Verbindungsalias | Option zum Auswählen authentifizierter Anmeldeinformationen.<br>**Hinweis:**<br>In der Tabelle „sys_alias“ werden Anmeldeinformationen und die Basis-URL für Hinweise gespeichert. |
| Zeitplan | Häufigkeit, mit der die Daten aktualisiert werden müssen. |
| Tag | Wochentag, an dem die Daten aktualisiert werden sollen. |
| Zeit | Wochenzeit, zu der die Daten aktualisiert werden sollen. |
| API-Konfiguration | |
| Flow | Option zum Auswählen des Flows.<br>Der Flow wird ausgelöst, wenn der Planer ausgeführt wird. Der Flow analysiert die Hinweise, extrahiert die CVRF-URL und speichert diese Details in den Aktualisierungstabellen. Sie können den vorhandenen Flow kopieren und nach Bedarf bearbeiten. Sie können beispielsweise Änderungen im Zusammenhang mit der Paginierung vornehmen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Flow-Aktion | Option zum Auswählen der Flow-Aktion.<br><br>Flow-Aktionen berücksichtigen die Schiebefensterfunktion. Sie können die Flow-Aktionen aktualisieren und den Abfrageparameter durch Ziehen direkt zur Aktion hinzufügen. |
| Zuordnungstabelle | Option zum Auswählen der Zuordnungstabelle.<br><br>Der Datensatz der Ergänzungsdatenzuordnungstabelle wird zum Extrahieren der CVRF-URL und der Advisory-ID aus der Payload der Advisories verwendet. |
| Hinweise aus Antwort | Option zur Eingabe des Tag-Namens aus der Nutzlast der Warnungen, aus der die Liste der Warnungen extrahiert werden kann. |
| Filterkriterien | |
| Zeitbereichsparameter | Option zum Auswählen des Zeitbereichs für die Anforderung und des Datumsformats für API-Aufrufe.<br><br>Der Anforderungsparameter für Startdatum/Enddatum ist der Parametername, der für Startdatum und Enddatum bei API-Aufrufen verwendet wird. Beispiel: StartDate, start_date, endDate, end_date. |
| Datumsformat | Option zur Eingabe des Datumsformats, z. B. mm/tt/jjjj..<br><br>Das Datumsformat ist das Format, das die API zum Filtern benötigt. Formate, die von GlideDate nicht unterstützt werden, funktionieren nicht. |
| Anfänglicher Bereich in Tagen | Geben Siedie Tage ein, für die die Daten abgerufen werden müssen, wenn der Scheduler zum ersten Mal ausgeführt wird.<br><br>Für nachfolgende Ausführungen wird der Schiebefenstermechanismus verwendet.<br><br>**Hinweis:**<br>Wenn Sie keinen Zeitbereich auswählen möchten, wählen Sie **Keine Parameter**aus. |
| Scannerzuordnungen | |
| Scannerquelle | Option zum Auswählen der Quelle des Drittparteieintrags (TPE). |
| Schwachstellenspalte | Option zum Auswählen des Stichworts. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Stichwörter | Option zur Eingabe des Stichworts für die Suche in der ausgewählten Schwachstellenspalte. |

4. Klicken Sie auf **Fertigstellen**.

### Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL

Importieren Sie CVRF-Daten, indem Sie die Lieferanten-URL im Setup-Assistenten konfigurieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.admin (veraltet) oder admin

#### Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden Daten von der URL abgerufen, die analysiert wird. Die Daten werden dann in der Tabelle sn_vul_solution mit Quelle als Lieferantenname gespeichert.

**Hinweis:**
Oracle veröffentlicht die CVRF-URL direkt, um Lösungen bereitzustellen. Wenn Sie also die Integration für den Import von Oracle-Daten konfigurieren möchten, stellen Sie sicher, dass Sie die CVRF-URL für Oracle haben, und führen Sie die folgenden Schritte aus.

#### Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Common Vulnerability Response Framework**.
2. Klicken **Sie auf Integration hinzufügen**.
3. Füllen Sie die Felder des Formulars aus.

#### Importieren Sie das CVRF-Formular

| Feld | Beschreibung |
|---|---|
| Importtyp | Typ des Imports. Wählen Sie **URL aus**. |
| Name | Eindeutiger Name für die Integration. |
| Lieferant | Name des Lieferanten.<br>**Hinweis:**<br>Das Feld **Quelle** der Lösungen wird mit dem Lieferantennamen ausgefüllt. |
| URL | URL, von der Sie die Lösungsdaten im CVRF-Format abrufen möchten. |
| Zeitplan | Häufigkeit, mit der die Daten aktualisiert werden müssen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Wenn das Status-Tag von CVRF „FINAL“ anzeigt, wird das Feld automatisch auf **On Demand** gesetzt, um unnötige Ausführungen zu verhindern. |
| Tag | Wochentag, an dem die Daten aktualisiert werden sollen. |
| Zeit | Wochenzeit, zu der die Daten aktualisiert werden sollen. |

4. Klicken Sie auf **Fertigstellen**.

### Problembehandlung beim Datenimport von Common Vulnerability Reporting Framework

Aktionen zur Fehlerbehebung können helfen, häufige Probleme beim Importieren von CVRF-Daten in die Anwendung Vulnerability Response zu beheben.

| Problem | Aktion |
|---|---|
| Dauer der Integrationsausführung ist lang | Wenn die Integration länger als erwartet ausgeführt wird, gehen Sie wie folgt vor:<br>1. Navigieren Sie zur Tabelle sn_vul_ds_import_q_entry.<br>2. Gruppieren Sie nach dem Feld **Status**. Sie können die Einträge sehen, die sich im Status „Abgeschlossen“, „In Bearbeitung“ oder „In der Warteschlange“ befinden. |
| Integration im API-basierten Import fehlgeschlagen | Wenn die Integration beim API-basierten Import fehlschlägt, gehen Sie wie folgt vor:<br>1. Navigieren Sie zu **Flow Designer**.<br>2. Öffnen Sie den Flow, der in der Konfiguration ausgewählt wurde.<br>**Hinweis:** Öffnen Sie im Fall von Cisco den Flow Advisory Parsing.<br>3. Klicken Sie auf **Ausführungen**.<br>4. Öffnen Sie die letzte Ausführung oder die Ausführung, die debuggt werden muss.<br>5. Überprüfen Sie den Flow in jeder Phase. |
| Integration im API-basierten Import mit Zeitüberschreitungsfehler fehlgeschlagen | Wenn die Integration in einem API-basierten Import aufgrund einer Zeitüberschreitung im empfohlenen Analyse-Flow fehlschlägt, gehen Sie wie folgt vor: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Problem | Aktion |
| --- | --- |
| | 1. Erhöhen Sie die Zeitüberschreitung, indem Sie sys_properties.LIST öffnen.<br>2. Suchen Sie in der Spalte Name nach sn_vul.CVRFFlowTimeout (inMiliSeconds).<br>**Hinweis:** Die Zeit wird in Millisekunden angegeben.<br>3. Öffnen Sie den Datensatz, und aktualisieren Sie den Wert mit einer großen Zahl.<br>4. Speichern Sie den Datensatz, und führen Sie die Integration erneut aus. |
| Fehler bei der Integration mit Fehler „Transformation von Scannerzuordnung zu Lieferantenzuordnungsdaten wird ausgeführt“ | Überprüfen Sie, ob die Integration während des URL- oder API-basierten Imports mit dem folgenden Fehler fehlschlägt:Scanner-Zuordnung zu Lieferantenzuordnungsdatentransformation wird ausgeführt. Die Daten werden erst ausgefüllt, nachdem die Transformation abgeschlossen ist. Versuchen Sie nach einiger Zeit die Ausführung.<br>Wenn dieser Fehler auftritt, warten Sie einige Zeit, und führen Sie die Integration erneut aus. |
| Importwarteschlange wird während des Dateiimports nicht erstellt | Während eines Dateiimports wird die Importwarteschlange manchmal nicht erstellt. Dieser Fehler bedeutet, dass die Transformation, die Scanner-Zuordnungsdaten Lieferantenzuordnungsdaten zuordnet, ausgeführt wird. Der Warteschlangeneintrag wird erstellt, sobald der Prozess abgeschlossen ist. |

## Zusätzliche Vulnerability Response Setup- und Konfigurationsaufgaben

Um Sie bei der Fehlerkorrektur zu unterstützen, können Sie diese zusätzlichen administrativen Setup-Aufgaben als Teil Ihrer Konfiguration außerhalb des Basis-Setups ausführen. Sie führen diese Aufgaben außerhalb des Setup-Assistenten aus.

Sie können die mit Vulnerability Response bereitgestellten Standardberichte verwenden, um Ihre Sicherheitslage zu überwachen. Sie können diese Berichte bearbeiten, wenn sie nicht zu Ihrer Umgebung passen, oder sie als Vorlagen zum Erstellen eigener Berichte verwenden.

Wenn die Anwendung Performance Analytics for Vulnerability Response installiert ist, können Sie Berichte, interaktive Dashboards und mehr erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Berichten .

E-Mail-Benachrichtigungen steigern die Produktivität und sorgen für einen reibungslosen Workflow.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchen Sie mit der Software-Risikobewertung nach Herausgeber, Produktname und Versionsnummer in Software Asset Management (SAM Foundation), um Ihr Risiko für angreifbare Software zu bestimmen.

Transparenz in Schwachstellenbibliotheken kann Flexibilität bei Gruppierungs- und Korrekturaufgaben bieten.

Konfigurieren Sie die Ausnahmeverwaltung so, dass Sie eine Ausnahme anfordern können, wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann.

Weitere zusätzliche Setup-Aufgaben finden Sie in den Themen nach dieser Übersicht.

### Schnellstarttests für Vulnerability Response

Überprüfen Sie, ob Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demokonten erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird. Weitere Informationen zum Einrichten und Ausführen der Testsuite für Führen Sie die Test-Suite Automated Test Framework (ATF) für aus Vulnerability Response ] finden Sie unter Vulnerability Response.

Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Vulnerability Response (sn_vul) und das Laden der Demodaten.

#### Vulnerability Response-Tests

| Test | Beschreibung | Release-Version |
|---|---|---|
| VR: Fehlerkorrektur-Zielregel erstellen | Erstellt eine Fehlerkorrektur-Zielregel. | Madrid |
| VR: Schwachstellengruppenregel erstellen | Erstellt eine Schwachstellengruppenregel. | Madrid |
| VR: Erstellen eines angreifbaren Elements über das Formular | Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich aus dem Formular „Angreifbares Element“ erstellen kann. | Madrid |
| VR: Schwachstellengruppen-Lebenszyklus | Ermittelt, ob ein Benutzer eine Schwachstellengruppe erfolgreich beheben kann. | Madrid |
| VR: Lebenszyklus von angreifbaren Elementen | Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich durch seinen Lebenszyklus bewegen kann, und ermittelt zudem, ob ein abgeschlossenes angreifbares Element erneut geöffnet werden kann. | Madrid |
| VR: Rollup-Rechner | Ermittelt, ob der Rollup-Risiko-Rechner eine | New York |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vulnerability Response-Tests (Fortsetzung)

| Test | Beschreibung | Release-Version |
|---|---|---|
| | Gesamtrisikopunktzahl für eine ganze Gruppe angreifbarer Elemente mit den Punktzahlen für alle angreifbaren Elemente in einer Schwachstellengruppe verfügbar machen kann. | |
| VR: Vulnerability Response-Zuweisungsregeln | Ermittelt, ob mit einem Mustersatz von Zuweisungsregeln angreifbare Elemente automatisch einer Zuweisungsgruppe zur Nachbesserung zugewiesen werden können. | New York |
| VR: Sicherheitsrisiko-Rechner | Testen Sie den Sicherheitsrisiko-Rechner. | New York |
| VR: CI-Suche – Qualys | Erstellt mithilfe der Methode „field_matching“ eine neue Suchregel mit der Bezeichnung „Suche nach Netzwerkadapter“ für Qualys. Ermittelt, ob Konfigurationselemente mit der neuen Suchregel erfolgreich nach Netzwerkadapter und IP-Adresse mit der Tabelle „Erkannte Elemente“ abgeglichen werden. | Orlando |
| VR: Normale Change-Anforderungen und Notfall-Change-Anforderungen erstellen | Ermittelt, ob der Benutzer erfolgreich normale Change-Anforderungen und Notfall-Change-Anforderungen aus einer Schwachstellengruppe erstellen kann. | Orlando |
| VR: Schwachstellengruppen aufteilen | Ermittelt, ob der Benutzer Schwachstellengruppen erfolgreich aufteilen kann. | Orlando |
| VR: SG-Status bei Abbruch von CHG aktualisieren | Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, abgebrochen wird. | Orlando |
| VR: SG-Status aktualisieren, wenn CHG zur Überprüfung wechselt | Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, in den Überprüfungsstatus wechselt. | Orlando |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vulnerability Response-Tests (Fortsetzung)

| Test | Beschreibung | Release-Version |
|---|---|---|
| VR: CI-Suche – Rapid7 | Testen Sie die CI-Suche mithilfe der vorhandenen Rapid7 Vulnerability Integration-Suchregel **IP-Adresse**. | Orlando |
| VR: CI-Suche – Qualys | Testen Sie die CI-Suche, indem eine neue Suchregel für Qualys Vulnerability Integration erstellt wird. | Orlando |
| VR: Ausnahmegenehmigungs-Workflow für VI | Erstellen Sie eine Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert. | Orlando |
| VR: Falsch positiver Genehmigungsworkflow für VI | Erstellen Sie eine falsch positive Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert. | Orlando |
| VR: Application Vulnerability Response (AVR) | Bestimmen Sie, ob Ihre Regeln und Rechner ordnungsgemäß funktionieren. Stellen Sie sicher, dass Updates funktionieren. | Orlando |
| Nachbesserungszielregeln: VI-Importtest | Testet die VR-Nachbesserungszielregeln während des Imports. | Paris |
| VR: Klassifizierungsregel | Beispiel für eine Klassifizierungsregel, die eine Schwachstelle automatisch klassifiziert. | Tokyo |

**Zugehörige Informationen**

Schnellstarttests

## Führen Sie die Test-Suite Automated Test Framework (ATF) für aus Vulnerability Response

Führen Sie die Test-Suite Automated Test Framework (ATF) aus, nachdem Sie die Anwendung Vulnerability Response installiert oder aktualisiert haben.

### Vorbereitungen

Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz wie vorgesehen funktioniert.

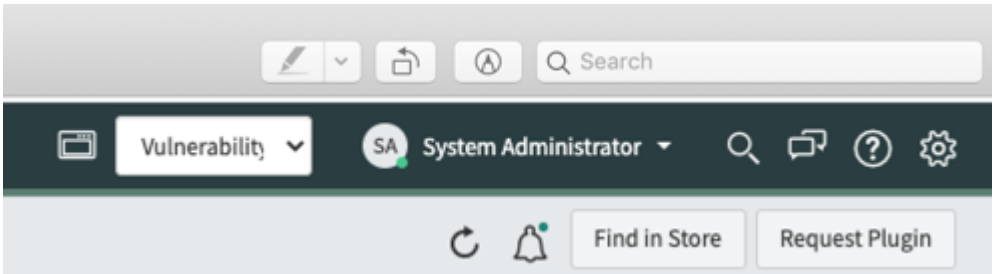
Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demokonten erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vergewissern Sie sich, dass Sie Demodaten installiert haben, als Sie Vulnerability Responseinstalliert haben. Zum Ausführen der Test-Suite Vulnerability Response sind Demodaten erforderlich.
- Führen Sie die folgenden Schritte aus, um den Test zu aktivieren:
  1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**.
  2. Wenn diese Option nicht ausgewählt ist, aktivieren Sie das Kontrollkästchen **Test-/ Testsuite-Ausführung** aktivieren.
  3. Klicken Sie auf **Speichern**.
  4. Wenn der Umfang im Header nicht auf **Vulnerability Response** festgelegt ist oder der Umfang nicht im Header angezeigt wird, klicken Sie im Browserfenster oben auf der Seite auf das .
  5. Klicken Sie im Fenster „Systemeinstellungen“ auf **Entwickler**.
  6. Wenn nicht ausgewählt, klicken Sie auf **Anwendungsauswahl in Header anzeigen,** und schließen Sie das Fenster.
  7. Klicken Sie in der Liste, die neben Systemadministratorangezeigt wird, auf **Vulnerability Response** für das Feld.

     Das Feld wird wie in der folgenden Abbildung angezeigt.




Erforderliche Rolle: admin oder atf_test_admin

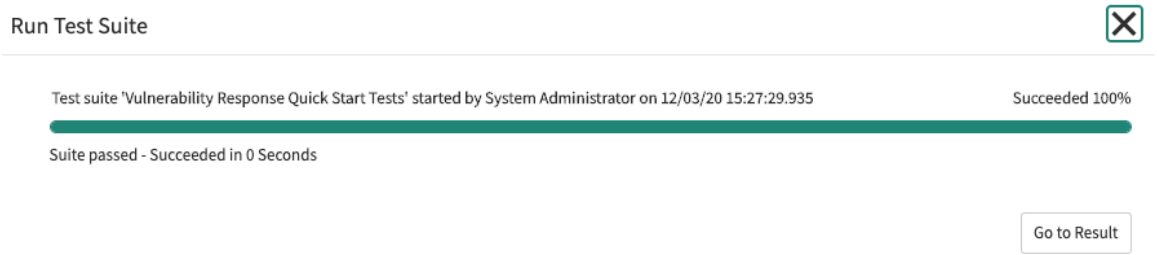
### Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Suites**.
2. Suchen Sie in der Liste „Test-Suites“ nach **Vulnerability Response-Schnellstarttests**.
3. Wählen Sie es aus, um den Datensatz zu öffnen.
4. Aktivieren Sie im geöffneten Datensatz das Kontrollkästchen **Aktiv**.
5. Klicken Sie auf **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wenn die Schaltfläche **Testsuite** ausführen nicht angezeigt wird, aktualisieren Sie Ihren Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf **Testsuite ausführen**, um den Test zu starten. Nach einigen Minuten zeigt das Dialogfeld „Test-Suite ausführen“ einen erfolgreichen Test an. Klicken **Sie auf Zu Ergebnis wechseln,** um weitere Informationen zu




erhalten.

## Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von Vulnerability Responsefortfahren.

Weitere Informationen zu automatisierten Tests für Vulnerability Response und automatisierten Tests, Test-Suites und zum Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF).

### Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren

Installieren Sie Empfehlungen für die Zuweisung von Schwachstellen, damit Sie die Zeit reduzieren können, die Sie für die Identifizierung von Besitzern für nicht oder falsch zugewiesene Schwachstellenergebnisse benötigen. Diese Anwendung ist als separates Abonnement im ServiceNow Storeverfügbar.

## Vorbereitungen

Bevor Sie die Funktion Empfehlungen für die Zuweisung von Schwachstellen von Vulnerability Response in Ihrer Instanz von [ Now Platform® ausführen, müssen Sie zuerst die Anwendung Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response herunterladen und installieren. Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Nicht-Produktions- oder Entwicklungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Weitere Informationen finden Sie unter ServiceNow Store-Anwendungen aktivieren.

Erforderliche Rolle: admin

| Setupaufgaben | Aktion |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Vulnerability Response wird in dieser Liste angezeigt, wenn er installiert ist.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |

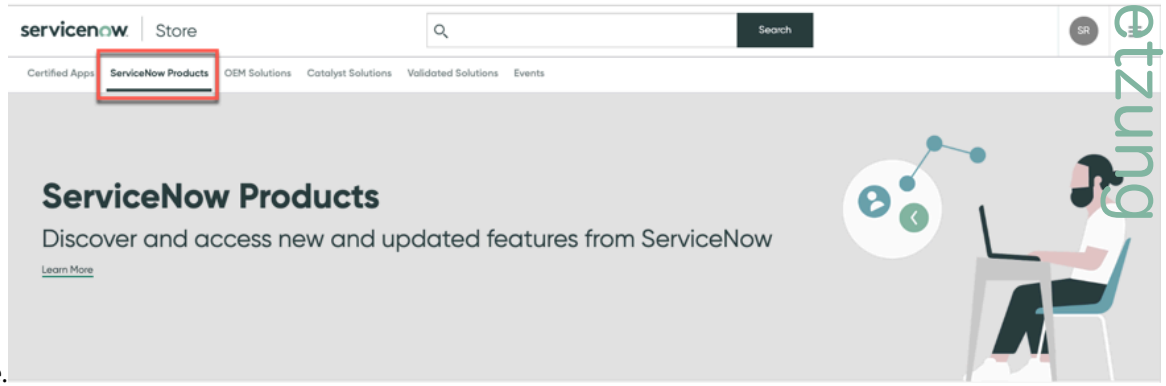


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Aktion |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Predictive Intelligence installiert und aktiviert ist. | Navigieren zu **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Predictive Intelligence wird in dieser Liste angezeigt, wenn er installiert ist.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Install Predictive Intelligence . |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Stellen Sie sicher, dass Sie über die folgenden erforderlichen Rollen für die Installation und Überprüfung der erwarteten Ergebnisse verfügen:<br>• vulnerability_admin: Erforderlich, um Empfehlungen für die Zuweisung von Schwachstellenzu aktivieren und zu konfigurieren. Sie können sie auch verwenden, um Zuweisungsempfehlungen für angreifbare Elemente und Korrekturaufgaben anzuzeigen und auszuwählen.<br>• ServiceNow admin: Erforderlich, um Anwendungen zu installieren. |

### Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie auf **Anmelden,** und geben Sie Ihre HI-Anmeldeinformationen ein.
3. Um die verfügbaren ServiceNow Produkte anzuzeigen, klicken Sie auf die Registerkarte ServiceNow **Produkte**.




4. Um alle zugeordneten Anwendungen anzuzeigen, die Sie für Empfehlungen für die Zuweisung von Schwachstellenerwerben, klicken Sie auf das Produkt Vulnerability Response.

   Auf der Seite werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Um Informationen zu einer Anwendung zu erhalten, klicken Sie auf den Link für die Anwendung.

5. Um zu überprüfen, ob Sie über die Berechtigung für Empfehlungen für die Zuweisung von Schwachstellenverfügen, klicken Sie auf **Opt-in**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
   Eine Nachricht zeigt an, dass Sie sich erfolgreich für die Anwendung entschieden haben.
7. Fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Now Platform -Instanz zu installieren.
8. **Wahlweise:** Wenn Sie Ihre Berechtigung für die Anwendung Empfehlungen für die Zuweisung von Schwachstellen in anderen Now Platform Instanzen verwalten möchten, klicken Sie auf **Berechtigung verwalten**.

   **Hinweis:**

   (Optional) Wenn die Schaltfläche **Berechtigung verwalten** nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung Empfehlungen für die Zuweisung von Schwachstellen, um sie anzuzeigen.

   a. Wählen Sie eine Option.

   b. Klicken Sie auf **OK** oder **Abbrechen**, um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihren Now Platform -Instanzen zu installieren.
9. Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Empfehlungen für die Zuweisung von Schwachstellen installieren möchten.
10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
11. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Empfehlungen für die Zuweisung von Schwachstellen (sn_vul_recom), und klicken Sie auf **Installieren**.
    Das Dialogfeld „Anwendungsinstallation“ wird angezeigt, und alle installierten Abhängigkeiten werden angezeigt.
12. **Wahlweise:** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen **Demodaten** laden, und klicken Sie auf **Installieren**.

    **Hinweis:**
    Wenn Sie das Kontrollkästchen Demodaten laden nicht aktivieren, können die **Demodaten** nachträglich nicht über den Anwendungsmanager installiert werden. Weitere Informationen dazu, wie Sie Demodaten nach der Erstinstallation installieren oder erneut installieren, finden Sie im Artikel Workaround to install demo data if application is opened (Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist) [KB0722909] in der Knowledge Base von Now Support.

    Diese Installation kann einige Zeit in Anspruch nehmen. Eine Nachricht wird im Dialogfeld „Installieren“ angezeigt, nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden.
13. Klicken Sie auf **Schließen**.
14. Informationen zum Konfigurieren von Empfehlungen für die Zuweisung von Schwachstellenfinden Sie unter Konfigurieren Sie Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response.

### Konfigurieren Sie Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response

Aktivieren Sie Empfehlungen für die Zuweisung von Schwachstellen, um die Zeit zu reduzieren, die Sie für die Identifizierung der Besitzer für nicht oder falsch zugewiesene Schwachstellenergebnisse benötigen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.manage_assignment_recom_config



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird
Diese Anwendung ist standardmäßig nicht aktiviert.

### Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsempfehlungen**.
2. Wählen Sie **Zuweisungsempfehlungen aktivieren aus**.
   Das **Feld Predictive Intelligence-Lösungsdefinition wird** angezeigt. Der Standardwert ist **Zuweisung angreifbarer Elemente**.
3. Klicken Sie auf **Speichern**.

## Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response

Erstellen und trainieren Sie ein Lösungsdefinitionsmodell für Vulnerability Response mithilfe von Predictive Intelligence. Sie können dieses Modell verwenden, um die Zuweisungsgruppe für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT) basierend auf vorhandenen Daten vorherzusagen.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur
1. Navigieren zu **Alle** > **Predictive Intelligence** > **Klassifizierung** > **Lösungsdefinitionen**.
2. Klicken Sie im Formular „Klassifizierungsdefinitionen“ auf **Zuweisung angreifbarer Elemente**.
   Dies ist die Standardlösungsdefinition.

   **Hinweis:**
   - Die standardmäßige Schulungshäufigkeit beträgt 30 Tage. Dies bedeutet, dass das Modell alle 30 Tage automatisch mit dem VI-Datensatz neu trainiert wird, der der konfigurierten Filterbedingung entspricht.
   - Felder aus der Tabelle „Angreifbares Element“ können für das Training verwendet werden. Die Standardlösungsdefinition wird für zwei VI-Felder trainiert: **Vulnerability.Summary** und **Configuration item.Name**. Sie können die für das Training verwendeten Felder anpassen, je nachdem, welche Felder Sie für die Vorhersage der Verantwortung für Schwachstellen in Ihrer Organisation hilfreich finden.

3. Informationen zum Erstellen und Trainieren der Klassifizierungslösung finden Sie unter Klassifizierungslösungen erstellen und trainieren.

   **Hinweis:**
   Sie können auch eine Ähnlichkeits- oder Clustering-Lösung erstellen und trainieren. Weitere Informationen finden Sie unter:
   - Ähnlichkeitslösung erstellen und trainieren.
   - Erstellen und trainieren Sie eine Clustering-Lösung.

4. Klicken Sie auf **Update & Retrain (Aktualisieren und neu trainieren)**.

   **Hinweis:**
   Informationen zum Konfigurieren erweiterter Einstellungen für ML-Lösungen finden Sie unter Erweiterte Einstellungen für ML-Lösungen konfigurieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie einen Vulnerability Response -Rechner

Ein Schwachstellenrechner ist eine vordefinierte Formel, um ein Zielfeld zu berechnen, wenn bestimmte Kriterien erfüllt sind. Rechner, die die Risikopunktzahl des angreifbaren Elements berechnen, können **Risikoregelnenthalten**.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Hinweis:**
Möglicherweise stellen Sie eine Leistungsverschlechterung fest, wenn Sie Schwachstellenrechner ausführen, die Skripts enthalten.

Ordnen Sie Ihre Regeln so, dass die einfachsten Regeln zuerst ausgeführt werden, und führen Sie nur Skripts für die Elemente aus, die nicht mit einer Bedingung und einem Vorlagenwert oder einer Risikoregel behandelt werden können.

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Sicherheitsrisiko-Rechner**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Formular „Schwachstellenrechner“.**

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Schwachstellenrechners. |
| Tabelle | Wird automatisch mit dem Namen der Tabelle für angreifbare Elemente ausgefüllt. |
| Anwendung | Automatisch ausgefüllt mit Vulnerability Response. |
| Zielfeld | Zu berechnendes Feld. |
| Beschreibung | Textbeschreibung des Rechners. |
| Aktiv | Schalten Sie den Rechner ein oder aus. |

4. Klicken Sie mit der rechten Maustaste auf den Header, um **Speichern**.
   Der Abschnitt „ **Regeln des Schwachstellenrechners“** wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf **Neu**klicken.

**Hinweis:**
Informationen zum Formular „ **Neue Risikoregeln“** (nur verfügbar, wenn das **Feld Ziel Risikopunktzahllautet**) finden Sie in Schritt 10.

6. Füllen Sie die Felder entsprechend aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Schwachstellenrechner – Regel“

| Feld | Beschreibung |
|---|---|
| Name | Name der Rechnerregel. |
| Bestellung | Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rechner | Automatisch mit dem übergeordneten Rechner ausgefüllt. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie diese Checkbox deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden. |
| Erweiterte Ansicht | Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte aus **Bedingungstyp** und **Werttyp**ausgewählt werden. |

7. Füllen Sie die Felder auf der Registerkarte **Wenn diese Bedingung erfüllt** ist entsprechend aus.

### Registerkarte „Wenn diese Bedingung erfüllt ist“

| Feld | Beschreibung |
|---|---|
| Name | Name der Rechnerregel. |
| Bestellung | Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rechner | Automatisch mit dem übergeordneten Rechner ausgefüllt. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie diese Checkbox deaktivieren, gilt diese Regel nicht für im System erstellte angreifbare Elemente. |
| Erweiterte Ansicht | Wenn diese Option ausgewählt ist, wählen Sie geskriptete Bedingungen und geskriptete Werte aus **Bedingungstyp** und **Werttyp**aus. |
| Bedingungstyp | Verfügbar, wenn Sie die **erweiterte Ansicht**auswählen. Zur Auswahl stehen:<br>○ Filter: Verwendet Filterbedingungen.<br>○ Filtergruppe: Informationen zum Definieren der Rechnerkriterien finden Sie unter Neue Filtergruppe erstellen.<br>○ Skript: Skriptbedingung, die verwendet wird, um zu bestimmen, wann dieser Rechner angewendet werden soll.<br>**Hinweis:**<br>Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zur Liste der **Schwachstellenrechner** zurück. Untersuchen Sie die Datensätze des Schwachstellenrechners, die im Lieferumfang des Basissystems enthalten sind. |
| Bedingung | Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll oder nicht.<br>Wenn Sie entweder die Bedingungstypen **Filtergruppe** oder **Skript** auswählen, wird dieses Feld ausgeblendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt. |

8. Klicken Sie auf die Registerkarte **Diese Werte festlegen**, und füllen Sie die Felder im Formular entsprechend aus.

**Legen Sie diese Felder auf der Registerkarte fest**

| Feld | Beschreibung |
|---|---|
| Werttyp | Verfügbar, wenn Sie die **erweiterte Ansicht**auswählen. Zur Auswahl stehen:<br>○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen.<br>○ Skript: Wird verwendet, um die Werte in jedem Feld festzulegen. |
| Skriptwerte | Verfügbar, wenn Sie den **Werttyp Skript** ausgewählt haben.<br>Definiert, auf welche Werte die Berechnungen angewendet werden sollen. |
| Vorlage | Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten.<br>Wenn Sie einen der **Werttypen Skript** auswählen, wird dieses Feld ausgeblendet. |

9. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.

**Hinweis:**
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie die **Schaltfläche Rechner erneut anwenden** verwenden. Er durchläuft alle aktiven angreifbaren Elemente (AEs). Wenn dieser Rechner zum Festlegen des Werts verwendet wird, wird der Wert für diese AEs neu berechnet. Da das erneute Anwenden eines Rechners sehr lange dauern kann, wird dies mit einer regelmäßigen Aufgabe erledigt.

10. Füllen Sie im Formular **„Neue Risikoregeln“** die entsprechenden Felder aus.

Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der aus diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollen, die Gewichtung auf 0 fest.

Sie können die Felder hinzufügen, löschen oder aktualisieren. Sie können auch den Gewichtungsprozentsatz für die Feldwerte konfigurieren. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Wenn Sie die Gewichtungen aktualisieren, zeigen Szenarien die verbleibenden Gewichtungen sowie die erwarteten Ergebnisse der **Risikopunktzahl** an.

| Feld | Beschreibung |
|---|---|
| Name | Name der Rechnerregel. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

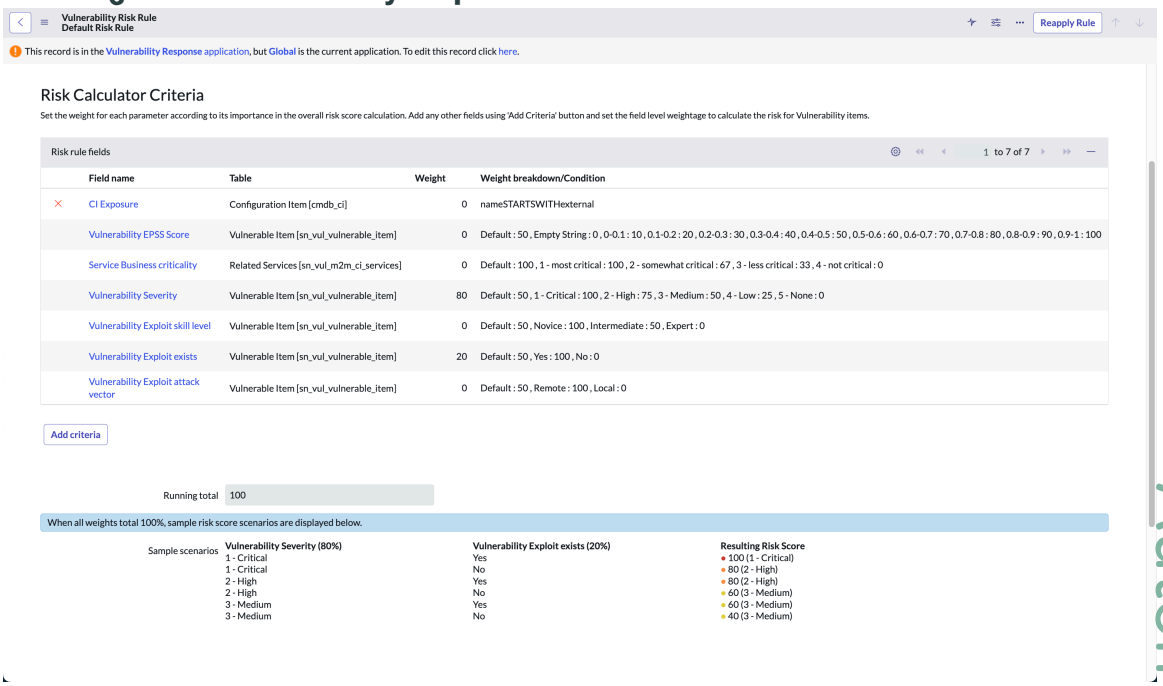
| Feld | Beschreibung |
|---|---|
| Bestellung | Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rechner | Automatisch mit dem übergeordneten Rechner ausgefüllt. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie diese Checkbox deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden. |
| Bedingung | Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll.<br>Wenn Sie entweder die Bedingungstypen **Filtergruppe** oder **Skript** auswählen, wird dieses Feld ausgeblendet. |
| **Gewichtungen** | |
| Schwachstellenschweregrad | Prozentsatz des Ergebnisses, der aus dem Schweregrad stammt. |
| EPSS-Punktzahl der Schwachstelle | Wahrscheinlichkeit der Ausnutzung der Schwachstelle. Standardmäßig ist die Gewichtung dieser Kriterien 0. Wenn Sie dies für die Berechnung der Risikopunktzahl verwenden möchten, legen Sie eine entsprechende Gewichtung für diese Kriterien fest. |
| Exploit vorhanden | Prozentsatz des Ergebnisses, der aus dem Vorhandensein eines Exploits stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0. |
| Exploit-Kompetenzniveau | Prozentsatz des Ergebnisses, der aus dem für den Exploit erforderlichen Kompetenzniveau stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0. |
| Exploit-Angriffsvektor | Prozentsatz des Ergebnisses, der von der Zielseite des Angriffs stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0. |
| Service Geschäftsrelevanz | Prozentsatz des Ergebnisses, der aus der Geschäftsrelevanz stammt. Wenn Sie Ihre CIs nicht mit Business Services verknüpft haben, setzen Sie die Gewichtung auf 0. |
| CI-Gefahrenpotenzial | Prozentsatz des Ergebnisses, der davon abhängt, ob das CI mit dem Internet verbunden ist. Wenn die Gewichtung nicht null ist, wird ein Bedingungsfilter angezeigt, um zu definieren, welche CIs mit Internetverbindung verbunden sind. Legen Sie den Filter so fest, dass Konfigurationselemente mit Internetzugriff ausgewählt werden. Sie können eine Vorschau der Datensätze anzeigen, die der Bedingung entsprechen. |
| Laufende Summe | Automatisch berechnete Prozentsätze. Wenn dieser Wert 100 erreicht, zeigt die Szenariovorschau Beispiel-Risikopunktzahlen in verschiedenen Szenarien an. |
| Risikopunktzahl-Szenarien | Wenn alle Gewichtungen 100 % ergeben, werden Risikopunktzahl-Szenarien angezeigt, die eine Vorschau der Risikopunktzahl in einigen der möglichen Szenarien bieten. |

Sie können Kriterien hinzufügen oder entfernen und die Gewichtung der einzelnen Kriterien mithilfe der eingebetteten Liste anpassen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Risikoregel-CI für Vulnerability Response v20.x




11. Klicken Sie auf **Absenden**.

## Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird

Wenn Sie keine Schwachstellenrechner verwenden, deaktivieren Sie den Standardrechner und alle anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die anfängliche Importleistung auswirken.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner**.
2. Öffnen Sie den entsprechenden Rechner.
3. Deaktivieren Sie die Checkbox **Aktiv**, um den Rechner zu deaktivieren.
4. Klicken Sie auf **Aktualisieren**.

## Erstellen, aktivieren oder ändern Sie Vulnerability Response Regeln für die automatische Löschung

Sie können die Löschregeln für das Löschen von angreifbaren Elementen (VI) und Korrekturaufgaben (RT) erstellen, aktivieren oder ändern. Verwenden Sie die automatische Löschung, um ältere Datensätze aus den VI- und RT-Tabellen zu entfernen.

### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rollen:

- admin: Ändern der Regeln für automatisches Löschen
- sn_vul.vulnerability_admin oder sn_vul.admin (veraltet): Modul zum automatischen Löschen anzeigen

### Warum und wann dieser Vorgang ausgeführt wird

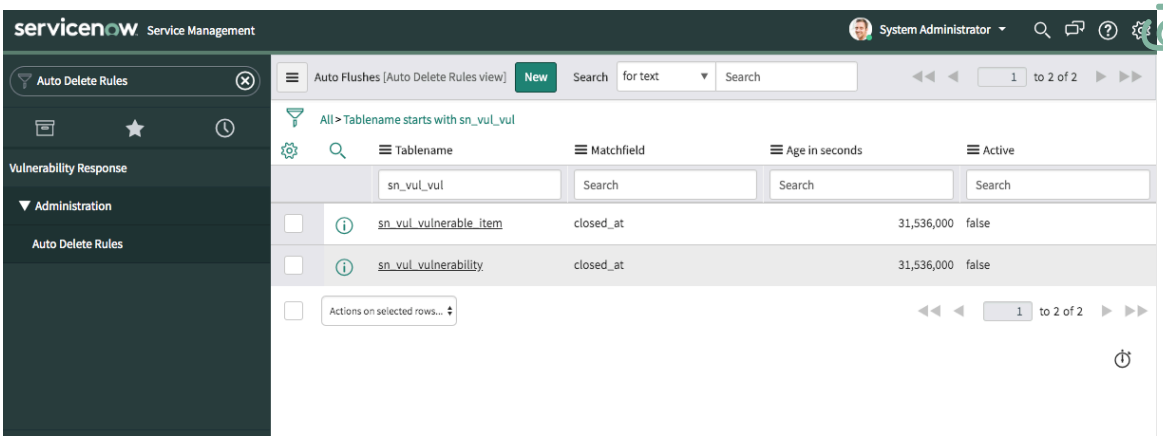
Im Laufe der Zeit sammelt sich wahrscheinlich eine große Menge geschlossener Datensätze in den Tabellen „VI“ und „VUL“ in Ihrer Instanz an. Viele dieser Datensätze waren möglicherweise länger als 365 Tage geschlossen, wurden jedoch nicht entfernt. Verwenden Sie Regeln für das automatische Löschen, um viele dieser älteren, geschlossenen Datensätze zu entfernen. Durch das Entfernen dieser Datensätze wird nicht nur die Anzahl der Datensätze in den Tabellen „VI“ und „VUL“ erheblich reduziert, durch das Löschen dieser Datensätze wird auch die hohe Leistung aufrechterhalten.

Obwohl das automatische Löschen von Zieldatensätzen standardmäßig 365 Tage lang geschlossen wurde, kann die allererste Ausführung versuchen, zu viele Datensätze in einer einzelnen Transaktion zu löschen. Abhängig von der Größe Ihrer Umgebung ziehen Sie es möglicherweise vor, den Löschvorgang zu staffeln, um den Umfang der Abfrage zu begrenzen. Sie können beispielsweise Ihre erste Ausführung für geschlossene Datensätze starten, die älter als 450 Tage sind. Nach Abschluss dieser Ausführung können Sie sich in kleineren Schritten (425, 400, 375) nach unten arbeiten, bis Sie die Anzahl der Datensätze reduziert haben, die älter als 365 Tage sind.

Mit Now Platform® werden zwei Regeln bereitgestellt, die geschlossene Datensätze, die bestimmte Bedingungen erfüllen, zusammen mit allen darauf verweisenden Datensätzen automatisch löschen. Eine Regel löscht angreifbare Elemente und die andere Regel löscht Korrekturaufgaben. Standardmäßig sind diese Regeln für das automatische Löschen deaktiviert, sodass Sie sie vor dem Löschen von Datensätzen manuell aktivieren müssen. Sie können die beiden vorkonfigurierten Regeln auswählen, die mit Ihrer Instanz bereitgestellt werden, oder eigene erstellen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für das automatische Löschen**.
   Die Listenansicht wird angezeigt.




2. Wählen Sie zum Bearbeiten die Löschregel für angreifbare Elemente (sn_vul_vulnerable_item) oder die Regel für Korrekturaufgaben (sn_vul_vulnerability) aus.

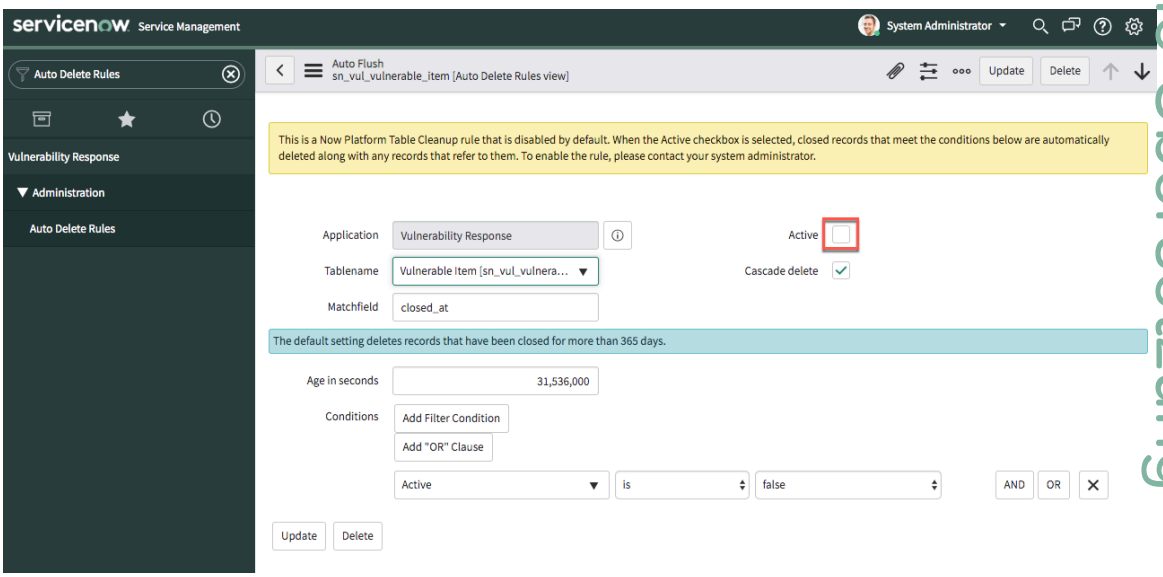
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie zum Erstellen einer neuen Regel auf **Neu**.
4. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie nach Bedarf.

| Feld | Beschreibung |
|---|---|
| Anwendung | Name der Anwendung, in der Datensätze gelöscht werden. Der Standardwert ist Vulnerability Response. |
| Tabellenname | Name der Tabelle, für die die Regel angewendet wird. |
| Feld abgleichen | Feld, für das das System die Dauer überwacht. |
| Aktiv | Option zum Aktivieren der Regel. Nach der Aktivierung kann der Datensatz gelöscht werden. |
| Löschung kaskadieren | Option zum Löschen aller übereinstimmenden Datensätze sowie aller darauf verweisenden Datensätze. Wenn diese Option nicht ausgewählt ist, werden nur übereinstimmende Datensätze gelöscht, nicht jedoch die Datensätze, die auf sie verweisen. |
| Alter in Sekunden | Alter des zu löschenden Schwachstellendatensatzes. Sowohl für VI- als auch für RT-Regeln beträgt das Alter 365 Tage. Dieses Alter wird in Sekunden angezeigt. |
| Bedingungen | Filterbedingungen, die die Datensätze in den Tabellen VI und RT (VUL) definieren, für die die Regeln gelten. |

5. Aktivieren Sie die Checkbox **Aktiv**, um eine Regel zu aktivieren.




Sobald die Regel aktiviert ist, löscht die stündliche Plattformfunktion **Auto Flush**die Datensätze aus der Tabelle, für die die Regel aktiviert ist.

Wenn Ihre Umgebung Millionen oder mehrere zehn Millionen Datensätze aufweist, die Ihren Löschkriterien entsprechen, sollten Sie sich an den Kundensupport von ServiceNow wenden, bevor Sie die Regeln für die automatische Löschung aktivieren, um Datensätze in einem schrittweisen Prozess zu löschen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie der Vulnerability Response-Homepage Diagramme zur Bedeutung von Schwachstellen hinzu

Sie können der Übersicht Diagramme zur Definition von Schwachstellenbedeutung und andere Visualisierungen hinzufügen.

#### Vorbereitungen

- Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.
- Das Plugin „Vulnerability Analytics“ muss aktiviert sein.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Übersicht**.
   Einige Berichte werden dem Dashboard standardmäßig hinzugefügt. Weitere Informationen zu diesen Berichten finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.
2. Klicken Sie in der Nähe des Dashboard-Headers auf das Kartenansichtssymbol und das + **Inhalt** hinzufügen, um das Dialogfeld zum Hinzufügen weiterer Widgets zu öffnen.
3. Wählen Sie in den Listen im Dialogfeld „ **Widgets** hinzufügen“ die Option Berichte aus, um weitere Vulnerability Response**Berichte** anzuzeigen.
4. Klicken Sie auf die Stelle auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie das Feld **Inhalt** hinzufügen.

### Definieren Sie Vulnerability Response E-Mail-Benachrichtigungen

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen zu wichtigen Updates und Aktivitäten wie Genehmigung und Ablehnung von falsch positiven Anforderungenzu teilen. Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie empfängt und was sie enthält.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

   Ausführliche Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

#### Ergebnisse

Wenn ein Empfänger ab v21.0 von Vulnerability Response auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Links werden in Vulnerability Manager Workspace für die Benutzer mit den Rollen sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager oder sn_vul_container.vulnerability_admingeöffnet.
- Links werden in IT Remediation Workspace für die Benutzer mit den Rollen sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owneroder sn_vul.app_developer geöffnet.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Benutzeroberfläche geöffnet.

### Definieren Sie E-Mail-Vorlagen für Vulnerability Response

Beim Erstellen einer E-Mail-Benachrichtigung müssen Sie angeben, wann sie gesendet werden soll, wer sie empfängt und was sie enthält.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **E-Mail-Vorlagen**.
2. Wählen Sie **Neu**.

Ausführliche Anweisungen zum Erstellen von E-Mail-Vorlagen finden Sie unter Construct an email message with a template .

### Erstellen oder bearbeiten Sie Benachrichtigungen für Korrekturziele

Schwachstellenadministratoren können die Benachrichtigung über das Korrekturziel bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welcher Inhalt in der Benachrichtigung enthalten sein soll.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels aus, oder wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

#### Ergebnisse
Wenn ein Empfänger ab v21.0 von Vulnerability Response auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Links werden in Vulnerability Manager Workspace für die Benutzer mit den Rollen sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager oder sn_vul_container.vulnerability_admingeöffnet.
- Links werden in IT Remediation Workspace für die Benutzer mit den Rollen sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner, oder sn_vul.app_developer geöffnet.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Benutzeroberfläche geöffnet.

### Konfigurieren Sie die Risikobewertung

Um das Zero-Day-Gefahren (aktueller Tag) Ihrer Assets durch angreifbare Software mit der Anwendung „Risikobewertung“ zu bewerten, stellen Sie zunächst sicher, dass die Anwendung ITSM Software Asset Management installiert ist.

Mit der Rolle „Schwachstellenschreiber“ (sn_vulnerability_write) können Sie das Modul „Risikobewertung“ anzeigen und bei Bedarf Risikobewertungsdatensätze für angreifbare Software in Ihrer Instanz mit der Anwendung Vulnerability Response erstellen und bearbeiten.

## Kompatibilität und Systemanforderungen

Die Anwendung Vulnerability Response ist auf der ServiceNow Storeverfügbar. Die Anwendung ITSM Software Asset Management (com.snc.asset_management) ist für das Risikobewertungsmodul erforderlich. Diese Anwendung verwaltet alle Ihre Assets und Softwarelizenzen, und die Version SAM Foundation dieser Anwendung ist Teil der Anwendung Vulnerability Response, die Sie aus dem ServiceNow Storeherunterladen. Die Anwendung „Risikobewertung“ funktioniert entweder mit den Anwendungen SAM Foundation oder SAM Pro Now Platform®.

Die Anwendung SAM Pro ist nicht Teil des Kernprodukts Vulnerability Response von ServiceNow Store und erfordert ein separates Abonnement.

Um sicherzustellen, dass die Anwendung SAM Foundation in Ihrer Instanz installiert ist, navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach com.snc.asset_management. Wenn die Anwendung nicht installiert ist, klicken Sie auf **Installieren**.

Da die Anwendung „Risikobewertung“ Zugriff auf die Asset-Daten in Ihrer Instanz Now Platform® erfordert, müssen die Asset-Verwaltungsanwendungen über Daten verfügen, auf die verwiesen werden kann. Die Tabelle „Software-Discovery-Modelle“ (cmdb_sam_sw_discovery_model) und die Softwareinstallationen (cmdb_sam_sw_install) erfordern Daten.

**Zugehörige Informationen**

Bewerten Sie Ihre Gefährdung durch angreifbare Software

### Konfigurieren Sie Exception Management für Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie behoben werden kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Begrenzen Sie die Dauer einer angeforderten Ausnahme und fügen Sie der Ausnahme oder falsch positiven Anforderung mithilfe des Moduls Vulnerability Response einen Fragebogen hinzu. Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Vulnerability Response angefordert. Sie können eine Ausnahme auch mit der GRC: Policy and Compliance Management -Integration anfordern.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.manage_exception_configuration

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Policy and Compliance Management installiert ist, GRC: Policy and Compliance Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Policy and Control-Ziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird dieser an die Person gesendet, die die Ausnahme oder falsch positive Anforderung auslöst. Sie können entweder den Standardfragebogen verwenden oder einen Fragebogen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste **Ausnahmen** verwalten mit auswählen.
   Sie können entweder Vulnerability Response oder GRC: Policy and Compliance Managementauswählen. Sie müssen das Plugin [ GRC aktivieren, um GRC: Policy and Compliance Management zum Anfordern einer Ausnahme zu verwenden. Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.
3. Wenn Sie die Option Vulnerability Response ausgewählt haben, geben Sie die folgenden Informationen ein:

**Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

| Feld | Beschreibung |
|---|---|
| Dauer | Zeitraum, für den eine Ausnahme angefordert werden kann. |
| Einheit | Zeiteinheit für den angegebenen Zeitraum. |
| Fragebogen aktivieren, um Ausnahme anzufordern | Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung. |
| Fragebogen, um Ausnahme anzufordern | Zeigt den Fragebogen an, den Sie ausgewählt haben, um eine Ausnahme anzufordern. Der **Ausnahmefragebogen** wird standardmäßig angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme** aktivieren aktivieren. |
| Fragebogen für Ausgleichskontrolle | Zeigt den Fragebogen an, den ein Korrekturbesitzer für Risikominderungsanforderungen beantworten muss. Ab v20.0 von Vulnerability Responsekönnen Sie Fragebögen für Risikominderungsanforderungen festlegen. Der **Fragebogen zur Vergütungskontrolle** ist standardmäßig ausgewählt.<br>**Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme** aktivieren aktivieren. |
| Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |
| Fragebogen, um falsch positive Meldung zu markieren | Zeigt den von Ihnen ausgewählten Fragebogen an, der als falsch positiv markiert werden soll. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt.<br>**Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Fragebogen zum Markieren von Falschmeldungen** aktivieren aktiviert ist. |

Wenn Sie den vorhandenen Fragebogen angepasst haben und ein Upgrade auf v20.0 durchführen, wird dieser benutzerdefinierte Fragebogen für die Anforderung zur Risikominderung anstelle des standardmäßigen **Fragebogens zur Ausgleichskontrolle**angezeigt.

4. Wenn Sie die Option GRC: Policy and Compliance Management ausgewählt haben, geben Sie die folgenden Informationen ein:

**Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

| Feld | Beschreibung |
| --- | --- |
| Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |
| Fragebogen, um falsch positive Meldung zu markieren | Zeigt den von Ihnen ausgewählten Fragebogen an, der als falsch positiv markiert werden soll. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. So konfigurieren Sie Fragebögen basierend auf Bedingungen für Ausnahme- und falsch positive Anforderungen:

   a. Wählen Sie im Abschnitt VR-Fragebogenkonfiguration die Option **Neu**aus.

   b. Füllen Sie im Formular „Fragebogenkonfiguration – Neuer Datensatz“ die Felder aus, und wählen Sie **Absenden**.
   Weitere Informationen zu den Feldern im Formular „Fragebogenkonfiguration“ finden Sie unter Felder des Formulars „Fragebogenkonfiguration“..
   Der erstellte Fragebogen wird im Abschnitt „VR-Fragebogenkonfiguration“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ angezeigt.

   Wenn Sie beispielsweise einen Fragebogen für falsch positive Anforderungen für kritische angreifbare Elemente konfigurieren möchten, wählen Sie die Genehmigungsregel „ **Falsch positive Ergebnisse für angreifbare Elemente** “ aus, geben Sie die Bedingung „ Risikobewertung ist 1 – Kritisch “ an, und wählen Sie den gewünschten Fragebogen im Formular „ Fragebogenkonfiguration “ aus .

6. Wählen Sie **Speichern**.

### Fügen Sie einen Ausnahmegenehmiger hinzu

Fügen Sie den Genehmigergruppen Benutzer hinzu, damit Sie eine Ausnahme anfordern können.

#### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

BisVulnerability Response v14.0 wurde eine Ausnahmeanforderung [] für ein angreifbares Element oder eine Korrekturaufgabe mit dem standardmäßigen zweistufigen Genehmigungsworkflow genehmigt. Die Anforderung muss von zwei Genehmigerebenen genehmigt werden.

**Hinweis:**
Bis Vulnerability Response v14.0 kann keine Ausnahme angefordert werden, wenn es keinen Genehmiger der ersten Ebene gibt. Wenn Sie jedoch ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmeverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

#### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.
2. Suchen Sie in der Spalte Name nach **Ausnahme**und klicken Sie auf **Ausnahmegenehmiger - Ebene 1**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Vulnerability Response v12.8.1 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie *sn_vul.exception_approver_L1*, *sn_vul.exception_approver_L2*oder *sn_vul.false_positive_approver_group*, um den Eigenschaftswert zu ändern.

3. Klicken Sie im Formular „Gruppenausnahmegenehmiger – Ebene 1“ auf die zugehörige Liste „Gruppenmitglieder“.
4. Klicken Sie auf **Neu**, um eine Liste zu erstellen.
5. Füllen Sie die Felder des Formulars aus.

**Benutzerformular**

| Feld | Beschreibung |
|---|---|
| Anwender-ID | Eindeutiger Bezeichner für den Benutzer |
| Vorname | Vorname des Benutzers. |
| Nachname | Nachname des Benutzers. |
| Titel | Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus. |
| Abteilung | Abteilung des Benutzers. |
| Passwort | Dem Benutzer zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder temporär sein. |
| Passwort muss zurückgesetzt werden | Option, mit der Benutzer das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten. |
| Gesperrt | Option, um den Benutzer für die Instanz zu sperren und alle aktiven Sitzungen des Benutzers zu beenden. Das System verhindert, dass Benutzer mit der Administratorrolle sich selbst aussperren. |
| Aktiv | Option zum Aktivieren dieses Benutzers. Nur Sie können einen inaktiven Benutzer in diesen Bereichen sehen:<br>○ Listen der Benutzer<br>○ Auswahlliste für Referenzfelder (Lupensymbol)<br>○ Autovervollständigen-Liste, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben |
| Nur Webservice-Zugang | Option, um diesen Benutzer als nicht interaktiven Benutzer festzulegen. |
| Interner Integrationsbenutzer | Option zum Festlegen dieses Benutzers als internen Integrationsbenutzer. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| E-Mail | E-Mail-Adresse des Benutzers. |
| Sprache | Bevorzugte Sprache des Benutzers. |
| Kalenderintegration | Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook. |
| Zeitzone | Zeitzone für den Standort dieses Benutzers. |
| Datumsformat | Bevorzugtes Datumsformat des Benutzers. |
| Telefon (geschäftlich) | Geschäftliche Telefonnummer des Anwenders. |
| Mobiltelefon | Mobiltelefon des Benutzers. |
| Foto | Foto, das Sie hochladen können, indem Sie **auf Hinzufügen klicken... klicken**. |

6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 1 bis 5, um einen Ausnahmegenehmiger – Ebene 2 zu erstellen.
   Der Genehmiger muss zu **Vulnerability Response** > **Meine Genehmigungen** navigieren und Anforderungen genehmigen.

**Hinweis:**
Informationen zum Genehmigen einer Ausnahme für GRC: Policy and Compliance Managementfinden Sie unter Optionales Setup für Policy and Compliance Management .

### Konfigurieren Sie Genehmigungsregeln für Exception Management

Verwenden Sie ab Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Meldungen zu genehmigen. Wenn Sie Vulnerability Response (VR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption workflow.
Wenn Sie Vulnerability Response v15.0 oder höher bereitgestellt haben, wird der Wert der Systemeigenschaft *sn_vul.flow_designer_activation* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Vulnerability Response bereits vor v15.0 verwenden, wird der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

**Hinweis:**
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Elemente
- Ausnahmeregel
- Falsch positive Werte für Korrekturaufgaben
- Falsch positiv für angreifbare Elemente

**Hinweis:**
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Weitere Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Tabelle | Tabelle, auf die die Regel angewendet wird. |
| Anwendung | Der Standardwert ist Vulnerability Response. |
| Regeltyp | Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, Falschmeldungen oder Ausnahmeregel. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungsregeln. |
| Ablaufdatum der Genehmigung (Tage)<br>Ab v21.0 von Vulnerability Response | Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann. |
| Genehmiger benachrichtigen (Tage)<br>Ab v21.0 von Vulnerability Response | Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen. |

4. Wählen Sie **Aktualisieren**.
Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

**Hinweis:**
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Example:**
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden wurden.

### Erstellen Sie Konfigurationen für eine Genehmigungsregel

Definieren Sie die Bedingungen, um übereinstimmende angreifbare Elemente, Korrekturaufgaben oder Ausnahmeregeln für eine Genehmigungsebene herauszufiltern.

## Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

## Warum und wann dieser Vorgang ausgeführt wird
Im Modul „Genehmigungskonfigurationen“ können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

**Hinweis:**
Verwenden Sie das Modul „Genehmigungsregeln“, um Genehmigungsregeln für die Ausnahmeverwaltungs-Workflows zu konfigurieren. Weitere Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie die Felder des Formulars aus.

### Formular „Genehmigungskonfiguration“

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. |
| Bestellung | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungskonfigurationsebenen. |
| Bedingung | Identifiziert die übereinstimmenden angreifbaren Elemente oder Korrekturaufgaben. |

5. Wählen Sie **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Bedingungen mit mehreren Genehmigungsebenen innerhalb einer Regel definieren. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Weitere Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management.

**Example:**
Sie können verschiedene Genehmigungspfade für verschiedene Arten von Schwachstellen oder Konfigurationselementen (mit Internetverbindung oder intern) definieren.

### Erstellen Sie Genehmigungsebenen für Exception Management

Definieren Sie die Ebenen der Benutzer und Benutzergruppen, die die Ausnahmeanforderungen genehmigen.

**Vorbereitungen**
Erforderliche Rolle: sn_vul.vulnerability_admin

**Prozedur**

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Wählen Sie im Abschnitt Genehmigerebenen eine Genehmigerebene aus.
5. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigerebene“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungsebene. |
| Erforderliche Genehmigung | Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind:<br>○ Ein Genehmiger erforderlich<br>○ Alle Anwender müssen genehmigen |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird. |
| Bestellung | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. |
| Genehmigungskonfiguration | Enthält die Genehmigungskonfigurationen |
| Zuweisen mit | Wählen Sie eine Option aus:<br>○ Anwender und Anwendergruppe<br>○ Genehmigungstabellenfeld<br>○ Skript |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Gruppen | Genehmigerebenengruppe, die aus mehreren Benutzern besteht. Der Benutzer muss eine der folgenden Rollen haben:<br>○ sn_vul.exception_approver: Für Ausnahmemanagement und Ausnahmeregeln<br>○ sn_vul.false_positive_approver: Für falsch positive Ergebnisse |
| Anwender | Bearbeiten Sie die in den Gruppen aufgeführten Benutzer. |

6. Um die Änderungen zu speichern, wählen Sie **Aktualisieren**.

**Hinweis:**
Vor v15.0 funktionierte der Workflow-Prozess nur, wenn Benutzer nur auf Ausnahmeebene 1 vorhanden waren. Ab v15.0 muss jedoch mindestens ein Benutzer auf jeder Ebene vorhanden sein.

Vor v15.0 wurde im Workflow das angreifbare Element oder die angreifbare Gruppe zurückgestellt, wenn kein Benutzer auf der zweiten Ebene vorhanden war. Wenn jedoch ab v15.0 kein Benutzer auf der zweiten Ebene vorhanden ist, wird die Genehmigungsanforderung automatisch abgelehnt.

**Example:**
Es kann unterschiedliche Genehmigungsebenen für Schwachstellen für Linux- und Windows-Server geben.

### Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer

Wenn Sie ab Vulnerability Response v15.0 Vulnerability Response (VR) zum ersten Mal bereitstellen, ist der Flow Designer für die Genehmigung von Ausnahmeanforderungen in der Ausnahmenverwaltung standardmäßig aktiviert. Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption workflow.

**Hinweis:**
Ab Vulnerability Response v19.0 wird nur Flow Designer für Neukunden unterstützt. Wenn Sie bereits Benutzer sind und ein Upgrade auf Vulnerability Response v19.0 durchführen, werden sowohl Flow Designer als auch der Ausnahmeverwaltungs-Workflow unterstützt.

### Workflow und Flow Designer im Vergleich

| Überlegungen | Workflow | Flow Designer |
|---|---|---|
| Version | Vor Version 15.0 von Vulnerability Response. | Ab Version 15.0 von Vulnerability Response. |
| Standardoption | Standardoption, wenn Sie bereits VR-Benutzer sind. | Standardoption für neue VR-Benutzer ab v15.0. |
| Festlegen des Genehmigungsprozesses | Die Ausnahmeverwaltung umfasst Ausnahme- und falsch positive Anforderungen sowie Ausnahmeregeln. | Beinhaltet die Definition verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow und Flow Designer im Vergleich (Fortsetzung)**

| Überlegungen | Workflow | Flow Designer |
|---|---|---|
| | | Die Ausnahmeverwaltung umfasst Ausnahme- und falsch positive Anforderungen sowie Ausnahmeregeln. |
| Upgrade auf Flow Designer | Sie können ein Upgrade von Workflow auf Flow Designer durchführen. Bestehende Anforderungen können jedoch nur mit dem Workflow genehmigt werden. | Flow Designer ist standardmäßig aktiviert. |
| Systemeigenschaft `sn_vul.flow_designer_activation` | Wenn Sie den Workflow für die Ausnahmeverwaltung vor v15.0 verwendet haben, ist die Systemeigenschaft auf „false“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „true“ fest.<br>**Hinweis:** Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. | Wenn Sie VR zum ersten Mal für v15.0 oder höher verwenden, wird der Wert der Systemeigenschaft standardmäßig auf „true“ festgelegt. |
| Modul „Genehmigungsregeln“ | Nach dem Festlegen der Systemeigenschaft auf „true“ wird die geplante Aufgabe „ **Modulfreigaberegeln aktivieren** “ innerhalb von 24 Stunden ausgeführt. Diese regelmäßige Aufgabe aktiviert das Modul „ **Genehmigungsregeln** “. Um dieses Modul sofort zu aktivieren, führen Sie diese Aufgabe manuell aus. | Wenn Sie VR zum ersten Mal aus VR v15.0 bereitgestellt haben, ist dieses Modul standardmäßig verfügbar. |
| Genehmigungsebenen | Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen. | Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel. |

### Fügen Sie einen falsch positiven Genehmiger hinzu

Nur Benutzer, die der Falschmeldungs-Genehmigergruppe hinzugefügt wurden, können Falschmeldungen für angreifbare Elemente (AEs) und Korrekturaufgaben (VULs) genehmigen. Das Gewähren eines falsch positiven Ergebnisses ist ein einstufiger Genehmigungsprozess.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Hinweis:**

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Navigieren zu **Alle** > > **Benutzeradministration** > **Gruppen**.
2. Suchen Sie in der Spalte **Name** nach **False Positive**, und klicken Sie auf die Option.
3. Navigieren Sie im Gruppenformular zu **Gruppenmitglieder** > **Neu** (oder **Bearbeiten**).
4. Erstellen Sie im Benutzerformular einen Datensatz, indem Sie die Benutzerdetails eingeben, und klicken Sie auf **Absenden**.
   Alle Rollen werden dem Benutzer gewährt. Die ausgewählten Benutzer werden der Liste Gruppenmitglieder hinzugefügt. Diese Mitglieder können Anforderungen genehmigen, um VIs oder Korrekturaufgaben als falsch positiv zu kennzeichnen. Nach der Genehmigung wird der Status des Datensatzes auf „Geschlossen“ gesetzt und erst am angegebenen Datum erneut geöffnet.

## Konfigurieren Sie einen Fragebogen für die Risikominderung

Ab Vulnerability Response v20.0 können Sie den Fragebogen der Risikominderungsanfrage für eine Reihe von gefilterten angreifbaren Elementen oder Korrekturaufgaben anpassen.

### Vorbereitungen

Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird

Der **Fragebogen für Ausgleichskontrollen für angreifbare Elemente** und **der Fragebogen für Ausgleichskontrollen für Genehmigungsregeln für angreifbare Gruppen** sind im Lieferumfang des Basissystems enthalten.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Aktivieren Sie im Formular „Einstellungen für VR-Ausnahmeverwaltung“ das Kontrollkästchen Fragebogen zum Anfordern einer Ausnahme aktivieren.
3. So konfigurieren Sie Fragebögen basierend auf Bedingungen für Risikominderungsanforderungen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie im Abschnitt VR-Fragebogenkonfiguration die Option **Neu**aus.

b. Wählen Sie im Formular „Fragebogenkonfiguration – Neuer Datensatz“ die Genehmigungsregel **Fragebogen für Ausgleichskontrollen für angreifbare Gruppen** oder **Fragebogen für Ausgleichskontrollen für angreifbare Elemente aus**, und geben Sie die Bedingung an.

c. Wählen Sie den gewünschten Fragebogen aus, und klicken Sie **auf Absenden**.
Weitere Informationen zu den Feldern im Formular „Fragebogenkonfiguration“ finden Sie unter Felder des Formulars „Fragebogenkonfiguration“..
Der erstellte Fragebogen wird im Abschnitt „VR-Fragebogenkonfiguration“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ angezeigt.

4. Wählen Sie im Formular Einstellungen für VR-Ausnahmeverwaltung die Option **Speichern** aus.

### Zeigen Sie Vulnerability Response-SLAs für Korrekturaufgaben an

Um sicherzustellen, dass angreifbare Elemente korrekt verarbeitet werden, können Sie eine Servicelevel-Vereinbarung (Service Level Agreement, SLA) für Vulnerability Response Korrekturaufgaben definieren.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Die SLAs in dieser Liste sind eine Teilmenge der SLA-Liste der Plattform, die spezifisch für Vulnerability Responseist.

Detaillierte Anweisungen hierzu finden Sie unter Create an SLA definition .

Wenn Sie die Zeit nachverfolgen, die zur Korrektur von AEs benötigt wird, sollten Sie Vulnerability Response Korrekturzielregelnverwenden. Korrekturzielregeln definieren die erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente (VI), insbesondere im Kontext von Vulnerability Response, während SLAs einen Zeitrahmen für die Korrektur der Schwachstelle selbst bieten können.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **SLA-Definitionen**.
2. Klicken Sie auf eine Definition.
**Aufgaben-SLAs** werden in den zugehörigen Listen der **Korrekturaufgaben**angezeigt.

### Konfigurieren Sie Watchdog

Verwenden Sie die Watchdog-Konfigurationsseite, um neue Watchdogs zu erstellen oder vorhandene Watchdogs mit Bedingungen zu aktualisieren, die Sie angeben möchten. Sie können die Benachrichtigung für jeden Watchdog aktivieren und benachrichtigt werden, wenn die Bedingungen erfüllt sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **WatchDog** > **Konfiguration**.
2. Wählen Sie den Watchdog aus, den Sie implementieren möchten.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Watchdog-Integration“**

| Feld | Beschreibung |
|---|---|
| Name | Name des Watchdogs |
| Aktiv | Legen Sie die Checkbox auf `true` fest, um den Watchdog zu aktivieren. |
| Bedingungstyp | Wählen Sie zwischen Filter oder Skript. |
| Erweiterte Bedingung | Dieses Feld wird nur angezeigt, wenn Skript unter Bedingungstyp ausgewählt wird. |
| Tabelle | Wählen Sie die Tabelle aus, um die Watchdog-Bedingung auszuführen. |
| Bedingung | Bedingung für die Auswertung des Watchdogs. |
| Benachrichtigen | Checkbox, um die Gruppen oder Benutzer zu benachrichtigen, wenn die Watchdog-Bedingung erfüllt ist. |
| Anwender | Liste der Benutzer, die informiert werden sollen, wenn die Watchdog-Bedingung erfüllt ist. |
| Gruppen | Gruppe, die informiert werden soll, wenn die Watchdog-Bedingung erfüllt ist. |
| Überwachungsprotokoll | |
| Watchdog | Verweis auf die Watchdog-Tabelle. |
| Anzahl | Anzahl der Datensätze, die die Watchdog-Kriterien erfüllen. |
| Notizen | Zusätzliche Hinweise für die Watchdog-Protokolle. |

4. Wählen Sie **Aktualisieren**.

## Erweiterte Vulnerability Response Konfigurationsaufgaben

Die folgenden Setup-Aufgaben erfordern Codierung oder fortgeschrittene ServiceNow Kenntnisse und werden nicht als Teil der Basiskonfiguration betrachtet.

Möglicherweise möchten Sie diese Aufgaben nur ausführen, wenn Sie über fortgeschrittene Codierungserfahrung oder Expertenwissen über Now Platformverfügen.

### Erstellen Sie domänengetrennte Importe für eine Integration

Wenn sich importierte Daten in einer bestimmten Domäne befinden müssen, muss der Benutzer, der zum Ausführen der Integrationen zugewiesen ist, zu dieser Domäne gehören.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:
import_admin und die Integrationsrolle für Ihre spezifische Integration konfigurieren, z. B. sn_vul.configure_r7_integration oder sn_vul_tenable.configure_integration.

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Satz von Aufgaben erfordert Codierung oder fortgeschrittene ServiceNow.

Die Importwarteschlangen enthalten Datenanhänge, die von den geplanten Aufgaben (Integrationen) verarbeitet werden. In einer domänengetrennten Umgebung müssen Sie die geplante Aufgabe der richtigen Importwarteschlange zuordnen.

### Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede Domäne, die Sie erstellen, einen Benutzer, und weisen Sie den Benutzer dieser Domäne zu.

   Stellen Sie sich diesen Benutzer als **run_as-** Platzhalter für die Domäne in Ihrer Schwachstellenintegration vor. Er entspricht dem **VR.System-** Benutzer in der globalen Domäne. Dieser Benutzer benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   **Hinweis:**
   Verwenden Sie diesen Benutzer nicht für andere Zwecke.

3. Erstellen Sie eine geplante Aufgabe in jeder Domäne.
   Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für die Domänentrennung.

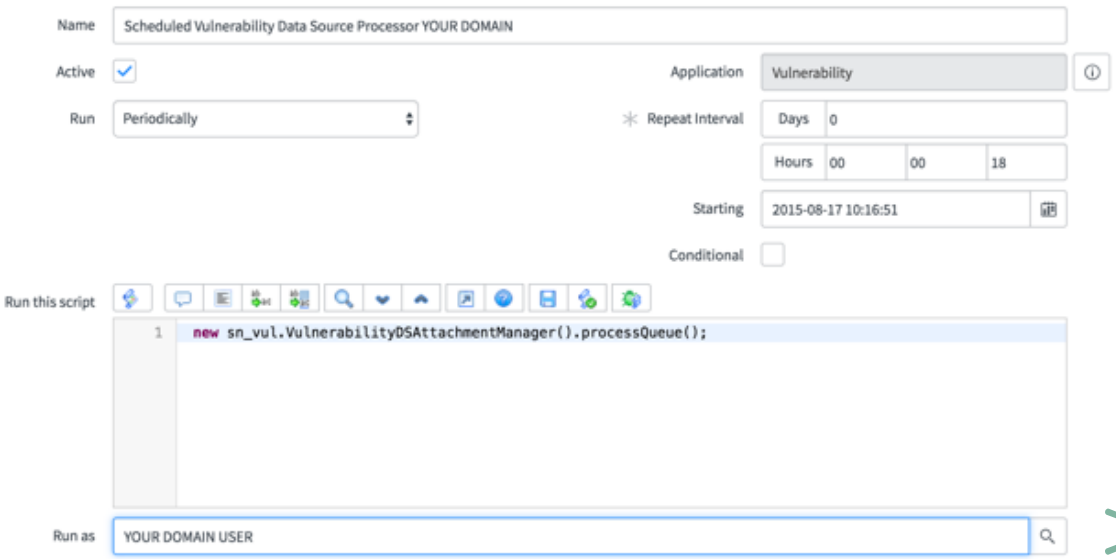
   a. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.

   b. Kopieren Sie den **geplanten Schwachstellen-Datenquellenprozessor** in die Domäne.

   c. Um die geplante Aufgabe zu identifizieren, hängen Sie die Domäne an den Namen an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Ändern Sie im Feld **Ausführen als** den Benutzer **run_as** in den Benutzer, den Sie in Schritt 2 erstellt haben.

Ab Version 20.1 von Vulnerability Responsewerden die folgenden Skriptänderungen mit dem Basissystem geliefert.

4. **Hinweis:**
   Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne **„run_as“ ausgeführt** wird.

Bearbeiten Sie die UI-Aktion **Jetzt** ausführen im **Integrationsauftrag Qualys Host Detection Integration** , um diesen Codeblock am Anfang der Datei hinzuzufügen.

**Example**

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. **Hinweis:**
   Bearbeiten Sie die folgenden Skripteinbindungen, sodass die Integration in der Benutzerdomäne **„run_as“ ausgeführt** wird.

Bearbeiten Sie die **VulnerabilityIntegrationUtils-Skripteinbindungsmethode addIntegrationRun**, um den hervorgehobenen Code hinzuzufügen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Bearbeiten Sie die **VulnerabilityIntegrationUtils-Skripteinbindungsmethode addProcessRun**, um den hervorgehobenen Code in der folgenden Abbildung hinzuzufügen.
addProcessRun-Code

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Bearbeiten Sie die **VulnerabilityIntegrationUtils-Skripteinbindungsmethode copyProcess**, um den hervorgehobenen Code in der folgenden Abbildung hinzuzufügen.
copyProcess-Code

Script

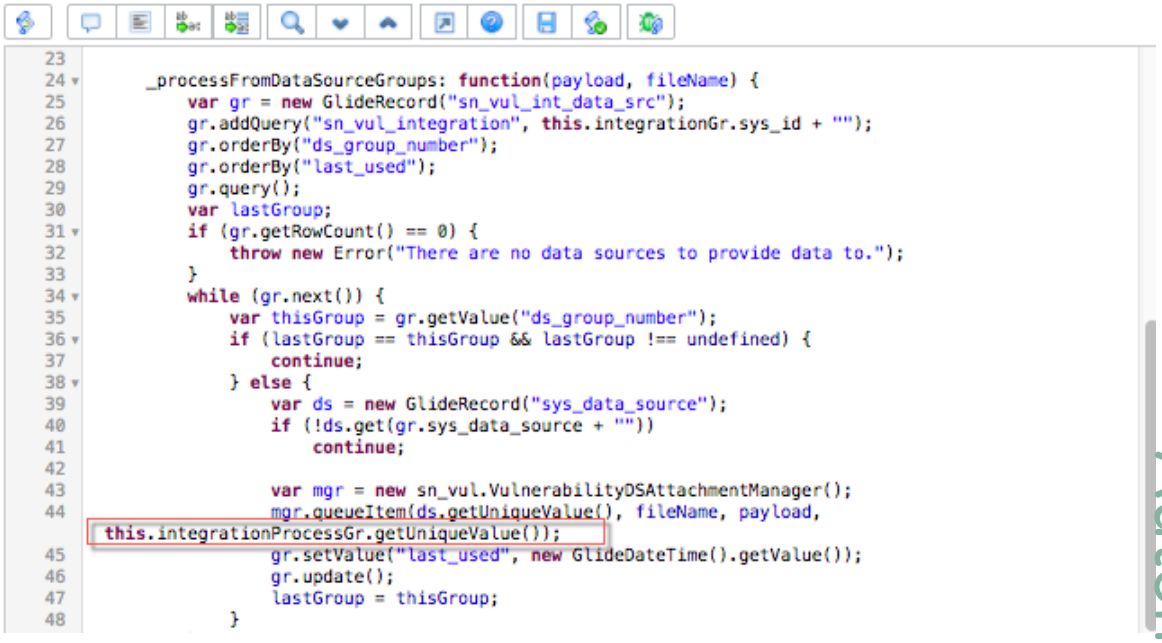
```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```

8. Bearbeiten Sie die **DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups**, um den folgenden ursprünglichen Code zu ändern:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

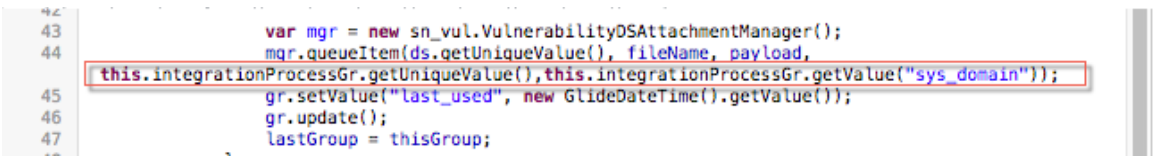
Ursprünglicher _processFromDataSourcesGroups-Code



```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

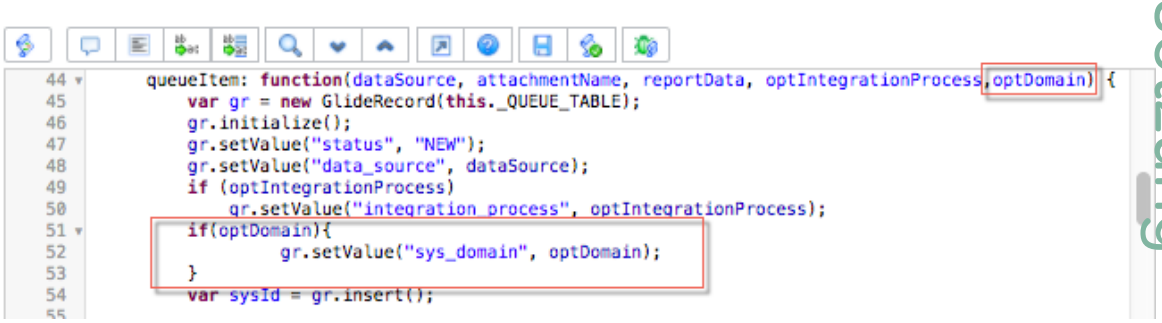
An:

_processFromDataSourcesGroups-Code bearbeitet



```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

9. Bearbeiten Sie die **VulnerabilityDSAttachmentManager-Skripteinbindungsmethode queueItem**, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen
queueItem



```
44      queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
45          var gr = new GlideRecord(this._QUEUE_TABLE);
46          gr.initialize();
47          gr.setValue("status", "NEW");
48          gr.setValue("data_source", dataSource);
49          if (optIntegrationProcess)
50              gr.setValue("integration_process", optIntegrationProcess);
51          if(optDomain){
52                  gr.setValue("sys_domain", optDomain);
53          }
54          var sysId = gr.insert();
```

_getNext

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
156     _getNext: function() {
157         // First go through the retries, if any
158         var gUser = new GlideRecord("sys_user");
159         gUser.get(gs.getUserID());
160         var sysDomainUser = gUser.getValue("sys_domain");
161         var gr = new GlideRecord(this._QUEUE_TABLE);
162         gr.addQuery("status", "RETRY");
163         gr.addQuery("sys_domain", sysDomainUser);
164         gr.orderBy("queued_on");
165         gr.query();
166         if (gr.next()) {
167             return gr;
168         }
169
170         // Then handle the regular queued items
171         gr = new GlideRecord(this._QUEUE_TABLE);
172         gr.addQuery("status", "QUEUED");
173         gr.orderBy("queued_on");
174         gr.addQuery("sys_domain", sysDomainUser);
175         gr.query();
176         if (gr.next()) {
177             return gr;
178         }
179
```

_processQueueEntry-Funktion

```
182     _processQueueEntry: function(entry) {
183         var schedGrId = this._getScheduledImportSet(entry.data_source);
184         if (gs.nil(schedGrId)) {
185             return;
186         }
187
188         var dataSourceGr = new GlideRecord("sys_data_source");
189         if (!dataSourceGr.get(entry.data_source)) {
190             gs.warn("Non existent data source - marking as complete");
191             entry.setValue("status", "COMPLETE");
192             entry.setValue("processing_notes", "Data source does not exist, could not process.");
193             entry.update();
194             return;
195         }
196
197         try {
198             this._deleteDataSourceAttachments(entry.data_source);
199             if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
200                 gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
201                 throw "Attachments not deleted";
202             }
203             var attachmentApi = new GlideSysAttachment();
204             attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
205             var schedGr = new GlideRecord("scheduled_import_set");
206             schedGr.get(schedGrId);
207             schedGr.setValue("data_source", entry.data_source);
208             schedGr.setValue("run_as", gs.getUserID());
209             schedGr.update();
```

An diesem Punkt sind Sie bereit für domänengetrennte Importe.

**Hinweis:**
Wenn Sie mehrere Bereitstellungen einer Vulnerability Response - oder Application Vulnerability Response -Integration haben, wiederholen Sie diesen Vorgang für jede Bereitstellung.

### Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge

Hintergrundaufträge in Vulnerability Response-Produkten sind so konzipiert, dass sie über einen längeren Zeitraum ausgeführt werden, um mehrere Prozesse für Ihre Datensätze auszuführen. Die Hintergrundauftragsprozessoren werden mit dem Basissystem geliefert, die über den Systembenutzer ausgeführt werden und Datensätze in der globalen Domäne erstellen.

**Vorbereitungen**
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**.
2. Erstellen Sie eine Domäne.

   Weitere Informationen zum Erstellen einer Domäne finden Sie unter Create a domain .

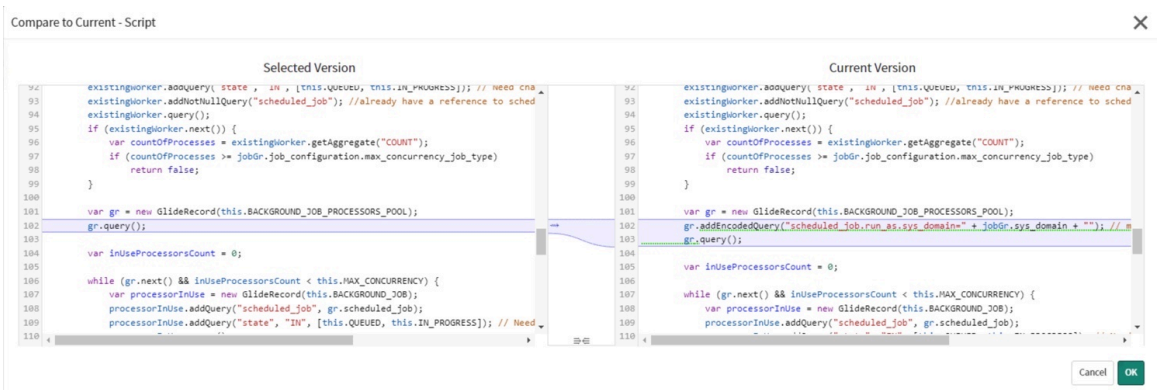
   Erstellen Sie für jede erstellte Domäne einen Benutzer, und weisen Sie den Benutzer der Domäne zu. Angenommen, dieser Benutzer ist ein run_as-Platzhalter für die Domäne. Dies entspricht dem VR.System-Benutzer in der globalen Domäne. Dieser Benutzer benötigt Zugriff auf Schwachstellendaten.
3. Ändern Sie run_as der geplanten Aufgaben *`Scheduled Background Job Manager`*und *`Close the parent background job`*.

   Wenn Sie mehrere Domänen erstellt haben, duplizieren Sie diese Aufgabe, und ändern Sie den Benutzer run_as entsprechend. Möglicherweise möchten Sie auch eine Kopie der vorherigen Jobs mit dem Benutzer „run_as“ der globalen Domäne in einem inaktiven Modus beibehalten.

   Im Lieferumfang des Basissystems sind zehn Prozessoraufträge (z. B. *`Background job processor 10`*) enthalten. Ändern Sie die Ausführung als dieser Aufträge in den domänengetrennten Benutzer. Wenn mehrere Domänen vorhanden sind, reichen zwei Jobs pro Domäne aus. Diese Jobs können jedoch bei Bedarf auch dupliziert werden. Behalten Sie zwei Prozessoraufträge mit dem Benutzer „run_as“ in der globalen Domäne bei.

   Ab Version 20.0 von Vulnerability Responsewerden die folgenden Skriptänderungen mit dem Basissystem geliefert.
4. Ändern Sie die Skripteinbindung *`BackgroundJobManager`*, und fügen Sie die folgende Zeile hinzu, wie in der folgenden Abbildung gezeigt.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```




**Hinweis:**
Lösen Sie die erneute Anwendung von Regeln aus der richtigen Domäne bei Bedarf aus.

### Erstellen Sie eine Vulnerability Response-CI-Suchregel

Das Modul **„CI-Suchregeln“** enthält Regeln, die verwendet werden, um den übereinstimmenden Datensatz für Hostinformationen zu finden, die während der Importe von Drittanbieter-Schwachstellenintegrationen empfangen wurden. Die Hostinformationen werden mit den erkannten Elementen, nicht abgeglichenen Konfigurationselementklassen und Configuration Management Database (CMDB)abgeglichen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird

Das Erstellen von CI-Suchregeln erfordert fortgeschrittene Kenntnisse von ServiceNow und Vulnerability Response. Anstatt eine der vorhandenen Suchregeln zu ändern, sollten Sie sie kopieren und die Kopie ändern. Wenn Sie zufrieden sind, dass die neue Regel das tut, was Sie wollen, deaktivieren Sie die ursprüngliche.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie, wenn Sie neue Regeln erstellen.

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „CI-Suchregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel. |
| Suchmethode | Für den Abgleich verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ **Skript**: Vorgefertigtes Skript (IP-Adresse, DNS-Name usw.) oder benutzerdefiniertes Skript.<br>○ **Feldabgleich**: Durchsuchen Sie die Tabelle oder das Feld in der CMDB. |
| Typ | Mit der **Skriptsuchmethode**verwendeter Typ. |
| Bestellung | Rangfolge für die Regel. Regeln mit der niedrigsten Reihenfolge werden zuerst ausgewertet. |
| Aktiv | Checkbox, ob die Regel aktiv oder deaktiviert ist. |
| Quelle | Quelle, die als Eingabe für diese Regel verwendet wird. |
| Quellenfeld | Quellfeld, das als Eingabe für diese Regel verwendet wird. Wählen Sie ein beliebiges Feld aus, es wird jedoch als -Zeichenfolgenwert behandelt. |
| Bedingung | Bedingung, auf deren Grundlage die CI-Suchregel angewendet wird. Diese Bedingung hängt vom Attribut des Drittanbieter-Scanners ab.<br>**Hinweis:**<br>Das Asset-Attribut ist Teil der Nutzlast. Sie wird vom Scanner einer Drittpartei empfangen. Beispiele für Nutzlasten finden Sie in der Tabelle „Erkannte Elemente“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Skript | Bearbeitbares Beispielskript, basierend auf dem **Typ**, wird angezeigt. Implementieren Sie das benutzerdefinierte Skript nach den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind.<br>**Hinweis:**<br>Die Prozessfunktion hat drei Parameter: `rule`, `sourceValue`und `sourcePayload`. |
| Tabelle durchsuchen | Tabelle, die in der CMDB durchsucht werden soll. Wird mit dem Feld verwendet, das der **Suchmethode**entspricht. |
| Feld durchsuchen | Feld, das Informationen enthält, die zum Suchen eines CI verwendet werden können. Wird mit der **Suchmethode**verwendet, die dem Feld entspricht. Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz befinden, z. B. ein Netzwerkadapter. |

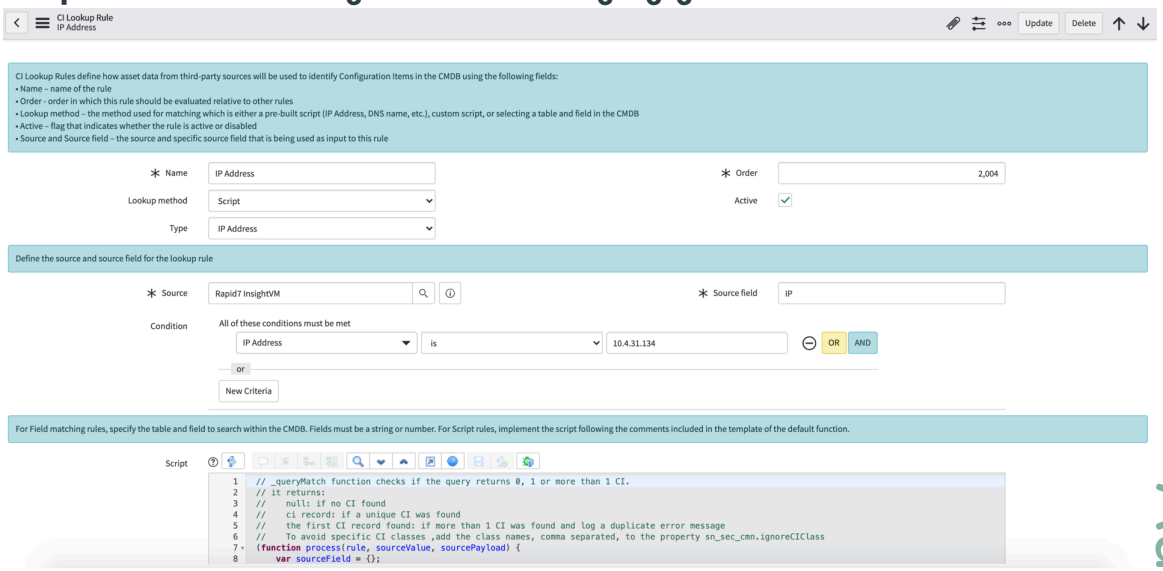
4. Klicken Sie auf **Absenden**.

Weitere Informationen zur Implementierung von CI-Suchregeln finden Sie unter, Schritte zum Verhindern doppelter oder verwaister Datensätze nach dem Ausführen von Vulnerability Response CI-Suchregeln.

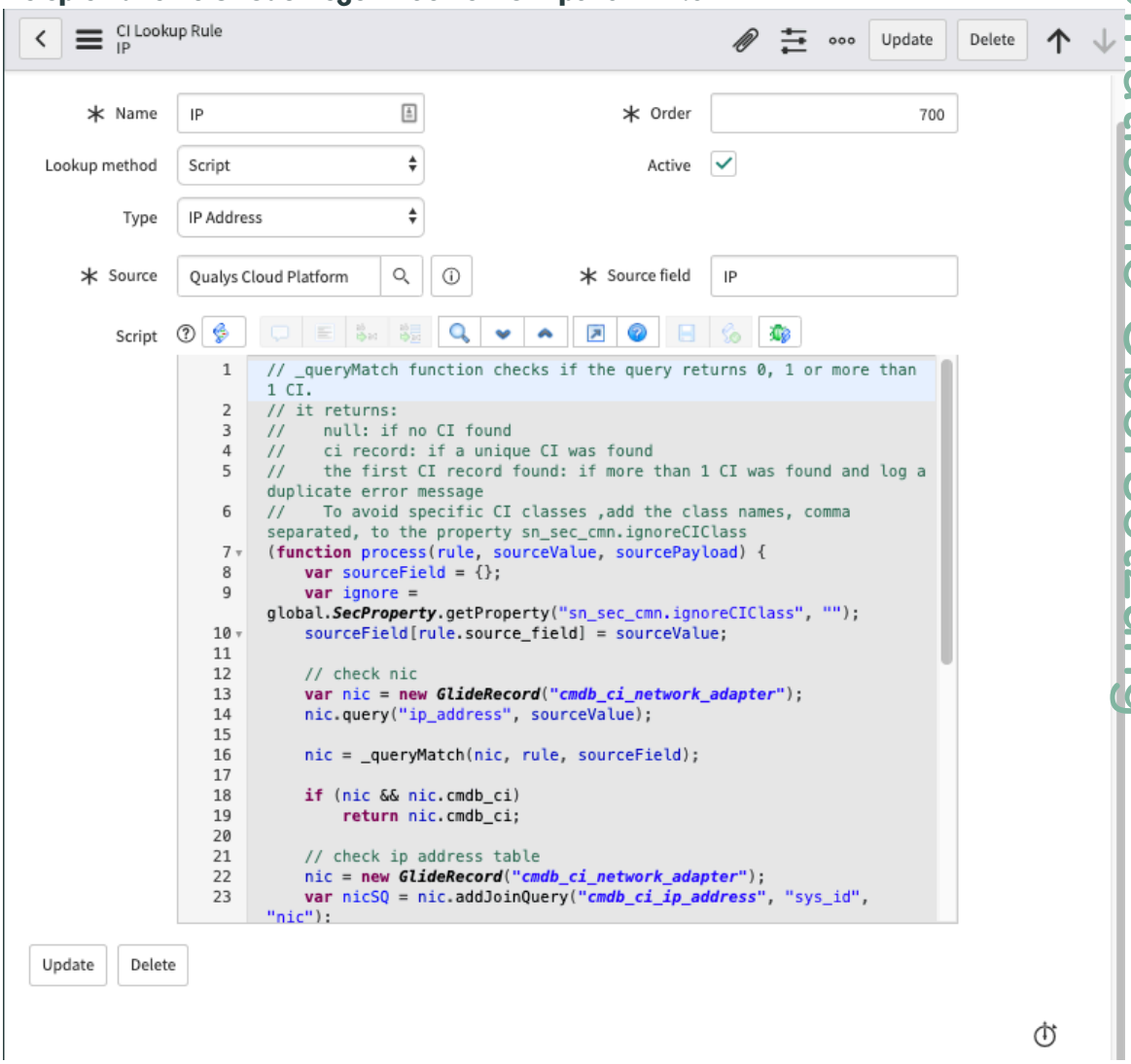


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Beispiel für eine CI-Suchregel mit einem Bedingungsgenerator für V12.0




## Beispiel für eine CI-Suchregel mit einem Skript vor V12.0




Automatische Übersetzung

### Zugehörige Informationen

Vulnerability Response Formularfelder für angreifbare Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### CI-Klassen ignorieren

Um beim Ausführen von CI-Suchregeln einige Configuration Item-Klassen (CI-Klassen) zu ignorieren, z. B. Load Balancer [cmdb_ci_lb], legen Sie die **Systemeigenschaft ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*] fest.

## Vorbereitungen

Erforderliche Rolle: admin

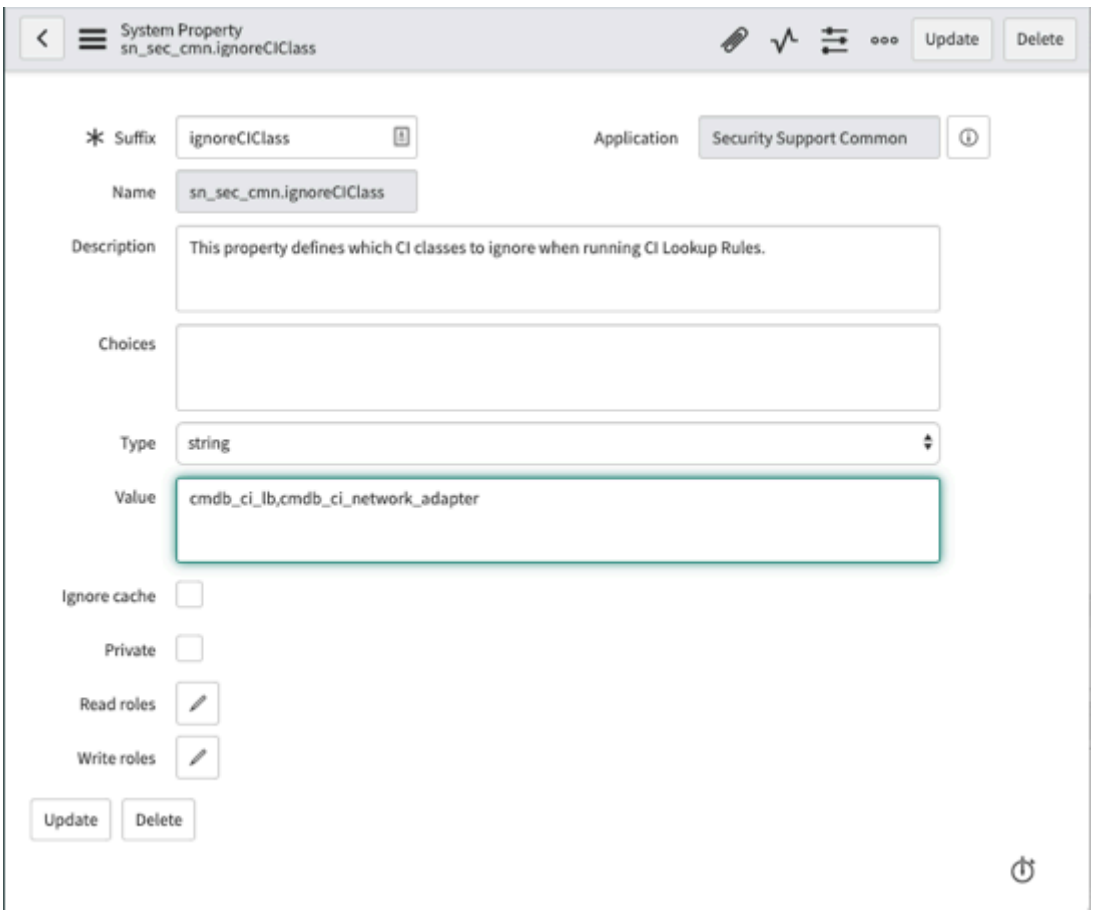
**Hinweis:**

Die **Systemeigenschaft ignoreCIClass** ist ab Vulnerability Response v9.0 verfügbar. Die Eigenschaftsfunktionalität ist jedoch nach einem Upgrade von einer früheren Version nicht verfügbar.

Wenn Sie ein Upgrade von einer Security Operations -Anwendung vor Version 9.0 durchgeführt haben, finden Sie unter KB0788209 Anweisungen zum Aktivieren dieser Funktionalität.

## Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Klicken Sie auf **Eingeben**.
3. Geben Sie im Menü **Suche** unter **Name**sn_sec_cmn.ignoreCIClassein.
4. Geben Sie im Textfeld **Wert** die CI-Klassen ein, die in einer durch Kommas getrennten Liste ausgeschlossen werden sollen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Diese Liste wird beim nächsten Import von CI-Suchregeln verwendet. Während des Imports erstellte angreifbare Elemente sind keinem CI eines Typs zugeordnet, der im Feld **Wert** der Systemeigenschaft sn_sec_cmn.ignoreCIClass aufgeführt ist.

### Filtern Sie stillgelegte CIs

Filtern Sie stillgelegte Konfigurationselemente (CIs), während Sie die CI-Suchregeln ausführen. Um stillgelegte CIs beim Ausführen der CMDB-CI-Suchregeln für Security Operations zu filtern, legen Sie die **Systemeigenschaft filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] auf „true“ fest.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Der Standardwert der Systemeigenschaft ist true. Diese Eigenschaft gilt nur für CI-Suchregeln in Vulnerability Response und hat keine Auswirkungen auf die IRE-Suchlogik.

#### Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Wählen Sie die **Eingabetaste**.
3. Geben Sie im Menü **Suche** unter **Name**sn_sec_cmn.filterOutDecommissionedCI ein, um die außer Betrieb genommenen CIs zu filtern.
4. **Geben Sie** im Textfeld Wert den Wert true oder false ein.
   Der Standardwert ist „true“.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird beim nächsten Import von den CI-Suchregeln verwendet. Die Systemeigenschaft sn_sec_cmn.filterOutDecommissionedCI filtert die außer Betrieb genommenen CIs heraus, während diese Suchregeln ausgeführt werden.

### CIs automatisch heraufstufen

Bearbeiten Sie die JSON-Zeichenfolge in der **Systemeigenschaft autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**], sodass Ihre Konfigurationselement-Suchregeln (Configuration Item, CI) alle CMDB-CIs von Security Operations automatisch zu übereinstimmenden Einträgen in der Tabelle [cmdb_ci] heraufstufen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Der Systemeigenschaftstyp ist „string“ und erfordert die Eingabe einer JSON-Zeichenfolge. Diese Eigenschaft ist standardmäßig aktiviert und stuft übereinstimmende CIs beim Ausführen der CI-Suchregeln herauf.

Benutzerdefinierte Suchskripts geben möglicherweise untergeordnete Tabellendatensätze aus dem Skript zurück. Für diese Eigenschaft übernimmt die Funktion *`_autoPromoteCI`* in *`CIIdentify Script Include`* das vom Suchskript zurückgegebene CI und durchläuft automatisch die Beziehungen, um zum Eintrag *`cmdb_ci`* zu gelangen und ihn zurückzugeben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die automatische Heraufstufungslogik zu überschreiben, d. h. um neue CI-Klassen hinzuzufügen oder zu aktualisieren, fügen Sie das JSON-Objekt im Feld Wert in der Systemeigenschaft [**sn_sec_cmn.auto PromoteFields**] hinzu.

### Prozedur

1. Geben Sie in der linken Navigationsleiste sys_properties.list ein.
2. Wählen Sie die **Eingabetaste**.
3. Suchen Sie die Systemeigenschaft [**sn_sec_cmn.autoPromoteFields**], und wählen Sie den Datensatz aus, um ihn zu öffnen.

   Standardzeichenfolge:

   ```
   {
    "dscy_switchport":"cmdb_ci",
    "cmdb_ci_network_adapter":"cmdb_ci",
    "cmdb_ci_nic":"cmdb_ci",
    "cmdb_ci_ip_address":"nic"
   }
   ```

4. Bearbeiten Sie im Textfeld **Wert** die Zeichenfolge im Standardpaarungsformat.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird beim nächsten Import von den CI-Suchregeln verwendet. Die Systemeigenschaft [sn_sec_cmn.autoPromoteFields] stuft die CIs herauf, während diese Suchregeln ausgeführt werden.

## Konfigurieren Sie den Schlüssel für angreifbare Elemente

Konfigurieren Sie die Granularität des Schlüssels für angreifbare Elemente (AEs) in der Anwendung Vulnerability Response, um zu definieren, was ein angreifbares Element (AE) in Ihrer Organisation ausmacht.

### Vorbereitungen

Erforderliche Rolle: admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Wichtige Begriffe

**Konfigurationselement (Configuration Item, CI)**

Ein vorhandenes Asset, das in Ihrer CMDB aufgeführt ist.

**Schwachstelle**

Ein Datensatz einer bekannten Schwachstelle, der aus dem National Institute of Standards and Technology (NIST), der National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE) oder Drittanbieterintegrationen mit Vulnerability Responseimportiert wurde.

**Angreifbares Element**

Ein angreifbares Element wird erstellt, wenn eine importierte Schwachstelle mit einem Konfigurationselement in Ihrer CMDB übereinstimmt.

**Erkennung**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein einzelnes, eindeutiges Vorkommen einer Schwachstelle, wie von den Scannern Ihrer Drittanbieterintegrationen gemeldet. Erkennungen werden importiert und sowohl im Erkennungs- als auch im Datensatz für angreifbare Elemente in Ihrer Instanz angezeigt. Wird auch als Erkennung angreifbarer Elemente bezeichnet.

Standardmäßig ist ein angreifbares Element eine eindeutige Kombination aus einem Configuration Item (CI), einer Schwachstelle und einer Integrationsinstanz. Um angreifbare Elemente mit höherer Granularität zu erstellen, fügen Sie eindeutige Ports aus Erkennungen angreifbarer Elemente hinzu, um die Behebung von Schwachstellen auf der Ebene zu verwalten, die Ihrer Meinung nach für Ihre Organisation am effektivsten ist.

Wenn Sie angreifbare Elemente mit höherer Granularität erstellen möchten, konfigurieren Sie den Schlüssel für angreifbare Elemente so, dass er port enthält. Wenn Port einbeziehen aktiviert ist, werden angreifbare Elemente durch eindeutige Ports aus Erkennungen angreifbarer Elemente erstellt.

Ab Vulnerability Response V17.1 können Sie Rapid7-Schwachstellen identifizieren und beheben, indem Sie Nachweise als VI-Schlüssel hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Nachweisen zu Rapid7-Schlüsseln für angreifbare Elemente.

Wählen Sie eine Option aus der folgenden Tabelle aus, um die Option Port einbeziehen zu aktivieren.

**Drei Szenarien für die erstmalige Aktivierung der Option Port einschließen mit dem VI-Schlüssel**

| Wenn... | Beschreibung |
|---|---|
| Mindestens eine der folgenden Bedingungen ist erfüllt:<br>• Sie führen ein Upgrade von einer Version von Vulnerability Response vor v10.0 durch, die keine Erkennung angreifbarer Elemente unterstützt.<br>• Sie sind ein neuer Kunde und haben keine Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) in Ihrer Now Platform® -Instanz.<br>• Sie haben bereits alle Datensätze für angreifbare Elemente und zugehörige Daten in Ihrer Instanz gelöscht und sind bereit, alle Ihre Vulnerability Response-Daten zu erstellen, beginnend mit einem neuen Import, um VIs einzubeziehen, die sich nach einem eindeutigen Port unterscheiden. | Aktivieren Sie Port einbeziehen.<br><br>Nachdem Port einbeziehen aktiviert ist, erstellen importierte Erkennungen ab dem nächsten Import angreifbare Elemente, die VIs enthalten, die sich durch einen eindeutigen Port unterscheiden. |
| Beide Bedingungen sind erfüllt:<br>• Sie haben Version 10.0 oder höher von Vulnerability Response und verfügen über vorhandene Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) in Ihrer Instanz, die Sie beibehalten möchten. | Aktivieren Sie Port einbeziehen. Ihre vorhandenen Erkennungen und die zugehörigen angreifbaren Elemente bleiben erhalten.<br><br>Nachdem Port einbeziehen aktiviert ist, erstellen neue Erkennungen ab dem nächsten Import neue angreifbare Elemente, die VIs enthalten, die sich nach einem eindeutigen Port unterscheiden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Drei Szenarien für die erstmalige Aktivierung der Option Port einschließen mit dem VI-Schlüssel (Fortsetzung)**

| Wenn... | Beschreibung |
|---|---|
| • Sie möchten mit der Erstellung neuer angreifbarer Elemente beginnen, um VIs einzuschließen, die sich durch einen eindeutigen Port unterscheiden. | |
| Beide Bedingungen sind erfüllt:<br>• Sie haben Vulnerability Response, Version 10.0 oder höher.<br>• Sie haben vorhandene Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente), möchten Ihre vorhandenen Daten jedoch nicht beibehalten, da Sie es vorziehen, Ihre Schwachstellendaten aus einem neuen Import zu erstellen, und VIs einbeziehen möchten, die sich durch einen eindeutigen Port unterscheiden. | 1. Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten aus Ihrer Instanz.<br>2. Aktivieren Sie Port einbeziehen.<br>Nachdem Port einbeziehen aktiviert ist, erstellen neue Erkennungen ab dem nächsten Import neue angreifbare Elemente, die VIs enthalten, die sich nach einem eindeutigen Port unterscheiden. |

**Hinweis:**

Wenn die Option Port einbeziehen aktiviert ist, kann für ein Konfigurationselement mehr als ein angreifbares Element erstellt werden. Wenn beispielsweise eine Schwachstelle für zwei Ports in einem Konfigurationselement vorhanden ist, Ports 80 und 443, werden ab dem nächsten Import zwei eindeutige VIs erstellt, eine für jeden Port.

**Hinweis:**

Stellen Sie sicher, dass Sie VIs erstellen, um VIs nach eindeutigen Ports einzubeziehen, bevor Sie diese Funktion aktivieren. Sobald Sie den VI-Schlüssel zum Einschließen des Ports aktiviert haben, müssen Sie zuerst Ihre Vulnerability Response-Daten löschen, bevor Sie „Port einbeziehen“ deaktivieren und zum Importieren von Schwachstellendaten mit der Standardgranularität des VI-Schlüssels zurückkehren können, d. h., wobei VIs für den Port erstellt, aber nicht unterschieden werden Ein eindeutiger Port. Weitere Informationen zum Löschen von Schwachstellendaten finden Sie unter Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten in Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.

   Das Feld Zuletzt aktualisiert zeigt das Datum an, an dem der VI-Schlüssel zuletzt konfiguriert wurde.

2. Klicken Sie auf das Kontrollkästchen Port einbeziehen, um es zu aktivieren.

3. Klicken Sie auf **Speichern**.
   Das Bestätigungsdialogfeld wird angezeigt.

   Wenn Sie in Ihrer Instanz keine Datensätze zur Erkennung angreifbarer Elemente haben, werden ab dem nächsten Import sowohl Erkennungen angreifbarer Elemente als auch angreifbare Elemente nach eindeutigem Port erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn in Ihrer Instanz vorhandene Erkennungen angreifbarer Elemente und angreifbare Elemente vorhanden sind, werden vorhandene Erkennungen und zugehörige angreifbare Elemente beibehalten. Durch neue Erkennungen wird ab dem nächsten Import eine neue Schwachstelle erstellt, die VIs enthält, die sich durch einen eindeutigen Port unterscheiden.

**Nächste Maßnahme**
Überprüfen Sie, ob angreifbare Elemente nach Port in den Datensätzen für die Erkennung angreifbarer Elemente und für angreifbare Elemente angezeigt werden. Weitere Informationen finden Sie unter Zeigen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente an.

### Hinzufügen von Nachweisen zu Rapid7-Schlüsseln für angreifbare Elemente

Fügen Sie Nachweise als Schlüssel für angreifbare Elemente (AEs) für die Rapid7 VIs hinzu. Durch das Einbeziehen des Nachweises für bestimmte Schwachstellen kann die Scanner-Integration von [ Rapid7 AEs für jeden von Rapid7erhaltenen Nachweis erstellen.

Ein VI-Schlüssel ist die Kombination aus Schwachstelle, Konfigurationselement (CI) und Integrationsinstanz. Durch die Aufteilung von Erkennungen in verschiedene AEs basierend auf Nachweisen werden mehrere AEs erstellt. Sie können die Schwachstellen den entsprechenden Korrekturbesitzern zuweisen.

Beispielsweise kann es zwei Erkennungen mit derselben Schwachstelle und demselben CI, aber mit unterschiedlichen Nachweisen geben, die zur Erstellung einer einzigen VI führen. Ab Vulnerability Response V17.1 können Sie Schwachstellen identifizieren und beheben, indem Sie Nachweise als VI-Schlüssel hinzufügen.

Sie können den Nachweis wie folgt als VI-Schlüssel hinzufügen:

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren** und wählen Sie die Option zum Einbeziehen von Nachweisen aus.

**Anwendungsfall: Einbindung von Nachweisen in den VI-Schlüssel für vorhandene AEs oder Aufteilung vorhandener AEs basierend auf dem Erkennungsnachweis**

Um VIs basierend auf Nachweisen zu erstellen, können Sie die R7 log4j-Schwachstellen verwenden. Sie können beispielsweise eine der mehreren R7 log4j-Schwachstellen verwenden, z. B. `R7-apache-log4j-core-cve-2021-44228`, `R7-amazon_linux-cve-2021-44228`oder `R7-amazon-linux-ami-2-`. cve-2021-44228 .

Wenn alle Erkennungen in einem VI denselben Nachweis haben, wird der vorhandene VI so aktualisiert, dass er „Nachweis im VI-Schlüssel (external_id)“ enthält. Wenn mehrere Erkennungen mit unterschiedlichen Nachweisen vorhanden sind, wird der vorhandene VI geschlossen. Die Erkennungen werden auf die neuen VIs mit „Nachweis im VI-Schlüssel (external_id)“ aufgeteilt.

**Hinweis:**

Wenn Sie die Schwachstellen-ID angeben, werden die vorhandenen VIs basierend auf dem Nachweis aufgeteilt. Die neuen Schwachstellen für diese Schwachstellen-ID weisen ebenfalls einen Nachweis als einen der VI-Schlüssel auf.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten in Vulnerability Response

Entfernen Sie dauerhaft alle Vulnerability Response-Daten (angreifbare Elemente oder Erkennungen angreifbarer Elemente) und zugehörige Daten und Datensätze aus der Anwendung Vulnerability Response in Ihrer Instanz Now Platform®.

#### Vorbereitungen

Löschen Sie Datensätze zur Erkennung angreifbarer Elemente, angreifbare Elemente, Schwachstellengruppen und alle zugehörigen Datensätze in der Anwendung Vulnerability Response aus Ihrer Instanz. Verwenden Sie diesen Prozess, um Ihre Instanz zu bereinigen, um Daten mit einem Neustart aus Ihren Drittanbieterintegrationen oder als Voraussetzung dafür zu importieren, dass die Schlüsselkonfiguration des angreifbaren Elements (AE) auf die Standardeinstellung zurückgesetzt wird. Weitere Informationen zum Konfigurieren des VI-Schlüssels finden Sie unter Konfigurieren Sie den Schlüssel für angreifbare Elemente.

**Hinweis:**

Mit dieser Aktion werden alle Datensätze für angreifbare Elemente und alle zugehörigen Daten aus Ihrer Instanz gelöscht. Diese Daten können nach dem Löschen nicht abgerufen werden. Außerdem müssen Sie den Datenimport anhalten und Ihre aktiven Drittanbieterintegrationen mit Vulnerability Responsedeaktivieren.

Das Löschen der Daten für angreifbare Elemente mit diesem Prozess ist erforderlich, bevor die VI-Schlüsselkonfiguration geändert wird. Durch das Entfernen aller Daten wird sichergestellt, dass alle angreifbaren Elemente und Erkennungen angreifbarer Elemente ab dem nächsten Import zugeordnet und mit den aktuellen Daten aktualisiert werden.

Stellen Sie vor dem Löschen Ihrer Daten sicher, dass die folgenden Bedingungen zutreffen:

- Sie haben v10.0 oder höher von Vulnerability Response installiert. Weitere Informationen finden Sie unter Vulnerability Response Erkennung angreifbarer Elemente aus Drittanbieterintegrationen.
- Sie möchten Port einbeziehen deaktivieren und die VI-Schlüsselkonfiguration auf die Standardeinstellung zurücksetzen.
- Sie haben vorhandene angreifbare Elemente und Erkennungen angreifbarer Elemente, möchten oder müssen diese jedoch nicht aktualisieren und beibehalten.
- Sie haben sich entschlossen, alle vorhandenen Vulnerability Response-Daten und zugehörigen Datensätze zu entfernen, um Ihre Instanz zu bereinigen.

Erforderliche Rolle: sn_vul.vulnerability_admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Integrationen von Sicherheitslücken**.
2. Erfassen Sie alle angezeigten aktiven Integrationen.

   Alle aktiven Integrationen, die mit geplanten Aufgaben aufgelistet sind, werden vor dem Löschen aller angreifbaren Elemente und zugehörigen Daten deaktiviert, sodass während der Datenentfernung keine neuen Daten importiert werden. Wenn Sie diese



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste aufzeichnen, können Sie Ihre Integrationen nach Abschluss des Löschvorgangs aktivieren.

3. Lesen Sie den Artikel How to delete Existing Vulnerability Response Data for Reimport (Wie lösche ich vorhandene Vulnerability Response-Daten für den erneuten Import) in der HI Knowledge Base.
4. Wenn eine Warnmeldung angezeigt wird, die verhindert, dass Sie in die Spalte Aktiv schreiben, führen Sie die folgenden Schritte aus, um aktive Integrationen zu deaktivieren.
   a. Klicken Sie in der Spalte Name auf ein Element, um den Datensatz zu öffnen.
   b. Wenn Sie das Kontrollkästchen Aktiv nicht bearbeiten können, klicken Sie auf den Link **hier**, um den Datensatz zu bearbeiten.
   c. Klicken Sie auf das Kontrollkästchen **Aktiv**, um die Integration zu deaktivieren und die nächste geplante Aufgabe abzubrechen.
   d. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Liste zurückzukehren.
   e. Vergewissern Sie sich, dass Sie alle aktiven Integrationen in der Liste „Integrationen“ deaktiviert haben. Nachdem Sie eine Integration deaktiviert haben, wird sie nicht mehr in der Liste der aktiven Integrationen angezeigt. Um eine Liste inaktiver Integrationen anzuzeigen und alle Integrationen zu suchen, die Sie deaktiviert haben, nachdem Sie alle Ihre Schwachstellendaten gelöscht haben, geben Sie in der Spalte Aktiv oben = falseein.
5. Fahren Sie mit den Schritten im KB-Artikel zum Löschen vorhandener Schwachstellendaten fort.
6. Nachdem Sie bestätigt haben, dass alle Daten erfolgreich gelöscht wurden, navigieren Sie zu **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.
7. Im Formular:
   - Wenn Sie Daten gelöscht haben, weil Sie Ihre Schwachstellendaten so erstellen möchten, dass der Port aus einem neuen Import einbezogen wird, aktivieren Sie Port einbeziehen, und klicken Sie auf **Speichern**.
   - Wenn Sie Daten gelöscht haben, weil Sie den VI-Schlüssel auf die Standardeinstellung zurücksetzen möchten, deaktivieren Sie Port einbeziehen, und klicken Sie auf **Speichern**.

   Weitere Informationen finden Sie unter Konfigurieren Sie den Schlüssel für angreifbare Elemente.

### Filtern innerhalb Vulnerability Response

Korrekturaufgabenregeln, Rechner und Zuweisungsregeln verwenden während des Imports Bedingungen, die mit dem **Bedingungsgenerator**erstellt wurden. Änderungen an den Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

Die im Lieferumfang des Basissystems enthaltenen Regeln und Rechner sind auf Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern erfordert Sorgfalt und erfordert möglicherweise sowohl ServiceNow als auch Vulnerability Response.

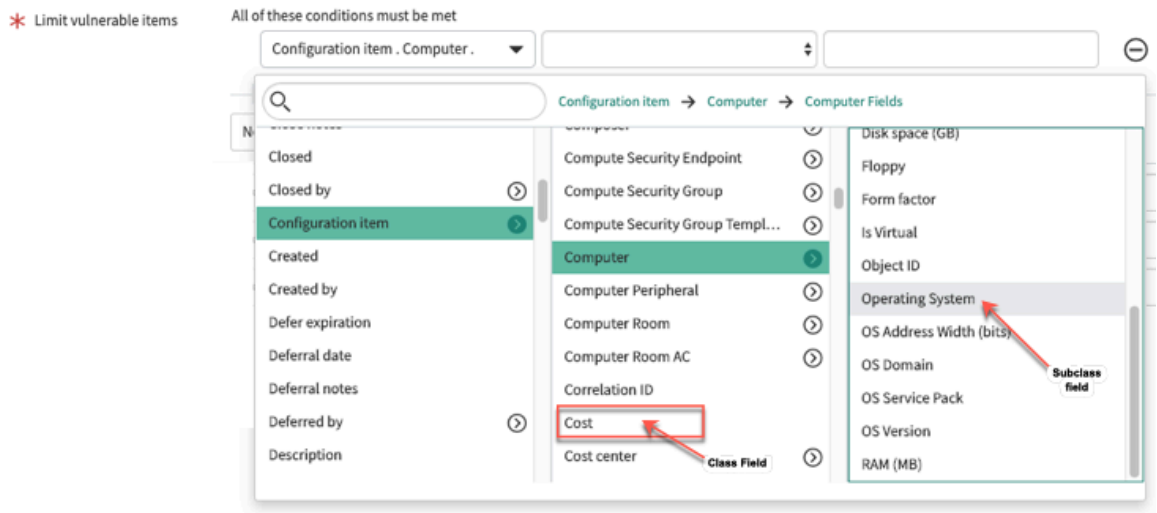
## Vermeiden Sie die Filterung basierend auf Unterklassenfeldern

Einige Tabellen unterstützen die Erweiterung. Ein Beispiel hierfür ist die Tabelle „CMDB CI“ [cmdb_ci]. Tabellen wie cmdb_ci_hardware und cmdb_ci_computer erweitern diese



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann die Erstellung und Auswertung dieses Filters teuer sein.




Beispiel: Filtern nach **Konfigurationselement** > **Kosten** würde die Leistung nicht beeinträchtigen, da **Kosten** ein Klassenfeld und kein Unterklassenfeld von **Konfigurationselement**ist.

**Konfigurationselement** > **Computer**ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser Prozess kann viele Millisekunden dauern, was sich schnell summiert, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigt.

**Hinweis:**
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann Auswirkungen auf die Leistung haben. Die Verwendung von [ist] ist, wo immer möglich, effizienter.

### Erstellen Sie eine Vulnerability Response -Schweregradzuordnung

Die SchweregradzuordnungVulnerability Response wandelt Quellschweregradfelder von Drittparteien in erkennbare Felder in Vulnerability Responseum.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response wird mit der National Vulnerability Database (NVD) zur normalisierten ServiceNow Schweregradzuordnung ausgeliefert. ServiceNow Integrationen von Drittparteien wie Qualys Vulnerability Integration stellen Schweregradzuordnungen bei der Installation bereit. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für benutzerdefinierte oder nicht standardmäßige Drittparteizuordnungen in Ihrer Umgebung vorgesehen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Feldzuordnung**

| Feld | Beschreibung |
|---|---|
| Quelle | Der Name der Quelle für die Schweregradzuordnung. |
| Quellwert | Der Quellschweregradwert. |
| Zielwert | Der Zielschweregradwert. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ 1 - Kritisch<br>○ 2 – Hoch<br>○ 3 – Mittel<br>○ 4 – Niedrig<br>○ 5 – Keine |

4. Wiederholen Sie Schritt 3 für jeden Quellschweregrad.
5. Klicken Sie auf **Absenden**.

## Definieren Sie Serviceklassifizierungen für die Berichterstellung Vulnerability Response und zugehörige Listen

Legen Sie mehr Wert auf Berichte und zugehörige Listen in Vulnerability Response, indem Sie Serviceklassifizierungen definieren. Darüber hinaus kann die Leistung der Vulnerability Response -Datenerfassung verbessert werden, indem die Anzahl der angeforderten Serviceklassifizierungen reduziert wird.

### Vorbereitungen

Erforderliche Rolle: admin

**Hinweis:**

Das Bearbeiten von Systemeigenschaften erfordert Kenntnisse von ServiceNow und Vulnerability Response.

### Prozedur

1. Geben Sie in der linken Navigationsleiste `sys_properties_list.do` ein.
2. Klicken Sie auf **Eingeben**.
3. Geben Sie im Menü **Suche** unter **Name** `sn_vul.service_classification` ein.
4. Öffnen Sie die Systemeigenschaft *`sn_vul.service_classifications`*.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie im Textfeld **Wert** die durch Kommas getrennte Liste der gewünschten Serviceklassifizierungen ein.

   **Hinweis:**
   Wenn diese Einstellung leer ist, werden alle Services aufgelistet.

   Beispiele:

   Um Business Services, technische Services und Anwendungsservices anzuzeigen und Serviceangebote, gemeinsam genutzte Services und nicht klassifizierte Services auszuschließen, legen Sie den Wert fest auf: **Business Service,Technischer Service,Anwendungsservice**.

   Um Anwendungsservices anzuzeigen, legen Sie den Wert auf **Anwendungsservice**fest.

6. Klicken Sie auf **Aktualisieren**.
   Die Daten in jedem Bericht und in der zugehörigen Liste für angreifbare Elemente werden bei der nächsten Ausführung des nächtlichen Performance Analytics-Auftrags nach Serviceklassifizierung gefiltert.

### Audit ausgewählter Felder in der Tabelle „Angreifbare Elemente“

Aktivieren Sie Auditing für Felder, die Sie in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item] angeben. Diese Prüfungsmethode ist nützlich, wenn Sie Felder prüfen möchten, die Sie standardmäßig nicht prüfen können.

#### Vorbereitungen
Erforderliche Rolle: admin

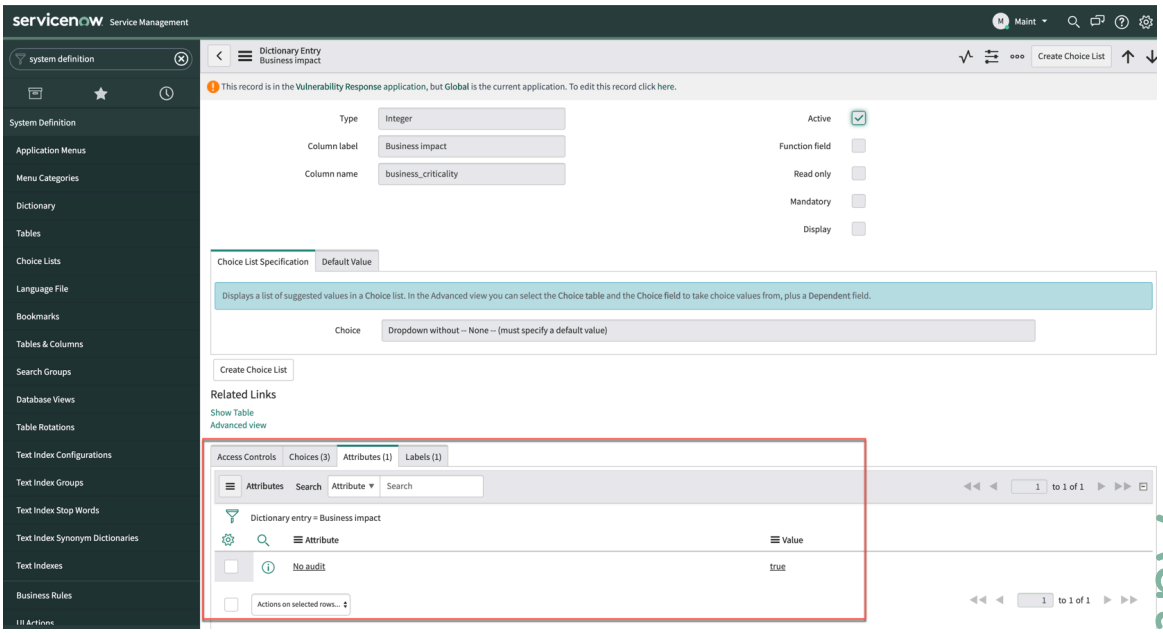
#### Warum und wann dieser Vorgang ausgeführt wird
Die Tabelle sn_vul_vulnerable_item ist standardmäßig überprüfbar. Felder, für die das Attribut no_audit auf „true“ festgelegt ist, können nicht geprüft werden. Weitere Informationen zum Auditing von Tabellen finden Sie unter Auditing für eine Tabelle aktivieren .

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Systemdefinition** > **Tabellen** und suchen Sie nach der Tabelle sn_vul_vulnerable_item.
   Die Liste der Wörterbucheinträge für die Tabelle wird angezeigt.
2. Um die Überwachung für ein Feld zu aktivieren, klicken Sie auf den Namen des Eintrags.
   Die Seite „Wörterbucheintrag“ für diesen Eintrag wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Navigieren zu **Attribute** > **Kein Audit**.
   Die Seite Dictionary-Attribut wird angezeigt.
4. Um das Attribut no audit=true zu entfernen, klicken Sie auf **Löschen**.
   Auditing für dieses Feld ist aktiviert.

### Vulnerability Response Konfiguration des Hintergrundauftrags-Frameworks

Definieren Sie das Hintergrundauftrags-Framework in Ihrer Now Platform® -Instanz. Diese Konfigurationsänderungen können Ihnen helfen, die Leistung zu verbessern, indem die Menge der Systemressourcen reduziert wird, die für die Ausführung Ihrer Hintergrundaufträge verwendet werden.

## Was können Sie im Hintergrundauftrags-Framework bearbeiten?

Mit dem Hintergrundauftrags-Konfigurationsmodul haben Sie die folgenden Einstellungsoptionen im -Framework:

- Sie können die Anzahl der Hintergrundaufträge definieren, die gleichzeitig für Vulnerability Response Prozesse ausgeführt werden.
- Für lange Aufgaben, die im Hintergrund ausgeführt werden und große Datenmengen verarbeiten, können Sie Partitionen erstellen, um Daten in kleineren Blöcken zu verarbeiten.
- Sie können einen Auftrag abbrechen.

## Warum das Hintergrundauftrags-Framework konfigurieren?

Hintergrundaufträge in Now Platform® sind so konzipiert, dass sie über einen längeren Zeitraum ausgeführt werden, um mehrere Prozesse für Ihre Datensätze in Vulnerability Responseauszuführen. Diese Aufgaben basierten zuvor auf Business Rules, die asynchron ausgeführt wurden. Es gibt keine Begrenzung für die Anzahl dieser Aufgaben, die in Ihrer Instanz im Hintergrund ausgeführt werden können, sodass die großen Mengen von Datensätzen, die von diesen Aufgaben betroffen sind, verarbeitet werden können. Wenn mehrere Aufgaben, deren Abschluss lange dauert, gleichzeitig im Hintergrund ausgeführt werden, sind die Systemressourcen betroffen, die zur Ausführung Ihrer geplanten Aufgaben verwendet werden, was sich wiederum negativ auf Ihre Leistung auswirken kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die Konfiguration des Hintergrundauftrags-Frameworks können Sie Ihre Leistung verbessern, indem Sie die Menge der Systemressourcen reduzieren, die für die Ausführung Ihrer Hintergrundaufträge verwendet werden.

## Wichtige Begriffe

**Stellenfähigkeit**

Beschreibt die jeweiligen Aufgaben. Beispielsweise kann ein bestimmter Auftrag die folgenden Fähigkeiten enthalten:

- Die Aufgabe kann parallel zu einer anderen Aufgabe desselben Typs ausgeführt werden.
- Der Auftrag kann partitioniert werden.
- Die Aufgabe kann während der Ausführung abgebrochen werden.

**Gleichzeitigkeit**

Bezieht sich auf Jobs oder Teile von Jobs, die parallel ausgeführt werden.

**Partition**

Partitionen sind Teile von Aufgaben, die aufgeteilt werden können, sodass sie parallel verarbeitet werden können, um eine bessere Leistung zu erzielen. Bezieht sich normalerweise auf Jobs mit langen Ausführungszeiten.

**Auftragskonfiguration**

Bezieht sich auf die Einstellungen für eine bestimmte geplante Aufgabe.

**Regelmäßige Aufgabe**

Regelmäßige Aufgaben sind automatisierte Aufgaben, die zu einem bestimmten Zeitpunkt oder nach einem wiederkehrenden Zeitplan ausgeführt werden können.

**Systemressourcen**

Bezieht sich auf die Menge der Systemressourcen, die Sie für eine bestimmte Anzahl von Hintergrundaufgaben und geplanten Aufgaben in Ihrer Umgebung benötigen.

**Systemeigenschaft**

Systemeigenschaften speichern Konfigurationsinformationen, die sich selten oder nie ändern. Jedes Mal, wenn Sie eine Systemeigenschaft ändern oder hinzufügen, leert das System den Cache, um alle Knoten im Cluster synchron zu halten. Diese Cacheleerung wirkt sich auf die Leistung aus.

**Business Rule**

Eine Business Rule ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder eine Tabelle abgefragt wird. Business Rules führen Aufgaben aus, z. B. das automatische Ändern von Werten in Formularfeldern, wenn bestimmte Bedingungen erfüllt sind, oder das Erstellen von Events für E-Mail-Benachrichtigungen und Skriptaktionen.

## Anwendungsfall zum Definieren des Hintergrundauftrags-Frameworks

Beispielsweise verarbeitet der Hintergrundauftrag, der Korrekturzielregeln für Datensätze angreifbarer Elemente (VITs) und Datensätze für angreifbare Elemente in Application Vulnerability Response (AVITs) anwendet, gleichzeitig große Mengen von Datensätzen mit mehreren Aufgaben.

Abhängig von der Größe des Imports und der Anzahl der Datensätze, die Sie in Ihrer Umgebung haben, kann dieser Auftrag eine große Menge Ihrer verfügbaren Systemressourcen verbrauchen und lange dauern, bis er erfolgreich abgeschlossen ist.

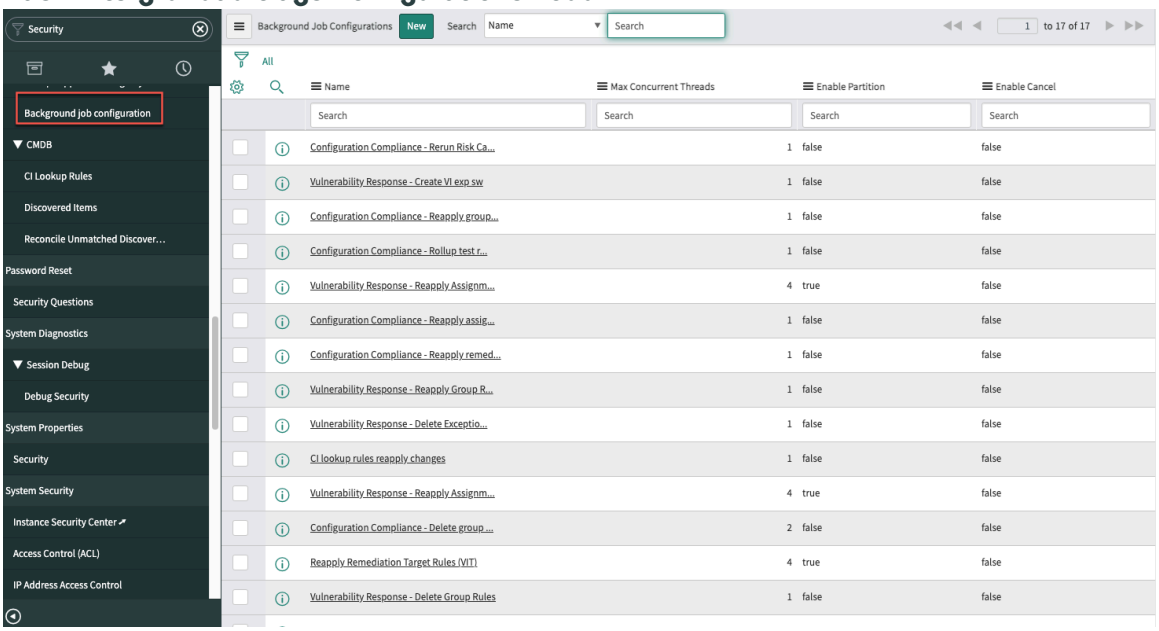


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemwartungsaufgaben oder andere regelmäßige Aufgaben werden möglicherweise langsamer ausgeführt.

Im Modul „Hintergrundauftragskonfiguration“ werden Aufträge nach Name und einer eindeutigen Konfigurations-ID aufgelistet. In diesen Datensätzen können Sie definieren, wie viele Aufgaben für einen bestimmten Hintergrundauftrag gleichzeitig ausgeführt werden sollen. Sie können den Auftrag auch so festlegen, dass Datenpartitionen verarbeitet werden, damit die Aufgaben schneller und einfacher abgeschlossen werden können und weniger Systemressourcen benötigt werden. Sie können einen Auftrag auch abbrechen, wenn er zu lange dauert.

**Das Hintergrundauftrags-Konfigurationsmodul**




Weitere Informationen zu den erforderlichen Schritten zum Definieren der Hintergrundauftragskonfigurationen finden Sie unter Definieren Sie Hintergrundauftragskonfigurationen in Vulnerability Response.

### Definieren Sie Hintergrundauftragskonfigurationen in Vulnerability Response

Definieren Sie, wie viele Aufgaben für einen bestimmten Hintergrundauftrag gleichzeitig ausgeführt werden sollen. Sie können den Auftrag auch so festlegen, dass Datenpartitionen importiert werden, damit die Aufgaben schneller und einfacher abgeschlossen werden können und weniger Systemressourcen benötigt werden. Sie können einen Auftrag auch abbrechen, wenn er zu lange dauert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.manage_background_job

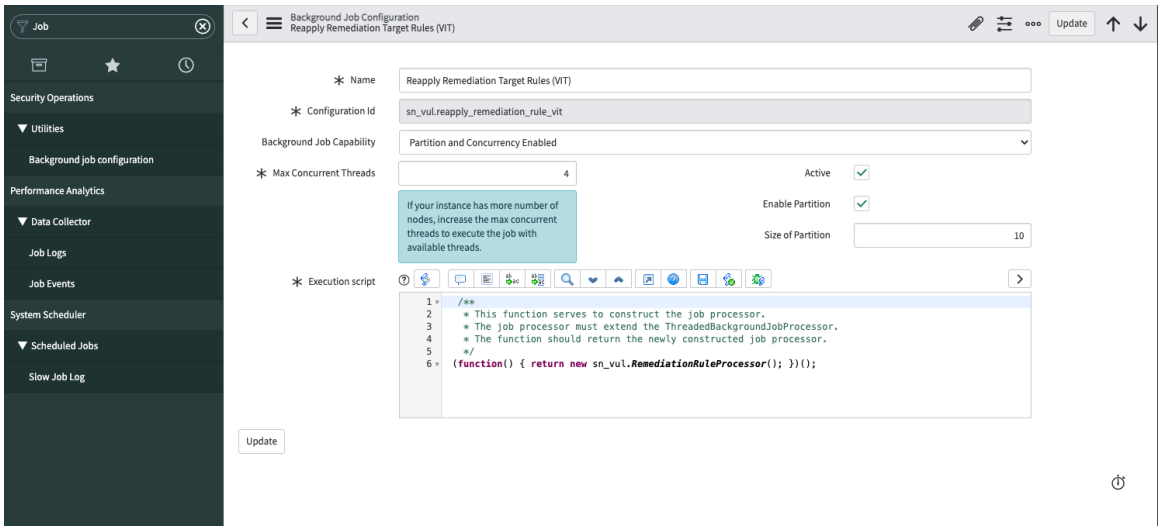
Im Abschnitt unter den Schritten finden Sie ein Beispiel.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Hintergrundauftrags-Konfigurationen**.
2. Klicken Sie in der Spalte Name auf einen Datensatz, um ihn zu öffnen.
3. Bearbeiten Sie die Felder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



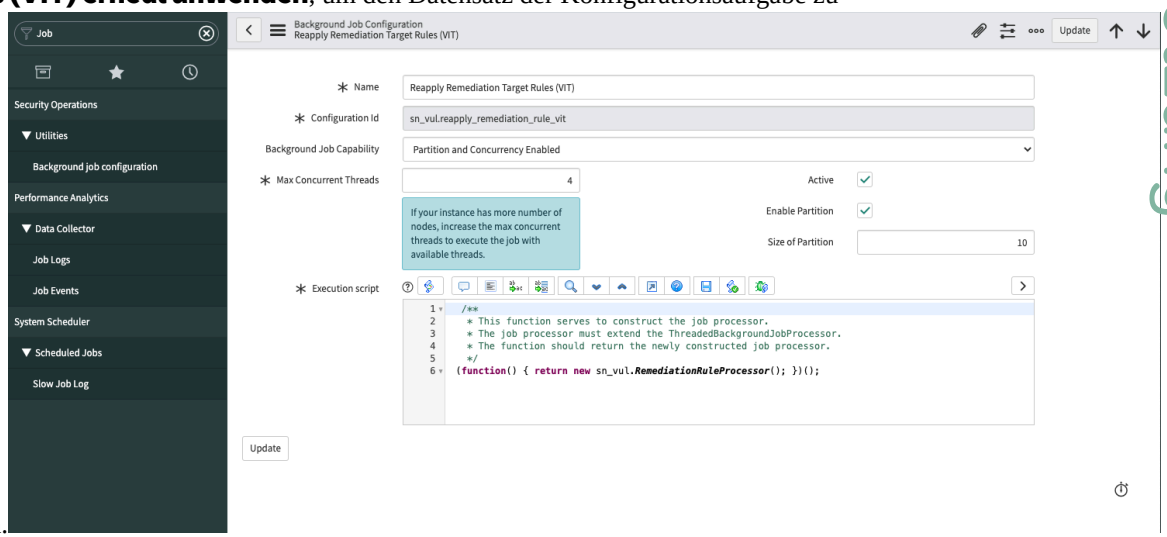

4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
   Im folgenden Beispiel erfahren Sie, wie Sie die Ergebnisse für Ihre Konfigurationsänderungen überprüfen.

   Es gibt zwei Auftragskonfigurationen für Korrekturzielregeln, die in der Anwendung enthalten sind, eine für angreifbare Elemente und eine für angreifbare Anwendungselemente:

   - Korrekturzielregeln (VIT) erneut anwenden
   - Korrekturzielregeln erneut anwenden (AVIT)

   Angenommen, Sie ändern Ihre Korrekturzielregeln und möchten sie erneut anwenden, ohne die meisten verfügbaren Systemverarbeitungsressourcen zu verwenden. Um die Verarbeitungsressourcen zu begrenzen, können Sie die Anzahl der ausgeführten Hintergrundaufträge und die Anzahl der pro Auftrag verarbeiteten Elemente im Modul „Hintergrundauftragskonfigurationen“ steuern.

5. Um diese Einstellungen festzulegen, navigieren Sie zu **Security Operations** > **Hintergrundauftrags-Konfigurationen** und klicken **Sie auf Remediation Target Rules (VIT) erneut anwenden**, um den Datensatz der Konfigurationsaufgabe zu öffnen.




   Nehmen wir für das Beispiel an, Sie wissen, dass Sie etwas mehr als 300 AEs haben.

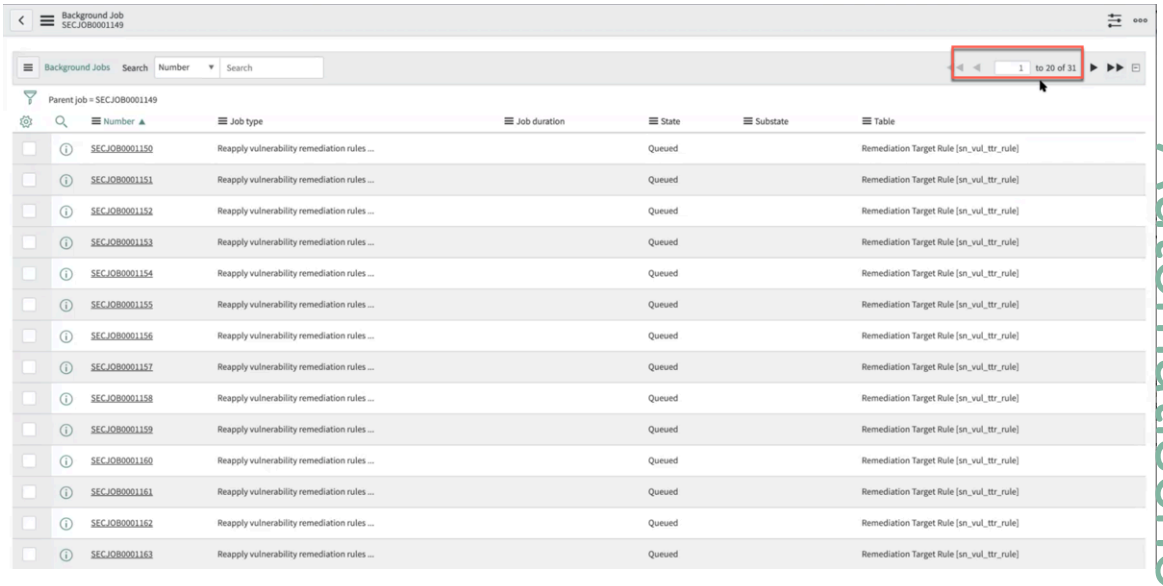
6. Ändern Sie im Datensatz der offenen Konfigurationsaufgabe den Wert der Partitionsgröße von **4** in **10**.



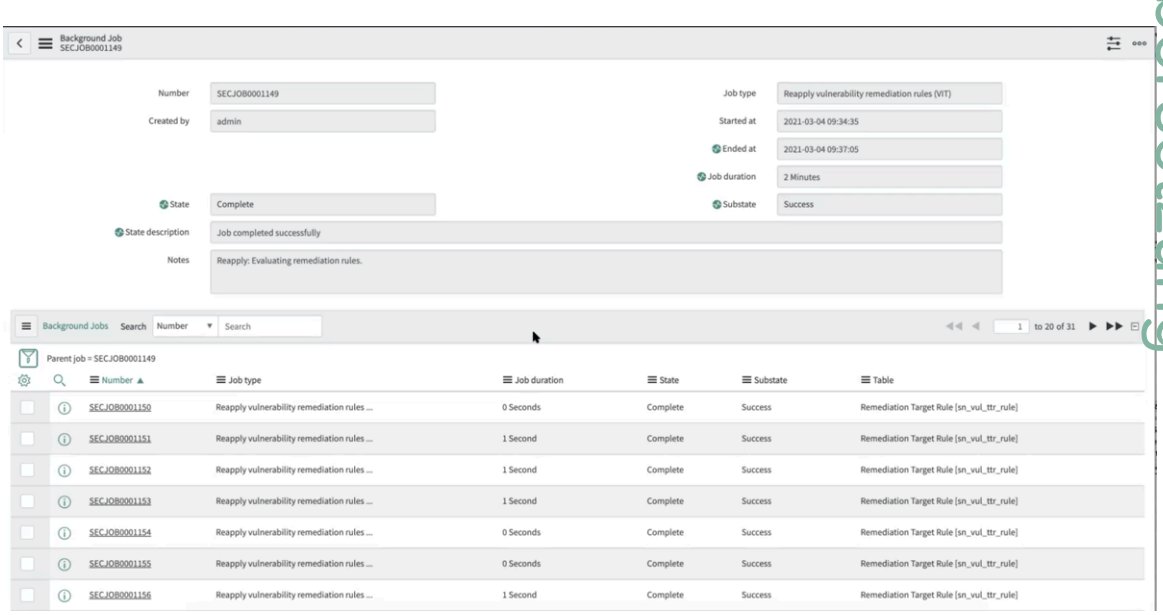
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Navigieren zu **Vulnerability Response** > **Nachbesserungszielregeln**, suchen Sie die geänderte Schwachstellenkorrekturregel Erneut anwenden, wählen Sie den Datensatz aus der Liste aus, und klicken Sie auf **Änderungen** übernehmen, um Ihre Zielregeln für Ihre vorhandenen VIs neu auszuwerten.
Die VIT-Aufgabe (Schwachstellenkorrekturregeln erneut anwenden) befindet sich in der Warteschlange.

8. Klicken Sie auf den Link **Status** anzeigen, um den Hintergrundauftragsdatensatz anzuzeigen und zu überprüfen, ob sich die Aufträge in der Warteschlange befinden (siehe folgende Abbildung).
In diesem Beispiel werden 31 Jobs erstellt, um Zielregeln für 307 AEs zu verarbeiten (maximal 10 Elemente pro Job). Diese Aufträge sind untergeordnete Aufträge des primären Hintergrundauftrags. Die untergeordneten Aufträge verarbeiten die Datensätze sequenziell.




Wenn alle Aufgaben erfolgreich abgeschlossen wurden, werden die Felder im Datensatz der Hintergrundaufgabe aktualisiert.




9. Navigieren Sie zu Ihren angreifbaren Elementen, und überprüfen Sie, ob sie Ihre neue Regeländerung widerspiegeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erweiterte parallele Verarbeitung für Hintergrundaufträge in Vulnerability Response

Mit dieser erweiterten Einstellung können Sie die Gesamtzahl der parallel verarbeiteten Hintergrundaufträge unabhängig vom Auftragstyp steuern.

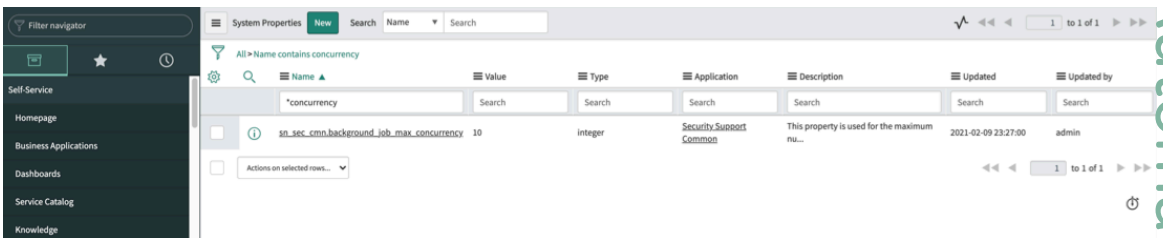
### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.manage_background_job

**Hinweis:**
Dieses Verfahren erfordert fortgeschrittene Programmierkenntnisse.

### Prozedur

1. Geben Sie im **Filternavigator sys_properties.list** ein, und suchen Sie die Systemeigenschaft *sn_sec_cmn.background_job_max_concurrency*.




2. Klicken Sie darauf, um den Datensatz zu öffnen.

   Standardmäßig führt die Systemeigenschaft *sn_sec_cmn.background_job_max_concurrency* maximal 10 Hintergrundaufträge parallel aus.

   Wenn Ihre Instanz eine geringe Anzahl von Knoten aufweist, können Sie diesen Wert in der Systemeigenschaft reduzieren. Angenommen, Sie haben sieben Zuweisungsregeln in Ihrer Gruppenregelliste. Im Konfigurationsdatensatz der Aufgabe „Zuweisungsregeln erneut anwenden“ werden drei Aufgaben für die maximale Anzahl gleichzeitiger Threads festgelegt. Ihr Gleichzeitigkeitswert für Ihr Framework ist 10, aber Ihr System ist eine einzelne Knoteninstanz, sodass Sie zwei partitionierte Aufgaben aus Ihrer Aufgabe „Zuweisungsregeln erneut anwenden“ gleichzeitig verarbeiten können. Wenn Sie die maximale Anzahl gleichzeitiger Threads auf einen Auftragsdatensatz für Zuweisungsregeln festlegen, werden alle Auftragstypen des Typs „Zuweisungsregeln erneut anwenden“ sequenziell verarbeitet.

   Umgekehrt können Sie diesen Wert erhöhen, wenn Ihre Instanz über mehr Knoten verfügt. Sie müssen jedoch auch weitere geplante Aufgaben hinzufügen, um diese Änderung vorzunehmen.

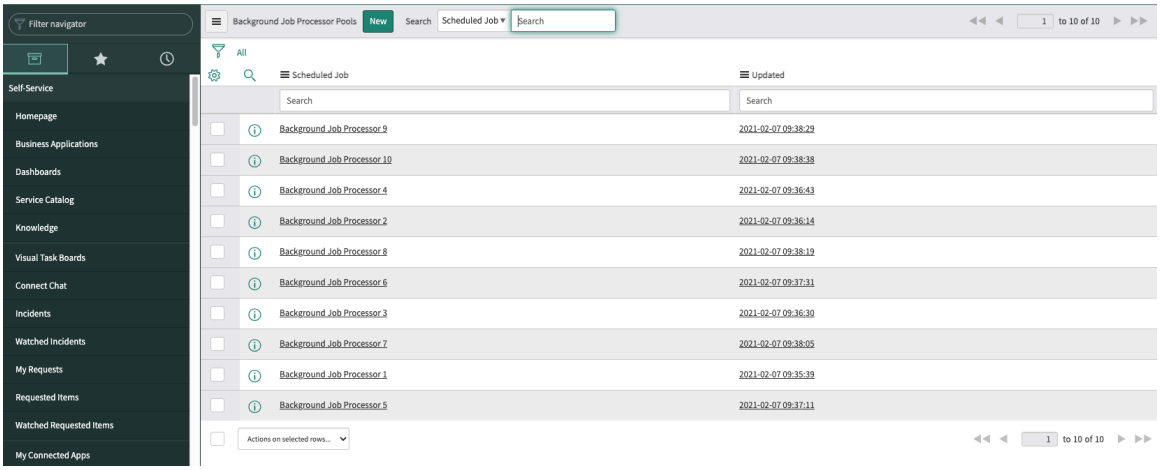
   Um die Anzahl der geplanten Aufgaben zu erhöhen, duplizieren Sie eine geplante Aufgabe so oft, bis der Wert erreicht ist, um den Sie die Systemeigenschaft erhöht haben. Zum Beispiel gibt es standardmäßig 10 geplante Aufgaben. Wenn Sie also 20 Jobs möchten, müssen Sie einen Job 10 Mal duplizieren.

   Die zehn geplanten Aufgaben, die in Now Platform® zur Verarbeitung enthalten sind, werden in der Tabelle sn_sec_cmn_background_job_processor_pool angezeigt.

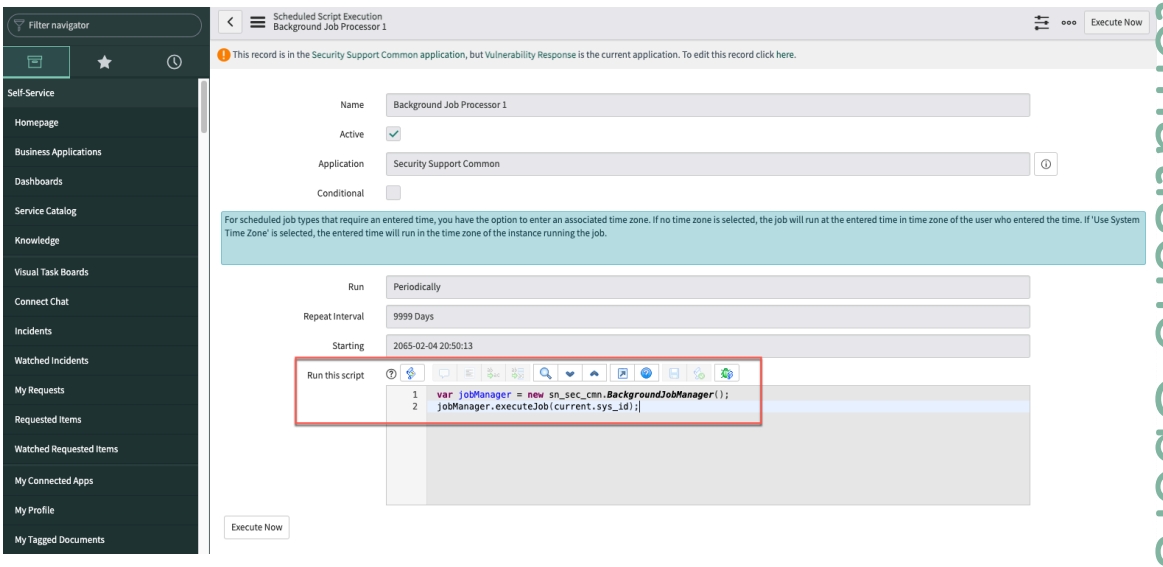
3. Geben Sie im **Filternavigator sn_sec_cmn_background_job_processor_pool.list**ein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Klicken Sie auf eine Aufgabe, um sie so oft wie erforderlich zu kopieren und zu duplizieren, sodass die Anzahl der Aufgaben dem Wert entspricht, um den Sie die Systemeigenschaft erhöht haben.




5. Nachdem die geplante Aufgabe definiert wurde, fügen Sie eine Referenz hinzu, indem Sie in der Liste sn_sec_cmn_background_job_processor_pool für die kopierte Aufgabe auf **Neu** klicken.

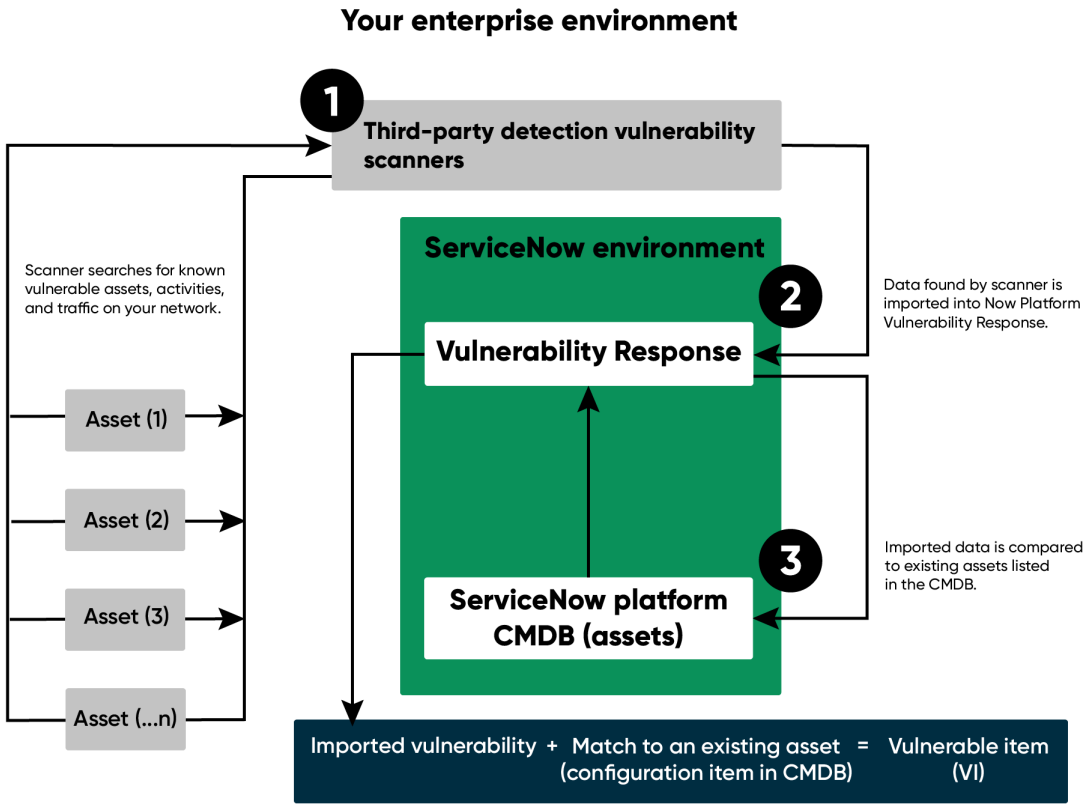
## Vulnerability Response-Integrationen

Vulnerability Response bietet Unterstützung für Integrationen von Drittparteien. In diesem Abschnitt finden Sie einige grundlegende Richtlinien für die Entwicklung eigener Integrationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Integrationen von Drittparteien




Importierte Schwachstellen aus der National Vulnerability Database (NVD) und Erkennungsdaten von Drittanbieter-Scannern werden mit den Assets in Ihrer CMDB abgeglichen. Wenn eine importierte Schwachstelle mit einem vorhandenen Asset übereinstimmt, wird ein angreifbares Element erstellt. Angreifbare Elemente werden automatisch in Aufgaben zur Korrektur gruppiert, mit Geschäftskontext risikobewertet, priorisiert und den entsprechenden Teams zur Korrektur zugewiesen.

### Hinweis:

Drittanbieterintegrationen werden separat behandelt. Wenn in Ihrer Umgebung mehr als eine Integrationsanwendung einer Drittpartei verwendet wird, erfolgt keine Deduplizierung angreifbarer Elemente (AEs) über Integrationen hinweg. Beispielsweise ist die VI-Deduplizierung zwischen Rapid7 und Qualys nicht verfügbar.

Es werden jedoch Diskrepanzen in der Erkennungsanzahl zwischen einem Drittanbieter-Scanner (z. B. Qualys) und VIs in Ihrer ServiceNow -Instanz erwartet, da die Deduplizierung über IPs, Ports usw. erfolgt.

Informationen zu Drittanbieterintegrationen, die von Application Vulnerability Response unterstützt werden, finden Sie unter, Integration von Application Vulnerability Response mit anderen Anwendungen.

- Integration von CISA Known Exploit Vulnerability (KEV)
- Informationen zur Integration von Microsoft Threat and Vulnerability Management Vulnerability
- Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Response
- Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Grundlegendes zu den NVD-Integrationen
- Qualys Vulnerability Integration
- Rapid7 Vulnerability Integration verstehen
- Shodan Exploit Integration
- Die Tenable Vulnerability-Integration verstehen
- Integration der Microsoft Security Response Center-Lösung

Integration der Microsoft Security Response Center-Lösung ist mit Vulnerability Solution Managementverfügbar. Weitere Informationen zur Installation und Konfiguration von Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integrationfinden Sie unter Anwendung Solution Management for Vulnerability Response installieren. Sie können Integration der Microsoft Security Response Center-Lösung und Red Hat Solution Integration im Setup-Assistenten konfigurieren, bearbeiten, planen und bei Bedarf starten.

## Zusätzliche Hinweise für -Integrationen

Wenn mehrere Bereitstellungen für eine Integration unterstützt werden, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

- Sie können viele der Integrationsanwendungen über den Setup-Assistenten installieren, konfigurieren, planen und bei Bedarf starten.
- Sie können die Anwendung Rapid7 Vulnerability Integration über den Setup-Assistenten installieren, die Konfiguration wird für diese Integration jedoch nicht über den Setup-Assistenten unterstützt. Weitere Informationen finden Sie unter Rapid7 Vulnerability Integration installieren.
- Die Anwendung Tenable for Vulnerability Response von Tenable wird von Tenable erstellt und verwaltet. Weitere Informationen finden Sie unter Tenable for Vulnerability Response.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

Ab VR v17.1 wurden die folgenden Namen der Integrationsprozessstatus aktualisiert:

| Statusname vor V17.1 | Statusname ab V17.1 |
|---|---|
| In Verarbeitung | Wird abgerufen |
| WartenAbgeschlossen | Warten/Bearbeitung läuft |

**Hinweis:**
Sie können die heruntergeladenen und verarbeiteten Anhänge anzeigen. Wenn der Status der Integrationsausführung `waitcomplete` lautet, wird der Prozentsatz der abgeschlossenen Integration angezeigt.

## Manuell erstellte Integrationen

Sie können nach Bedarf andere Integrationen hinzufügen, die nicht als ServiceNow Store -Anwendungen verfügbar sind. Weitere Informationen finden Sie unter Erstellen Sie manuell eine Schwachstellenintegration.

## Grundlegendes zu den NVD-Integrationen

Die NVD-Integrationen verwenden Daten, die aus der National Vulnerability Database (NVD) des National Institute of Standards and Technology (NIST) importiert wurden, um die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen. Führen Sie diese Integration als Teil der Ersteinrichtung von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

NIST NVD erfasst Daten zu gemeinsamen Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVE) und Common Platform Enumeration (CPE) und stellt diese Daten Now Platform®zur Verfügung. Die Lösung lässt sich problemlos in Vulnerability Response integrieren, um CVE- und CPE-Schwachstellen abzubilden und die Daten in Ihrer Instanz zu ergänzen.

**Wichtig:**
Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Nach der Installation wird die Integration der NIST National Vulnerability Database Integration-API (nur CVE) automatisch als regelmäßige Aufgabe aufgerufen und täglich



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ausgeführt. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

**Tipp:**
Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich.

## Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Vulnerability Response Integration mit NVD v1.2 | |

## Anfänglicher Import von Schwachstellendaten mit den NVD- und CWE-Integrationen

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000-Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus. Sie führen CWE-Aktualisierungen **bei Bedarf** standardmäßig aus dem Integrationsdatensatz durch und müssen sie konfigurieren.

   **Hinweis:**
   Planen Sie das CWE-Update so, dass es vor dem Update der NVD-Datenbank ausgeführt wird. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

2. Vergewissern Sie sich, dass die Anwendung Vulnerability Response Integration with NVD installiert ist und ein anfänglicher Datenimport aus der NIST National Vulnerability Database Integration – API (nur CVE) oder der NIST National Vulnerability Database Integration – API (CVE und CPE) erfolgreich ist.

   Überprüfen Sie für CPEs, ob ein anfänglicher Datenimport aus der NIST National Vulnerability Database Integration – API (nur CPE) erfolgreich war.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nach der Installation des Plugins wird standardmäßig die NIST National Vulnerability Database Integration - API (nur CVE) aktiviert. Sie wird täglich ausgeführt. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Integration with the NIST National Vulnerability Database.

3. Bibliotheken von Drittanbietern werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

## Importierte Schwachstellendaten und angreifbare Elemente verstehen

In Ihrer Instanz Now Platform wird jede importierte Schwachstelle durch einen Schwachstelleneintrag in den Quellbibliotheken von Scanner-Produkten von Drittanbietern wie Qualysdargestellt. Die angreifbaren Elemente (AEs), die in Ihrer Instanz importiert und aktualisiert werden, sind Verweise auf Bibliotheken von Drittanbietern, z. B. die Bibliothek Qualys. Eine Drittanbieterbibliothek kann wiederum auf den NVD verweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie beispielsweise Schwachstellendaten von Drittanbietern aus einem Produkt wie Qualyserfassen, erfassen Sie VIs, die auf eine QID (BezeichnerQualys ) verweisen. Im Fall von Qualysverweist diese QID wiederum auf ein CVE aus der NVD-Bibliothek. Wenn Sie in der Anwendung Vulnerability Response in einer Korrekturaufgabe oder einem Datensatz für ein angreifbares Element auf diese QID klicken und die NVD- und CWE-Integrationen zur Datenerfassung ausgeführt haben, werden aktuelle, angereicherte Schwachstellendaten angezeigt, mit denen Sie die Beziehungen zwischen und sehen können Ihre VIs und CVEs, CWEs und CPEs.

Bevor Sie ein Scanner-Produkt einer Drittpartei wie Qualys ausführen, das über eine eigene Bibliothek verfügt, müssen Sie mindestens die Integration von NIST National Vulnerability Database Integration – API (nur CVE) installieren und ausführen (enthält auch CISA-bezogene Details). , CWE-Integration zur Erfassung von Schwachstellendaten. Diese NVD- und CWE-Datenimporte ergänzen Ihre Vulnerability Response - oder Application Vulnerability Response -Daten, bevor Daten mit einem Drittanbieterprodukt importiert werden.

Weitere Informationen zum Verwalten von NVD-, CWE- und Bibliotheken von Drittanbietern und zum Anzeigen dieser Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern und Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an.

Nachdem Sie den erfolgreichen NVD-Import überprüft haben, Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus, um Ihre Schwachstellendaten weiter anzureichern.

Führen Sie die NVD- und CWE-Importe durch, bevor Sie Schwachstellendaten mit einem Drittanbieterprodukt importieren. Bibliotheken von Drittanbietern werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

## Die NVD-Integrationen suchen

Um die NVD-Integrationen anzuzeigen, navigieren Sie zu **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

**Hinweis:**
Standardmäßig ist nur die Integration mit der NIST National Vulnerability Database Integration - API (nur CVE) aktiv.

### NVD-Integrationen

| Integration | Beschreibung |
|---|---|
| NIST National Vulnerability Database Integration – API (nur CVE) | Ruft nur NIST NVD-Schwachstellendaten (CVE) ab. Standardmäßig ist diese Integration automatisch auf die tägliche Ausführung festgelegt. |
| NIST National Vulnerability Database | Ruft CPE-Daten aus NIST NVD ab. Diese Integration ist standardmäßig inaktiv.<br><br>Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formales Namensformat, eine Methode zum Überprüfen von Namen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**NVD-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| Integration-API (nur CPE) | mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in angreifbarer Software gespeichert.<br><br>Diese Integration wird täglich ausgeführt und ist standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter NIST National Vulnerability Database–API aktivieren (nur CPE). |
| NIST National Vulnerability Database Integration-API (Nicht zugeordnete CPE) | Ruft CPE-Daten ab, die dem abgerufenen CVE aus NIST NVD zugeordnet sind. Diese Integration ist standardmäßig inaktiv.<br><br>Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formales Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in einer zugehörigen Liste für den NVD-Schwachstelleneintragsdatensatz gespeichert. Diese Integration wird bei Bedarf ausgeführt und ist standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter Aktivieren der NIST National Vulnerability Database–API (Nicht zugeordnete CPE). |

**Wichtig:**
Die Integration „NIST National Vulnerability Database Integration-API (CVE und CPE)“ ist veraltet.

Informationen zu Integrationsausführungsstatus finden Sie unter, Zeigen Sie den Ausführungsstatus der NVD-Integration (National Vulnerability Database) an.

### Vorbereitung der NVD-Integrationen

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die NVD-Integrationen setzen voraus, dass Sie mit der NIST National Vulnerability Database (NVD) vertraut sind.

### Vorbereitungen

Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Nehmen Sie vor dem Ausführen der NVD-Integrationen die erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

### Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus

Data-Importe aus dem CWE bereichern die Schwachstellendaten in Ihrer Instanz weiter. Verwenden Sie CWE-Datensätze (Common Weakness Enumeration), die aus der CWE-Datenbank heruntergeladen wurden, als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Führen Sie diese Integration als Teil der Ersteinrichtung von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Hinweis:**
Planen Sie das CWE-Update so, dass es vor dem Update der NVD-Datenbank ausgeführt wird. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**.

Aktualisieren Sie allgemeine Schwachstellendatensätze aus der Common Weakness Enumeration-Datenbank regelmäßig. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über die Seite „Common Weakness Enumerations“ eskalieren.

- Wenn Sie über die Administratorrolle verfügen, können Sie der geplanten Aufgabe Repositorys hinzufügen.
- Wenn Sie sn_vul.vulnerability_read haben, können Sie die geplante Aufgabe ausführen.
- Wenn Sie sn_vul.vulnerability_write haben, können Sie die Details der geplanten Aufgabe bearbeiten.

### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die geplante Aufgabe **CWE Comprehensive 2000 Integration** (CWE Comprehensive 2000-Integration) aus.
3. Ändern Sie die Felder nach Bedarf.

**Formular „Schwachstellenintegration“.**

| Feld | Beschreibung |
|---|---|
| Name | Name des geplanten Auftrags. |
| Aktiv | Gibt an, ob die geplante Aufgabe aktiv ist. Wenn die Aufgabe für einen bestimmten Zeitraum nicht ausgeführt werden soll, können Sie die gewünschten Parameter einrichten und die Aufgabe deaktivieren. |
| Run-Kosten | Häufigkeit, mit der der Auftrag ausgeführt werden soll. Nachfolgende Felder werden basierend auf Ihrer Einstellung in diesem Feld angezeigt oder ausgeblendet.<br>**Hinweis:** Das CWE-Update ist standardmäßig **On Demand**. Legen Sie einen geplanten Zeitraum fest, der vor Ihren NVD-Updates liegt.<br>Zur Auswahl stehen:<br>○ Täglich: Wählen Sie eine **Uhrzeit**aus<br>○ Wöchentlich: (häufigste Auswahl) Wählen Sie einen **Tag** und eine**Uhrzeit aus**<br>○ Monatlich: Wählen Sie **Tag** und **Uhrzeit**aus<br>○ Regelmäßig: Wählen Sie ein **Wiederholungsintervall**, ein **Startdatum** und eine Startzeit aus<br>○ Einmal: Wählen Sie ein **Startdatum** und eine Startzeit aus |
| Tag | Der Tag, an dem die geplante Aufgabe ausgeführt werden soll.<br>Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, werden in diesem Feld die Wochentage angezeigt. Wenn Sie im Feld **Ausführen** die Option **Monatlich** ausgewählt haben, werden in diesem Feld die Tage des Monats angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Planen Sie das CWE-Update so, dass es vor dem Update der NVD-Datenbank ausgeführt wird. Der Standardtag für das NVD-Update ist **Wöchentlich** am **Montag**. |
| Zeit | Die Uhrzeit, zu der die geplante Aufgabe gestartet werden soll.<br>**Hinweis:**<br>Planen Sie das CWE-Update so, dass es vor dem Update der NVD-Datenbank ausgeführt wird. Die Standardzeit für das NVD-Update ist 01:00:00 |
| Integrationsskript | Das Skript zum Abrufen von Daten aus den **Datenquellen**, die in der zugehörigen Liste „Datenquellen“ angegeben sind. |
| Quellenintegration | [Schreibgeschützt] |
| Quelleninstanz | [Schreibgeschützt] |
| Anwendung | [Nur Lesen] Der Name der Anwendung, für die Sie die geplante Aufgabe ausführen. |
| Wiederholungsintervall | Die Anzahl der Tage und Stunden, bevor die geplante Aufgabe erneut ausgeführt wird. Dieses Feld wird angezeigt, wenn **Regelmäßig** in der Liste **Ausführen** ausgewählt wird. |
| Wird gestartet | Datum und Uhrzeit für den Start der regelmäßigen Updates. Dieses Feld wird angezeigt, wenn **Regelmäßig** in der Liste **Ausführen** ausgewählt wird. |
| Bedingt | Das Kontrollkästchen zum Hinzufügen von bedingten Parametern. |
| Bedingung | Die Bedingungen zum Ausführen der geplanten Aufgabe. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Bedingt** aktiviert ist. |
| Berichtsprozessorstrategie | Die Strategie zum Abrufen von Daten und Verarbeiten der geplanten Aufgabe.<br>○ Um Daten aus den Datenquellen in der zugehörigen Liste „ **Datenquellen“** mithilfe des Skripts im Feld „ **Integrationsskript“ abzurufen**, wählen Sie **Datenquellenanhang**aus.<br>○ Um einen benutzerdefinierten Prozessor im **SkriptfeldBerichtsprozessor**auszuwählen, wählen Sie Benutzerdefinierter Berichtsprozessor aus. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Berichtsprozessor-Skript | Das Skript, das ausgeführt werden soll, wenn die geplante Aufgabe ausgeführt wird. Dieses Feld wird angezeigt, wenn **Benutzerdefinierter Berichtsprozessor** in der Liste **„Berichtsprozessorstrategie“** ausgewählt ist. |
| Prozessorwerksskript | Das Skript zum Erstellen des Berichtsprozessors. Dieses Feld wird angezeigt, wenn **Benutzerdefinierter Berichtsprozessor** in der Liste **„Berichtsprozessorstrategie“** ausgewählt ist. |

4. Klicken Sie mit der rechten Maustaste in den Header, um Ihre Änderungen zu **speichern**.
5. Um den Scheduled Job sofort auszuführen, klicken Sie auf **Jetzt ausführen**.
   Sie kehren zur Ansicht „Schwachstellenintegrationen“ zurück.
6. Um den Fortschritt des Imports zu überwachen, wählen Sie erneut die geplante Aufgabe „ **CWE Comprehensive 2000-Integration** “ und dann die Registerkarte Ausführungen der **Schwachstellenintegration** aus.

   Informationen zu den importierten Einträgen finden Sie unter Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an.

### Installieren Sie Vulnerability Response Integration with the NIST National Vulnerability Database

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt NIST National Vulnerability Database (NVD) ordnungsgemäß in Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer dem Schwachstellenmanager in Vulnerability Response oder der App-Sec Manager-Gruppe in Application Vulnerability Responsezu. Weitere Informationen zu Gruppenrollen in Vulnerability Response finden Sie unter, Verwalten Sie Personas und granulare Rollen für Vulnerability Response. Weitere Informationen zu Gruppenrollen in Application Vulnerability Response finden Sie unter Application Vulnerability Response -Benutzergruppen und -Rollen.<br>• Der Schwachstellenmanager oder App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rolle: admin

**Hinweis:**
Nehmen Sie vor dem Ausführen der NVD-Integrationen die erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie die NVD-Integrationen installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Storenach der Anwendung Vulnerability Response Integration with NVD.
4. Wählen Sie die Anwendungskachel aus.
   Detaillierte Informationen zur Anwendung, die Sie installieren, werden angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Wählen Sie **App anfordern**, und geben Sie Ihre Anmeldeinformationen Now Support ein.
6. Wählen **Sie Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance**(Instanz validieren) aus.
8. Wählen Sie **Anforderung aus**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Alle** > **Systemanwendungen** > **Anwendungen** > **Alle**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen **Sie Installieren**aus.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Nächste Maßnahme

Informationen zu Änderungen nach der Erstinstallation finden Sie unter Optionale NVD-Integrationsänderungen und -aktivitäten.

## Aktivieren der NIST National Vulnerability Database–API (Nicht zugeordnete CPE)

Um CPE-Daten (Common Platform Enumeration) für abgerufene CVE-Daten (Common Vulnerabilities and Exposures) zu erfassen, können Sie einen vollständigen Datenimport mit einer geplanten Aufgabe bei Bedarf durchführen.

### Vorbereitungen

Die Integration der National Vulnerability Database Integration (NVD)–API (Unmapped CPE) des National Institute of Standards and Technology (NIST) erfasst Daten (CPE), die ein formales Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat für enthalten Bindung von Text und Tests an einen Namen. Diese Informationen werden in einer zugehörigen Liste für den NVD-Schwachstelleneintragsdatensatz gespeichert.

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration–API (Unmapped CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.

   **Hinweis:**
   Die Integration ist so vorkonfiguriert, dass sie bei Bedarf ausgeführt wird. Durch Aktivieren der Integration wird sie automatisch nach der Integration der NIST NVD Integration-API (nur CVE) ausgeführt. Das Ändern anderer Integrationsparameter erfordert sowohl ServiceNow als auch Vulnerability Response und Fachwissen und kann zu unvollständigen Daten führen.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
   b. Wählen Sie NIST National Vulnerability Database Integration–API (Unmapped CPE) Integration (Nicht zugeordnete CPE-Integration) aus.
   c. Wechseln Sie zur Registerkarte **Integrationsdetails**.
   Unabhängig vom Wert im Feld **Importieren seit** werden die CPEs für alle abgerufenen CVEs abgerufen.
4. Wählen Sie **Jetzt** ausführen aus, um eine erste Integrationsausführung mit vollständigem Support durchzuführen.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt. Informationen zum Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus der NVD-Integration (National Vulnerability Database) an.

## NIST National Vulnerability Database–API aktivieren (nur CPE)

Um CPE-Daten (Common Platform Enumeration) zu erfassen, können Sie einen vollständigen Datenimport mit einer täglichen geplanten Aufgabe durchführen.

### Vorbereitungen

Die Integration mit der National Vulnerability Database Integration (NVD)–API (nur CPE) des National Institute of Standards and Technology (NIST) erfasst (CPE-)Daten, die ein



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

formales Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat für enthält Bindung von Text und Tests an einen Namen. Diese Informationen werden in einer Tabelle für angreifbare Software gespeichert.

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration–API (nur CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
   - Die Integration ist so vorkonfiguriert, dass sie täglich ausgeführt wird. Das Ändern anderer Integrationsparameter erfordert Fachwissen von ServiceNow und kann zu unvollständigen Daten führen.
   - Durch die Aktivierung dieser Integration werden automatisch die Integrationen NIST National Vulnerability Database Integration – API (nur CVE) und NIST National Vulnerability Database Integration – API (Nicht zugeordnetes CPE) aktiviert und das Feld „Ausführen“ auf „On-Demand“ gesetzt.
   - Darüber hinaus löst eine erfolgreiche Integrationsausführung der Integration der NIST National Vulnerability Database-API (nur CPE) automatisch die Integration der NIST National Vulnerability Database-API (nur CVE) aus. Bei erfolgreichem Abschluss der Integration der NIST National Vulnerability Database-API (nur CVE) wird automatisch die Integration der NIST National Vulnerability Database-API (nicht zugeordnetes CPE) ausgelöst.

   **Hinweis:**
   Das Feld Importieren seit Datum in der Integration von NIST National Vulnerability Database Integration – API (nur CPE) ist standardmäßig leer. Lassen Sie das Feld leer, um Daten der letzten 357 Tage abzurufen.

   Um Verlaufsdaten während des ersten Imports aus dem NVD-Scan abzurufen, legen Sie ein Startdatum im Integrationsdatensatz der NIST National Vulnerability Database Integration – API (nur CPE) fest.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
   b. Wählen Sie NIST National Vulnerability Database Integration–API (Nur CPE) Integration aus.
   c. Wechseln Sie zur Registerkarte **Integrationsdetails**.
   d. Legen Sie den Wert des Felds **Importieren seit** auf das früheste Datum fest, das Sie abrufen möchten. Bei jedem erfolgreichen Import wird dieses Datum auf das Datum und die Uhrzeit des ausgewählten Tages zurückgesetzt.
4. Wählen Sie **Jetzt** ausführen aus, um eine erste Integrationsausführung mit vollständigem Support durchzuführen.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt. Informationen zum Status der Integrationsausführung finden Sie unter Zeigen Sie den Ausführungsstatus der NVD-Integration (National Vulnerability Database) an.

### Optionale NVD-Integrationsänderungen und -aktivitäten

Konfigurieren Sie optionale Änderungen speziell für die NVD-Integrationen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Ändern anderer NVD-Integrationseinstellungen als die hier aufgeführten erfordert fortgeschrittene Kenntnisse von ServiceNow und Vulnerability Response und geht über den Umfang der Produktdokumentation hinaus.

### Führen Sie einen manuellen NVD-Integrationsimport durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie einen vollständigen Datenimport unabhängig von der täglichen oder wöchentlichen geplanten Aufgabe durchführen.

#### Vorbereitungen

**Hinweis:**
Die Integrationen NIST National Vulnerability Database Integration-API (nur CPE) und NIST National Vulnerability Database Integration-API (Unmapped CPE) sind standardmäßig inaktiv. Weitere Informationen finden Sie unter NIST National Vulnerability Database–API aktivieren (nur CPE) und Aktivieren der NIST National Vulnerability Database–API (Nicht zugeordnete CPE).

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie und Integration aus, z. B. die Integration der NIST National Vulnerability Database Integration – API (nur CVE).
3. Wählen Sie **Jetzt ausführen**.

   **Hinweis:**
   Wenn die Integration der NIST National Vulnerability Database Integration-API (Unmapped CPE) aktiviert ist, werden die zugehörigen CPE-Daten in der zugehörigen Liste „Angreifbare Software“ des NVD-Schwachstelleneintrags gespeichert. Weitere Informationen finden Sie unter Vulnerability Response Felder des Formulars „Schwachstelle“..

4. Informationen zu Integrationsausführungsstatus finden Sie unter, Zeigen Sie den Ausführungsstatus der NVD-Integration (National Vulnerability Database) an.

### Zeigen Sie den Ausführungsstatus der NVD-Integration (National Vulnerability Database) an

Verwenden Sie die zugehörige Liste „Ausführungen von **Schwachstellenintegrationen“**, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Korrekturentscheidungen zu treffen.

#### Vorbereitungen

So zeigen Sie den Ausführungsstatus der NVD-Integration an:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vulnerability Response und die Anwendung Vulnerability Response integration with NVD integration müssen installiert und konfiguriert sein.
- Die NVD-Integrationsimporte müssen ausgeführt werden. Die Integration der NIST National Vulnerability Database Integration-API (nur CVE) wird standardmäßig ausgeführt.

**Hinweis:**
Die Integrationen NIST National Vulnerability Database Integration-API (nur CPE) und NIST National Vulnerability Database Integration-API (Unmapped CPE) sind standardmäßig inaktiv. Weitere Informationen finden Sie unter NIST National Vulnerability Database–API aktivieren (nur CPE) und Aktivieren der NIST National Vulnerability Database–API (Nicht zugeordnete CPE).

Erforderliche Rolle: sn_vul.vulnerability_admin oder App-Sec Manager

### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter.

Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn der letzte verarbeitete Datensatz älter als eine Stunde ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Wenn Sie das Statusdiagramm der NVD-Integrationsausführung nicht verwenden, Navigieren Sie zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie einen **Link** für eine Integration aus.
3. Wählen Sie die zugehörige Liste „ **Schwachstellenintegrationsausführungen“** aus.
4. Vergewissern Sie sich, dass alle Importe erfolgreich waren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Trouble?**

Zu den häufigsten Ursachen für eine fehlgeschlagene Ausführung gehören:

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

Wenn eine dieser Bedingungen auftritt, wählen Sie **Jetzt ausführen**aus, und führen Sie die Integration erneut aus.

**Zugehörige Informationen**

Vulnerability Response Felder des Formulars „Schwachstelle“.

### Fügen Sie CVEs zu Drittparteieinträgen hinzu

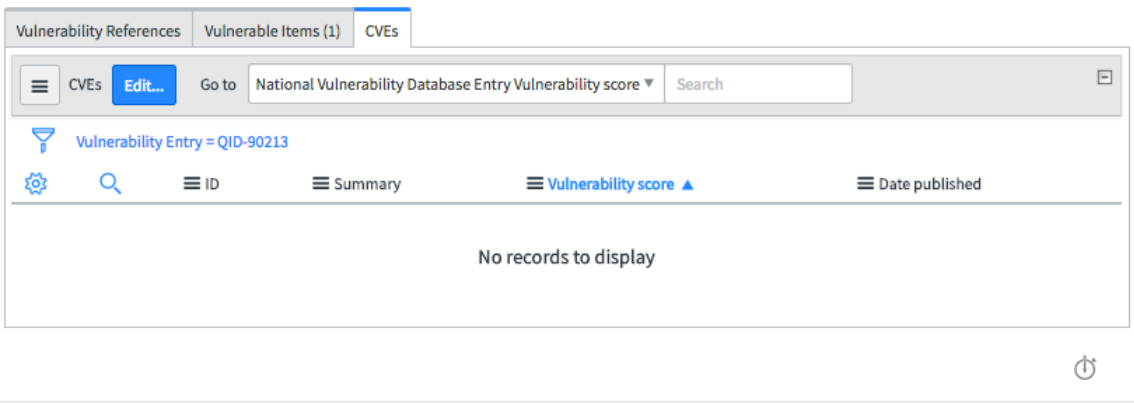
Informationen zu allgemeinen Schwachstellen und Gefährdungen (CVE) können sich auf eine einzelne Drittpartei-Schwachstelle beziehen. Sie wird normalerweise während eines Drittanbieterintegrationsimports hinzugefügt. Sie können jedoch mehrere CVEs (Schwachstellen) manuell hinzufügen.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei**.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie auf die Registerkarte **CVEs** der zugehörigen Liste.




4. Klicken Sie auf **Bearbeiten**.
5. Wählen Sie aus, welche CVEs hinzugefügt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können Bedingungsfilter verwenden, um die CVE-Sammlung zu verfeinern.

6. Klicken Sie auf **Speichern**.

**Zugehörige Informationen**

Vulnerability Response Felder des Formulars „Schwachstelle“.

### Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder von Drittparteien importiert wurden, um zu entscheiden, ob eine Korrekturaufgabe eskaliert werden soll.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken**.

   Weitere Informationen zu bestimmten Feldern finden Sie unter Vulnerability Response Felder des Formulars „Schwachstelle“..

   Die folgenden Bibliotheken sind verfügbar:

| Bibliotheken | Beschreibung |
|---|---|
| NVD | Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken, einschließlich Exploits. |
| CWE | Liste der von der Community entwickelten Softwareschwachstellentypen.<br><br>Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur als Referenz. |
| Drittpartei | Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste der zugehörigen Referenzen, angreifbaren Elemente, Exploits und CVEs. |

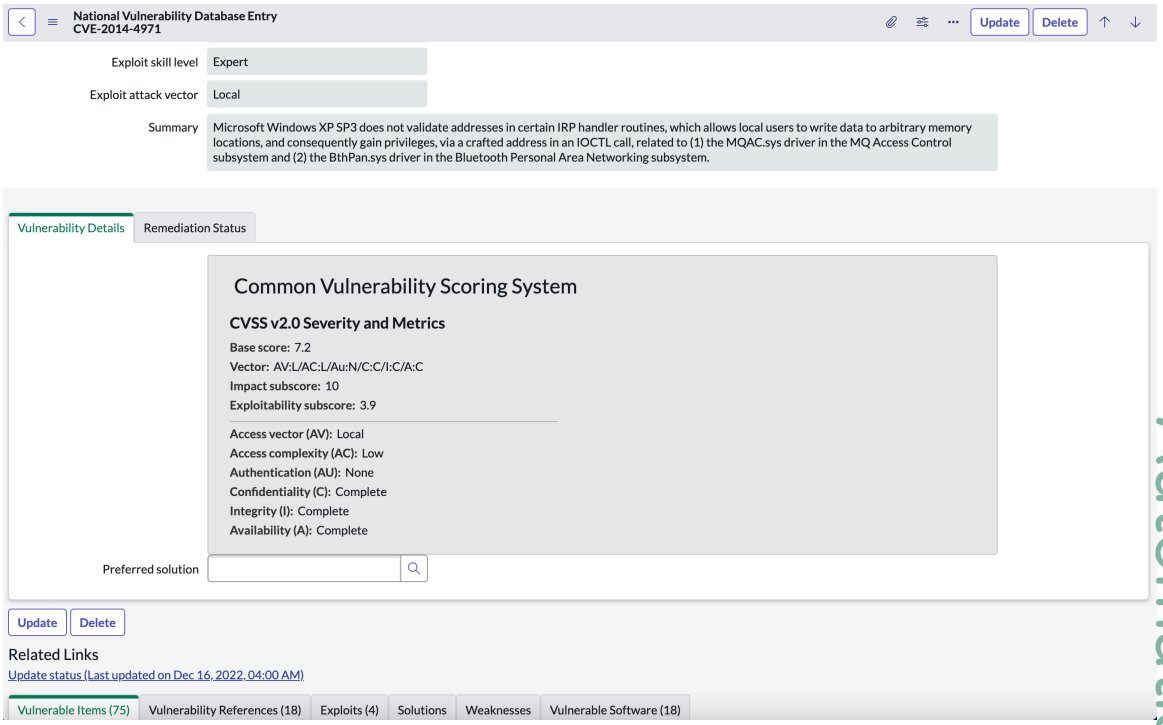
2. Wählen Sie eine Bibliothek aus, um Schwachstellen anzuzeigen.
3. Klicken Sie auf einen Link in der Liste, um einen Datensatz zu öffnen.

   Ein CVE-Datensatz in der Bibliothek „National Vulnerabilities Database Entries“. Weitere Informationen finden Sie unter **Zugehörige Links**. Nach einem Datenimport können Sie eine Schwachstelle auswählen und ihre Beziehungen zu angreifbaren Elementen, Exploits, möglichen Lösungen, potenziellen Patches und Verweisen auf KB-Artikel in der HI



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Knowledge Base untersuchen. Wenn Vulnerability Solution Management installiert ist, können Sie eine bevorzugte Lösung für NVD-Datensätze anzeigen, sofern eine verfügbar ist.




## Integration von CISA Known Exploit Vulnerability (KEV)

Die Vulnerability Response -Integration mit dem KEV-Katalog (CISA Known Exploited Vulnerabilities) erfasst Daten, damit Sie diese Schwachstellen effektiv priorisieren und beheben können.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

CISA ermöglicht Behörden und Unternehmen die dringende und priorisierte Korrektur von aktiv ausgenutzten Schwachstellen.

## Über CISA

Die Cybersecurity & Infrastructure Security Authority (CISA) ist eine US-Behörde für Cybersicherheit und Infrastruktursicherheit, die einen Bericht über die am häufigsten ausgenutzten Schwachstellen veröffentlicht. Die Lösung lässt sich problemlos in Vulnerability Response integrieren, um CVE-Schwachstellen (Common Vulnerabilities and Exposures) abzubilden und die Daten in Ihrer Instanz anzureichern. Für diese Informationen wird dann ein Rollup in die Tabelle „Drittpartei-Schwachstelleneinträge“ durchgeführt. Das früheste Fälligkeitsdatum wird für den Rollup zu den angreifbaren Elementen berücksichtigt.

**Hinweis:**
Das Kontrollkästchen **CISA** vorhanden für von CISA abgerufene CVEs.

Aus der CISA-Integration abgerufene Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CVE-ID
- Fälligkeitsdatum
- Hinzugefügt am
- Lieferant/Projekt
- Produkt
- Known Ransomware (ab v21.0 von Vulnerability Responsewird ein neues Feld „ **Known To Be Used in Ransomware Kampagnen** “ aus dem CISA-Katalog für bekannt ausgenutzte Schwachstellen (KEVs) erfasst. Dies wird durch die Kennzeichnung des Felds **Known Ransomware** in der Datenbanktabelle „National Vulnerability Entry“ (Nationaler Schwachstelleneintrag) angezeigt. Die Kennzeichnung wird auf der Ebene von Common Vulnerabilities and Exposures (CVE) festgelegt und per Rollup zum Drittparteieintrag (TPE) zusammengefasst.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

## Geplante Aufgaben

Die CISA-Integration wird automatisch als tägliche regelmäßige Aufgabe aufgerufen. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

## Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Vulnerability Response v16.5, v18.0<br><br>Vulnerability Response Integration mit CISA v1.0, v1.2 | |

## Anzeigen der CISA-Integration

Um die CISA-Integration anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen** > **CISA Known Exploit Vulnerability-Integration**.

Die folgenden Integrationen sind im Basissystem enthalten.

**Hinweis:**
Standardmäßig ist nur die CISA-Integration aktiv.

### CISA-Integration

| Integration | Beschreibung |
|---|---|
| Integration von Cybersicherheit und Infrastruktursicherheitsbehörde (CISA). | Ruft CISA-Schwachstellendaten (CVE) ab und erweitert die vorhandenen Schwachstellendaten. Diese Integration wird automatisch auf die tägliche Ausführung festgelegt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an.

### Vorbereitung der CISA-Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die CISA Known Exploited Vulnerability-Integration setzt voraus, dass Sie mit der Cybersecurity & Infrastructure Security Authority (CISA) vertraut sind.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Nehmen Sie vor dem Ausführen der CISA-Integration die erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Installieren Sie die Anwendung ServiceNow® Vulnerability Response Integration with CISA

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit der Berater für bekannt genutzte Schwachstellen der Cybersecurity & Infrastructure Security Authority (CISA) in Vulnerability Responseintegriert werden kann. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response Integration with NVD installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren Sie Vulnerability Response Integration with the NIST National Vulnerability Database. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer dem Schwachstellenmanager in Vulnerability Responsezu. Weitere Informationen zu Gruppenrollen in Vulnerability Response finden Sie unter, Verwalten Sie Personas und granulare Rollen für Vulnerability Response.<br>• Der Schwachstellenmanager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie Vulnerability Response integration with CISA installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in [ ServiceNow Storenach der Anwendung Vulnerability Response integration with CISA.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Wählen Sie **App anfordern aus**, und geben Sie Ihre Anmeldeinformationen Now Support ein.
6. Wählen **Sie Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance**(Instanz validieren) aus.
8. Wählen Sie **Anforderung aus**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie dann **Installieren**aus.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Nächste Maßnahme

**Hinweis:**
Für die CISA -Integration ist keine Konfiguration erforderlich.

## Informationen zur Integration des Exploit Prediction Scoring System (EPSS).

Übersicht über die EPSS-Integration mit Vulnerability Response.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Übersicht

Die Integration des Exploit Prediction Scoring System (EPSS) importiert EPSS-Daten im Zusammenhang mit allgemeinen Schwachstellen und Gefährdungen (CVEs) aus First.org, um Schwachstellen zu priorisieren und zu beheben. Weitere Informationen finden Sie unter https://www.first.org . Das Exploit Prediction Scoring System (EPSS) ist eine datengesteuerte Maßnahme zur Schätzung der Wahrscheinlichkeit, dass eine Softwareschwachstelle ausgenutzt wird. Das EPSS-Modell erzeugt eine Wahrscheinlichkeitspunktzahl zwischen 0 und 1 (0 und 100 %). Je höher die Punktzahl, desto größer die Wahrscheinlichkeit, dass eine Schwachstelle ausgenutzt wird.

Datenimporte aus der EPSS-Integration ergänzen die NVD-Daten in Ihrer Instanz weiter. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration als Teil der Ersteinrichtung von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Wichtig:**
Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist VR.System. Ändern Sie diesen Wert nicht.

## Anfänglicher Import von Daten mit der EPSS-Integration

1. Führen Sie einen ersten Import von EPSS-Daten mit der First.org-EPSS-Integration durch. Weitere Informationen finden Sie unter Konfigurieren Sie eine regelmäßige Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.

   **Wichtig:**
   Sie führen standardmäßig **tägliche** EPSS-Aktualisierungen aus dem Integrationsdatensatz durch und müssen sie konfigurieren, wenn sie als geplante Aufgabe ausgeführt werden soll.

2. Bibliotheken von Drittanbietern werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

   **Wichtig:**
   Es wird empfohlen, die Integrationen der NIST National Vulnerability Database Integration – API (nur CVE) vor EPSS durchzuführen.

Führen Sie die EPSS-Importe durch, bevor Sie Schwachstellendaten mit einem Drittanbieterprodukt importieren. Bibliotheken von Drittanbietern werden als regelmäßige Aufgaben aktualisiert. Weitere Informationen zu Drittanbieterintegrationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen.

**Wichtig:**
Die folgende Integration ist im Basissystem enthalten. Die Integration ist standardmäßig aktiviert.

Nach der ersten Ausführung führen die geplanten Aufgaben des Basissystems die Integrationen automatisch der Reihe nach aus. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Bei Aktivierung der EPSS-Integration werden die Felder „EPSS-Punktzahl“, „EPSS-Perzentil“ und „EPSS – Zuletzt geändert“ der Tabelle „Schwachstelleneinträge“ hinzugefügt. Für vorhandene CVEs werden diese Felder nach erfolgreichem Abschluss des ersten Importauftrags automatisch aktualisiert. Wenn neue CVEs vorhanden sind, die der Tabelle „Schwachstelleneinträge“ nach Abschluss der geplanten Aufgabe von EPSS hinzugefügt werden, geben die neu hinzugefügten CVEs ihre Quelle als EPSS an. Für die Punktzahlen wird mithilfe des Basissystems `Rollup EPSS score from NVD to TPEs calculator`ein Rollup zu vorhandenen TPEs aus CVEs aus der NVD-Tabelle durchgeführt. Sie können auch den Rechner ändern. Weitere Informationen finden Sie unter Vulnerability Response Rollup-Rechner.

### Zugehörige Informationen

Erstellen Sie einen Vulnerability Response -Rechner

## Konfigurieren Sie eine regelmäßige Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren

Passen Sie die geplante Aufgabe des Basissystems an, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

**Wichtig:**
Sie müssen das Plugin Vulnerability Response integration with CISA (com.snc.vulnerability.cisa) herunterladen und aktivieren, um die EPSS-Integration zu aktivieren.

Im Folgenden finden Sie die Liste der neuen Felder, die in der NVD-Tabelle zum Speichern von EPSS-Daten hinzugefügt wurden.

- EPSS-Punktzahl
- EPSS-Perzentil
- EPSS – Zuletzt geändert

**Hinweis:**
Konfigurieren Sie die Listenansicht oder Formularansicht gemäß der Anforderung, um neu hinzugefügte Felder anzuzeigen.

Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird

Daten, die aus der EPSS-Integration importiert werden, erweitert die NVD-Daten in Ihrer Instanz weiter. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration als Teil der Ersteinrichtung von Vulnerability Response aus und importieren Sie Schwachstellendaten in Ihre Instanz.

**Hinweis:**
Standardmäßig befindet sich die First.org-EPSS-Integration im Status „ **Aktiv** “. Die regelmäßige Aufgabe des Basissystems ist standardmäßig so konfiguriert, dass sie täglich ausgeführt wird.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**.
2. Suchen und wählen Sie First.org EPSS-Integration.
3. Ändern Sie die Felder nach Bedarf.
4. Klicken Sie mit der rechten Maustaste auf den Header, um Ihre Änderungen zu **speichern**.
5. Wählen Sie **Jetzt**ausführen aus, um die geplante Aufgabe sofort auszuführen.
   Sie kehren zur Ansicht „Schwachstellenintegrationen“ zurück.
6. Auswahlvorgang **First.org-EPSS** > **Registerkarte „Ausführungen der Schwachstellenintegration“.** , um den Fortschritt des Imports anzuzeigen.
   Nach erfolgreichem Abschluss der geplanten Aufgabe werden die EPSS-Punktzahlen, das Perzentil und die Zeitstempel der letzten EPSS-Punktzahl der letzten Änderung in den CVEs aktualisiert.

### Nächste Maßnahme

- Weitere Informationen finden Sie unter Fügen Sie der Geschäftsregel des Risikorechners die Bedingung „EPSS-Punktzahl“ hinzu.
- Informationen zu den importierten Einträgen finden Sie unter Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an.

#### Fügen Sie der Geschäftsregel des Risikorechners die Bedingung „EPSS-Punktzahl“ hinzu

Ändern Sie die Geschäftsregel, um die EPSS-Punktzahlbedingung zum Risikorechner hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

**Hinweis:**
Das folgende Verfahren ist erforderlich, damit für die EPSS-Updates für Schwachstellen ein Rolldown zu den angreifbaren Elementen durchgeführt wird.

Erforderliche Rolle: sn_vul.manage_risk_score_configuration

### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business Rule**.
2. Suchen Sie nach **Kennzeichnung für Neuberechnung festlegen**.

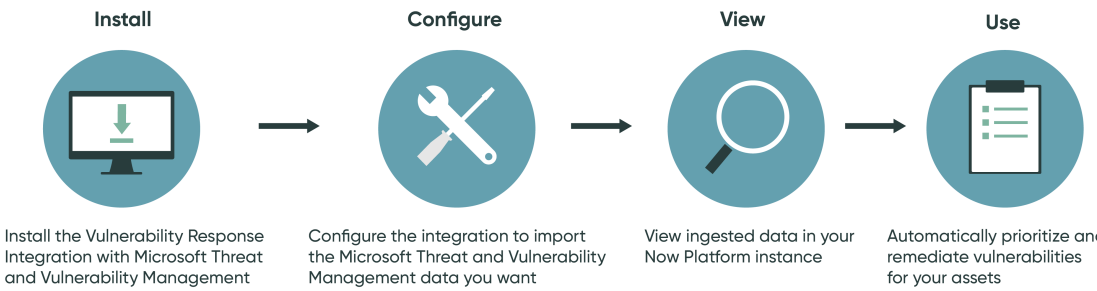
   **Hinweis:**
   Es gibt zwei *Set recalculate flag* Business Rules. Sie können beide verwenden.

3. Navigieren Sie zur Registerkarte Zeitpunkt **für Ausführung**.
4. Wählen **Sie „ODER“** -Klausel hinzufügen aus **, wählen** Sie „ EPSS-Punktzahl “ aus dem Auswahlfeld aus und ändern Sie das Feld „ **Operator** auswählen“.
5. Wählen Sie **Aktualisieren**.

## Informationen zur Integration von Microsoft Threat and Vulnerability Management Vulnerability

Die Anwendung Vulnerability Response integration with Microsoft Threat and Vulnerability Management (MS TVM) verwendet Daten, die aus MS TVM importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement von ServiceNow Storeverfügbar.

Sie können die MS TVM Vulnerability-Integration verwenden, um Scanner-Daten von Drittanbietern zu Ihren Assets und Schwachstellen zu importieren. Sie können dann Berichte über Schwachstellen und angreifbare Elemente in den Vulnerability Response -Dashboards anzeigen.




## Verfügbare Versionen

| Release-Version | Versionsinformationen |
|---|---|
| Vulnerability Response Integration mit MS TVM v2.2 | Weitere Informationen zu veröffentlichten Versionen der Vulnerability Response-Anwendung, zur Kompatibilität und zu Schemaänderungen finden Sie im Artikel |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Release-Version | Versionsinformationen |
| --- | --- |
| | Vulnerability Response Compatibility Matrix and Release Schema Changes [KB0856498] (Kompatibilitätsmatrix und Release-Schemaänderungen) in der HI Knowledge Base . |

## Domänentrennung und MS TVM

Importieren Sie Schwachstellenintegrationsdaten in eine angegebene Domäne, indem Sie einen Benutzer in dieser Domäne zuweisen, der die Integrationen ausführen soll. Informationen zum Erstellen von domänengetrennten Importen für die MS TVM Vulnerability-Integration finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

## Begriffe und Hauptfunktionen der Integrationen

### Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle von einem Drittanbieter-Scanner wird mit einem vorhandenen Asset (Konfigurationselement) in Ihrem CMDBabgeglichen. Das MS TVM-Produkt bezeichnet diese Übereinstimmungen als Schwachstellen.
- Eine importierte Schwachstelle von einem Drittanbieter-Scanner stimmt nicht mit einem vorhandenen Asset in Ihrem CMDBüberein. In diesem Fall wird auch ein nicht abgeglichenes Configuration Item (CI) mit einem angreifbaren Element erstellt.

  Verwenden Sie die Identification and Reconciliation Engine (IRE), um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“..

### Schwachstelleneinträge von Drittparteien

Schwachstelleneinträge von Drittparteien werden aus Scannern von Drittparteien wie MS TVM importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in Ihrer Now Platform -Instanz aufgeführt. Außerdem werden Einträge in der National Vulnerability Database (CVE) aus MS TVM importiert. Die Exploit-Informationen, die diesen beiden Eintragstypen zugeordnet sind, stammen aus MS TVM. Diese Exploit-Informationen können zur Risikoberechnung verwendet werden.

**Hinweis:**
Eine Drittpartei-Schwachstelle wird nur für Schwachstellen abgerufen, denen kein CVE zugewiesen ist. MS TVM kann einen temporären Namen für die Schwachstelle hinzufügen, z. B. `TVM-XXXX-XXXX`. Dieser Name wird aktualisiert, nachdem eine CVE-ID zugewiesen wurde.

### Konfigurationselement (Configuration Item, CI)

CIs sind die vorhandenen Assets, die in Ihrem CMDBaufgeführt sind.

### Erkanntes Element

Erkannte Elemente sind die Assets, die aus dem MS TVM-Computerimport erfasst werden und vorhandenen CIs in CMDBentsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse Nicht abgeglichen von CMDBerstellt. Aktivieren Sie das CMDB CI Class Models-Plugin. Die Identification and Reconciliation Engine (IRE) erstellt CIs mithilfe neuer Klassen. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die erkannten Elementdatensätze aktualisiert, um diesen Status widerzuspiegeln. Erkannte Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

**CI-Suchregeln**

Wenn Daten aus MS TVM importiert werden, verwendet Vulnerability Response automatisch Computerdaten (Asset-Daten), um nach Übereinstimmungen in CMDBzu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden.

**Instanz**

Eine Instanz verweist auf mehrere Konten von MS TVM. Jeder Account kann eine Instanz in der MS TVM-Anwendung sein.

**Integration**

Eine Integration ist eine regelmäßige Aufgabe, die Informationen aus einer Drittanbieterquelle abruft, z. B. die Integration der MS TVM-Computer.

**Bereitstellung**

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne Integration als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen von MS TVM in Ihrer Umgebung haben.

Die MS TVM-Integration umfasst auch die folgenden wichtigen Funktionen:

- Sie können die Assets in Ihrer Umgebung identifizieren und die CIs für Ihre vorhandenen erkannten Elemente, angreifbaren Elemente und Erkennungsdatensätze aktualisieren, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufträge für alle MS TVM-Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben auch bei Bedarf ausführen.
- Sie können angreifbare Elemente gruppieren.
- Sie können CI-Suchregeln konfigurieren, um zu definieren, wie die Asset-Daten aus Drittanbieterquellen zum Identifizieren von CIs in CMDBverwendet werden.

## Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Administrator**

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung MS TVM zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**sn_vul.vulnerability_admin**

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der MS TVM-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle Vulnerability Response Anwendungen und Regeln für installierte Drittanbieterintegrationen.

**sn_vul_msft_tvm.configure_integration**

Diese Rolle enthält die granulare Rolle sn_vul_msft_tvm.read_integration. Benutzer mit dieser Rolle können die Vulnerability Response-Integration mit der Anwendung Microsoft Threat and Vulnerability Management konfigurieren.

**sn_vul_msft_tvm.read_integration**

Benutzer mit dieser Rolle können nur die Datensätze der Vulnerability Response-Integration mit der Microsoft Threat and Vulnerability Management-Anwendung anzeigen.

**Vulnerability Response-Gruppe**

Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.

## MS TVM-Integrationen

Mehrere Quellen werden für alle MS TVM-Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in Vulnerability Responsehinzufügen und bereitstellen. Sie installieren und konfigurieren auch die Anwendung Vulnerability Response Integration with the MS TVM über den Setup-Assistenten.

Um die MS TVM-Integrationen anzuzeigen, navigieren Sie zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integrationen**. Vulnerability Response bietet Integrationen mit MS TVM-Endpunkten, um die Daten gemäß den geplanten Zeitintervallen zu importieren. Die folgenden Integrationen sind im Basissystem enthalten.

### MS TVM-Integrationen

| Ausführungssequen | Zeitplan | Integration | Beschreibung |
|---|---|---|---|
| 1 | Täglich | Integration von Microsoft TVM-Empfehlungen | Ruft eine Liste aller umsetzbaren Sicherheitsempfehlungen zur Behebung der Schwachstellen ab. |
| 2 | Täglich | Integration von Microsoft TVM Vulnerability (CVE). | Ruft eine Liste der Einträge der nationalen Schwachstellendatenbank und der Schwachstelleneinträge von Drittparteien sowie deren Exploit-Informationen ab. |
| 3 | Täglich | Microsoft TVM Machines-Integration | Ruft alle Asset-Daten (Computerdaten), |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**MS TVM-Integrationen (Fortsetzung)**

| Ausführungssequer | Zeitplan | Integration | Beschreibung |
|---|---|---|---|
| | | | einschließlich Computer-Tags, aus Microsoft TVM ab und verarbeitet sie in Ihrer Instanz. |
| 4 | Wöchentlich<br>**Hinweis:** Nach der Installation wird diese Integration nach dem Computerimport automatisch ausgeführt. | Microsoft TVM Machines-Schwachstellenintegration (vollständiger Import) | Ruft alle offenen Schwachstellen in allen Assets ab. |
| 5 | Täglich | Microsoft TVM Machines-Schwachstellenintegration (Delta-Import) | Ruft alle Informationen ab, die sich im vollständigen Import von Schwachstellen der Organisation geändert haben, einschließlich der neuen, behobenen und aktualisierten Schwachstellen. |

Angreifbare Elemente werden gemäß den von Ihnen festgelegten Gruppenregeln in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Vulnerability Response Übersicht über Zuweisungsregeln.

## CI-Suchregeln

Wenn Daten aus MS TVM importiert werden, verwendet Vulnerability Response automatisch Computerdaten (Asset-Daten), um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie den VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

**Hinweis:**
Sobald Sie eine Regel entfernt haben, können Sie sie nicht wiederherstellen. Anstatt eine vorhandene Regel zu entfernen, sollten Sie sie deaktivieren.

Die folgenden MS TVM-Suchregeln werden mit dem Basissystem geliefert:

- MAC_ADDRESS
- FQDN
- IP



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können mehrere Werte für IP_ADDRESS und MAC_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich.

### Erkannte Elemente

Sie können die CIs anzeigen, die während eines Imports aus der MS TVM Machines-Integration erkannt wurden.

**Hinweis:**
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen finden Sie unter Erkannte Elemente.

### Computer-Tags

Computer-Tags, auch als Host-Tags bezeichnet, werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie weisen Ihren Computern Tags zu.

Alle Computer-Tags werden als Teil der MS TVM Machines-Integration importiert. Computer-Tags werden im Allgemeinen zum Filtern in Vulnerability Response Zuweisungsregeln und Regeln für Schwachstellengruppen verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.

**Hinweis:**
Führen Sie die MS TVM-Computerintegration aus, bevor Sie Vulnerability Response Zuweisungs- oder Korrekturaufgabenregeln in der Anwendung Vulnerability Response erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein Paris-Tag erstellt wird, kann kein PARIS-Tag in der Computer-Tag-Tabelle gespeichert werden. Paris und PARIS werden vom System als dasselbe Computer-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das gespeichert und erkannt wird.
- Die Verwendung von Computer-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Gruppenschlüssel sind Spalten in der Korrekturaufgabentabelle, während Maschinen-Tags nur zur Verwendung im Bedingungsgenerator vorgesehen sind.
- Computer-Tags werden von der globalen Systemeigenschaft sn_vul.import_host_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „ true “ festgelegt. Durch das Deaktivieren von Tags werden sie in allen Now Platform® Instanzen deaktiviert.

### Nächste Schritte

Nachdem Sie die Integration von Vulnerability Response mit Microsoft Threat and Vulnerability Management aus dem ServiceNow® Storeheruntergeladen haben, werden Installation und Konfiguration vom Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with the MS TVM mithilfe des Setup-Assistenten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitung auf die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

Sie können sich auf die Integration von ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability vorbereiten, indem Sie Setup-Aufgaben ausführen.

## Bevor Sie eine Prüfliste verwenden

Um Vulnerability Response Integration with the MS TVM zu installieren und zu konfigurieren, können Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Now Platform® -Instanz importieren.

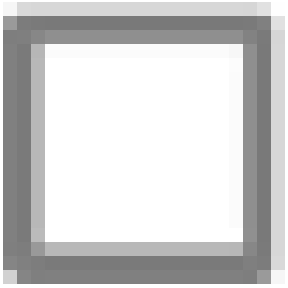
### Prüfliste zur Vorbereitung der Integration

| Aufgabe | Beschreibung |
|---|---|
| | Vergewissern Sie sich, dass Sie über eine der folgenden Informationen verfügen:<br>• ClientSecret, ClientId und TenantId für Ihr MS TVM-Konto<br>• Benutzername, Passwort, Client-ID und Mandanten-ID für Ihr MS TVM-Konto. Wie Sie diese Informationen erhalten, erfahren Sie unter Richten Sie Microsoft Azure für die MS TVM-Integration ein. |
| | Wenn noch nicht installiert und aktiviert, installieren Sie die Anwendung Vulnerability Response, bevor Sie die Drittanbieteranwendung installieren.<br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 14.0 von Vulnerability Response oder höher. |
| | Wenn Sie die Anwendung noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response integration with MS TVM in Ihre Instanz Now Platform® ] herunter.<br>Weitere Informationen finden Sie unter . |
| | Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren werden.<br>Vergewissern Sie sich, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support von ServiceNow®. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

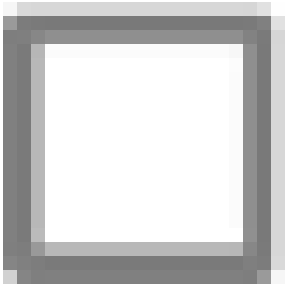
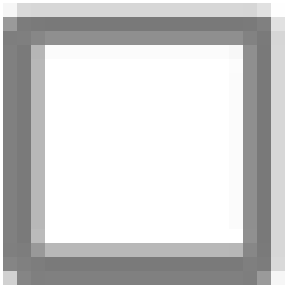
**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

| Aufgabe | Beschreibung |
| --- | --- |
|  | Vergewissern Sie sich, dass Sie über die folgenden Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu beheben:<br>**Administrator**<br>Verwendet den Setup-Assistenten, um die Vulnerability Response-Integration mit der MS TVM-Anwendung zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.<br>**sn_vul.vulnerability_admin**<br>Schließt die Konfiguration der MS TVM-Integration ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administrator konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittanbietern.<br>**sn_vul_msft_tvm.configure_integration**<br>Konfiguriert die MS TVM-Schwachstellenintegration. Diese Rolle enthält die granulare Rolle sn_vul_msft_tvm.read_integration.<br>**sn_vul_msft_tvm.read_integration**<br>Zeigt Datensätze der MS TVM Vulnerability-Integration an (liest sie).<br>**Vulnerability Response-Gruppe**<br>Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.<br>Wenn dies noch nicht geschehen ist, ziehen Sie es möglicherweise vor, zusätzliche Gruppen zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen .<br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

| Aufgabe | Beschreibung |
|---|---|
|  | Installieren Sie die Vulnerability Response -Integration mit NVD, und führen Sie die NIST National Vulnerability Database Integration - API aus (nur CVE). |
|  | Um die Leistung beim ersten Import zu verbessern, können Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren.<br>• Deaktivieren Sie Schwachstellenrechner, wenn Sie sie nicht verwenden. Diese und die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Weitere Informationen finden Sie unter Standardschwachstellenrechner deaktivieren, wenn er nicht verwendet wird.<br>• Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung der Erfassung auswirken kann. |

Sie sind bereit für Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with the MS TVM mithilfe des Setup-Assistenten.

### Richten Sie Microsoft Azure für die MS TVM-Integration ein

Richten Sie Ihr -Konto im Azure-Portal von Microsoft ein, um remote auf die Microsoft Threat and Vulnerability Management-API (MS TVM) zuzugreifen. Sie benötigen dieses Konto, damit Sie auf den MS TVM-Mandanten zugreifen und Informationen zu Computern, Schwachstellen und Sicherheitsempfehlungen sammeln können.

#### Vorbereitungen

Erforderliche Rolle: Microsoft Azure-Portaladministrator.

#### Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Setup-Aufgaben in Ihrem Microsoft Azure-Portal aus, bevor Sie die Anwendung ServiceNow® für diese Integration installieren.

Informationen zum Überprüfen, ob Sie Zugriff auf die aktuellen Inhalte haben, finden Sie auf der Microsoft -Dokument-Website. Wenn Sie im Azure-Portal von Microsoft keine Anwendungs-ID für die OAuth 2.0-Authentifizierung erstellt haben, führen Sie die Schritte in diesem Verfahren aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

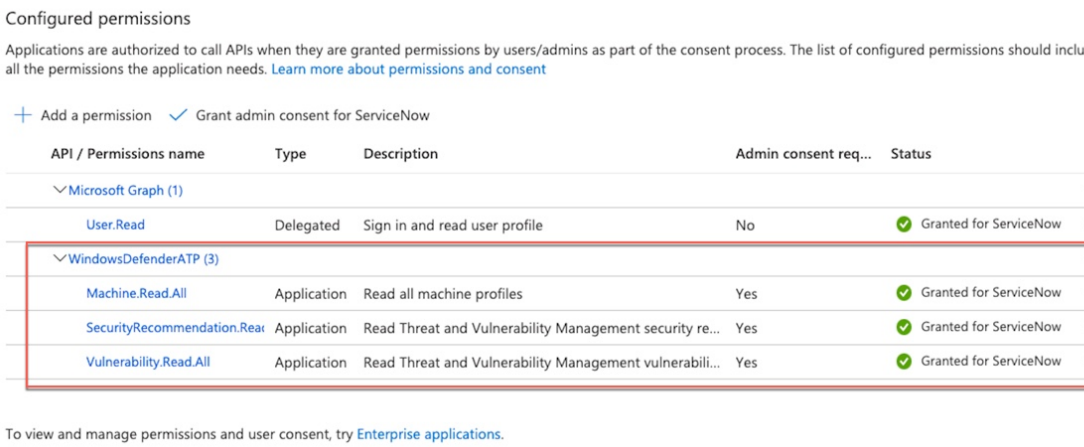
## Prozedur

1. Melden Sie sich beim Microsoft Azure-Portal mit den Anmeldeinformationen Ihres Azure-Portaladministrators an.
2. Klicken Sie im linken Navigationsbereich der Startseite auf **Azure Active Directory**.
3. Klicken Sie im Übersichtsbereich auf **App-Registrierungen (Vorschau)**.
4. Klicken Sie im Bereich App-Registrierungen (Vorschau) auf **Neue Registrierung**.
   Das Formular „Anwendung registrieren“ wird angezeigt.
5. Füllen Sie die Felder des Formulars aus.

**Anwendungsformular registrieren**

| Feld | Beschreibung |
|---|---|
| **Name** | Name für die Anwendung. In diesem Beispiel wird ServiceNow MS TVM-Integration eingegeben. |
| **Unterstützte Account-Typen** | Klicken Sie für diesen Account unter Unterstützte Account-Typen auf **Accounts nur in diesem Organisationsverzeichnis (nur ServiceNow – Einzelmandant)**. |
| **Umleitungs-URL (optional)** | Wenn Sie einen Wert für dieses Feld eingeben, wird er von der Integration nicht verwendet. |

6. Klicken Sie auf **registrieren**.
   Die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) werden erstellt. Geben Sie diese Werte auf der Konfigurationsseite in die Felder **Client-ID** und **Mandanten-ID** während des Konfigurationsschritts im Setup-Assistenten für die ServiceNow VR-TVM-Integration ein. Dieser Schritt wurde in Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with the MS TVM mithilfe des Setup-Assistentenbeschrieben.
7. Wenn die Anwendungs-ID (Client) im Bereich ServiceNow MS TVM-Integration angezeigt wird, klicken Sie auf **API**-Berechtigungen anzeigen.
8. Navigieren zu **Fordern Sie API-Berechtigungen an** > **APIs, die meine Organisation verwendet**, und klicken Sie dann auf **Windows Defender ATP**.
9. Klicken Sie im Bereich ServiceNow MS TVM-Integration – API-Berechtigungen auf Berechtigung **hinzufügen**.
10. Gewähren Sie Lesezugriff auf Computer, Schwachstellen und Sicherheitsempfehlungen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. Klicken Sie **auf Administratoreinwilligung gewähren für**<your organization name> .

**Hinweis:**
Führen Sie die folgenden Aktionen aus, um sich als -Anwendung von einer ServiceNow -Instanz aus zu authentifizieren:

a. Navigieren zu **ServiceNow MS TVM-Integration** > **Zertifikate und Geheimnisse**, und klicken Sie dann auf **Neuer geheimer Clientschlüssel**.

b. Füllen Sie die Felder des Formulars aus.

**Formular „Geheime Clientschlüssel“**

| Feld | Beschreibung |
|---|---|
| Beschreibung | Name der Anwendung. |
| Läuft ab | Ablaufdatum. |

c. Klicken Sie auf **Hinzufügen**.

Das Feld **Wert** wird mit dem neuen geheimen Clientschlüssel ausgefüllt, der Ihr neues Passwort ist.

**Hinweis:**
Sie benötigen dieses Passwort, wenn Sie die Integration in Ihrer Now Platform -Instanz konfigurieren. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with the MS TVM mithilfe des Setup-Assistenten.

d. Bewahren Sie dieses Passwort an einem sicheren Ort auf. Nachdem Sie diese Seite verlassen haben, ist dieses Passwort nicht mehr verfügbar.

Sie haben erfolgreich eine Anwendungs-ID für die Authentifizierung im Azure-Portal Microsoft erstellt.

### Nächste Maßnahme
Sie sind bereit, Ihre Now Platform® -Instanz für die Integration einzurichten.

## Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with the MS TVM mithilfe des Setup-Assistenten

Installieren und konfigurieren Sie die Vulnerability Response -Integration mit der Anwendung Microsoft Threat and Vulnerability Management (MS TVM), damit Sie die aus MS TVM importierten Daten verwenden können, um Schwachstellen für Ihre Assets zu priorisieren und zu beheben.

### Vorbereitungen
Bevor Sie ServiceNow® Microsoft Threat and Vulnerability Management Vulnerability Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Microsoft Threat and Vulnerability Management aus dem ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response ] installieren und konfigurieren.

Vergewissern Sie sich vor der Installation der Anwendung MS TVM, dass Sie alle Elemente der Prüfliste Vorbereitung auf die Microsoft Threat and Vulnerability Management-Schwachstellenintegration abgeschlossen haben. Informationen zum Einrichten Ihres Microsoft Azure-Kontos finden Sie unter Richten Sie Microsoft Azure für die MS TVM-Integration ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und Installation der Microsoft Threat and Vulnerability Management-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) zur Konfiguration der Anwendung im Setup-Assistenten nach der Installation.

### Warum und wann dieser Vorgang ausgeführt wird

Führen Sie das folgende Verfahren aus, bevor Sie die MS TVM-Integration installieren und konfigurieren.

**Hinweis:**

Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einiger Zeit werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie die Kachel **„Microsoft Threat and Vulnerability Management“**, und klicken Sie auf **Installieren**.

   Die Anwendung Vulnerability Response Integration with Microsoft Threat and Vulnerability Management, die Sie aus dem ServiceNow Store heruntergeladen haben, ist installiert.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.

### Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation im Setup-Assistenten zu **Integrationskonfiguration** > **Scannerintegrationen** im Setup-Assistenten, um mit der Konfiguration fortzufahren. Weitere Informationen zu den Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die MS TVM-Schwachstellenintegration mit dem Setup-Assistenten.

### Datenabrufeinstellungen für die Microsoft Threat and Vulnerability Management-Integration

Sie können Datenabrufeinstellungen verwenden, um Typ und Umfang der Daten zu bestimmen, die Sie aus der ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability-Integration in Ihre Now Platform® Instanz importieren möchten.

Datenabrufeinstellungen helfen Ihnen, die Daten zu steuern, die Sie importieren möchten. Sie können die Werte dieser Filter in Integrationsinstanzen festlegen. Um die Integrationsinstanzen anzuzeigen, navigieren Sie zu **Microsoft Threat and Vulnerability Management Schwachstellenintegration** > **Integrationsinstanzen** und klicken Sie auf Ihre MS TVM-Integration.

Klicken Sie auf der Seite „ **Integrationsinstanz“ auf Integrationsinstanzparameter**, um eine Liste von Parametern anzuzeigen, oder klicken Sie auf die Registerkarte **Schwachstellenintegrationen**, um einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Datenabrufeinstellungen und Filter für die MS TVM-Integrationen in Ihrer Now Platform -Instanz

Die folgenden Einstellungen sind für die MS TVM-Integrationen in Ihrer Now Platform -Instanz verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Now Platform -Instanz angezeigt. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardeinstellungen belassen.

MS TVM

**vi_size_limit**

Definiert die Anzahl der Datensätze für angreifbare Elemente, die in den Ergebnissatz der MS TVM-Integration für maschinelle Schwachstellen aufgenommen werden sollen. Diese Einstellung muss im Format int32 vorliegen. Der Standardwert beträgt 2.000.

**Schwachstellen_Größe_Grenze**

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz aus der CVE-Integration (MS TVM Vulnerability) aufgenommen werden sollen. Diese Einstellung muss im Format int32 vorliegen. Der Standardwert beträgt 2.000.

**Recommendations_size_limit**

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz aus der Integration von MS TVM-Empfehlungen aufgenommen werden sollen. Diese Einstellung muss im Format int32 vorliegen. Der Standardwert beträgt 2.000.

**asset_size_limit**

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz der MS TVM Machines-Integration aufgenommen werden sollen. Diese Einstellung muss im Format int32 vorliegen. Der Standardwert beträgt 2.000.

**machine_filter**

Filtert die Computer, die von MS TVM stammen. Dieser Filter wird auf die Integration von MS TVM-Computern angewendet. Der Standardwert ist das Einbeziehen von Computern, auf denen „onBoardingStatus“ gleich „onBoarded“ ist.

### REST-Nachrichten für die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

Sie können die REST-Nachrichten für die Schwachstellenintegration von ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) verwenden, um Aufrufe an die MS TVM-API zu tätigen.

## MS TVM-Zugriffstoken

Sie können auch die REST-Nachrichten für das MS TVM-Zugriffstoken verwenden, um das Zugriffstoken aus der MS TVM-API abzurufen, damit Sie REST API-Anforderungen authentifizieren können. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Authentifizierungsanforderungen an MS TVM aus.

## MS TVM-Integration

Sie können die REST-Nachricht für die MS TVM-Integration verwenden, um Informationen aus MS TVM abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an MS TVM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### REST-Methoden

| REST-Methode | Beschreibung der Methode |
|---|---|
| GET-Schwachstellen | Ruft Informationen zu Schwachstellen und Exploits aus MS TVM ab. |
| GET Software-Schwachstellen nach Computer | Ruft alle offenen Schwachstellen ab. |
| GET-Empfehlungen | Ruft die Liste aller umsetzbaren Sicherheitsempfehlungen ab, die sich auf die Organisation auswirken. |
| GET-Computer | Ruft die Sammlung von Assets ab. |
| GET Software-Schwachstellen-Changes nach Computer | Ruft alle Informationen ab, die sich im vollständigen Import von Schwachstellen der Organisation geändert haben, einschließlich neuer, behobener und aktualisierter Schwachstellen. |

### Datentransformation für die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

Nachdem Sie die Daten identifiziert haben, die Sie importieren möchten, werden die Daten aus der Anwendung ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz transformiert.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen transformieren importierte Microsoft Schwachstellenschweregrade von Drittparteien in Standardschweregrade für die Verarbeitung in Ihrer Instanz. Weitere Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.

## Import von MS TVM-Computern

Die Daten von den importierten Computern werden zuerst in die Tabelle „MS TVM-Computerimport“ [sn_vul_msft_tvm_machines_import] geladen.

Die MS TVM-Computertransformation wird verwendet, um die importierten Computerinformationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von MS TVM-Computern verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **Microsoft TVM Machines Transform**.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### MS TVM-Computer transformieren Zuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Eindeutige ID für Assets. Diese ID ist der source_id des erkannten Elementdatensatzes zugeordnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**MS TVM-Computer transformieren Zuordnungsfelder (Fortsetzung)**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_ipaddresses.macAddress | mac_address | MAC-Adresse, die von der API dem Host-MAC-Adressfeld des cmdb_ci-Datensatzes zugeordnet wird. |
| u_ipaddresses.ipAddress | ip_address | IP-Adressfeld, das dem IP-Adressfeld des cmdb_ci-Datensatzes zugeordnet ist. |
| u_lastseen | last_scan_date | Feld, das dem Feld „last_scan_date“ im Datensatz des erkannten Elements zugeordnet ist. |
| u_machinetags | | Tags, die in sn_sec_cmn_host_tag gespeichert sind. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_tag gespeichert. |
| u_osplatform | os | Feld, das dem BS-Feld im cmdb_ci-Datensatz zugeordnet ist. |
| u_computerdnsname | fqdn | Feld, das das dnsname-Feld der API dem fqdn-Feld im cmdb_ci-Datensatz zuordnet. |

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

## Timing und Zweck des MS TVM-Computer-Transformationszuordnungsskripts

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das verwendet wird, um Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host vorhanden ist. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen (sn_vul_msft_tvm). Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

Die MicrosoftTVMMachinsProcessor-Skripteinbindung wird aus dem onBefore-Transformationsskript aufgerufen. Sie übernimmt die Ausgabe der Integration der Microsoft TVM-Computer und wandelt sie in ein CI um. Alle Änderungen an dieser Skripteinbindung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können die Transformation der Daten der Microsoft TVM-Computer in der Tabelle „CI“ und „Erkannte Elemente“ ändern.

## Integration von MS TVM-Schwachstellen

Die importierten Schwachstellendaten werden zuerst in die Tabelle „Microsoft TVM CVE (Schwachstellen)“ [sn_vul_msft_tvm_vulnerabilities_import] geladen.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von MS TVM-Schwachstellen verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **Microsoft TVM Vulnerabilities Transform**.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### Microsoft TVM-Schwachstellen-Transformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Ordnet auf die ID-Spalte des sn_vul_entry-Datensatzes zu. |
| u_severity | source_severity | Ordnet das Feld Schweregrad dem Schweregrad zu. Der Standardwert ist 5. |
| u_publishedon | date_published | Ordnet das Feld u_publishedon dem Veröffentlichungsdatum zu. |
| u_publicexploit | public_exploit | Ordnet den vom Scanner bereitgestellten u_publicexploit der öffentlichen Exploit-Spalte in der Schwachstelleneintragstabelle zu. |
| u_cvssv3 | v3_base_score | Ordnet die cvssv3-Punktzahl der v3-Basispunktzahl im Datensatz des Schwachstelleneintrags zu. |
| u_description | Zusammenfassung | Ordnet die Beschreibung dem Zusammenfassungsfeld im Datensatz des Schwachstelleneintrags zu. |
| u_exploitinkit | malware_kit | Ordnet das Feld u_exploitinkit dem Malware-Kit in der Exploit-Tabelle zu. |
| u_exploittypes | type | Ordnet den Exploit-Typ dem Typ in der Exploit-Tabelle zu. |
| u_exploit verifiziert | is_exploit_verified | Ordnet das Feld u_exploitverified dem überprüften Exploit in der Exploit-Tabelle zu. |
| u_exploituris | Exploit_Links | Ordnet das Feld u_exploituris den Exploit-Links in der Exploit-Tabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Erstellen oder Aktualisieren der Werte im NVD oder in der Drittpartei-Eintragstabelle verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Werte der neuen Elemente verwendet wird, die erstellt wurden, und der Elemente, die aktualisiert und ignoriert wurden. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Import von MS TVM-Empfehlungen

Die importierten Empfehlungsdaten werden zuerst in die Tabelle „MS TVM-Empfehlungsimport“ [sn_vul_msft_tvm_recom_import] geladen.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie die Daten aus dem Import von MS TVM-Empfehlungen verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach **MS TVM Recommendation Transform**.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### MS TVM-Empfehlungs-Transformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_recommendedvendor | Recommended_vendor | Ordnet das Feld u_recommendedvendor der Spalte Lieferant zu. |
| u_weaknesses | Schwachstellen | Ordnet das Feld u_weaknesses der Spalte „Schwächen“ zu. |
| u_exposedmachinescount | src_exposed_machines_cnt | Ordnet das Feld u_exposedmachinescount der Spalte Anzahl der exponierten Computer zu. |
| u_status | Status | Ordnet den Status dem Feld Status im Empfehlungsdatensatz zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MS TVM-Empfehlungs-Transformationszuordnungsfelder (Fortsetzung)

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_productname | product_name | Ordnet das Feld u_productname dem Produktnamen im Empfehlungsdatensatz zu. |
| u_nonproductiv_impactedassets | non_prod_impacted_assets | Ordnet das Feld u_nonproductiv_impactedassets der Spalte Betroffene Assets im Empfehlungsdatensatz zu. |
| u_activealert | active_alert | Ordnet das Feld u_activealert der Spalte „Aktive Warnung“ im Empfehlungsdatensatz zu. |
| u_recommendedversion | Recommended_version | Ordnet das Feld u_recommendedversion der Spalte „Empfohlene Version“ im Empfehlungsdatensatz zu. |
| u_totalmachinecount | total_computer_count | Ordnet das Feld u_totalmachinecount der Spalte Gesamtanzahl der Computer im Empfehlungsdatensatz zu. |
| u_exposureimpact | Exposure_impact | Ordnet das Feld u_exposureimpact der Spalte Risikoauswirkung im Empfehlungsdatensatz zu. |
| u_recommendationname | Empfehlungsname | Ordnet das Feld u_recommendationname der Spalte „Empfehlungsname“ im Empfehlungsdatensatz zu. |
| u_subcategory | Unterkategorie | Ordnet das Feld u_subcategory der Spalte „Unterkategorie“ im Empfehlungsdatensatz zu. |
| u_id | source_id | Ordnet die Empfehlungs-ID aus MS TVM der Spalte Quell-ID zu. |
| u_remediationtype | remediation_type | Ordnet das Feld u_remediationtype der Spalte „Korrekturtyp“ im Empfehlungsdatensatz zu. |
| u_relatedcomponent | related_component | Ordnet das Feld u_relatedcomponent der Spalte Zugehörige Komponente im Empfehlungsdatensatz zu. |
| u_recommendedprogram | Recommended_program | Ordnet das Feld u_recommendedprogram der Spalte „Empfohlenes Programm“ im Empfehlungsdatensatz zu. |
| u_recommendationcategory | Empfehlungskategorie | Ordnet das Feld u_recommendationcategory der Spalte „Empfehlungskategorie“ im Empfehlungsdatensatz zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**MS TVM-Empfehlungs-Transformationszuordnungsfelder (Fortsetzung)**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_publicexploit | public_exploit | Ordnet das Feld u_publicexploit der Spalte „Öffentlicher Exploit“ im Empfehlungsdatensatz zu. |
| u_vendor | Lieferant | Ordnet das Feld u_vendor der Spalte Lieferant im Empfehlungsdatensatz zu. |
| [Skript] | integration_instance | Name der Instanz, aus der die Empfehlung importiert wird. |
| [Skript] | sys_domain | Domäne, in die dieser Datensatz importiert wird. |

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

**MS TVM-Empfehlungs-Transformationszuordnungsskript**

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das verwendet wird, um Werte in den Empfehlungen zu aktualisieren und zu überprüfen, ob die Empfehlungen vorhanden sind. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Werte von erstellten, aktualisierten und ignorierten Elementen verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Import von MS TVM-Computer-Schwachstellen

Die Transformationszuordnung für MS TVM-Computerschwachstellen wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus MS TVM importiert werden.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem MS TVM-Computer-Schwachstellenimport verarbeitet werden.

Um auf die MS TVM-Transformationszuordnungen für offene und feste Schwachstellen zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach der **Transformation für MS TVM-Computer-Schwachstellen**.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MS TVM-Computer-Schwachstellen transformieren Zuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | Erkennungsschlüssel | Ordnet das Feld u_id der Spalte „Erkennungsschlüssel“ in der Erkennungstabelle zu. |
| u_diskpaths | Nachweis | Ordnet das Feld u_diskpaths der Nachweisspalte in der Erkennungstabelle zu. |
| u_registrypaths | Nachweis | Ordnet das Feld u_registrypaths der Nachweisspalte in der Erkennungstabelle zu. |
| u_recommendedsecurityupdateid | Bevorzugte_Lösung | Ordnet das Feld u_recommendedsecurityupdateid der Spalte Bevorzugte Lösung in der Tabelle für angreifbare Elemente zu, wenn die Lösung mit derselben ID in der Tabelle sn_vul_solution vorhanden ist. |
| u_recommendationreference | Empfehlung | Ordnet das Feld u_recommendationreference der Spalte „Empfehlung“ in der Tabelle für angreifbare Elemente zu. |
| u_cveid | Schwachstelle | Ordnet das Feld u_cveid der Spalte „Schwachstelle“ in der Tabelle für angreifbare Elemente zu. |
| u_status | source_status | Ordnet das Feld u_status der Spalte Quellstatus in der Erkennungstabelle zu. |
| u_eventtimestamp | temporal_score | Ordnet das Feld u_eventtimestamp der Spalte Zuletzt gefunden in der Tabelle für angreifbare Elemente zu. |
| u_lastseentimestamp | last_seen | Ordnet das Feld u_lastseentimestamp der Spalte Zuletzt gesehen in der Tabelle für angreifbare Elemente zu. |
| u_firstseentimestamp | first_seen | Ordnet das Feld u_firstseentimestamp der Spalte „Zuerst gesehen“ in |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**MS TVM-Computer-Schwachstellen transformieren Zuordnungsfelder (Fortsetzung)**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | der Tabelle für angreifbare Elemente zu. |
| u_recommendedsecurityupdate | solution_summary | Ordnet das Feld u_recommendedsecurityupdate der Spalte Lösungszusammenfassung in der Tabelle für angreifbare Elemente zu. |
| u_recommendedsecurityupdate | solution_summary | Ordnet das Feld u_recommendedsecurityupdatorl der Spalte Lösungszusammenfassung in der Tabelle für angreifbare Elemente zu. |

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das verwendet wird, um zu überprüfen, ob der Schwachstelleneintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das verwendet wird, um die Anzahl der aus MS TVM importierten VIs und Erkennungen zu aktualisieren. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

### Statusdiagramm der Integrationsausführung für die Microsoft Threat and Vulnerability Management-Schwachstellenintegration

Sie können das Modul „Microsoft Threat and Vulnerability Management (MS TVM) Integration Run Status“ verwenden, um eine grafische Ansicht des Status der MS TVM-Integrationsausführungen bereitzustellen.

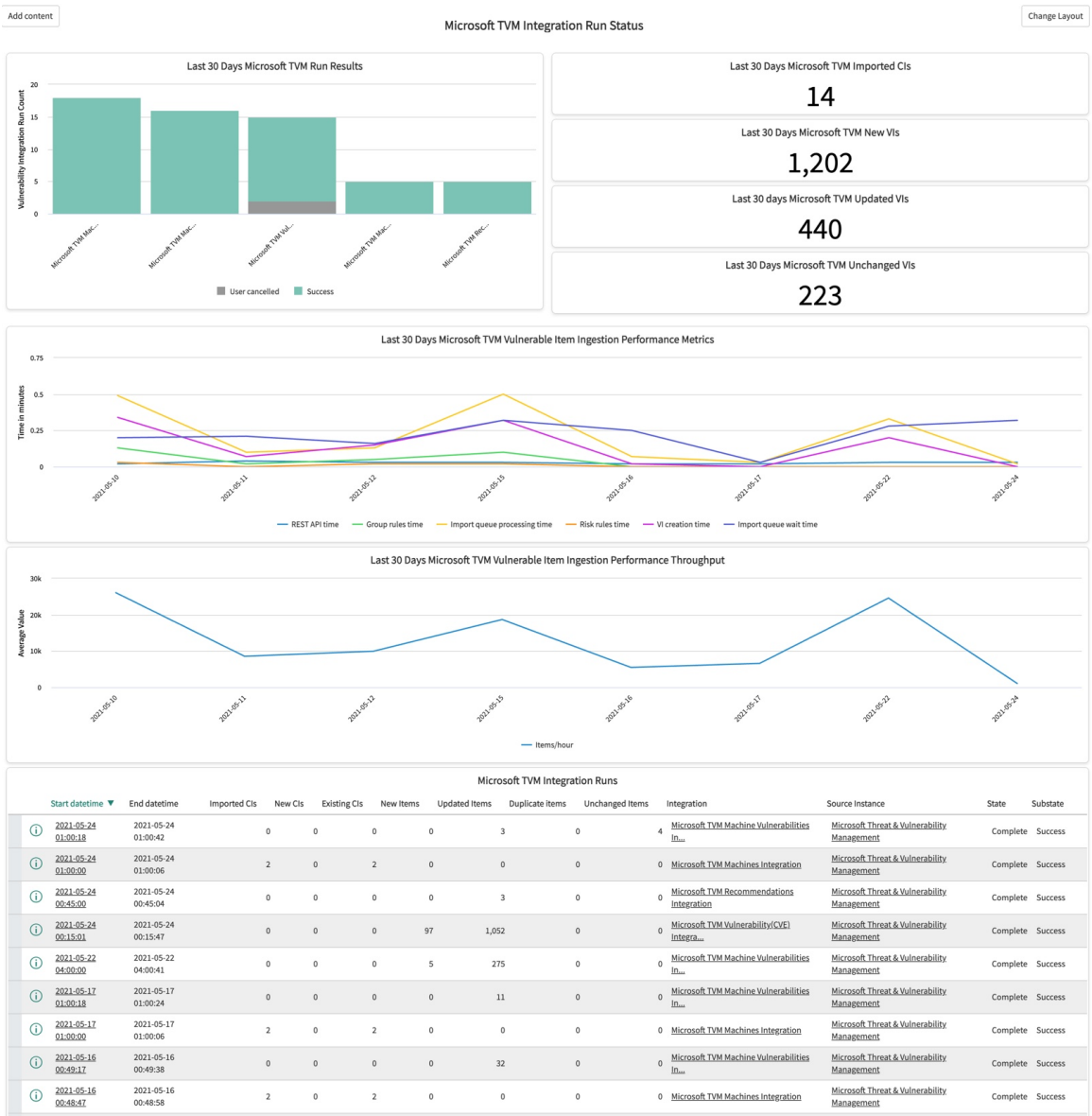
Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Diagramm können Sie auf einen beliebigen Teil des Diagramms zeigen, um eine Zusammenfassung der Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf ein beliebiges Teil im Balkendiagramm klicken, wird eine Liste mit detaillierteren Informationen geöffnet.




## Statusdiagrammberichte der MS TVM-Integrationsausführung

| Name | Beschreibung |
|---|---|
| Microsoft TVM-Ergebnisse der letzten 30 Tage | Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Dieser Bericht zeigt sowohl die erfolgreichen als auch die fehlgeschlagenen Ausführungen. Jede Ausführung wird im Diagramm als Balken angezeigt. |
| Neue Microsoft TVM-VIs der letzten 30 Tage | Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. |
| Aktualisierte Microsoft TVM-VIs der letzten 30 Tage | Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Beschreibung |
|---|---|
| Unveränderte Microsoft TVM-VIs der letzten 30 Tage | Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. |
| MS TVM-Integrationsausführungen | Integrationsausführungsdatensätze in einer Liste.<br>**Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |
| Angreifbares Microsoft TVM-Element – Leistungsmetriken der letzten 30 Tage | Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage. |
| Angreifbares Microsoft TVM-Element – Erfassungsleistungsdurchsatz der letzten 30 Tage | Täglicher Durchsatz bei der Erfassung angreifbarer Elemente, der für die Integration der Microsoft TVM-Hosterkennung in den letzten 30 Tagen gemessen wurde. |
| Von Microsoft TVM importierte CIs der letzten 30 Tage | Anzahl der neuen Konfigurationselemente, die in den letzten 30 Tagen importiert wurden |

### Überprüfen Sie den Ausführungsstatus der Microsoft Threat and Vulnerability Management-Integration

Verwenden Sie den Importausführungsstatus von Microsoft Threat and Vulnerability Management (MS TVM), um den Erfolg Ihrer Integrationsausführungen zu überprüfen und nach Problemen zu suchen.

#### Vorbereitungen

Dieses Verfahren geht von den folgenden Annahmen aus:

- Sie haben Vulnerability Response und die MS TVM Vulnerability-Integration installiert und konfiguriert.
- Importe von MS TVM-Schwachstellenintegrationen werden geplant und ausgeführt.

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Microsoft Threat and Vulnerability Management** > **Integrationen**.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf die zugehörige Liste Ausführungen der Schwachstellenintegration.
2. Vergewissern Sie sich, dass der Status der Importe Abgeschlossen ist und der Substatus Erfolg lautet. Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:
   - Netzwerkunterbrechung.
   - Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt.
3. **Wahlweise:** Wenn Sie eine dieser Bedingungen sehen, die zu einer fehlgeschlagenen Ausführung geführt haben, klicken Sie auf **Jetzt** ausführen, und führen Sie die Integration erneut aus.

## Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Response

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen von Assets mit der Vulnerability Response Patch Orchestration-Integration mit dem HCL BigFix-Produkt verwalten.

## Patch-Orchestration mit Vulnerability Response

Die Patch-Orchestration mit Vulnerability Response verwendet geplante Importe aus Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellen-Scannern. Scanner-Erkennungsdaten stimmen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, die sie beheben können. Senden Sie Patch-Anforderungen zur Genehmigung, planen Sie Patch-Updates, um angreifbare Elemente zu beheben, und überwachen Sie den Korrekturfortschritt anhand von Datensätzen in der Anwendung Vulnerability Response in Ihrem Now Platform®.

## Vulnerability Response Patch Orchestration mit HCL BigFix

Wenn die Integrationsanwendung Vulnerability Response Patch Orchestration with HCL BigFix mit den Anwendungen ServiceNow® Vulnerability Solution Management, Patch Orchestration und Vulnerability Response verwendet wird, können Schwachstellenmanager und Analysten die folgenden Aufgaben ausführen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weiteren Kontext und Informationen zu den Arten von Patches und Anbieterlösungen (Patches) anzeigen.
- Zeigen und überwachen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in den Vulnerability Response Arbeitsbereichen.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

- Stellen Sie Patches, die vom BigFix-Produkt unterstützt werden, für Windows, CentOS, MAC, Oracle und andere Assets in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten bereit, um Arbeitskonflikte zu vermeiden.
- Identifizieren Sie nicht gepatchte Assets mit Schwachstellen oder Assets, die nicht erfolgreich durch geplante Patches aus importierten Erkennungsdaten von Scannern von Drittanbietern aktualisiert wurden.
- Planen Sie verfügbare Patches aus dem IT-Korrekturarbeitsbereich oder aus der klassischen Umgebung für angreifbare, nicht gepatchte Assets aus Datensätzen für Patch-Updates, Korrekturaufgaben und erkannte Elemente.

## Wichtige Begriffe in den Anwendungen Vulnerability Response und BigFix

**Konfigurationselement (Configuration Item, CI)**

CIs sind die vorhandenen Assets, die in Ihrem Configuration Management Database (CMDB)aufgeführt sind. BigFix ruft CIs, Computer auf.

**Computergruppen**

Im BigFix-Produkt verwendete Terminologie, die sich auf eine Gruppe von Assets bezieht.

**Angreifbares Element**

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

**Instanz**

Ein eindeutiger Account der BigFix-Anwendung. Jeder Benutzeraccount kann eine Instanz in der BigFix-Anwendung sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Now Platform -Instanz.

**Integration**

Eine Integration ist eine geplante Aufgabe in Now Platform, die Informationen aus einer Drittanbieterquelle abruft, z. B. die Integration mit den BigFix-Computern.

**Lösung**

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: „Potenziell“ und „Bevorzugt“. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben häufig viele mögliche Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

**Patch**

Software-Updates, die Schwachstellen beheben. In der BigFix-Anwendung werden Patches als Fixlets bezeichnet. Beispielsweise verfügt BigFix über Fixlets für Windows, CentOS, MAC, Oracle und andere Produkte.

**Bevorzugter Patch**

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Nach der Bereitstellung werden Patches den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie beheben.

**Korrekturaufgabe**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen der angreifbaren Elemente in der Anwendung Vulnerability Response von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

**Bereitstellung**

Die Bereitstellung für die Zwecke dieser Integration bezieht sich auf das Anwenden, Initiieren oder Planen eines Patches auf einem Computer. BigFix ruft diese Bereitstellungen als Aktionen auf. Sie können für die Patches, die Sie von BigFix in Ihrem Now Platformheruntergeladen haben, Bereitstellungen (Aktionen erstellen) durchführen. Navigieren Sie zu erkannten Elementen, Patches oder Korrekturaufgaben aus einzelnen Datensätzen in Vulnerability Response. Sie können Patches mit regelmäßigen Aufgaben auf einzelnen Computern oder in Computergruppen bereitstellen.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Eine einzelne vorhandene Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise könnten in Ihrer Umgebung mehrere Bereitstellungen der BigFix Vulnerability-Integration vorhanden sein.

## Vulnerability Solution Management und Vulnerability Response Patch Orchestration with HCL BigFix Integration

Das Lösungsmanagement wird von der Anwendung [ Vulnerability Solution Management bereitgestellt, einer Anwendung von Now Platform, die Ihre Schwachstellenergebnisse mit der Aufgliederung der Lösungen (Patches) korreliert, die sie beheben. Identifizieren Sie die Softwarepatches von Drittanbietern für Produkte und Services, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen auf Ihre Organisation haben. Zusammen mit den Informationen zu Scannern von Drittanbietern arbeiten die Anwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with HCL BigFix zusammen, um ein Rollup bevorzugter Patches von der Lösung über die Schwachstelle bis zum angreifbaren Element durchzuführen, um Sie beim Beheben und Schließen zu unterstützen Schwachstellen in Ihrer Umgebung.

Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with HCL BigFix Integration sind alle in ServiceNow® Storeverfügbar.

## Erforderliche Now Platform-Rollen

Für die Installations-, Konfigurations- und Korrekturaufgaben der -Integration sind die folgenden Rollen in Ihrer Now Platform -Instanz erforderlich.

**Administrator**

Benutzer mit dieser Rolle erhalten Berechtigungen für Anwendungen in der ServiceNow Store und laden sie in Now Platform -Instanzen herunter.

**sn_vul.vulnerability_admin**

Benutzer mit dieser Rolle aktivieren Anwendungen in der Instanz Now Platform und schließen die Konfiguration der Anwendung Vulnerability Response ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administratorbenutzer konfiguriert alle VR-Anwendungen, -Regeln und -Integrationen von Drittanbietern.

**sn_vul_bigfix.configure_integration**

Benutzer mit dieser Rolle konfigurieren die Anwendung „BigFix Patch Orchestration Integration“. Diese Rolle enthält die granulare Rolle sn_vul_bigfix.read_integration.

**sn_vul_bigfix.read_integration**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer mit dieser Rolle können die Datensätze der Anwendung Vulnerability Response und der Anwendung BigFix Patch Orchestration Integration sowie Patch-Orchestration-Daten anzeigen (schreibgeschützt).

**sn_vul_patch_orch.configure_patch**

Benutzer mit dieser Rolle können Patches konfigurieren und anwenden.

**sn_vul_patch_orch.read_patch**

Benutzer mit dieser Rolle können Patch-Informationen anzeigen (schreibgeschützt).

**Genehmiger**

Weisen Sie Benutzer den Genehmigergruppen „Genehmigerebene 1“ und „Genehmigerebene 2“ zu, wenn übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden sollen.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zu den Rollen Vulnerability Response in Ihrem Now Platformfinden Sie unter Vulnerability Response Personas und granulare Rollen.

## CI-Suchregeln

Wenn Daten aus der BigFix-Anwendung importiert werden, sucht die Anwendung Vulnerability Response automatisch nach Übereinstimmungen in Configuration Management Database (CMDB) anhand von Computerdaten (Asset-Daten). CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen für angreifbare Elemente (AEs) hinzuzufügen, wenn AEs erstellt werden.

Die folgenden CI-Suchregeln werden mit dem Basissystem ausgeliefert und dazu verwendet, CIs (Assets) zu identifizieren und der Anwendung Vulnerability Response hinzuzufügen:

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Sie können mehrere Werte für die IP_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich. Weitere Informationen dazu, wie CI-Suchregeln funktionieren und wie sie funktionieren, finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

## MID-Server

Die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix ist eine lokale Integration. Sie erfordert einen eigenständigen MID Server, der nicht Teil eines MID Server-Clusters ist. Der MID Server ist erforderlich, um Skripts auf Remotecomputern von Ihrer Instanz aus auszuführen und Daten vom BigFix-Server zu importieren. APIs für diese Integration werden mit MID Servern aufgerufen, die Sie in Ihrer Now Platform -Instanz eingerichtet haben. Weitere Informationen finden Sie unter Bereiten Sie sich auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix vor.

### Integrationen und Abhängigkeiten der Vulnerability Response Patch Orchestration-Integration mit HCL BigFix

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für die Vulnerability Response Patch Orchestration mit HCL BigFix Integration erforderlich. Diese Anwendungen sind im ServiceNow® Storeverfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Patch-Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind im ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familien-Releases finden Sie im Artikel KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes in der HI Knowledge Base.

| Anwendung und Release-Version |
|---|
| Vulnerability Response |
| Vulnerability Solution Management |
| Anwendung Vulnerability Response Patch Orchestration |
| Vulnerability Response Patchen Sie Orchestration mit der Anwendung HCL BigFix |
| Security Support Common |
| Security Support Orchestration |
| Eine unterstützte Schwachstellen-Scanner-Anwendung einer Drittpartei |

## Vulnerability Response Patchen Sie die Anwendungstabellen der Orchestration

Die Anwendung Vulnerability Response Patch Orchestration enthält die folgenden Tabellen:

| Tabelle | Beschreibung |
|---|---|
| Patch-Update [sn_vul_patch_orch_update] | Speichert Informationen zu den Patches, die für verschiedene Instanzen verfügbar sind |
| Geräte-Update [sn_vul_patch_orch_m2m_src_ci_update] | Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden. |
| Sammlung [sn_vul_patch_orch_collection] | Speichert Sammlungsdaten aus verschiedenen Instanzen. |
| Gerätesammlung [sn_vul_patch_orch_m2m_src_ci_collection] | Speichert Sammlungsdaten zu erkannten Elementen. |
| Patch-Bereitstellung [sn_vul_patch_orch_deployment] | Speichert Informationen zu bereitgestellten Patches für Sammlungen und CIs. |
| Potenzieller Patch [sn_vul_patch_orch_m2m_vuln_patch] | Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können. |

## Vulnerability Response Patch Orchestration Integrations with HCL BigFix

Die von ServiceNow® Engineering entwickelten Integrationen bilden die orchestrierte Lösungsbereitstellung mit dem BigFix-Produkt. Die folgenden Integrationen sind in der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung Vulnerability Response Patch Orchestration Integration with HCL BigFix enthalten, die Sie aus dem ServiceNow® Storeherunterladen können.

Nachdem Sie die Integrationsanwendung in Ihrer Instanz Now Platform installiert haben, navigieren Sie zum Anzeigen dieser Integrationen zu **Integrationen** > **Integration der BigFix Patch Orchestration** > **Integrationen**. Die Anwendung Vulnerability Response verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen mit BigFix-Endpunkten importiert werden.

| Integration | Beschreibung |
|---|---|
| Integration der BigFix-Sammlung | • Diese Integration ist für die tägliche Ausführung geplant und wird in der verketteten Integrationsausführung zuerst ausgeführt.<br>• Ruft die Computer und Computergruppen, aus denen die Computergruppen (Konfigurationselemente) bestehen, aus der BigFix-Anwendung ab. |
| BigFix Fixlet-Integration | • Wenn geplant, wird diese Integration durch den Abschluss der BigFix Collection-Integration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Ruft Informationen zu allen verfügbaren Fixlets (Patches) vom BigFix-Server ab. |
| Fixlet-Integration für BigFix-Geräte | • Wenn geplant, wird diese Integration durch den Abschluss der BigFix Fixlet-Integration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Ruft Informationen zu den Fixlets, die sich derzeit auf Computern (Assets) befinden, vom BigFix-Server ab. |
| Integration von BigFix Actions | • Wenn geplant, wird diese Integration durch den Abschluss der BigFix Device Fixlet-Integration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Ruft Informationen zu den vom IT-Team geplanten Patches auf dem BigFix-Server ab. |



### Bereiten Sie sich auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix vor

Bereiten Sie die Integration vor, indem Sie die folgenden Setup-Aufgaben ausführen.

#### Vorbereitungen

Erforderliche Rollen: admin für die Installation der Anwendungen und die Zuweisung von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

#### Warum und wann dieser Vorgang ausgeführt wird

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

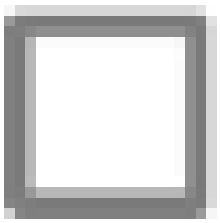
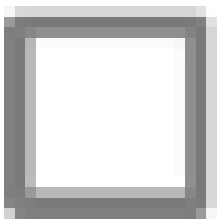
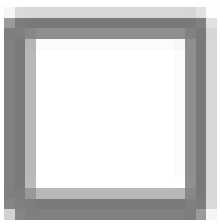
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix.

### Prozedur

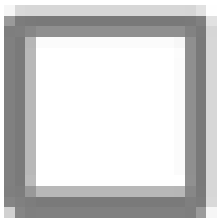
1. Befolgen Sie die bereitgestellte Prüfliste, um eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Patch Orchestration with HCL BigFix zu gewährleisten.
2. Es empfiehlt sich, die folgende Prüfliste auszudrucken und sicherzustellen, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

   Importieren Sie nach der Installation und Konfiguration Informationen zu Schwachstellen und Patches in Ihre Now Platform® -Instanz.

| Aufgabe | Beschreibung |
|---|---|
|  | (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.0 von Vulnerability Response oder höher. |
|  | Wenn noch nicht installiert, holen Sie sich Berechtigungen und installieren Sie die Scanner-Anwendung einer Drittpartei, um Schwachstellendaten zu importieren.<br><br>Unter Vulnerability Response-Integrationen finden Sie weitere Informationen zu Scannern von Drittanbietern, die von Vulnerability Responseunterstützt werden.<br><br>Weitere Informationen finden Sie unter . |
|  | Falls noch nicht installiert, holen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix in Ihre Now Platform® -Instanz herunter.<br>Weitere Informationen finden Sie unter . |
| | Rufen Sie BigFix-Anmeldeinformationen ab.<br><br>Vergewissern Sie sich, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre BigFix-Produkte erforderlich sind, damit Sie darauf zugreifen können. |

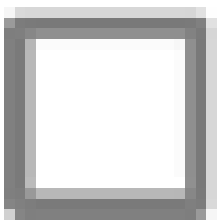


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
|  | Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, die die Integrationen verwalten und angreifbare Elemente korrigieren.<br>**Administrator**<br>Der Systemadministrator erhält Berechtigungen, lädt die Anwendung BigFix Patch Orchestration und die anderen für die Integration erforderlichen Anwendungen herunter und installiert sie. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten in Vulnerability Response oder aus dem Modul „Benutzerverwaltung“ zu.<br>**sn_vul.vulnerability_admin**<br>Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der BigFix-Integrationen und der anderen Anwendungen von Drittanbietern ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, Regeln, Drittanbieterintegrationen, Vulnerability Response Patch Orchestration- und Vulnerability Solution Management-Anwendungen.<br>**sn_vul_bigfix.configure_integration**<br>Benutzer mit dieser Rolle konfigurieren die Anwendung „BigFix Patch Orchestration Integration“. Diese Rolle enthält die granularen Rollen sn_vul_bigfix.read_integration und connection_admin, mit denen der Benutzer eine Verbindung zur BigFix-Konsole herstellen und die Integrationsinstanzen in Now Platformkonfigurieren kann.<br>**sn_vul_bigfix.read_integration**<br>Benutzer mit dieser Rolle können die Datensätze der Anwendung Vulnerability Response und der Anwendung BigFix Patch Orchestration Integration sowie Patch-Orchestration-Daten anzeigen (schreibgeschützt).<br>**sn_vul_patch_orch.configure_patch**<br>Benutzer mit dieser Rolle können Patches konfigurieren und anwenden. Von diesem Benutzer angeforderte Patches aus Datensätzen für angreifbare Elemente und Patch-Updates werden zur Genehmigung gesendet, wenn das Change-Management aktiv ist und Genehmiger zugewiesen sind.<br>**sn_vul_patch_orch.read_patch**<br>Benutzer mit dieser Rolle können Patch-Informationen zu Datensätzen anzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind.<br>**Genehmiger**<br>Benutzer, die der Genehmigerebene 1 und optional der Genehmigerebene 2 zugewiesen sind, genehmigen übermittelte Patch-Anforderungen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Gruppe „Genehmiger Ebene 1“ übermittelt.<br>Weitere Informationen zum Genehmigungsprozess finden Sie unter Patch-Orchestration mit Vulnerability Response. Weitere Informationen zum Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.<br>Der Systemadministrator führt die anfängliche Zuweisung von Rollen zu Benutzern und Gruppen für die Integration durch. Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Falls noch nicht erstellt, ziehen Sie es möglicherweise vor, zusätzliche Gruppen für die Rollen „Korrekturspezialist“ und „Schwachstellenanalyst“ zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen. |
|  | Vergewissern Sie sich, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Jobs in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind.<br>○ Die Vulnerability Response Patch Orchestration mit HCL BigFix ist eine lokale Integration, für die Sie einen eigenständigen MID Server verwenden müssen. Weitere Informationen zu MID Servern in Ihrer Instanz finden Sie unter MID Server.<br>○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es. |

### Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix.

#### Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix

Laden Sie die Anwendung Vulnerability Response Patch Orchestration with HCL BigFix aus dem ServiceNow® Storeherunter.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rollen: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und Installation der Anwendung. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)), um die Vulnerability Response Patch Orchestration mit HCL BigFix und anderen Anwendungen nach der Installation zu konfigurieren.

### Warum und wann dieser Vorgang ausgeführt wird

Vergewissern Sie sich vor der Installation der Anwendung, dass Sie alle Elemente der Prüfliste in Bereiten Sie sich auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix vorabgeschlossen haben.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

### Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie nach der Anwendung **Vulnerability Response Patch Orchestration with HCL BigFix**, und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung installiert, die Sie aus dem ServiceNow Storeheruntergeladen haben.

3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.

### Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation zu **Alle** > **Integration der BigFix Patch Orchestration** > **Konfiguration** , um mit der Konfiguration fortzufahren.

## Konfigurieren Sie die Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren BigFix-Kontoinformationen, und validieren Sie Ihre Anmeldeinformationen.

### Vorbereitungen

Erforderliche Rollen: sn_vul.vulnerability_admin und sn_vul_bigfix.configure_integration

### Prozedur

1. Navigieren zu **Integration der BigFix Patch Orchestration** > **Konfiguration**.
2. Füllen Sie die Felder mit Ihren BigFix-Informationen und -Anmeldeinformationen aus.

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Der Name des BigFix-Instanzkontos, das Sie verwenden möchten, z. B. BigFix Patch Management Integration. |
| Hostname | Geben Sie die URL für den BigFix-Host ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Benutzername | Geben Sie Ihren BigFix-Account-Benutzernamen ein. |
| Passwort | Geben Sie das Passwort Ihres BigFix-Accounts ein. |
| MID-Server | Geben Sie den Namen des eigenständigen MID Servers aus der Liste ein, den Sie verwenden möchten. Weitere Informationen zu MID Servern und Setup-Aufgaben finden Sie unter Bereiten Sie sich auf die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix vorNow Platform®. |

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen BigFix und Ihrer Instanz Now Platform® wird im Validierungsstatusfeld angezeigt. Wenn kein erfolgreicher Test angezeigt wird, folgen Sie den Eingabeaufforderungen.
4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer Instanz mehrere Konfigurationen von hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:
   a. Navigieren zu **Integration der BigFix Patch Orchestration Integrationsinstanzen**.
   b. Vergewissern Sie sich, dass der Anwendungsbereich Vulnerability Response Patch Orchestration with HCL BigFixim Feld Anwendungsbereich angezeigt wird.
   c. Klicken Sie auf **Neu**.
   d. Füllen Sie das Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Name für die Integrationsinstanz. |
| Anwendung | Vulnerability Response Patch Orchestration mit HCL BigFix |
| Integration | [Nur Lesen] BigFix Patch Management ist die Standardeinstellung. |
| Aktiv | Der Standardwert ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv. |

   e. Klicken Sie auf **Absenden**.
   Ihre neue Integrationsinstanz wird in der Liste „Integrationsinstanzen“ angezeigt.
   f. Wiederholen Sie die Schritte 1 bis 3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.
5. Richten Sie Genehmigungen für Patch-Anforderungen ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist eine Systemeigenschaft [**sn_vul_patch_orch.patch_approval_required**] aktiviert, sodass Patch-Bereitstellungen, wenn sie geplant sind, zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind.

Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen können, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

**Hinweis:**
Wenn Sie die Genehmigungssystemeigenschaft deaktivieren, kann jeder Benutzer mit der Rolle „sn_vul_patch_orch.configure_patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

So deaktivieren Sie als Benutzer mit der Rolle „sn_vul.vulnerability_admin“ die Systemeigenschaft:

**a.** Navigieren zu **sys.properties.list**.

**b.** Suchen Sie **sn_vul_patch_orch.patch_approval_required**, und klicken Sie darauf, um den Datensatz zu öffnen.

**c.** Geben Sie im Feld Wert falseein.

**d.** Klicken Sie auf **Aktualisieren**.

**6.** Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie Genehmiger für Patch-Anforderungen zuweisen. Führen Sie als Benutzer mit der Rolle „sn_vul.vulnerability_admin“ die folgenden Schritte aus.

**a.** Navigieren zu **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.

**b.** Wenn die **Genehmigungsregel für die Bereitstellung von Patch-Updates** nicht in der Liste angezeigt wird, klicken Sie oben links auf dem Bildschirm rechts neben dem grünen Filtersymbol auf **Alle**, um die gesamte Liste anzuzeigen.

**c.** Klicken Sie in der Liste auf **Genehmigung der Patch-Aktualisierung bereitstellen**.

**d.** Klicken Sie im Datensatz auf der Registerkarte Genehmigungskonfiguration auf **Standardkonfiguration Patch-Aktualisierungsgenehmigung**.

**e.** Klicken Sie im Datensatz auf **Ebene 1 – Genehmigung der Patch-Aktualisierung**.

**f.** Fügen Sie Benutzer in dieser Gruppe hinzu.

Die dieser Gruppe zugewiesenen Benutzer genehmigen Patch-Anforderungen, die von Benutzern mit der Rolle sn_vul_patch_orch.configure_patch übermittelt wurden. Navigieren Sie zu **Meine Genehmigungen**, um die Anforderungen anzuzeigen und zu verarbeiten.

**7.** Klicken Sie auf**Aktualisieren**, um Ihre Änderungen zu speichern.

**8.** **Wahlweise:** Sie können mehrstufige Genehmigungen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie bei angezeigtem Genehmigungsdatensatz für das Standardkonfigurations-Patch-Update auf **Neu**.

**b.** Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungsebene, z. B. **Ebene 2 – Genehmigung der Patchaktualisierung**. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird. |
| Erforderliche Genehmigung | Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind:<br>▪ Ein Genehmiger erforderlich<br>▪ Alle Anwender müssen genehmigen |
| Reihenfolge | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rolle | Wählen Sie eine Rolle für die Gruppe aus der Liste aus. |
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. |
| Genehmigungskonfiguration | Enthält die Genehmigungskonfigurationen |
| Zuweisen mit | Wählen Sie eine Option aus:<br>▪ Anwender und Anwendergruppe<br>▪ Genehmigungstabellenfeld<br>▪ Skript |
| Gruppen | Genehmigerebenengruppe, die aus mehreren Benutzern besteht. Der Benutzer muss eine der folgenden von Ihnen angegebenen Rollen haben. |
| Benutzer | Bearbeiten Sie die in den Gruppen aufgeführten Benutzer. |

**c.** Klicken Sie auf **Absenden**, um Ihre Änderungen zu speichern.

### Anzeigen von Patch-Daten für die Patch-Orchestration-Integration Vulnerability Response mit HCL BigFix

Patch-Daten und Patch-Rollup-Daten sowie Schwachstelleninformationen und der Korrekturstatus Ihrer Schwachstellen werden in Datensätzen in Ihrer Instanz angezeigt.

## Patch-Daten in den Vulnerability Response -Arbeitsbereichen anzeigen

Erforderliche Rollen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind

Im IT-Korrekturarbeitsbereich können Sie Patches anzeigen:

- In der Ansicht „Startseite“, in der Sie auf Bewertungslisten klicken können, um Datensätze für bevorzugte Lösungen für VIs, angreifbare CIs und bevorzugte Patches für VIs anzuzeigen.
- In der Listenansicht, in der Sie alle Patch-Update-Datensätze (VPUs) über die Links „Patches“ und die Ihnen zugewiesenen angreifbaren Elemente (VITs) mit Patches anzeigen können.

Sie können Patches aus den folgenden Datensätzen planen:

- Aus Patch-Update (VPU)
- Korrekturaufgabe (RT)
- SDI-Datensätze (Discovery Item).

In Vulnerability Manager Workspace können Sie Patches anzeigen:

- In der Ansicht „Homepage“ zu Überwachungsthemen, in der Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und, falls der Patch heruntergeladen wurde, alle auf der Registerkarte **Angreifbare Elemente** anzeigen können.
- Über die Listenansicht der Korrekturmaßnahmen, in der Sie Patch-Daten zu VI-Datensätzen auf der Registerkarte „**Angreifbare Elemente** “ anzeigen können.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**.

## Patch Aktualisieren Sie Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie Patch-Datensätze (VPU) in Vulnerability Response Arbeitsbereichen aus der Listenansicht im IT-Korrekturarbeitsbereich an. Patch-Update-Datensätze in der klassischen Ansicht und in Vulnerability Response Workspaces enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Anbietern, die von der Anwendung Vulnerability Solution Management importiert werden.
- Quell-Korrekturstatus, der die Gesamtzahl der Geräte mit einer bestimmten Schwachstelle enthält, die durch einen Patch behoben werden kann, sowie alle Geräte, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIs und die Gesamtzahl der VIs umfasst, für die ein Patch als bevorzugter Patch gilt.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links für Datensätze in der Klassenansicht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Daten werden auf Registerkarten in Datensätzen in den Vulnerability Response Arbeitsbereichen angezeigt.

- Patch-Anforderungen, die die Korrekturbesitzer zur Genehmigung übermittelt haben.

### Status-Rollup für Datensätze angreifbarer Elemente

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Rollup für Patch-Daten und -Status für Patch-Orchestration in Vulnerability Response.

### Datensätze, die ein Rollup für die Anzahl aktiver VIs durchführen

Um ein Rollup aller Patches für alle Schwachstellen zu vermeiden, übernimmt die geplante Aufgabe nur Änderungen an der aktiven AEs-Anzahl. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup zu den folgenden Datensätzen in Vulnerability Responsedurchgeführt :

- VIT
- RT
- Schwachstellenlösung
- Patch-Update

### Anzeigen von Daten für Patches ohne Lösungen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

### Patchen Sie Daten auf dem Vulnerability Response

Die Dashboards für Schwachstellenmanagement (PA) und CISO sind in einem Abonnement mit der Anwendung Performance Analytics für die Anwendung Vulnerability Response enthalten. Wenn Sie ein Abonnement für Performance Analyticshaben, aber keine Patch-Orchestration-Integration installiert haben, wird die Registerkarte „Korrektur“ im CISO-Dashboard angezeigt, aber nicht mit Daten ausgefüllt.

Navigieren Sie für das Dashboard für Schwachstellenmanagement (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**. Klicken Sie auf die Registerkarte **Remediation**, und scrollen Sie zum Ende der Seite, um Patch-Update-Daten anzuzeigen: geplante und nicht geplante Patches, Patches mit verfehlten Zieldaten und wöchentliche Anzahlen.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**. Scrollen Sie bei ausgewählter Registerkarte Übersicht zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches mit fehlendem Zieldatum.

Weitere Informationen zu den Dashboards [ Vulnerability Response finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet, Patchen Sie die Orchestration mit den Vulnerability Response -Arbeitsbereichenund Patch-Orchestration-Daten werden in den Vulnerability Response -Dashboards angezeigt.

#### Planen Sie Patches mit der Vulnerability Response Patch Orchestration-Integration HCL BigFix

Planen Sie Patches aus Datensätzen für Patch-Updates und Korrekturaufgaben in der Anwendung Vulnerability Response in Ihrer Instanz Now Platform.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Ab Version 16.1 können Sie Patches aus den Vulnerability Response Arbeitsbereichen oder aus der klassischen Umgebung planen.

Erforderliche Rollen:

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind

### Prozedur

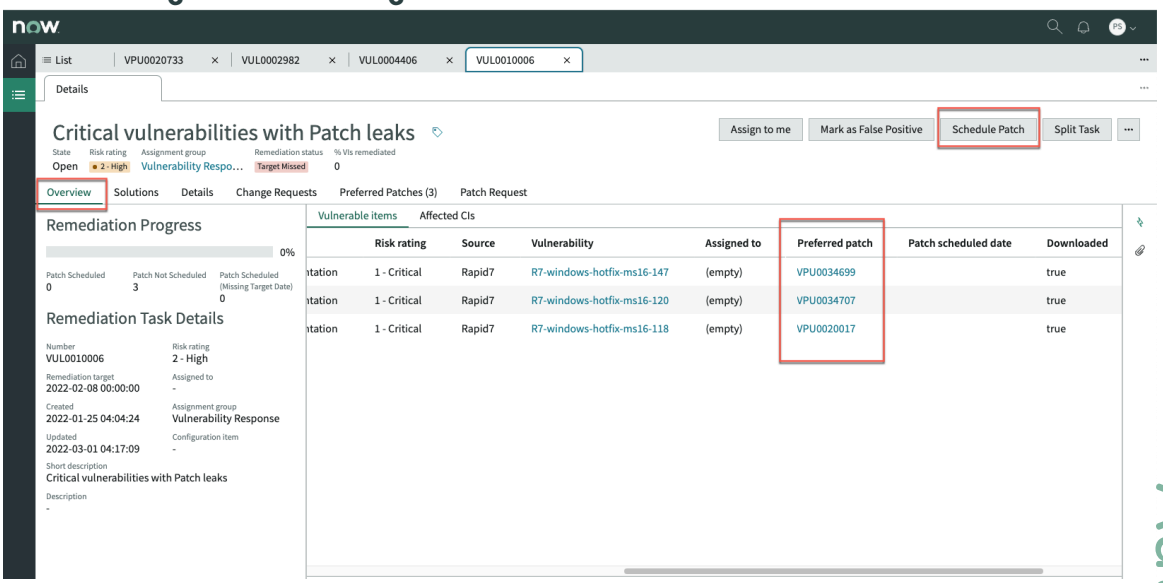
1. Navigieren Sie in den Arbeitsbereichen für Schwachstellen Vulnerability Response als Benutzer mit der Rolle „sn_vul.remediation_owner“ zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Klicken Sie auf der Homepage auf **Bevorzugter Patch für AEs**.
   Die Liste der Patch-Update-Datensätze für die VIs mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.
3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie darauf, um ihn zu öffnen.
4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** , und suchen Sie nach einem Patch-Update-Datensatz.
   Der Patch-Update-Datensatz wird angezeigt. Möglicherweise möchten Sie die Daten überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.
5. In der folgenden Tabelle finden Sie die angezeigten Daten und Ihre Möglichkeiten.
6. Klicken Sie **auf Patch planen**.
7. Füllen Sie im Dialogfeld die Felder aus.
8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller übermittelten Anforderungen in anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** aus der Listenansicht.
9. Alternativ können Sie Patches aus Korrekturaufgaben (Remediation Tasks, RT) planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

**Hinweis:**
Die Option zum Planen eines Patch aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn Patches den VIs in der Aufgabe zugeordnet (zugeordnet) sind. Diese Patches werden in der Spalte Bevorzugter Patch angezeigt, wenn Sie mit ausgewählter Registerkarte Übersicht rechts neben Datensätzen für Korrekturaufgaben scrollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Korrekturaufgabe mit bevorzugten Patches**




10. Klicken Sie im RT-Datensatz auf **Patch** planen, und führen Sie die oben aufgeführten Schritte aus, um den Patch im Dialogfeld zu planen.
11. Sie können Patches für die zuvor in der klassischen Umgebung aufgeführten Schritte planen. Führen Sie die folgenden Schritte aus, um diese Datensätze zu finden.

    a. Navigieren Sie in der klassischen Umgebung zu **Vulnerability Response** > **Patches** > **Alle**.

    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.

    c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** und suchen Sie einen Datensatz.
    Sie verfolgen den Korrekturstatus auf der Registerkarte Korrekturstatus nach. Am Ende des Datensatzes werden Patch-Daten unter Zugehörige Links angezeigt.

    d. Klicken Sie auf Patch planen, und füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Bereitstellungsname | Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen. |
| Patch-Update | Wählen Sie einen der verfügbaren Patches in der Liste aus. |
| Assets | Wählen Sie eines aus:<br>▪ Computergruppe: Wählen Sie diese Option aus, wenn Sie eine Sammlung (eine Gruppe von Assets) für diesen Patch auswählen möchten. Die Gruppen bestehen aus den Konfigurationselementen, die aus der BigFix-Anwendung importiert werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ▪ Computerliste: Wählen Sie diese Option aus, wenn Sie einzelne Computer (Assets) für diesen Patch auswählen möchten. Im angezeigten Dialogfeld können Sie Daten zu Hersteller, Standort, Klasse, Datum der letzten Aktualisierung und Wartungsplan anzeigen. |
| Startzeit und Endzeit | Geben Sie die Start- und Endzeiten für das Zeitfenster ein. Geben Sie an, wann der Patch mit der Bereitstellung beginnen soll, und geben Sie den letzten Tag an, an dem der Patch installiert werden kann. |

### REST-Nachrichten für die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix

Die Vulnerability Response Patch Orchestration Integration with HCL BigFix-REST-Nachrichten werden für Aufrufe an die BigFix-API verwendet.

## BigFix-Anmeldung

Sie können die REST-Nachrichten auch für die BigFix-Anmeldung verwenden, damit Sie REST-API-Anforderungen authentifizieren können. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Authentifizierungsanforderungen an BigFix aus.

| Parametername | Wert | Beschreibung |
|---|---|---|
| sourceType | kumulativ | Gibt an, dass die Quellintegration Daten aus abruft. Von Code verwendet. Änderungen werden nicht empfohlen. |
| sortDIR | desc | Gibt die Sortierrichtung für die aus der Integration abgerufenen Daten an. Änderungen werden nicht empfohlen. |
| sortField | Schweregrad | Gibt das Feld an, auf dem die Datensortierung basiert. Änderungen werden nicht empfohlen. |
| type | Schwachstelle | Gibt den Typ der Daten an, die aus der Integration für die Asset-Integration abgerufen werden sollen. Änderungen werden nicht empfohlen. |

## BigFix-Integration

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Informationen aus BigFix abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an BigFix zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**REST-Methoden**

| REST-Methode | Beschreibung |
|---|---|
| GET Daten abrufen | Ruft basierend auf der angegebenen Abfrage die Informationen aus BigFix zu einem der folgenden Elemente ab:<br>• Computer/Computergruppen<br>• Fixlets<br>• Relevante Fixlets auf Computern<br>• Aktionen |

| Parametername | Wert | Beschreibung |
|---|---|---|
| URL | Dynamische Werte basierend auf dem Benutzer | Gibt den Endpunkt der BigFix-Konsole an |

## BigFix-Patch bereitstellen

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Patches von Now Platform® für BigFix zu planen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an BigFix zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

| REST-Methode | Beschreibung |
|---|---|
| POST-Bereitstellungs-Patch | Plant den Patch für die BigFix-Konsole auf einzelnen/mehreren Computern. |

| Parametername | Wert | Beschreibung |
|---|---|---|
| URL | Dynamische Werte basierend auf dem Benutzer | Gibt den Endpunkt der BigFix-Konsole an. |
| Titel | Dynamische Werte basierend auf dem Benutzer | Titel der Bereitstellung. |
| einstellungen_tag | XML-Tag-benannte Einstellungen mit Werten | Gibt Einstellungen an, die unterschiedliche Parameter haben und während der Planung des Patch an BigFix gesendet werden. |
| computer_tag | Computer mit XML-Tag-Namen und Werten | Gibt eine Liste der Computer an, auf denen der Patch geplant wird. |
| site_name | Wert aus der Patch-Aktualisierung | Name der Site, in der das Fixlet vorhanden ist |
| fixlet_id | Wert aus der Patch-Aktualisierung | ID des Fixlets. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Datentransformation für die Patch-Orchestration-Integration mit HCL BigFix

Daten werden aus der Patch-Orchestration von Vulnerability Response mit der HCL BigFix-Integration abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz von Now Platform® transformiert.

## Import der BigFix-Sammlung

Die Daten aus den importierten Assets (Computer und Computergruppen) werden in die Tabelle „BigFix-Sammlungsimport“ [sn_vul_bigfix_collection_import] geladen. Das Import-TM für BigFix-Computer und Computergruppen (Transformationszuordnung?) wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der BigFix-Sammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach BigFix Computer und Computergruppen Import TM. In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### BigFix-Computer und Computergruppen importieren Transformationszuordnungsskript-Timing

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Sammlungen sowie der Beziehung zwischen ihnen. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_bigfix]. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## BigFix Fixlet-Import

Die Daten aus den importierten Fixlets werden in die Tabelle „BigFix Fixlet-Import“ [sn_vul_bigfix_patch_update_import] geladen.

BigFix Fixlet Import TM wird verwendet, um die importierten Informationen zu transformieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix Fixlet-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach dem BigFix Fixlet Import-TM.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### BigFix Fixlet-Transform Map-Felder importieren

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | article_id | Eindeutige ID eines Fixlets in einer Site. |
| u_id | source_id | Eindeutige ID eines Fixlets in einer Site. |
| U_site_name | Sn_vul_bigfix_site_name | Name der Site in BigFix, auf die das Fixlet angewiesen ist. |
| U_display_name | Titel | Titel des Fixlets. |
| [Skript] | Bulletin_id | Quell-ID der Lösung. |
| [Skript] | Sn_vul_solution | Lösung basierend auf der Quell-ID. |
| U_Quelle | bulletin_source | Quellanbieter der Lösung. |
| [Skript] | Date_release | Release-Datum des Fixlets. |
| U_category | Update_category | Kategorie des Fixlets. |
| [Skript] | Ist_höchste_Ersetzung | Boolescher Wert, der angibt, ob das Fixlet die höchste Ersetzung ist oder nicht. |
| [Skript] | Ist_heruntergeladen | Boolescher Wert, ob das Fixlet heruntergeladen wurde oder nicht. |
| [Skript] | integration_instance | Name der Instanz, aus der das Fixlet importiert wird. |
| U_source_severity | Source_severity | Schweregrad des Fixlets. |
| U_applicable_count | Num_total | Gesamtzahl der Geräte mit fehlenden Fixlets. |
| [Skript] | Last_modified | Datum der letzten Änderung des Fixlets. |

### Timing des BigFix Fixlet-Transformationszuordnungsskripts

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Timing des BigFix Fixlet-Transformationszuordnungsskripts (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Fixlets verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Import von BigFix-Geräte-Fixlets

Die Daten aus den importierten relevanten Fixlets auf Computern werden in die Tabelle „BigFix Device Fixlet Import“ [sn_vul_bigfix_device_patch_import] geladen.

Das BigFix Device Fixlet TM wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Fixlet-Import des BigFix-Geräts verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie das BigFix Device Fixlet TM.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

**Timing des BigFix Device Fixlet-Transformationszuordnungsskripts**

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Sammlungen sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_bigfix]. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Timing des BigFix Device Fixlet-Transformationszuordnungsskripts (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| | Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Import von BigFix-Aktionen

Die Daten aus den importierten Aktionen werden in die Tabelle „BigFix Actions Import“ [sn_vul_bigfix_deployment_import] geladen.

Das Import-TM für BigFix Actions wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix Actions-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach dem BigFix Fixlet Import-TM.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

**BigFix Actions Importieren von Transformationszuordnungsfeldern**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Eindeutige ID einer Aktion. |
| U_name | Name | Name der Aktion |
| [Skript] | Sn_vul_bigfix_discovered_item | Referenz des erkannten Elements, auf dem der Patch bereitgestellt wird |
| U_status | Status | Status der Aktion |
| [Skript] | Sn_vul_patch_orch_update | Referenz des Patches |
| U_apply_count | Anzahl_Erfolg | Erfolgsanzahl der Aktion. |
| U_retry_count | Erneut versuchen | Anzahl der Wiederholungen der Aktion. |
| [Skript] | Bereitstellungszeit | Startzeit der Aktion. |
| [Skript] | Frist | Endzeit der Aktion. |
| [Skript] | Source_created | Erstellungszeit der Aktion. |
| [Skript] | integration_instance | Name der Instanz, aus der die Aktion importiert wird. |

**BigFix Actions importieren das Timing des Transformationszuordnungsskripts**

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**BigFix Actions importieren das Timing des Transformationszuordnungsskripts (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| | Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Aktionen verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Beispiel-Workflow für die Integration von Vulnerability Response Patch Orchestration mit HCL BigFix

Ein Beispiel für die Funktionsweise der Patch-Orchestration mit dem HCL BigFix-Produkt.

### Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gepatcht. Das letzte Patch-Zeitfenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der kritischen Natur dieser Schwachstelle können Sie nicht zwei weitere Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für Vulnerability Manager Workspace.
- sn_vul.remediation_owner, um den Arbeitsbereich des IT-Korrekturbesitzers anzuzeigen.
- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches.
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind.

### Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenmanager oder Analyst, der im Arbeitsbereich des Schwachstellenmanagers arbeitet, sollten Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIs mit kritischen Schwachstellen zu erfassen. Mit der Integration von Patch Orchestration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. In der folgenden Tabelle sind einige Beispiele mit den Bedingungen aufgeführt, die Sie für Überwachungsthemen für die Patch-Orchestration festlegen können. Verwenden Sie diese Beispiele, um die Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Weitere Informationen zum Einrichten des Überwachungsthemas finden Sie unter Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Beispiele für Überwachungsthemen für die Patch-Orchestrierung in Vulnerability Manager Workspace**

| Name des Überwachungsthemas | Beschreibung |
|---|---|
| Kritische Schwachstellen mit Patch-Lecks | Risikobewertung ist 1 – kritisch UND<br>Grund ist „Patch nicht geplant“. |
| Kritische Schwachstellen mit geplanten Patches (fehlende SLA) | Grund ist „Patch geplant“ (fehlendes Zieldatum) |
| Kritische Schwachstellen mit geplanten Patches | Risikobewertung ist 1 – kritisch UND<br>Geplantes Patch-Datum ist nicht leer UND<br>Grund ist „Patch geplant“. |

- Nachdem Sie als Schwachstellenmanager oder Analyst die Überwachungsthemen und Korrekturmaßnahmen erstellt haben, generieren Sie Korrekturaufgaben. Über VI-Datensätze und Korrekturaufgaben können Sie Detailinformationen zur Registerkarte „Erkennungen“ anzeigen und Datensätze erkannter Elemente suchen, die die von Ihnen nachverfolgte Schwachstelle aufweisen, zusammen mit den vom BigFix-Produkt importierten Assets.
- Als Schwachstellenanalyst oder Administrator können Sie die mit der Schwachstelle verknüpften Patch-Daten überwachen. Sie können auch einen Patch oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem erkannten Elementdatensatz bereitstellen.

Als IT-Korrekturspezialist haben Sie verschiedene Möglichkeiten, wie Sie die Schwachstelle mit einer Patch-Bereitstellung beheben.

- Sie können den Patch aus einem Patch-Update-Datensatz (VPU#) planen.
- Wenn angreifbaren Elementen (AEs) bevorzugte Lösungen zugeordnet sind und sie Ihnen oder Ihren Gruppen zugewiesen sind, können Sie die Patches aus einer Korrekturaufgabe mit diesen angreifbaren Elementen planen.

## Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrekturarbeitsbereich auf die Ansicht Homepage.
2. Klicken Sie in der **Startansicht auf die Bewertungsliste Zugewiesene** Korrekturaufgaben, um die Datensätze anzuzeigen.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung in der Korrekturaufgabe (VUL#) auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen möglicherweise, dass Ihr Schwachstellenmanager ein Überwachungsthema mit der Bezeichnung „Kritische Schwachstellen mit Patch-Lecks zur Erfassung von VIs (VIT#)“ mit dieser kritischen Schwachstelle erstellt hat.

   Wenn der Datensatz geöffnet ist, können Sie auch die AEs und die bevorzugten Patches überprüfen und feststellen, ob Sie oder einer Ihrer Gruppenmitglieder bereits Patch-Anforderungen zur Genehmigung eingereicht haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn Sie über genügend Informationen verfügen, möchten Sie möglicherweise jetzt eine Patch-Anforderung über diese Korrekturaufgabe senden.

   **Hinweis:**
   Wenn den mit dem Datensatz verknüpften VIs keine Patches zugeordnet sind, ist die Schaltfläche **Patch** planen im Datensatz nicht verfügbar.

4. Klicken Sie auf **Patch planen**, und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen eines Patch finden Sie unter Planen Sie Patches mit der Vulnerability Response Patch Orchestration-Integration HCL BigFix.

5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, angreifbare Elemente, Lösungen und Patches klicken, um diese Datensätze anzuzeigen.

   In diesem Beispiel kennen Sie möglicherweise anstelle eines Überwachungsthemennamens die Artikel-ID oder die Bulletin-ID und den Titel des Patch. Wenn dies der Fall ist, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen einer der VIs mit dieser Schwachstelle zugewiesen ist. Über Patch-Update-Datensätze können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung senden möchten.

6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche haben oder Daten anzeigen und Patches aus der klassischen Umgebung planen möchten, führen Sie die folgenden Schritte aus.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.

   b. Suchen Sie den gewünschten Patch-Update-Datensatz.
      Möglicherweise möchten Sie die Datensätze nach Punktzahlen kritischer Risiken filtern.

   c. Überprüfen Sie die zugehörigen Felder „AEs“ und „Prozentsatz der korrigierten AEs“ auf der Registerkarte „Korrekturstatus“.
      Wenn für die VIs Patches verfügbar sind, wird die Schaltfläche **Patch** planen oben rechts im Datensatz angezeigt.

   d. Wenn Sie eine Anforderung senden möchten, klicken Sie auf **Patch planen**.
      Weitere Informationen zum Planen eines Patch finden Sie unter Planen Sie Patches mit der Vulnerability Response Patch Orchestration-Integration HCL BigFix.

   e. Angenommen, Sie haben keine Patch-ID-Informationen, können aber das Feld Kurzbeschreibung der Korrekturaufgaben, die Ihrer Gruppe zugewiesen sind, auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht.

   f. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.

   g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
      Überprüfen Sie im geöffneten Datensatz die Registerkarte Remediation Status (Korrekturstatus) auf VIs und % der korrigierten VIs. Klicken Sie auf die zugehörigen Links für VI-Datensätze, bevorzugte Lösungen, bevorzugte Patches und Patch-Anforderungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn den mit dem Datensatz verknüpften VIs keine Patches zugeordnet sind, ist die Schaltfläche **Patch** planen im Datensatz nicht verfügbar.

**h.** Klicken Sie im Datensatz auf **Patch** planen, wenn Sie eine Patch-Anforderung senden möchten.

## Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM

Verwalten Sie Patches und Patch-Bereitstellungen für die kritischen Schwachstellen in Ihren Assets mit der Vulnerability Response -Integration mit dem Microsoft System Center Configuration Manager (SCCM).

## Patch-Orchestration mit Vulnerability Response

Die Patch-Orchestration mit Vulnerability Response verwendet geplante Importe aus Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellen-Scannern. Scanner-Erkennungsdaten stimmen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, die sie beheben können. Sie übermitteln Patch-Anforderungen zur Genehmigung, planen Patch-Updates, um angreifbare Elemente zu beheben, und überwachen den Fortschritt der Korrektur – alles von Ihrer Now Platform® -Instanz aus.

## Vulnerability Response Patch-Orchestration mit Microsoft SCCM

Wenn Vulnerability Response Patch Orchestration mit der SCCM-Anwendung Microsoft mit den Anwendungen ServiceNow® Vulnerability Solution Management, Patch Orchestration und Vulnerability Response verwendet wird, können Schwachstellenmanager und Analysten die folgenden Aufgaben ausführen:

- Weiteren Kontext und Informationen zu den Arten von Patches und Anbieterlösungen (Patches) anzeigen.
- Zeigen und überwachen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in den Vulnerability Response Arbeitsbereichen.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

- Stellen Sie Patches, die vom SCCM-Produkt [ Microsoft unterstützt werden, für Windows, CentOS, macOS, Oracleund andere Assets in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten bereit, um Konflikte mit der Arbeit zu vermeiden.
- Identifizieren Sie nicht gepatchte Assets mit Schwachstellen oder Assets, die nicht erfolgreich durch geplante Patches aus importierten Erkennungsdaten von Scannern von Drittanbietern aktualisiert wurden.
- Planen Sie verfügbare Patches entweder über den IT-Korrekturarbeitsbereich oder über die klassische Benutzeroberfläche für angreifbare, nicht gepatchte Assets aus Datensätzen für Patch-Updates, Korrekturaufgaben und erkannte Elemente.

## Wichtige Begriffe in den SCCM-Anwendungen Vulnerability Response und Microsoft .

**Konfigurationselement (Configuration Item, CI)**

CIs sind die vorhandenen Assets, die in Ihrem Configuration Management Database (CMDB)aufgeführt sind. Microsoft SCCM ruft CIs und Geräte auf.

**Sammlungen und Gerätesammlungen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.


Automatische Übersetzung

Im SCCM-Produkt Microsoft verwendete Terminologie, die sich auf eine Gruppe von Assets bezieht.

**Angreifbares Element**

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

**Instanz**

Ein eindeutiger Account der SCCM-Anwendung Microsoft. Jedes Benutzerkonto kann eine Instanz in der SCCM-Anwendung Microsoft sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für eine Now Platform -Instanz.

**Integration**

Eine Integration ist eine geplante Aufgabe in Now Platform, die Informationen aus einer Drittanbieterquelle abruft, z. B. die Integration mit den Microsoft -SCCM-Computern.

**Lösung**

Im Kontext dieser Integration gibt es zwei Arten von Lösungen: „Potenziell“ und „Bevorzugt“. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben kann. Schwachstellen haben häufig viele mögliche Lösungen. Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte, erkannte Schwachstelle.

**Patches**

Software-Updates, die Schwachstellen beheben. In der SCCM-Anwendung Microsoft werden Patches als Patches bezeichnet. Zum Beispiel verfügt Microsoft SCCM über Patches für Windows, CentOS, MAC, Oracle und andere Produkte.

**Bevorzugter Patch**

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Nach der Bereitstellung werden Patches den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie beheben.

**Korrekturaufgabe oder, vor v15.0 von Vulnerability Response, Schwachstellengruppen**

Listen der angreifbaren Elemente in der Anwendung Vulnerability Response von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

**Bereitstellung**

Die Bereitstellung für die Zwecke dieser Integration bezieht sich auf das Anwenden, Initiieren oder Planen eines Patches auf einem Computer. Sie können die von Microsoft SCCM heruntergeladenen Patches in Now Platform bereitstellen, indem Sie zu erkannten Elementen, Patches oder Korrekturaufgaben aus einzelnen Datensätzen in Vulnerability Responsenavigieren. Sie können Patches mit regelmäßigen Aufgaben auf einzelnen Computern oder in Computergruppen bereitstellen.

Die Bereitstellung in Now Platform kann sich auch auf eine Integration beziehen, die mehrere Quellen unterstützt. Eine einzelne vorhandene Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise könnten in Ihrer Umgebung mehrere Bereitstellungen der Microsoft SCCM Vulnerability-Integration vorhanden sein.

## Vulnerability Solution Management und die Vulnerability Response Patch Orchestration-Integration mit Microsoft SCCM

Die Anwendung Vulnerability Solution Management ist eine Anwendung von Now Platform, die Ihre Schwachstellenergebnisse mit der Aufgliederung der Lösungen (Patches) korreliert, die sie beheben. Identifizieren Sie die Softwarepatches von Drittanbietern für Produkte und Services, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen auf Ihre Organisation haben. Zusammen mit den Informationen zu



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scannern von Drittanbietern arbeiten die Anwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration with Microsoft SCCM zusammen, um ein Rollup bevorzugter Patches von der Lösung über die Schwachstelle bis hin zum angreifbaren Element durchzuführen, um Sie bei der Behebung von und zu unterstützen Schließen Sie Schwachstellen in Ihrer Umgebung. Die Integrationsanwendungen Solution Management for Vulnerability Response, Vulnerability Responseund Vulnerability Response Patch Orchestration Microsoft SCCM sind alle in ServiceNow® Storeverfügbar.

## Erforderliche Now Platform-Rollen

Für die Installations-, Konfigurations- und Korrekturaufgaben der -Integration sind die folgenden Rollen in Ihrer Now Platform -Instanz erforderlich.

**Administrator**

Benutzer mit dieser Rolle erhalten Berechtigungen für Anwendungen in der ServiceNow Store und laden sie in Now Platform -Instanzen herunter.

**sn_vul.vulnerability_admin**

Benutzer mit dieser Rolle aktivieren Anwendungen in der Instanz Now Platform und schließen die Konfiguration der Anwendung Vulnerability Response ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Dieser Administratorbenutzer konfiguriert alle VR-Anwendungen, -Regeln und -Integrationen von Drittanbietern.

**sn_vul_sccm.configure_integration**

Benutzer mit dieser Rolle konfigurieren die Anwendung Microsoft SCCM Patch Orchestration Integration. Diese Rolle enthält die granulare Rolle sn_vul_sccm.read_integration.

**sn_vul_sccm.read_integration**

Benutzer mit dieser Rolle können die Datensätze der Anwendung MicrosoftVulnerability Response und der Anwendung SCCM Patch Orchestration Integration sowie Patch-Orchestration-Daten anzeigen (schreibgeschützt).

**sn_vul_patch_orch.configure_patch**

Benutzer mit dieser Rolle können Patches konfigurieren und anwenden.

**sn_vul_patch_orch.read_patch**

Benutzer mit dieser Rolle können Patch-Informationen anzeigen (schreibgeschützt).

**Genehmiger**

Weisen Sie Benutzer den Genehmigergruppen „Genehmigerebene 1“ und „Genehmigerebene 2“ zu, wenn übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden sollen.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

## CI-Suchregeln

Wenn Daten aus der SCCM-Anwendung Vulnerability ResponseMicrosoft importiert werden, sucht die Anwendung Configuration Management Database (CMDB) [] anhand der Ressourcen-ID-Daten automatisch nach Übereinstimmungen in . CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen für angreifbare Elemente (AEs) hinzuzufügen, wenn AEs erstellt werden. Die folgenden CI-Suchregeln werden mit dem Basissystem ausgeliefert und dazu verwendet, CIs (Assets) zu identifizieren und den erkannten Elementen hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Suchregel basiert auf den Daten, die vom Service Graph Connector mit SCCM übernommen werden. Sie müssen die CMDB-Integration installieren und ausführen, bevor Sie die SCCM-Integrationen ausführen. Wenn Sie mehrere Installationen des SCCM-Servers haben, können Sie den Service Graph Connector-Verbindungsalias auf der SCCM-Patch-Orchestration-Konfigurationsseite konfigurieren.

### MID-Server

Die Vulnerability Response Patch Orchestration mit Microsoft SCCM ist eine lokale Integration. Sie erfordert einen eigenständigen Windows MID Server, der nicht Teil eines MID Server-Clusters ist. Der MID Server ist erforderlich, um Skripts auf Remotecomputern von Ihrer Instanz aus auszuführen, um Daten vom SCCM-Server zu importieren. APIs für diese Integration werden mit MID Servern aufgerufen, die Sie in Ihrer Now Platform -Instanz eingerichtet haben. Bereiten Sie die Patch-Orchestration-Integration von [ Vulnerability Response mit Microsoft SCCM vor

#### Integrationen und Abhängigkeiten von Vulnerability Response Patch Orchestration mit der Anwendung Microsoft SCCM

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für die Integration von Vulnerability Response Patch Orchestration mit Microsoft System Center Configuration Manager (SCCM) erforderlich. Diese Anwendungen sind im verfügbar ServiceNow® Store

## Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Patch-Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen und der klassischen Benutzeroberfläche in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind im ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familien-Releases finden Sie im Artikel KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes in der HI Knowledge Base.

| Anwendung und Release-Version |
|---|
| Vulnerability Response |
| Vulnerability Solution Management |
| Anwendung Vulnerability Response Patch Orchestration |
| Vulnerability Response Patch Orchestration with Microsoft SCCM |
| Security Support Common |
| Security Support Orchestration |
| Service Graph Connector mit SCCM |

## Vulnerability Response Tabellen der Patch-Orchestration-Anwendung

Die Anwendung Vulnerability Response Patch Orchestration enthält die folgenden Tabellen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| Patch-Update [sn_vul_patch_orch_update] | Speichert Informationen zu den Patches, die für verschiedene Instanzen verfügbar sind |
| Geräte-Update [sn_vul_patch_orch_m2m_src_ci_update] | Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in Datensätzen für erkannte Elemente angezeigt werden. |
| Sammlung [sn_vul_patch_orch_collection] | Speichert Sammlungsdaten aus verschiedenen Instanzen. |
| Gerätesammlung [sn_vul_patch_orch_m2m_src_ci_collection] | Speichert Sammlungsdaten zu erkannten Elementen. |
| Patch-Bereitstellung [sn_vul_patch_orch_deployment] | Speichert Informationen zu bereitgestellten Patches für Sammlungen und CIs. |
| Potenzieller Patch [sn_vul_patch_orch_m2m_vuln_patch] | Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können. |

## Vulnerability Response Patch Orchestration mit Microsoft SCCM-Integrationen

Die von ServiceNow® Engineering entwickelten Integrationen bilden die orchestrierte Lösungsbereitstellung mit dem SCCM-Produkt Microsoft. Die folgenden Integrationen sind in der Anwendung Microsoft SCCM Patch Orchestration Integration enthalten, die Sie aus dem ServiceNow® Storeherunterladen können.

Nachdem Sie die Integrationsanwendung in Ihrer Instanz Now Platform installiert haben, navigieren Sie zum Anzeigen dieser Integrationen zu **Integrationen** > **SCCM Patch Orchestration-Integration** > **Integrationen**. Die Anwendung Vulnerability Response verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen mit Microsoft SCCM-Endpunkten importiert werden.

| Integration | Beschreibung |
|---|---|
| Microsoft SCCM-Sammlungsintegration | • Diese Integration ist für die tägliche Ausführung geplant und wird in der verketteten Integrationsausführung zuerst ausgeführt.<br>• Ruft die Gerätesammlungen aus den SCCM-Sammlungen ab. |
| Microsoft Integration der SCCM-Gerätesammlung | • Wenn geplant, wird diese Integration durch den Abschluss der SCCM-Sammlungsintegration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Diese Integration ruft die Geräte in jeder Sammlung ab. Diese Integration erstellt Datensätze in der Tabelle „Erkannte Elemente“ und der Tabelle „Gerätesammlung“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integration | Beschreibung |
| --- | --- |
| Microsoft SCCM-Patch-Update-Integration | • Wenn geplant, wird diese Integration durch den Abschluss der SCCM-Gerätesammlungsintegration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Ruft vom SCCM-Server Informationen zu den Patches ab, die auf Geräten (Assets) installiert sind oder fehlen. |
| Microsoft Integration von SCCM-Bereitstellungen | • Wenn geplant, wird diese Integration durch den Abschluss der Patch-Update-Integration ausgelöst. Sie können sie auch bei Bedarf ausführen.<br>• Ruft Informationen zu den vom IT-Team geplanten Patches auf dem SCCM-Server ab. |

### Bereiten Sie die Patch-Orchestration-Integration von [ Vulnerability Response mit Microsoft SCCM vor

Bereiten Sie die Integration vor, indem Sie die folgenden Setup-Aufgaben ausführen.

#### Vorbereitungen

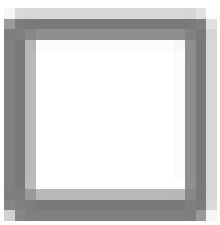
Erforderliche Rollen: admin für die Installation der Anwendungen und die Zuweisung von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

#### Warum und wann dieser Vorgang ausgeführt wird

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

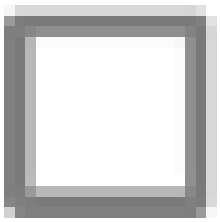
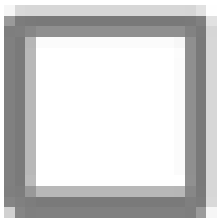
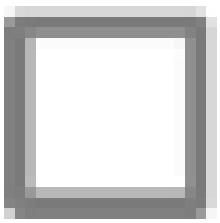
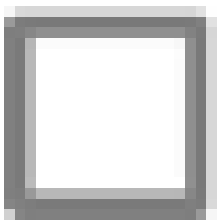
#### Prozedur

1. Befolgen Sie die folgende Prüfliste, um eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Patch Orchestration with Microsoft SCCM zu gewährleisten.
2. Möglicherweise möchten Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Informationen zu Schwachstellen und Patches in Ihre Now Platform® -Instanz importieren.

| Aufgabe | Beschreibung |
| --- | --- |
|  | (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
|  | Wenn noch nicht installiert, holen Sie sich Berechtigungen und installieren Sie die Scanner-Anwendung einer Drittpartei, um Schwachstellendaten zu importieren.<br><br>Unter Vulnerability Response-Integrationen finden Sie weitere Informationen zu Scannern von Drittanbietern, die von Vulnerability Responseunterstützt werden.<br><br>Weitere Informationen finden Sie unter . |
|  | Wenn noch nicht installiert, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Patch Orchestration with Microsoft SCCM in Ihre Instanz Now Platform® ] herunter.<br><br>Weitere Informationen finden Sie unter . |
|  | Rufen Sie Microsoft SCCM-Anmeldeinformationen ab.<br><br>Vergewissern Sie sich, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre Microsoft -Produkte erforderlich sind, damit Sie darauf zugreifen können. |
|  | Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, die die Integrationen verwalten und angreifbare Elemente korrigieren.<br><br>**Administrator**<br><br>Der Systemadministrator erhält Berechtigungen, lädt die Anwendung Microsoft SCCM Patch Orchestration und die anderen für die Integration erforderlichen Anwendungen herunter und installiert sie. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten in Vulnerability Response oder aus dem Modul „Benutzerverwaltung“ zu.<br><br>**sn_vul.vulnerability_admin**<br><br>Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Microsoft SCCM-Integrationen und der anderen Anwendungen von Drittanbietern ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, Regeln, Drittanbieterintegrationen, Vulnerability Response Patch Orchestration- und Vulnerability Solution Management-Anwendungen. |

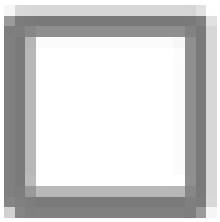


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | **sn_vul_sccm.configure_integration**<br>Benutzer mit dieser Rolle konfigurieren die Anwendung Microsoft SCCM Patch Orchestration Integration. Diese Rolle enthält die granularen Rollen sn_vul_sccm.read_integration und connection_admin, mit denen der Benutzer eine Verbindung zur SCCM-Konsole herstellen und die Integrationsinstanzen in Now Platformkonfigurieren kann.<br>**sn_vul_sccm.read_integration**<br>Benutzer mit dieser Rolle können die Datensätze der Anwendung MicrosoftVulnerability Response und der Anwendung SCCM Patch Orchestration Integration sowie Patch-Orchestration-Daten anzeigen (schreibgeschützt).<br>**sn_vul_patch_orch.configure_patch**<br>Benutzer mit dieser Rolle können Patches konfigurieren und anwenden. Von diesem Benutzer angeforderte Patches aus Datensätzen für angreifbare Elemente und Patch-Updates werden zur Genehmigung gesendet, wenn das Change-Management aktiv ist und Genehmiger zugewiesen sind.<br>**sn_vul_patch_orch.read_patch**<br>Benutzer mit dieser Rolle können Patch-Informationen zu Datensätzen anzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind.<br>**Genehmiger**<br>Benutzer, die der Genehmigerebene 1 und optional der Genehmigerebene 2 zugewiesen sind, genehmigen übermittelte Patch-Anforderungen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Gruppe „Genehmiger Ebene 1“ übermittelt.<br>Weitere Informationen zum Genehmigungsprozess finden Sie unter Konfigurieren Sie die Integration von Vulnerability Patch Orchestration mit Microsoft SCCM.<br>Weitere Informationen zum Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.<br>Der Systemadministrator führt die anfängliche Zuweisung von Rollen zu Benutzern und Gruppen für die Integration durch. Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Falls noch nicht erstellt, ziehen Sie es möglicherweise vor, zusätzliche Gruppen für die Rollen „Korrekturspezialist“ und |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | „Schwachstellenanalyst“ zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen . |
|  | Vergewissern Sie sich, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Jobs in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind.<br>○ Die Vulnerability Response Patch Orchestration mit Microsoft SCCM ist eine lokale Integration, für die Sie einen eigenständigen Windows MID Server verwenden müssen. Weitere Informationen zu MID Servern in Ihrer Instanz finden Sie unter MID Server .<br>○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es. |

### Installieren Sie die Anwendung Vulnerability Response Patch Orchestration with Microsoft SCCM

Laden Sie die Anwendung aus dem ServiceNow Storeherunter.

#### Vorbereitungen

Vergewissern Sie sich vor der Installation der Anwendung, dass Sie alle Elemente der Prüfliste in Bereiten Sie die Patch-Orchestration-Integration von [ Vulnerability Response mit Microsoft SCCM vorabgeschlossen haben.

Erforderliche Rollen: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und Installation der Anwendung. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) zum Konfigurieren von Vulnerability Response Patch Orchestration Microsoft SCCM und anderen Anwendungen nach der Installation.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, ist keine Berechtigung erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

#### Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie nach der Anwendung **Vulnerability Response Patch Orchestration with Microsoft SCCM**, und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung installiert, die Sie aus dem ServiceNow Storeheruntergeladen haben.
3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation zu **Alle** > **Microsoft SCCM Patch Orchestration-Integration** > **Konfiguration** , um mit der Konfiguration fortzufahren.

## Konfigurieren Sie die Integration von Vulnerability Patch Orchestration mit Microsoft SCCM

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren Kontoinformationen, und validieren Sie Ihre Anmeldeinformationen.

### Vorbereitungen

Erforderliche Rollen: sn_vul.vulnerability_admin und sn_vul_sccm.configure_integration

### Prozedur

1. Navigieren zu **Alle** > **Microsoft SCCM Patch Orchestration-Integration** > **Konfiguration**.
2. Füllen Sie die Felder mit Ihren Microsoft SCCM-Informationen und -Anmeldeinformationen aus.

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Der Name des Microsoft SCCM-Instanzkontos, das Sie verwenden möchten, z. B. Microsoft SCCM Patch Management Integration. |
| Hostname | Geben Sie die URL für den SCCM-Host Microsoft ein. |
| Benutzername | Geben Sie den Benutzernamen Ihres SCCM-Kontos Microsoft ein. |
| Passwort | Geben Sie das Passwort Ihres Microsoft SCCM-Kontos ein. |
| MID-Server | Geben Sie den Namen des eigenständigen MID Servers aus der Liste ein, den Sie verwenden möchten. Weitere Informationen zu MID Servern und Setup-Aufgaben finden Sie unter Bereiten Sie die Patch-Orchestration-Integration von [ Vulnerability Response mit Microsoft SCCM vorNow Platform®. |

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen Microsoft SCCM und Ihrer Instanz Now Platform® wird im Feld Validierungsstatus angezeigt. Wenn kein erfolgreicher Test angezeigt wird, folgen Sie den Eingabeaufforderungen.
4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer Instanz mehrere Konfigurationen von hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:

   a. Navigieren zu **Alle** > **Microsoft SCCM Patch Orchestration-Integration Integrationsinstanzen**.

   b. Vergewissern Sie sich, dass der Anwendungsbereich Vulnerability Response Patch Orchestration with Microsoft SCCMim Feld Anwendungsbereich angezeigt wird.

   c. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Füllen Sie das Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Name für die Integrationsinstanz. |
| Anwendung | Vulnerability Response Patch Orchestration mit Microsoft SCCM |
| Integration | [Nur lesen] Microsoft SCCM Patch Management ist die Standardeinstellung. |
| Aktiv | Der Standardwert ist aktiviert. Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv. |

**e.** Klicken Sie auf **Absenden**.
Ihre neue Integrationsinstanz wird in der Liste „Integrationsinstanzen“ angezeigt.

**f.** Wiederholen Sie die Schritte 1 bis 3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.

**5.** Richten Sie Genehmigungen für Patch-Anforderungen ein.
Standardmäßig ist eine Systemeigenschaft [**sn_vul_patch_orch.patch_approval_required**] aktiviert, sodass Patch-Bereitstellungen, wenn sie geplant sind, zur Überprüfung und Genehmigung an Benutzer übermittelt werden, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind.

Wenn Sie möchten, dass Benutzer mit der Rolle sn_vul_patch_orch.configure_patch Patches ohne Genehmigung planen können, können Sie die Eigenschaft [**sn_vul_patch_orch.patch_approval_required**] deaktivieren. Möglicherweise möchten Sie Genehmigungen aktiviert lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

**Hinweis:**
Wenn Sie die Genehmigungssystemeigenschaft deaktivieren, kann jeder Benutzer mit der Rolle „sn_vul_patch_orch.configure_patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

So deaktivieren Sie als Benutzer mit der Rolle „sn_vul.vulnerability_admin“ die Systemeigenschaft:

**a.** Navigieren zu **Alle** > **sys.properties.list**.

**b.** Suchen Sie **sn_vul_patch_orch.patch_approval_required**, und klicken Sie darauf, um den Datensatz zu öffnen.

**c.** Geben Sie im Feld Wert `false`ein.

**d.** Klicken Sie auf **Aktualisieren**.

**6.** Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie Genehmiger für Patch-Anforderungen zuweisen. Führen Sie als Benutzer mit der Rolle „sn_vul.vulnerability_admin“ die folgenden Schritte aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**.

b. Wenn die **Genehmigungsregel für die Bereitstellung von Patch-Updates** nicht in der Liste angezeigt wird, klicken Sie oben links auf dem Bildschirm rechts neben dem grünen Filtersymbol auf **Alle**, um die gesamte Liste anzuzeigen.

c. Klicken Sie in der Liste auf **Genehmigung der Patch-Aktualisierung bereitstellen**.

d. Klicken Sie im Datensatz auf der Registerkarte Genehmigungskonfiguration auf **Standardkonfiguration Patch-Aktualisierungsgenehmigung**.

e. Klicken Sie im Datensatz auf **Ebene 1 – Genehmigung der Patch-Aktualisierung**.

f. Fügen Sie Benutzer in dieser Gruppe hinzu.

Die dieser Gruppe zugewiesenen Benutzer genehmigen Patch-Anforderungen, die von Benutzern mit der Rolle sn_vul_patch_orch.configure_patch übermittelt wurden. Navigieren Sie zu **Meine Genehmigungen**, um die Anforderungen anzuzeigen und zu verarbeiten.

7. Klicken Sie auf**Aktualisieren**, um Ihre Änderungen zu speichern.
8. **Wahlweise:** Sie können mehrstufige Genehmigungen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.

a. Klicken Sie bei angezeigtem Genehmigungsdatensatz für das Standardkonfigurations-Patch-Update auf **Neu**.

b. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungsebene, z. B. **Ebene 2 – Genehmigung der Patchaktualisierung**. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird. |
| Erforderliche Genehmigung | Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind:<br>▪ Ein Genehmiger erforderlich<br>▪ Alle Anwender müssen genehmigen |
| Reihenfolge | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rolle | Wählen Sie eine Rolle für die Gruppe aus der Liste aus. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. |
| Genehmigungskonfiguration | Enthält die Genehmigungskonfigurationen |
| Zuweisen mit | Wählen Sie eine Option aus:<br>▪ Anwender und Anwendergruppe<br>▪ Genehmigungstabellenfeld<br>▪ Skript |
| Gruppen | Genehmigerebenengruppe, die aus mehreren Benutzern besteht. Der Benutzer muss eine der folgenden von Ihnen angegebenen Rollen haben. |
| Anwender | Bearbeiten Sie die in den Gruppen aufgeführten Benutzer. |

**c.** Klicken Sie auf **Absenden**, um Ihre Änderungen zu speichern.

### Anzeigen von Patch-Daten und Patch-Daten-Rollups für die Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM

Patch-Daten und Patch-Rollup-Daten sowie Schwachstelleninformationen und der Korrekturstatus Ihrer Schwachstellen werden in Datensätzen in Ihrer Instanz angezeigt.

## Patch-Daten in den Vulnerability Response -Arbeitsbereichen anzeigen

Erforderliche Rollen:

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind

Im IT-Korrekturarbeitsbereich können Sie die Patches anzeigen:

- In der Ansicht „Startseite“, in der Sie auf Bewertungslisten klicken können, um Datensätze für bevorzugte Lösungen für VIs, angreifbare CIs und bevorzugte Patches für VIs anzuzeigen.
- In der Listenansicht, in der Sie alle Patch-Update-Datensätze (VPUs) über die Links „Patches“ und die Ihnen zugewiesenen angreifbaren Elemente (VITs) mit Patches anzeigen können.

Sie können Patches aus den folgenden Datensätzen planen:

- Aus Patch-Update (VPU)
- Korrekturaufgabe (RT)
- SDI-Datensätze (Discovery Item).

In Vulnerability Manager Workspace können Sie Patches anzeigen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Ansicht „Homepage“ zu Überwachungsthemen, in der Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und, falls der Patch heruntergeladen wurde, alle auf der Registerkarte **Angreifbare Elemente** anzeigen können.
- Über die Listenansicht der Korrekturmaßnahmen, in der Sie Patch-Daten zu VI-Datensätzen auf der Registerkarte „**Angreifbare Elemente** “ anzeigen können.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**.

## Patch Aktualisieren Sie Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie Patch-Datensätze (VPU) in Vulnerability Response Arbeitsbereichen aus der Listenansicht im IT-Korrekturarbeitsbereich an. Patch-Update-Datensätze in der klassischen Umgebung und in Vulnerability Response Workspaces enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Anbietern, die von der Anwendung Vulnerability Solution Management importiert werden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer bestimmten Schwachstelle enthält, die durch einen Patch behoben werden kann. Darüber hinaus sind auch alle Geräte und enthalten, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIs und die Gesamtzahl der VIs umfasst, für die ein Patch als bevorzugter Patch gilt.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links für Datensätze in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in den Vulnerability Response Arbeitsbereichen angezeigt.
- Patch-Anforderungen, die die Korrekturbesitzer zur Genehmigung übermittelt haben.

## Status-Rollup für Datensätze angreifbarer Elemente

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Rollup für Patch-Daten und -Status für Patch-Orchestration in Vulnerability Response.

## Datensätze, die ein Rollup für die Anzahl aktiver VIs durchführen

Um ein Rollup aller Patches für alle Schwachstellen zu vermeiden, übernimmt die geplante Aufgabe nur Änderungen an der aktiven AEs-Anzahl. Für diese Anzahländerungen und zugehörigen Daten wird ein Rollup zu den folgenden Datensätzen in Vulnerability Responsedurchgeführt :

- VIT
- RT
- Schwachstellenlösung
- Patch-Update



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Anzeigen von Daten für Patches ohne Lösungen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

## Patchen Sie Daten auf dem Vulnerability Response

Die Dashboards für Schwachstellenmanagement (PA) und CISO sind in einem Abonnement mit der Anwendung Performance Analytics für die Anwendung Vulnerability Response enthalten. Wenn Sie ein Abonnement für Performance Analyticshaben, aber keine Patch-Orchestration-Integration installiert haben, wird die Registerkarte „Korrektur“ im CISO-Dashboard angezeigt, aber nicht mit Daten ausgefüllt.

Navigieren Sie für das Dashboard für Schwachstellenmanagement (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**. Klicken Sie auf die Registerkarte **Remediation**, und scrollen Sie zum Ende der Seite, um Patch-Update-Daten anzuzeigen: geplante und nicht geplante Patches, Patches mit verfehlten Zieldaten und wöchentliche Anzahlen.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**. Scrollen Sie bei ausgewählter Registerkarte Übersicht zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches mit fehlendem Zieldatum.

Weitere Informationen zu den Dashboards [ Vulnerability Response finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet, Patchen Sie die Orchestration mit den Vulnerability Response -Arbeitsbereichenund Patch-Orchestration-Daten werden in den Vulnerability Response -Dashboards angezeigt.

### Planen von Patches mit der Microsoft SCCM-Integration mit Vulnerability Response

Planen Sie Patches aus Datensätzen für Patch-Updates und Korrekturaufgaben in der Anwendung Vulnerability Response in Ihrer Instanz Now Platform.

#### Vorbereitungen

Ab Version 16.1 können Sie Patches aus den Vulnerability Response Arbeitsbereichen oder aus der klassischen Umgebung planen.

Erforderliche Rollen:

- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind

#### Prozedur

1. Navigieren Sie in den Arbeitsbereichen für Schwachstellen Vulnerability Response als Benutzer mit der Rolle „sn_vul.remediation_owner“ zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Klicken Sie auf der Homepage auf **Bevorzugter Patch für AEs**.
   Die Liste der Patch-Update-Datensätze für die VIs mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.
3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie darauf, um ihn zu öffnen.

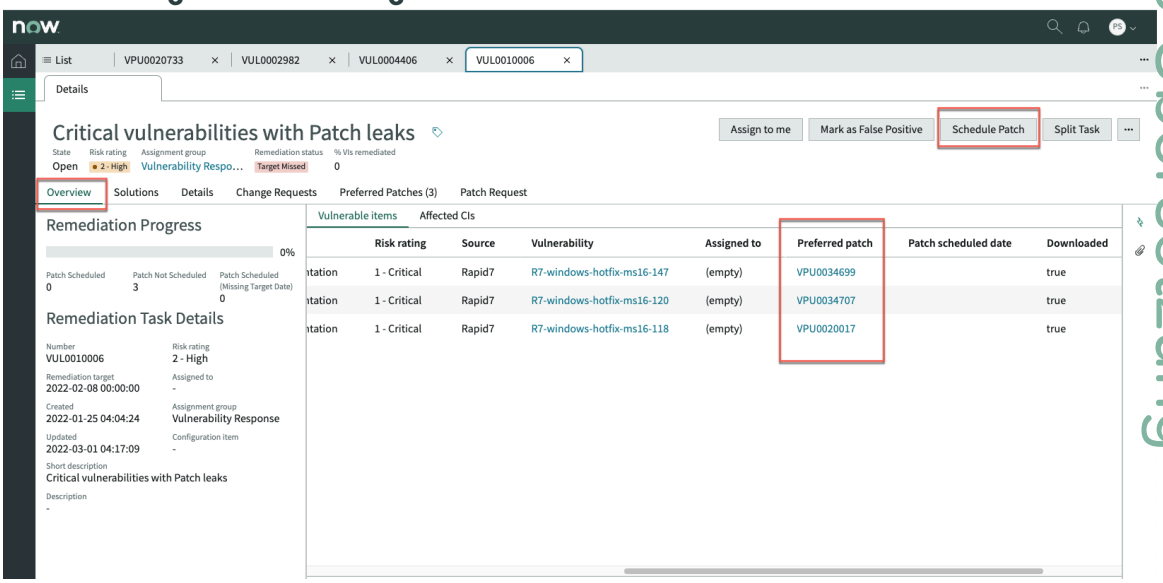
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** , und suchen Sie nach einem Patch-Update-Datensatz.
   Der Patch-Update-Datensatz wird angezeigt. Möglicherweise möchten Sie die Daten überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.
5. In der folgenden Tabelle erfahren Sie, welche Daten im Arbeitsbereich für IT-Fehlerkorrekturen angezeigt werden und was Sie tun können.
6. Klicken Sie **auf Patch planen**.
7. Füllen Sie im Dialogfeld die Felder aus.
8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller übermittelten Anforderungen in anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** aus der Listenansicht.
9. Alternativ können Sie Patches aus Korrekturaufgaben (Remediation Tasks, RT) planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

**Hinweis:**
Die Option zum Planen eines Patch aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn Patches den VIs in der Aufgabe zugeordnet (zugeordnet) sind. Diese Patches werden in der Spalte Bevorzugter Patch angezeigt, wenn Sie mit ausgewählter Registerkarte Übersicht rechts neben Datensätzen für Korrekturaufgaben blättern.

**Korrekturaufgabe mit bevorzugten Patches**




10. Klicken Sie im RT-Datensatz auf **Patch** planen, und führen Sie die oben aufgeführten Schritte aus, um den Patch im Dialogfeld zu planen.
11. **Wahlweise:** Sie können Patches für die vorherigen Schritte in der klassischen Umgebung planen. Führen Sie die folgenden Schritte aus, um diese Datensätze zu finden.
    a. Navigieren Sie in der klassischen Umgebung zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.
    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** und suchen Sie einen Datensatz.
Sie verfolgen den Korrekturstatus auf der Registerkarte Korrekturstatus nach. Am Ende des Datensatzes werden Patch-Daten unter Zugehörige Links angezeigt.

d. Klicken Sie auf **Patch planen**, und füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Bereitstellungsname | Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen. |
| Beschreibung | Fügen Sie weiteren Text zum Patch hinzu. Diese Informationen werden im Feld Beschreibung des Patch-Update-Datensatzes angezeigt. |
| Bereitstellungstyp | Wählen Sie eine Option aus der Liste aus.<br>▪ Erforderlich – Dieser Patch ist ein erforderliches Update.<br>▪ Verfügbar – Dieser Patch ist nicht erforderlich, aber für die Bereitstellung verfügbar. |
| Sammlung | Wählen Sie eine Sammlung (Gruppe von Assets) aus der Liste aus, um fortzufahren. Diese Gruppen sind die aus SCCM importierten Asset-Sammlungen. |
| Bereitstellungszeit basierend auf | Wählen Sie eine Zeitzone aus der Liste aus, auf der Ihr Bereitstellungszeitfenster basieren soll. |
| Verfügbare Zeit | Legen Sie den Wert für den Zeitpunkt fest, zu dem der Patch zum ersten Mal für die Bereitstellung verfügbar wird. |
| Frist | Legen Sie die Frist fest. Dieser Wert gibt den letzten Tag an, an dem der Patch installiert werden kann. |

e. Klicken Sie auf **Bereitstellen**.

### REST-Nachrichten für Vulnerability Response Patch Orchestration mit Microsoft SCCM

Die Vulnerability Response Patch Orchestration mit Microsoft SCCM verwendet die SCCM Windows Management Instrumentation (WMI)-Klassen, um die SCCM-Server-API aufzurufen.

## Übersicht

Der SMS-Provider stellt der API einen Interoperabilitätszugriff über HTTPS bereit, der als Verwaltungsservice bezeichnet wird. Der Verwaltungsservice ist eine REST-API (Representational State Transfer), die auf dem Protokoll Open Data (OData) v4 basiert.

Weitere Informationen zur Verwendung des Verwaltungsservice mit dieser Integration finden Sie unter Was ist der Verwaltungsservice in Configuration Manager?



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Da die erforderliche Authentifizierung das NTLM-Protokoll von Windows New Technology LAN Manager verwendet, werden Aufrufe an die APIs über den MID Server mit PowerShell-Skripts durchgeführt.

## Microsoft SCCM-Integration

Sie können die REST-Nachricht für die Microsoft SCCM-Integration verwenden, um Informationen aus Microsoft SCCM abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an Microsoft SCCM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

WMI-Klassennamen:

- SMS_Sammlung
- SMS_DeploymentSummary

| Parametername | Wert | Beschreibung |
|---|---|---|
| URL | Dynamische Werte basierend auf dem Benutzer | Gibt den Endpunkt der SCCM-Konsole an |

## Microsoft SCCM-Patch bereitstellen

Sie können die REST-Nachricht für die Microsoft SCCM-Integration verwenden, um Patches von Ihrem Now Platform® auf dem Microsoft SCCM zu planen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an SCCM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

| REST-Methode | Beschreibung |
|---|---|
| POST-Bereitstellungs-Patch | Plant den Patch für die SCCM-Konsole auf einzelnen/mehreren Computern. |

| Parametername | Wert | Beschreibung |
|---|---|---|
| URL | Dynamische Werte basierend auf dem Benutzer | Gibt den Endpunkt der SCCM-Konsole an. |
| Titel | Dynamische Werte basierend auf dem Benutzer | Titel der Bereitstellung. |
| einstellungen_tag | XML-Tag-benannte Einstellungen mit Werten | Gibt Einstellungen an, die unterschiedliche Parameter haben und während der Planung des Patch an SCCM gesendet werden. |
| computer_tag | Computer mit XML-Tag-Namen und Werten | Gibt eine Liste der Computer an, auf denen der Patch geplant wird. |
| site_name | Wert aus der Patch-Aktualisierung | Name der Site, auf der der Patch vorhanden ist |
| Patch_id | Wert aus der Patch-Aktualisierung | ID des Patch |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Datentransformation für die Integration von Patch Orchestration mit Microsoft SCCM

Daten werden aus der Patch-Orchestration mit Microsoft SCCM-Integration abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Now Platform® -Instanz transformiert.

## Import der SCCM-Sammlung

Die Daten aus den importierten Sammlungen werden in die Tabelle „SCCM-Sammlungsimport“ [sn_vul_sccm_collection_import] geladen. Die SCCM-Sammlungen (Transformationszuordnung) werden verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der SCCM-Sammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach SCCM-Sammlungstransformation. In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_collectionid | source_id | Eindeutige ID der Sammlung. |
| u_name | Name | Name der Sammlung |
| u_membercount | device_count | Anzahl der Geräte in dieser Sammlung. |
| [Skript] | integration_instance | Name der Instanz, aus der der Patch importiert wird. |

### SCCM-Sammlungsimport-Transformationszuordnungsskript-Timing

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Import von SCCM-Patch-Updates

Die Daten aus den importierten Patches werden in die Tabelle „SCCM-Patch-Update-Import“ [sn_vul_sccm_patch_update_import] geladen.

Die SCCM-Patch-Update-Transformation wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Patch-Update-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** , und suchen Sie die SCCM-Patch-Update-Transformation.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### SCCM-Patch-Update Import-Transformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| [Skript] | URLs | URLs für den Patch |
| u_nummissing | num_missing | Anzahl der Geräte, auf denen dieser Patch fehlt. |
| [Skript] | date_release | Datum der Patch-Veröffentlichung. |
| u_bulletinid | Bulletin_ID | Bulletin-ID für den Patch |
| u_numtotal | num_total | Gesamtanzahl der Geräte. |
| u_localizeddescription | Beschreibung | Beschreibung für den Patch |
| [Skript] | is_highest_Supersedence | Ist der Patch mit der höchsten Ersetzung. |
| u_numnotapplicable | num_not_applicable | Anzahl der Geräte, die für diesen Patch nicht geeignet sind. |
| u_iscontentprovisioned | is_downloaded | Wenn Patch auf den SCCM-Server heruntergeladen wird. |
| u_numunknown | num_unknown | Gesamtzahl der unbekannten Geräte. |
| u_articleid | article_id | Artikel-ID des Patch. |
| u_localizeddisplayname | Titel | Titel des Patch |
| u_ci_id | source_id | Eindeutige ID für den Patch in SCCM. |
| u_numpresent | num_present | Anzahl der Geräte, auf denen der Patch installiert ist |
| [Skript] | integration_instance | Name der Instanz, aus der der Patch importiert wird. |
| [Skript] | sn_vul_solution | Lösung basierend auf der Quell-ID. |
| [Skript] | last_modified | Datum der letzten Patch-Änderung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### SCCM-Patch-Update Import-Transformationszuordnungsfelder (Fortsetzung)

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_severity | source_severity | Schweregrad des Patch. |

### SCCM-Patch-Update Import-Transformationszuordnungsskript-Timing

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## SCCM-Geräte-Patch-Update-Import

Die Daten aus den importierten relevanten Patches auf Geräten werden in die Tabelle „SCCM-Geräte-Patch-Update-Import“ [sn_vul_sccm_device_patch_import] geladen.

SCCM-Geräte-Patch-Update-Transformation wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Update-Import des SCCM-Gerätepatches verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** , und suchen Sie die Update-Transformation des SCCM-Geräte-Patch.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### SCCM-Geräte-Patch-Update-Transformationszuordnungs-Skript-Timing

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**SCCM-Geräte-Patch-Update-Transformationszuordnungs-Skript-Timing (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und Patches sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_sccm]. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

## Import der SCCM-Gerätesammlung

Die Daten aus den importierten Gerätesammlungen werden in die Tabelle „SCCM-Gerätesammlungsimport“ [sn_vul_sccm_device_collection_import] geladen.

Die Importtransformation der SCCM-Gerätesammlung wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Gerätesammlungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie die SCCM-Gerätesammlungstransformation.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

**Timing des Transformationszuordnungsskripts für Gerätesammlungsimport**

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Erstellen und Aktualisieren von CIs basierend auf den CI-Suchregeln und -sammlungen sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript Werte in der Bereichsvariablen [sn_vul_sccm]. Dieses Skript ist für den |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Timing des Transformationszuordnungsskripts für Gerätesammlungsimport (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| | internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

**SCCM-Gerätesammlung Import-Transformationszuordnungsfelder**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Eindeutige ID einer Aktion. |
| U_name | Name | Name der Aktion |
| [Skript] | Sn_vul_sccm_discovered_item | Referenz des erkannten Elements, auf dem der Patch bereitgestellt wird |
| U_status | Status | Status der Aktion |
| [Skript] | Sn_vul_patch_orch_update | Referenz des Patches |
| U_apply_count | Anzahl_Erfolg | Erfolgsanzahl der Aktion. |
| U_retry_count | Erneut versuchen | Anzahl der Wiederholungen der Aktion. |
| [Skript] | Bereitstellungszeit | Startzeit der Aktion. |
| [Skript] | Frist | Endzeit der Aktion. |
| [Skript] | Source_created | Erstellungszeit der Aktion. |
| [Skript] | integration_instance | Name der Instanz, aus der die Aktion importiert wird. |

## SCCM-Bereitstellungsimport

Die Daten aus importierten Bereitstellungen werden in die Tabelle „SCCM-Bereitstellungsimport“ [sn_vul_sccm_deployment_import] geladen.

Die Importtransformation der SCCM-Bereitstellung wird verwendet, um die importierten Informationen zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Bereitstellungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** und suchen Sie nach der SCCM-Bereitstellungstransformation.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### SCCM-Bereitstellungstransformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Eindeutige ID einer Bereitstellung. |
| u_name | Name | Name der Bereitstellung. |
| [Skript] | Frist | Frist für die Bereitstellung. |
| u_numberinprogress | count_progress | Anzahl der Geräte, die für die Bereitstellung ausgeführt werden. |
| [Skript] | deployment_time | Startzeit der Bereitstellung. |
| [Skript] | integration_instance | Name der Instanz, aus der die Bereitstellung importiert wird. |
| [Skript] | source_created | Erstellungszeit der Bereitstellung. |
| [Skript] | sn_vul_patch_orch_update | Referenz des Patch |
| [Skript] | sn_vul_patch_orch_collection | Referenz des erkannten Elements, für das der Patch bereitgestellt wird. |
| u_softwarename | Name | Name der Bereitstellung. |
| u_numberother | count_other | Andere Anzahl von Geräten für die Bereitstellung. |
| u_numberunknown | count_unknown | Unbekannter Statusanzahl von Geräten für die Bereitstellung. |
| u_deploymentid | source_id | Eindeutiger Bezeichner der Bereitstellung. |
| u_numberErfolg | count_success | Erfolgsanzahl der Geräte für die Bereitstellung. |
| u_numbererrors | count_error | Fehleranzahl der Geräte für die Bereitstellung. |
| u_numbertargeted | count_total | Gesamtanzahl der Geräte für die Bereitstellung. |

### SCCM-Bereitstellungs-Import-Transformationszuordnungs-Skript-Timing

| Skript | Beschreibung |
|---|---|
| OnStart (wenn für einen Importsatz eine Transformation erstellt wurde). | Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**SCCM-Bereitstellungs-Import-Transformationszuordnungs-Skript-Timing (Fortsetzung)**

| Skript | Beschreibung |
|---|---|
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

### Beispiel-Workflow für die Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM

Ein Beispiel für die Funktionsweise der Patch-Orchestration mit Microsoft SCCM.

#### Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gepatcht. Das letzte Patch-Zeitfenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der kritischen Natur dieser Schwachstelle können Sie nicht zwei weitere Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin für Vulnerability Manager Workspace.
- sn_vul.remediation_owner, um den Arbeitsbereich des IT-Korrekturbesitzers anzuzeigen.
- Rolle sn_vul_patch_orch.configure_patch zum Konfigurieren und Planen von Patches.
- sn_vul_patch_orch.read_patch, um Patch-Informationen in Datensätzen anzuzeigen (schreibgeschützt). Diese Rolle wird mit den Rollen sn_vul.remediation_owner und sn_vuln.vulnerability_analyst geerbt, die für die Arbeitsbereiche IT Remediation und Vulnerability Manager erforderlich sind.

#### Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenmanager oder Analyst, der im Arbeitsbereich des Schwachstellenmanagers arbeitet, sollten Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIs mit kritischen Schwachstellen zu erfassen. Mit der Integration von Patch Orchestration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. In der folgenden Tabelle sind einige Beispiele mit den Bedingungen aufgeführt, die Sie für Überwachungsthemen für die Patch-Orchestration festlegen können. Verwenden Sie diese Beispiele, um die Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Weitere Informationen zum Einrichten des Überwachungsthemas finden Sie unter Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema.

**Beispiele für Überwachungsthemen für die Patch-Orchestrierung in Vulnerability Manager Workspace**

| Name des Überwachungsthemas | Beschreibung |
|---|---|
| Kritische Schwachstellen mit Patch-Lecks | Risikobewertung ist 1 – kritisch UND<br>Grund ist „Patch nicht geplant“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Beispiele für Überwachungsthemen für die Patch-Orchestrierung in Vulnerability Manager Workspace (Fortsetzung)**

| Name des Überwachungsthemas | Beschreibung |
|---|---|
| Kritische Schwachstellen mit geplanten Patches (fehlende SLA) | Grund ist „Patch geplant“ (fehlendes Zieldatum) |
| Kritische Schwachstellen mit geplanten Patches | Risikobewertung ist 1 – kritisch UND<br>Geplantes Patch-Datum ist nicht leer UND<br>Grund ist „Patch geplant“. |

- Nachdem Sie als Schwachstellenmanager oder Analyst die Überwachungsthemen und Korrekturmaßnahmen erstellt haben, generieren Sie Korrekturaufgaben. Über VI-Datensätze und Korrekturaufgaben können Sie Detailinformationen zur Registerkarte „Erkennungen“ anzeigen und Datensätze erkannter Elemente suchen, die die von Ihnen nachverfolgte Schwachstelle aufweisen, zusammen mit den vom SCCM-Produkt importierten Assets.
- Als Schwachstellenanalyst oder Administrator können Sie die mit der Schwachstelle verknüpften Patch-Daten überwachen. Sie können auch einen Patch oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem erkannten Elementdatensatz bereitstellen.

Als IT-Korrekturspezialist haben Sie verschiedene Möglichkeiten, wie Sie die Schwachstelle mit einer Patch-Bereitstellung beheben.

- Sie können den Patch aus einem Patch-Update-Datensatz (VPU#) planen.
- Wenn angreifbaren Elementen (AEs) bevorzugte Lösungen zugeordnet sind und sie Ihnen oder Ihren Gruppen zugewiesen sind, können Sie die Patches aus einer Korrekturaufgabe mit diesen angreifbaren Elementen planen.

### Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrekturarbeitsbereich auf die Ansicht Homepage.
2. Klicken Sie in der **Startansicht auf die Bewertungsliste Zugewiesene** Korrekturaufgaben, um die Datensätze anzuzeigen.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung in der Korrekturaufgabe (VUL#) auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen möglicherweise, dass Ihr Schwachstellenmanager ein Überwachungsthema mit der Bezeichnung „Kritische Schwachstellen mit Patch-Lecks zur Erfassung von VIs (VIT#)“ mit dieser kritischen Schwachstelle erstellt hat.

   Wenn der Datensatz geöffnet ist, können Sie auch die AEs und die bevorzugten Patches überprüfen und feststellen, ob Sie oder einer Ihrer Gruppenmitglieder bereits Patch-Anforderungen zur Genehmigung eingereicht haben.
3. Wenn Sie über genügend Informationen verfügen, möchten Sie möglicherweise jetzt eine Patch-Anforderung über diese Korrekturaufgabe senden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn den mit dem Datensatz verknüpften VIs keine Patches zugeordnet sind, ist die Schaltfläche **Patch** planen im Datensatz nicht verfügbar.

4. Klicken Sie auf **Patch planen**, und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen eines Patch finden Sie unter Planen von Patches mit der Microsoft SCCM-Integration mit Vulnerability Response.
5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, angreifbare Elemente, Lösungen und Patches klicken, um diese Datensätze anzuzeigen.
   In diesem Beispiel kennen Sie möglicherweise anstelle eines Überwachungsthemennamens die Artikel-ID oder die Bulletin-ID und den Titel des Patch. Wenn dies der Fall ist, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen einer der VIs mit dieser Schwachstelle zugewiesen ist. Über Patch-Update-Datensätze können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung senden möchten.
6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche haben oder Daten anzeigen und Patches aus der klassischen Umgebung planen möchten, führen Sie die folgenden Schritte aus.

   a. Navigieren zu **Vulnerability Response** > **Patches** > **Alle**.

   b. Suchen Sie den gewünschten Patch-Update-Datensatz.
      Möglicherweise möchten Sie die Datensätze nach Punktzahlen kritischer Risiken filtern.

   c. Überprüfen Sie die zugehörigen Felder „AEs“ und „Prozentsatz der korrigierten AEs“ auf der Registerkarte „Korrekturstatus“.
      Wenn für die VIs Patches verfügbar sind, wird die Schaltfläche **Patch** planen oben rechts im Datensatz angezeigt.

   d. Wenn Sie eine Anforderung senden möchten, klicken Sie auf **Patch planen**.
      Weitere Informationen zum Planen eines Patch finden Sie unter Planen von Patches mit der Microsoft SCCM-Integration mit Vulnerability Response.

   e. Angenommen, Sie haben keine Patch-ID-Informationen, können aber das Feld Kurzbeschreibung der Korrekturaufgaben, die Ihrer Gruppe zugewiesen sind, auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht.

   f. Navigieren zu **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.

   g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
      Überprüfen Sie im geöffneten Datensatz die Registerkarte Remediation Status (Korrekturstatus) auf VIs und % der korrigierten VIs. Klicken Sie auf die zugehörigen Links für VI-Datensätze, bevorzugte Lösungen, bevorzugte Patches und Patch-Anforderungen.

      **Hinweis:**
      Wenn den mit dem Datensatz verknüpften VIs keine Patches zugeordnet sind, ist die Schaltfläche **Patch** planen im Datensatz nicht verfügbar.

   h. Klicken Sie im Datensatz auf **Patch** planen, wenn Sie eine Patch-Anforderung senden möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Qualys Vulnerability Integration verstehen

Die Produktsensoren von Qualys erfassen die Daten und senden sie automatisch an die Anwendung Qualys, die die Informationen kontinuierlich analysiert und korreliert. Die Lösung lässt sich problemlos in Vulnerability Response als Qualys Vulnerability Integration integrieren, um Schwachstellen in CIs und Business Services zuzuordnen und so Auswirkungen und Priorität potenziell böswilliger Bedrohungen zu bestimmen.

Konfigurieren Sie Qualys Vulnerability Integration mit **Schwachstelle** > **Administration** > **Setup-Assistent** , um den Datenabruf flexibler und skalierbarer zu machen.

Wenn Sie mehrere Bereitstellungen der Anwendung Qualys Cloud Platform haben, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen und ihre Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen mehreren Bereitstellungen überschneiden. Daten aus jeder Bereitstellung werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar. Qualys Vulnerability Integration Knowledge Base-Datensätze werden über Bereitstellungen hinweg normalisiert, wodurch sichergestellt wird, dass Instanzen derselben Schwachstelle in allen Bereitstellungen als dieselbe Schwachstelle behandelt werden.

**Hinweis:**
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber Sie können sie deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

**Hinweis:**
Qualys Vulnerability Integration erstellt zwar Integrationen für Geräteliste, Asset-Gruppe, dynamische Suchliste und statische Suchliste, sie sind jedoch für den normalen Betrieb nicht erforderlich.

## Verfügbare Versionen

| Release-Version für Washington DC | Releasehinweise |
|---|---|
| Qualys Vulnerability Integration v12.7, v12.8 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Installierte Komponenten

Eine aktuelle Liste der Rollen, Integrationsaufgaben und Tabellen, die mit der Integration installiert werden, sowie einen Link zu Anweisungen zum Anzeigen der derzeit in Ihrer Instanz installierten Elemente finden Sie unter Mit dem installierte Komponenten Qualys Vulnerability Integration.

## Primäre und unterstützende Integrationen

Qualys Primäre und unterstützende Integrationen ergänzen die Schwachstellendaten in Ihrer Instanz, indem Daten aus der Qualys-Schwachstellenintegration abgerufen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Eine Reihe von geplanten Aufgaben ruft die Integrationen automatisch auf. Sie können sie auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Primäre und unterstützende Integrationen können geändert werden.

Die Qualys -Integrationen werden als regelmäßige Aufgaben ausgeführt. Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Dieser Wert darf nicht geändert werden.

**Hinweis:**
Wenn Sie keinen gültigen Run-as-Benutzer festlegen, führt dies bei jeder Ausführung der Integration zu mehreren, häufig doppelten Datenabrufanhängen für die Datenquellendatensätze. Mehrere Anhänge in der Datenquelle erhöhen die Verarbeitungszeit, was zu inkonsistenten Transformationsergebnissen führt.

Während des Imports werden noch nicht vorhandene CVE-Datensätze als NVD-Datensätze erstellt und standardmäßig in Drittanbietereinträgen für Qualys referenziert.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Primäre Integrationen

Eine primäre Integration ist ein Einstiegspunkt für die Interaktion von Qualys Cloud Platform mit der API Qualys, die nach einem Zeitplan aufgerufen wird.

Zeigen Sie die primären Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.

## Unterstützende Integrationen

Eine unterstützende Integration ist ein Prozess, der nicht nach einem Zeitplan oder ohne Aufruf durch eine primäre Integration ausgeführt werden soll.

Zeigen Sie die unterstützenden Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Unterstützende Integrationen**.

## Service Graph Connector für Qualys

Ab Version 2.2 ist Service Graph Connector für Qualys über den ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Service Graph Connector for Qualys .

Daten aus den Datenquellenfeldern Qualys werden mit der Global Asset API und der Asset Management and Tagging API importiert.

Globale Asset-API:

- Eine CSAM-Lizenz ist erforderlich.
- Asset-Informationen umfassen Details wie Hardwarekategorie und Betriebssystemkategorie.

Asset Management and Tagging-API:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine CSAM-Lizenz ist nicht erforderlich
- Asset-Informationen enthalten keine Details zur Hardwarekategorie und BS-Kategorie.

Weitere Informationen finden Sie unter Service Graph Connector for Qualys APIs

.

### CIs mit der Identification and Reconciliation Engine (IRE) erstellen

Sie können die Identification and Reconciliation Engine verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Drittanbieter-Scanner importiert wurde. Aktivieren Sie das Plugin „CMDB CI Class Models“, um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.. Weitere Informationen zum Konfigurieren der Kategorisierung nicht abgeglichener Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

### Suchlisten

Suchlisten werden in Qualys verwendet, um benutzerdefinierte Gruppen von Schwachstellen zu erstellen. Sie können sie speichern und zum Erstellen von Tickets und zum Anpassen von Schwachstellenprüfungen und Berichten verwenden. Mit dem Modul „Suchlisten“ können Sie Suchlistendaten aus Qualys nach Zeitplan in Ihre Instanz herunterladen.

Suchlisten werden mithilfe der Datentransformationszuordnungen „ Dynamischer Suchlistenimport “ und/oder „ Statischer Suchlistenimport “ aus Qualys abgerufen. In jeder dieser Transformationen können Sie Zeitpläne für die Durchführung des Imports definieren.

### Optionsprofile

Optionsprofile sind mit den Scan-Einstellungen von Qualys verfügbar. Ein Optionsprofil ist erforderlich, wenn Sie einen Scan von Ihrem Now Platformaus initiieren.

Optionsprofile werden durch die Option Profile List Integration aus dem Produkt Qualys importiert. Möglicherweise möchten Sie die Integration von Optionsprofillisten nach einem Import aus den Integrationen von Suchlisten, der dynamischen Suchliste QualysQualys und der statischen Suchlistenintegration [] ausführen, damit Sie sehen können, welche Suchlisten Optionsprofilen zugeordnet sind.

### Asset-Gruppen

Asset-Gruppen werden in der Plattform Qualys eingerichtet. Asset-Gruppen geben an, welche Scanner-Geräte zum Scannen übereinstimmender IP-Adressen verwendet werden, wenn ein Scan über Now Platforminitiiert wird.

Asset-Gruppen, denen Geräte zugeordnet sind, werden von der Asset-Gruppenlisten-Integration aus Qualys abgerufen.

Initiieren Sie die Integration der Geräteliste, nachdem Sie Asset-Gruppen importiert haben, um die Felder „Gerätename“ und „Gerätestatus“ in den Datensätzen Qualys „ Standardanwendungen“ in Now Platform auszufüllen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Host-Tags

Alle Host-Tags werden als Teil der Qualys Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Zuweisungs- und Schwachstellengruppenregeln verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

**Hinweis:**
Die Qualys -Hostlisten-Integration sollte vor dem Erstellen von Zuweisungs- oder Korrekturaufgabenregeln in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag hat den Vorzug.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags gesteuert**. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Wenn Sie Tags deaktivieren, werden sie in allen Instanzen deaktiviert.

Host-Tags (auch Asset-Tags genannt) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Host-Tags“ können Sie Host-Tag-Daten von Qualys nach Zeitplan in Ihre Instanz herunterladen.

### Öffnen Sie aufgelöste angreifbare Elemente erneut, die nicht durch Scans geschlossen wurden

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf „Gelöst“ festgelegt, aber nicht von den Integrationsausführungen einer Drittpartei auf „Geschlossen/Korrigiert“ umgestellt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Wenn der Scanner bei Erkennungen von Qualys weiterhin VIs findet, die auf „Gelöst“ festgelegt wurden, dann aber durch nachfolgende Scans nicht in „Geschlossen/Korrigiert“ geändert wurden, werden diese VIs wieder in den Status „Offen“ verschoben, wenn das Datum des letzten Funds nach dem liegt Datum der Lösung.

### Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen dafür, wie Daten aus Qualysabgerufen werden. Viele Datensätze können mit Schwachstellen mit geringem Schweregrad verknüpft werden, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/-Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder welcher geeignete Schweregrad auch immer gewünscht wird)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

**Zugehörige Informationen**

Qualys-REST-Nachrichten

### wird vorbereitet Qualys Vulnerability Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Es ist wichtig, dass Sie sich auf die Integration vorbereiten, indem Sie diese Verfahren ausführen. Qualys Vulnerability Integration setzt voraus, dass Sie mit Qualys Cloud Platform-Scans in Ihrer Umgebung vertraut sind und diese ausführen.

**Hinweis:**
Nehmen Sie die erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor, bevor Sie die Integrationen ausführen.

## Wichtige Voraussetzungen

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Verwenden Sie die Filterung, um die Anzahl der Elemente für den anfänglichen Import zu begrenzen, und stufen Sie Ihre Bereitstellung ein, indem Sie die Filter in nachfolgenden Importen anpassen.

Die Scanner Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

## Auszuführende Aktionen

- Bestimmen Sie ein anfängliches Startdatum für Integrationen mit dem **Import** von Hosterkennungslisten.

  Erwägen Sie, das Feld **Startzeit** auf einige Stunden oder Tage in der Vergangenheit festzulegen. Wählen Sie idealerweise das Datum des letzten Qualys-Scans aus. Das Startdatum kann Schwachstellen enthalten, die vor der Verwendung der Schwachstellenmanagementlösung erkannt wurden. Legen Sie die früheste Startzeit für den Beginn Ihres Scan-Zyklus fest. Wenn es also eine Woche dauert, bis alle Hosts gescannt sind, legen Sie diesen Wert auf eine Woche vor diesem Zeitpunkt fest.

- Fügen Sie Benutzer zu den Rollen für admin, sn_vuln.admin und sn_vul_qualys.admin hinzu. Weitere Informationen finden Sie unter Einem Benutzer eine Rolle zuweisen .

- Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

- Wenn Sie keine Schwachstellenrechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird, zusätzlich zu den anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die anfängliche Importleistung auswirken.

- Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Deaktivieren Sie vor dem ersten Import die Business Rules.
- Wenn Sie einen anderen Scanner als den Qualys-Standard verwenden möchten, finden Sie weitere Informationen unter Scanner-Appliances einrichten.
- Halten Sie die URL des Qualys-Servers und die Anmeldeinformationen für die Authentifizierung bereit. Die Anmeldeinformationen müssen ausreichende Berechtigungen zum Abrufen von Wissens-, Scan- und Erkennungsinformationen für ein Qualys-Abonnement bereitstellen.
- Wenn Sie Host-Tags in Vulnerability Response Zuweisungs- oder Schwachstellengruppenregeln verwenden möchten, stellen Sie sicher, dass die Qualys Hostlisten-Integration vor dem Erstellen von Regeln ausgeführt wurde.

### Qualys Vulnerability Integration installieren

Bevor Sie Qualys Vulnerability Integration in Ihrer Instanz ausführen, müssen Sie die Anwendung Qualys Vulnerability Integration installieren und konfigurieren. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Erforderliche Rolle: admin zum Herunterladen und Installieren der Anwendung

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Rufen Sie Berechtigungen für die Anwendung Qualys Vulnerability Integration ab, und laden Sie sie in Ihre Instanz Now Platform® ] herunter. | Wenn die Anwendung noch nicht in Ihre Instanz heruntergeladen wurde, finden Sie weitere Informationen unter . |
| Bereiten Sie sich auf die Integration vor. | Weitere Informationen finden Sie unter wird vorbereitet Qualys Vulnerability Integration. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.

   Nach einiger Zeit werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie die Kachel Qualys Vulnerability Integration, und klicken Sie auf **Installieren**.
3. Befolgen Sie die Anweisungen im Setup-Assistenten.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.
4. Navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen**, um mit der Konfiguration fortzufahren.
   Weitere Informationen zur Ergänzung der Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie Qualys Vulnerability Integration mit dem Setup-Assistenten.

### Nächste Maßnahme

Aktivieren Sie die Scanner, da die Scanner in der Anwendung Vulnerability Response standardmäßig inaktiv sind. Weitere Informationen zum Aktivieren der Scanner Qualys finden Sie unter Aktivieren Sie die Scanner Qualys ..

## Aktivieren Sie die Scanner Qualys .

Sie müssen die Scanner nach der Installation von Qualys Vulnerability Integration aktivieren, da die Scanner in der Anwendung Vulnerability Response standardmäßig deaktiviert sind.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und wählen Sie den Datensatz aus, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld **Quelle** für ein angreifbares Element und Datensätze für Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

## Mit dem installierte Komponenten Qualys Vulnerability Integration

Die folgenden Rollen, Integrationsaufgaben und Tabellen werden mit Qualys Vulnerability Integrationinstalliert.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Anwendungsdateien-Tabelle, sodass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert sein, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Befolgen Sie diese Schritte, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im **Filternavigator sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **UND**und dann **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

## Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| sn_vul_qualys.read | Hat Lesezugriff auf die Datensätze Qualys Vulnerability Integration. | |
| sn_vul_qualys.user | Benutzer für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben | sn_vul_qualys.read |
| sn_vul_qualys.admin | Administrator fürQualys Vulnerability Integration. Sie können beispielsweise die Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen. | • sn_vul_qualys.user<br>• sn_vul.vulnerability_analyst |
| sn_vul.configure_qualys_integration | Kann die konfigurieren Qualys Vulnerability Integration | sn_vul_qualys.admin |

## Integrationsaufträge installiert

| Integrationsauftrag | Beschreibung |
|---|---|
| Qualys Integration statischer Suchlisten | Synchronisiert Qualys Suchlisten, um angreifbare Einträge zu finden. Ruft nur statische Listentyp-Datensätze ab. |
| Qualys Umfassende Integration der Hosterkennung | Ruft Host- und Schwachstellendaten von Qualys ab und verarbeitet sie in Ihrer Instanz. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integrationsauftrag | Beschreibung |
|---|---|
| | Sie koordiniert die REST-Nachrichtenaufrufe an die Host-Erkennungs-API.<br><br>Die Ausgabe dieser Integration sind angreifbare Elemente. Diese Integration importiert alle Status der Schwachstelle: Neu, Behoben, Aktiv und Erneut geöffnet. Standardmäßig ist diese Integration inaktiv und wird wöchentlich ausgeführt.<br><br>**Hinweis:**<br>Nachdem diese Integration aktiviert wurde, importiert die tägliche umfassende Aufgabe nur die Status Neu, Repariert und Erneut geöffnet. |
| Qualys Hostlisten-Integration | Ruft einmal pro Woche authentifizierte und nicht authentifizierte Host-Scan-Daten und Host-Tags von Qualys ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden. |
| Qualys Integration der Hosterkennung | Ruft Host- und Schwachstellendaten von Qualys ab und verarbeitet sie in Ihrer Instanz. Sie koordiniert die REST-Nachrichtenaufrufe an die Hostlisten-Erkennungs-API.<br><br>Die Ausgaben dieser Integration sind angreifbare Elemente.<br><br>Qualys Host-Tags werden in diese Integration importiert. |
| Qualys Ticket-Integration | Ruft Qualys Tickets ab und fügt sie Ihrer Instanz hinzu. Sie koordiniert die REST-Nachrichtenaufrufe an die Ticketlisten-API.<br><br>Es gibt oft weniger Tickets als Hosterkennungen, da Qualys Einstellungen die Erkennungen einschränken können, die zu einem Ticket führen. |
| Qualys Integration der Optionsprofilliste | Ruft Optionsprofile aus dem Produkt Qualys ab. Optionsprofile enthalten Scan-Einstellungen, die erforderlich sind, wenn Sie Scans von Ihrer Now Platform -Instanz aus initiieren. |
| Qualys Integration der Geräteliste | Ruft Scanner-Geräteinformationen von Qualysab. |
| Qualys Asset-Gruppenintegration | Ruft Asset-Gruppeninformationen aus Qualysab. Asset-Gruppen werden verwendet, um zu identifizieren, welche Scanner-Geräte zum Scannen übereinstimmender Konfigurationselemente verwendet werden sollen. |
| Qualys Knowledge Base (Auffüllung) | Ruft Qualys Knowledge Base-Einträge ab. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integrationsauftrag | Beschreibung |
|---|---|
| | Geplant zur Ausführung nach der Qualys Host-Erkennungsintegration. Aktualisiert Ihre Instanz mit allen QIDs, die in der Host-Erkennungsintegration referenziert wurden, aber nicht im System vorhanden waren. |
| Qualys Knowledge Base | Ruft Qualys Knowledge Base-Einträge ab. Die abgerufenen Daten basieren auf dem Datum, an dem die Schwachstellen von Qualys aktualisiert wurden, und seit der letzten Ausführung der Integration.<br><br>Diese Daten sind nützlich, um Verlaufsdaten in Ihre Instanz auszufüllen und sicherzustellen, dass die Qualys Bezeichner (QIDs) auf dem neuesten Stand sind. |
| Qualys Dynamische Suchlistenintegration | Synchronisiert Suchlisten Qualys, um angreifbare Einträge zu finden, und ruft Datensätze dynamischer Listentypen ab. |
| Die Erkennungen für den aktualisierten Schlüssel für werden korrigiert Qualys | Eine Hash-Kombination von Feldern, die eine Möglichkeit zum Identifizieren und Verknüpfen einer Erkennung mit einem Qualys angreifbaren Element bietet. |
| Qualys Aktualisiert vorhandene erkannte Elemente mit dem Netzwerkpartitionsbezeichner | Aktualisiert Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Qualys Schwachstellenintegrationsdaten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartitionsbezeichners einzubeziehen. |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Schwachstelle der Suchliste<br><br>sn_vul_qualys_m2m_search_list_vul | Speichert die Zuordnung zwischen der Suchliste Qualys und einer Schwachstelle. |
| Qualys Schwachstellen-Scanner<br><br>sn_vul_qualys_scanner | Tabelle, die Schwachstellenscanner erweitert, um Scanner-Informationen für die Funktion zum erneuten Scannen von Qualys zu speichern. |
| Qualys Suchlisten<br><br>sn_vul_qualys_search_list | Speichert Suchlisten, die von der Qualys -Suchlistenintegration abgerufen wurden. |
| Qualys Geräteimport<br><br>sn_vul_qualys_appliance_imp | Tabelle, die die Import Set-Zeile erweitert. Die Transformation der Feldzuordnung wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |
| Qualys CI<br><br>sn_vul_qualys_ci | Tabelle wird nicht mehr verwendet. |
| Host-Erkennung-Nummerierung | Tabelle wird nicht mehr verwendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| sn_vul_qualys_host_detection_pagination | |
| Qualys Integrationsausführung<br>sn_vul_qualys_integration_run | Tabelle wird nicht mehr verwendet. |
| Qualys Integration<br>sn_vul_qualys_integration | Tabelle, die die Schwachstellenintegration erweitert und alle Integrationen speichert, die Qualysentsprechen. |
| Qualys Import statischer Suchlisten<br>sn_vul_qualys_statisch_search_list_imp | Tabelle, die die Import Set-Zeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle Qualys Suchlisten umzuwandeln. |
| Qualys Knowledge Base<br>sn_vul_qualys_knowledge_base | Tabelle, die die Import Set-Zeile erweitert. Die Transformation der Feldzuordnung wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |
| Qualys Ticketliste<br>sn_vul_qualys_ticket_list_imp | Tabelle, die die Import Set-Zeile erweitert. Die Transformation der Feldzuordnung wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |
| Qualys Optionsprofil<br>sn_vul_qualys_option_profile | Tabelle, in der die von Qualysabgerufenen Optionsprofile gespeichert werden. Diese Tabelle wurde beim erneuten Scannen verwendet. |
| Qualys Dynamischer Suchlistenimport<br>sn_vul_qualys_dynamic_search_list_imp | Tabelle, die die Import Set-Zeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle Qualys Suchlisten umzuwandeln. |
| Qualys Importsatz erneut ausführen<br>sn_vul_qualys_import_rerun | Tabelle wird nicht mehr verwendet. |
| Qualys Import von Optionsprofilen<br>sn_vul_qualys_option_profile_import | Tabelle, die die Import Set-Zeile erweitert. Die Transformation der Feldzuordnung wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |



### Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Qualys Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Sie Ihre Assets in der Anwendung Vulnerability Response unter anderem anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, sie werden jedoch als ein CI in Ihrer CMDB gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise können, wie in den folgenden Tabellen gezeigt, mehrere Assets (CIs) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche als einzelnes CI (CI 1) identifiziert und gespeichert.

**Standardmäßige IP-Suche und CI-Erstellung**

| Quelle | IP-Adresse | NETWORK_ID | Konfigurationselement |
|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 |

| Quelle | IP-Adresse | REPOSITORY_ID | Konfigurationselement |
|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 |

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse haben, damit Sie sie als unterschiedliche Assets identifizieren können. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die regelmäßige Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] vorhandenen CI-Datensätzen aus importierten Daten hinzu. Vorhandene von der IRE erstellte CIs werden ebenfalls aktualisiert. Die regelmäßige Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie die Aufgabe bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

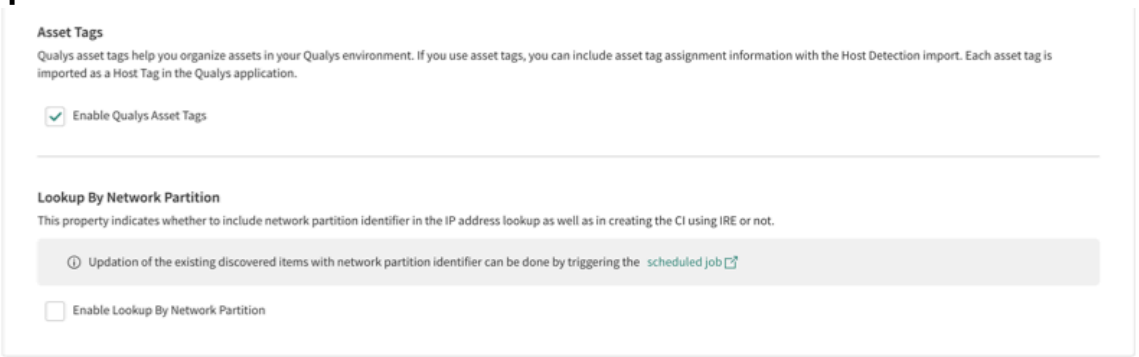
Ab Version 14.0 von Vulnerability Response und Version 12.1 von Qualys Vulnerability Integration Vulnerability Integration wird CMDB CI Class Models (1.0.21.) unterstützt. Die Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

### Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Qualys Vulnerability Integration aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen **Suche nach Netzwerkpartition aktivieren** Checkbox aus dem **Suche nach Netzwerkpartition**




Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

### Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID in IP-Suche und CI-Erstellung enthalten

| Quelle | IP-Adresse | NETWORK_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 | CI 2 |

| Quelle | IP-Adresse | REPOSITORY_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Qualys: Integrationen mit Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 | CI 2 |

Die Suchregeln IP-Adresse und unvollständige IP-Adresse für CI-Identifizierung enthalten das Attribut für den Netzwerkpartitionsbezeichner automatisch für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration.

Nachdem Sie die regelmäßige Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie bei Bedarf regelmäßige Aufgaben starten. Die CIs in Ihren vorhandenen Datensätzen für erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden automatisch aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Optionale Qualys-Änderungen

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Qualys-Integration.

Sie können dieses Startdatum im Setup-Assistenten oder in der primären Integration zurücksetzen oder Geschäftsregeln ändern, um sie während eines ersten Imports zu deaktivieren.

### Deaktivieren Sie benachrichtigungsbezogene Geschäftsregeln vor dem ersten Datensatzimport

Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Business Rules viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Geschäftsregeln müssen geändert werden, um sie während des Imports zu deaktivieren.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu**Alle** > **Systemdefinition** > **Business-Regeln**.
2. Suchen Sie nach **betroffenen CI-Benachrichtigungen**.
3. Öffnen Sie die Geschäftsregel, und fügen Sie diese Bedingung ein: `current.sys_class_name != „sn_vul_vulnerable_item“`.
4. Klicken Sie auf **Aktualisieren**.
5. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
   - Betroffene Kostenstellenbenachrichtigungen
   - Betroffene Gruppenbenachrichtigungen
   - Betroffene Standortbenachrichtigungen

**Hinweis:**
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Geschäftsregeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und die Leistung Ihrer Instanz beeinträchtigen.

### Ändern Sie ein anfängliches Startdatum

Während der Installation mit dem Setup-Assistenten legen Sie ein anfängliches Startdatum für die Qualys-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen (siehe unten).

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
2. Klicken Sie **auf Qualys Host Detection Integration**(Integration der Qualys-Hosterkennung).
3. Klicken Sie auf **Integrationsdetails**.
4. Legen Sie das Feld **Startzeit** auf einen Wert in der Vergangenheit fest, damit alle gescannten und erkannten Schwachstellen seit diesem Zeitpunkt erkannt werden.

   Wenn Sie Qualys mit dem Setup-Assistenten konfiguriert haben, ist das Feld **Startzeit** vorausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum.

   **Hinweis:**
   Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Qualys-API-Ratenbeschränkungen überschreiten und Ausführungszeitüberschreitungen auslösen.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie auf **Jetzt** ausführen, um den Vorgang sofort auszuführen.

#### Erweiterte Qualys-Konfigurationen und -Änderungen

Konfigurieren Sie erweiterte optionale Änderungen, und optimieren Sie einige der Daten speziell für die Qualys-Integration. Die meisten dieser Änderungen erfordern Codierung oder fortgeschrittene ServiceNow - oder Qualys Cloud Platform -Kenntnisse.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ändern Sie die Zuordnungswerte für Qualys zu ServiceNow für Priorität und Status

Ändern Sie die Zuordnungswerte für Priorität und Status entsprechend Ihren Anforderungen.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Dies ist eine erweiterte Anpassungsoption.

#### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
2. Suchen Sie nach **Map Qualys Values**, und öffnen Sie es.
3. Klicken Sie auf die Registerkarte **Erweitert**.
4. Ändern Sie gemäß Ihren Anforderungen.
   Zu den häufigsten Änderungen gehören das Hinzufügen neuer Statuswerte oder das Überarbeiten der Relevanz oder Priorität.
5. Klicken Sie auf **Aktualisieren**.

### Beschränken Sie die Fähigkeit, in einen Datensatz basierend auf einer Zuweisungsgruppe zu schreiben

Sie können Schreib-/Leserechte für Datensätze basierend auf der Zugehörigkeit zu einer zugewiesenen Gruppe einschränken. Ändern Sie Bedingungen und Skripts basierend auf bestimmten Anforderungen.

#### Vorbereitungen
Erforderliche Rolle: security_admin (erweiterte Rolle von Administrator)

**Hinweis:**
Diese Aktion wird im Bereich „Schwachstelle“ ausgeführt.

#### Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**.
2. Suchen Sie nach ACLs, die mit `sn_vul` beginnen.
3. Wählen Sie einen Zugriffssteuerungsdatensatz aus, z. B. `sn_vul_vulnerable_item`, **Operation write**.
4. Aktivieren Sie ggf. das Kontrollkästchen **Erweitert** im Datensatz, um die **Rolleneinträge** anzuzeigen.
5. Ändern Sie das **Rollenskript** entsprechend Ihren Anforderungen.
   Skriptbeispiel für das Ändern des Zugriffs nach Gruppe.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Klicken Sie auf **Aktualisieren**.

### Richten Sie Scannergeräte ein

Wenn Sie Scans von Ihrem Now Platform® anstatt direkt von Qualys aus initiieren, können Sie Scans für IP-Adressbereiche einrichten.

## Vorbereitungen

Die Daten stammen aus der Integration Qualys basierend auf Asset-Gruppen Qualys und den zugehörigen Standardgeräten (Scannern).

Wenn für die Ziel-IP-Adressbereiche keine Geräte konfiguriert sind, wird das Gerät, das als Standard für die Integrationsinstanz festgelegt ist, für den Scan verwendet.

Erforderliche Rolle: sn_vul_qualys.admin

## Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Scannergeräte**.
2. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Gerätename | Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen.<br><br>Geben Sie den Namen für die Scanner-Appliance Qualys ein, die zum Aufrufen von Scans für übereinstimmende Konfigurationselemente verwendet werden soll.<br><br>Verwenden Sie den Wert `Extern`, wenn der Scan mit einem externen Scanner gestartet werden soll. |
| Geräte-ID | Geben Sie den Gerätebezeichner für das Scannergerät Qualys ein, das zum Aufrufen von Scans für übereinstimmende Konfigurationselemente verwendet werden soll.<br><br>Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen.<br><br>Verwenden Sie den Wert `0`, wenn der Scan mit einem externen Scanner gestartet werden soll. |
| Gerätestatus | Zeigt den letzten Status des Scannergeräts in den von der Qualys -Integration zurückgegebenen Daten an. Bei manuell erstellten Datensätzen wird der Status nur aktualisiert, wenn eine gültige **Geräte-ID** angegeben ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Asset-Gruppen-ID | Zeigt den Bezeichner der Asset-Gruppe Qualys an, von der dieser Datensatz erstellt wurde. Dieses Feld zeigt nur für Datensätze einen Wert an, die durch die Qualys -Integration erstellt wurden. |
| Asset-Gruppenname | Zeigt den Namen der Asset-Gruppe Qualys an, die diesen Datensatz erstellt hat. Dieses Feld zeigt nur für Datensätze einen Wert an, die durch die Qualys -Integration erstellt wurden. |
| Reihenfolge | Geben Sie einen Wert ein, der zur Bestimmung der Scan-Priorität verwendet werden soll. Bei Geräten mit in Konflikt stehenden Kriterien wird einem Gerät mit einem niedrigeren Reihenfolgewert eine höhere Priorität zugewiesen. |
| Manuell erstellt | Gibt an, ob dieser Datensatz vom Benutzer manuell erstellt wurde. |
| Filtergruppe verwenden | Aktivieren Sie dieses Kontrollkästchen, um eine Filtergruppe für die Suche nach übereinstimmenden Konfigurationselementen zum Scannen anzugeben. |
| Filtergruppe | Wählen Sie die Filtergruppe aus, die Sie für die Suche nach übereinstimmenden Konfigurationselementen zum Scannen verwenden möchten. Dieses Feld wird nur angezeigt, wenn Sie **Filtergruppe verwenden**ausgewählt haben. |
| IPs | Kommagetrennte Liste von IP-Adressen oder IP-Adressbereichen, die von diesem Gerät beim Aufrufen von Scans verwendet werden sollen. |
| Integrationsinstanz | Die Qualys Integrationsinstanz, die dieser Appliance zugeordnet ist. |
| Optionsprofil | Wählen Sie das Optionsprofil aus, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten. |

3. Klicken Sie auf **Aktualisieren**.

### Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und -scans

Qualys Schwachstellenprüfungen können durchgeführt werden, um Softwareschwachstellen zu finden, die sich auf Ihre CIs auswirken. Sie können Scans aus einem Datensatz für angreifbare Elemente initiieren oder direkt einen Scan-Datensatz für Konfigurationselemente (CIs) und IP-Adressen erstellen.

Wenn Sie Qualys angreifbare Elemente direkt über den Bildschirm „Angreifbare Elemente“ scannen, haben Sie auch die Möglichkeit, mehrere angreifbare Elemente gleichzeitig zu scannen.

Wenn Security Incident Response aktiviert ist, können Sie auch einen Scan aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Sicherheitsscan-Anforderung initiieren.

Scans, die von Qualys angreifbaren Elementen, Security Incident Catalog, Security Incidents oder Sicherheitsscananforderungen übermittelt werden, werden vom Standardscanner Qualys ausgeführt.

Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten.

- Optionsprofile enthalten Qualys Scan-Einstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys -Scan von Ihrem Now Platform®aus initiieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie den von ServiceNow initiierten Qualys IP-Scan

Der im Basissystem enthaltene Scanner Qualys bietet eine Baselineintegration zum Initiieren von Scans basierend auf IP-Adressen.

#### Vorbereitungen

Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten.

- Optionsprofile enthalten Qualys Scan-Einstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys-Scan von Ihrem Now Platform®aus initiieren.

Erforderliche Rolle: sn_vul_qualys.admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Öffnen Sie den Datensatz Qualys.
3. Aktivieren Sie die Kontrollkästchen**Aktiv** und **Standard**.

   Die Auswahl von **Aktiv** ist erforderlich, um den Scanner [ Qualys zum automatischen Scannen von Qualys VIs zu verwenden. Sie müssen auch nicht **Standard** auswählen, damit er automatisch ausgeführt wird.

   Vor v12.0 ist **Active** erforderlich, um den Scanner zu verwenden. Wenn auch **Standard** ausgewählt ist, wird der Scanner automatisch verwendet, ohne dass er während des Scanvorgangs ausgewählt werden muss.
4. Klicken Sie für das Feld Quellintegration auf das Suchsymbol, und wählen Sie die Option für **Qualys**aus, z. B. **Qualys Cloud Platform**.
5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
7. Öffnen Sie die **Integration von Qualys-Asset-Gruppenlisten**.
   a. Aktivieren Sie die Checkbox **Aktiv**.
   b. Klicken Sie auf **Jetzt ausführen**.
8. Befolgen Sie diese Schritte, um Ihre Scanner-Appliances auszufüllen.

**Hinweis:**
Möglicherweise möchten Sie die Integration von Optionsprofillisten nach einem Import aus den Integrationen von Suchlisten, der dynamischen Qualys-Suchliste und der statischen Qualys-Suchlistenintegration ausführen, damit Sie sehen können, welche Suchlisten Optionsprofilen zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Öffnen Sie die **Integration von Qualys-Optionsprofillisten**.

b. Aktivieren Sie die Checkbox **Aktiv**.

c. Klicken Sie auf **Jetzt ausführen**.

d. Befolgen Sie die in Richten Sie Scannergeräte ein aufgeführten Schritte, um Ihre Scanner-Appliances zu konfigurieren.
Kehren Sie nach Abschluss dieser Schritte hierher zurück, um mit der Konfiguration fortzufahren.

e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.

f. Öffnen Sie die **Qualys-Appliance-Listenintegration**.

g. Aktivieren Sie die Checkbox **Aktiv**.

h. Klicken Sie auf **Jetzt ausführen**.
Ihre Qualys Scanner-Appliances sind jetzt korrekt ausgefüllt.

**Zugehörige Informationen**

Qualys Vulnerability Integration verstehen

### Scannen Sie mehrere Qualys Schwachstellen oder angreifbare Elemente

Sie können mehrere Qualys Schwachstellen oder angreifbare Elemente gleichzeitig scannen, die mindestens ein betroffenes Configuration Item (CI) oder eine im Formular ausgefüllte IP-Adresse enthalten.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Prozedur

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
   - Navigieren zu **Alle** > **Vulnerability Response** > **Alle angreifbaren Elemente**.
2. Aktivieren Sie die Kontrollkästchen für die Datensätze, die Sie scannen möchten.
3. Klicken Sie auf die Liste **Aktionen für ausgewählte Zeilen** und klicken Sie auf **Erneut nach angreifbaren Elementen scannen**.
   Eine Nachricht mit einem Link zum Scan wird angezeigt, und die Arbeitsnotizen werden aktualisiert.
4. Klicken Sie auf den Link, um den Fortschritt oder die Ergebnisse des Scans anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie den automatischen Scan Qualys für gelöste Korrekturaufgaben

Sie können den Scan so planen, dass er automatisch ausgeführt wird, um Ihre Qualys angreifbaren Elemente zu aktualisieren.

#### Vorbereitungen

Nachdem eine Korrekturaufgabe auf **Gelöst gesetzt**wurde, wird automatisch ein Scan initiiert, um den Status der zugehörigen angreifbaren Elemente zu aktualisieren.

- Der Scan ist standardmäßig deaktiviert.
- Aktivieren Sie den Scan mit dem Integrationsinstanzparameter **scan_on_resolved** im **Qualys** -Datensatz unter **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**. Weitere Informationen finden Sie in den folgenden Schritten.
- Dieser Scan ist instanzspezifisch. Wenn Sie mehrere Instanzen haben und diesen Scan aktivieren oder deaktivieren möchten, müssen Sie den Parameter **scan_on_resolved** in den Integrationsinstanzparametern in jeder Instanz deaktivieren, die Sie ändern möchten.
- Wenn der Scan aktiviert ist, können Sie den Scan bei Bedarf initiieren oder den Scan so planen, dass er nur innerhalb eines bestimmten Zeitfensters ausgeführt wird. Unter Konfigurieren Sie Qualys erneute Scans so, dass sie nur innerhalb geplanter Intervalle ausgeführt werden erfahren Sie, wie Sie die Start- und Endzeiten für das Zeitfenster festlegen.

Erforderliche Rolle: sn_vul_qualys.admin

#### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.
2. Wählen Sie **Qualys** aus, um den Datensatz zu öffnen.
   Die Integrationsinstanzparameter für Qualys werden auf einer Registerkarte angezeigt.
3. Um den automatischen Scan zu aktivieren, suchen Sie den Parameter `scan_on_resolved`.
4. Geben Sie in der Spalte Wert für die Eigenschaft `true`ein.
5. Klicken Sie auf **Aktualisieren**.

### Konfigurieren Sie Qualys erneute Scans so, dass sie nur innerhalb geplanter Intervalle ausgeführt werden

Legen Sie für die Qualys Schwachstellenintegration die Start- und Endzeitparameter für Scans so fest, dass erneute Scans nur während der gewünschten Stunden ausgeführt werden oder verfügbar sind.

#### Vorbereitungen

Diese Konfiguration gilt sowohl für geplante erneute Scans als auch für erneute Scans, die Sie manuell im Produkt Qualys von Ihrer Instanz Now Platform® ] aus initiieren.

Durch Festlegen der Start- und Endzeitparameter für Scans für Integrationsinstanzen können Sie Zeitfenster angeben, in denen erneute Scans im Produkt Qualys verfügbar sind. Sie können beispielsweise angeben, dass erneute Scans nur außerhalb der Geschäftszeiten verfügbar sind, z. B. von Mitternacht bis 10 Uhr.

Diese Einstellung ist instanzspezifisch. Wenn Sie mehrere Instanzen haben, müssen Sie die Werte scan_start_time und scan_end_time in den Integrationsinstanzparametern in jeder Instanz konfigurieren, die Sie ändern möchten.

Erforderliche Rolle: sn_vul_qualys.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**.
2. Klicken Sie auf **Qualys**, um den Datensatz zu öffnen.
   Die Integrationsinstanzparameter für Qualys werden angezeigt.
3. Geben Sie für den Parameter scan_start_time in der Spalte Wert die Zeit in der UTC-Zeitzone im 24-Stunden-Format (00:00 bis 24:00) für die Startzeit des Fensters ein, für das erneute Scans verfügbar sein sollen.
4. Geben Sie für scan_end_time in der Spalte Wert Zeiten im gleichen Format (00:00 bis 24:00) für die Endzeit des verfügbaren Fensters ein.
   Wenn Sie beispielsweise eine Startzeit von 00:00 für den Parameter scan_start_time und eine scan_end_time von 10:00 Uhr desselben Morgens eingeben, werden Scans, die außerhalb des Zeitfensters von Mitternacht bis 10 Uhr geplant oder manuell gestartet wurden, in die Warteschlange gestellt und um gestartet Startzeit des Zeitfensters des folgenden Tages, 00:00.

   Wenn im selben Beispiel ein Fehlerkorrektur-Besitzer manuell einen erneuten Scan um 11:00 Uhr initiiert, wird der erneute Scan nicht sofort gestartet, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange, in diesem Beispiel (00:00).
5. Klicken Sie auf **Aktualisieren**, um Ihre Einstellungen zu speichern.

## Qualys Quotenbegrenzungen für Schwachstellen Scans

Sie können die Häufigkeit definieren, mit der verschiedene Arten von Scans ausgeführt werden, um die Anzahl der Anforderungen zu begrenzen, die an einen externen Scanner gesendet werden. Nachdem Sie Quotengrenzen definiert haben, können Sie sie auf die Scanner Qualys anwenden.

## Definieren Sie Qualys Scan-Ratengrenzen

Sie können die Rate definieren, mit der verschiedene Arten von Scans ausgeführt werden, um die Last in Ihrer Scan-Warteschlange auszugleichen. In der Quotengrenze definierte Bedingungen bestimmen, ob die Quotengrenzen auf Einträge in der Warteschlange angewendet werden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Quotengrenzdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Quotengrenzdefinition**

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie einen beschreibenden Namen an, der die Bedingungen angibt, die der Warteschlangeneintrag erfüllen muss. Beispiel: Scans pro Minute |
| Bedingungen der Warteschlange | Geben Sie Bedingungen ein, anhand derer bestimmt wird, ob ein Scan-Eintrag in der Warteschlange dieser Quotenbegrenzung unterliegt. Die Bedingungen sollten nicht für einen bestimmten Scanner spezifisch sein. |
| Auswertungsskript | Schreiben Sie ein Skript mit der Logik, um den Eintrag in der Warteschlange auszuwerten. Es ist wichtig, dass das Skript true/false zurückgibt, um zu definieren, ob der Eintrag verarbeitet wird. Basieren Sie das Bewertungsskript auch auf dem Eintrag in der Warteschlange, der ausgewertet wird. |

4. Klicken Sie auf **Absenden**.

### Wenden Sie Scan-Ratenbegrenzungen auf Qualys Scanner an

Nachdem Sie Scan-Ratengrenzen mithilfe von **Quotengrenzdefinitionen**definiert haben, können Sie Quotengrenzen auf bestimmte Qualys -Scanner anwenden.

## Vorbereitungen

Erforderliche Rolle: sn.vul_admin

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scannerquotengrenzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Scanner-Quotenbegrenzung**

| Feld | Beschreibung |
|---|---|
| Scanner | Wählen Sie den Scanner aus, auf den Sie eine Quotenbegrenzung anwenden möchten. |
| Quotengrenze | Wählen Sie die Quotengrenze aus, die Sie auf diesen Scanner anwenden möchten. |
| Schwellenwert | Geben Sie den Schwellenwert ein, dem der ausgewählte Scanner für die ausgewählte Quotengrenze unterliegen soll. Wenn der Scanner beispielsweise 4 Scans pro Minute zulässt und die Quotengrenze als Anforderungen pro Minute definiert ist, wäre der Schwellenwert 4. |

4. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie die Schwachstellen-Scan-Warteschlange Qualys an

An die Integration von Qualys für die Schwachstellen-Scan-Integration übermittelte Schwachstellen-Scan-Anforderungen werden in die Warteschlange gestellt, um die Systemressourcen nicht zu überlasten. Sie können den Status von Anforderungen in der Warteschlange nach Bedarf anzeigen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird
In der Liste der Scans in der Warteschlange enthält jeder Scan einen automatisch generierten Scan-Namen, der das gescannte CI identifiziert.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scan-Warteschlange**.
   Alle Qualys Scan-Anforderungen, die übermittelt wurden, werden in einer Liste angezeigt. Die **Spalte** Status zeigt den aktuellen Status jedes Eintrags in der Warteschlange an. Der Status **Abgeschlossen** gibt an, dass der Scan die Warteschlange verlassen hat. Dies bedeutet nicht unbedingt, dass die Verarbeitung des Scans abgeschlossen ist. Wenn die Scans abgeschlossen sind oder fehlgeschlagen sind, wird in der Spalte Wird **verarbeitet** der entsprechende Arbeitsnotiztext angezeigt.

   **Hinweis:**
   Wenn ein Hash-Wert zum Scannen übermittelt wurde und der **Scanner** kein Ergebnis findet, zeigt der **Status Abgeschlossen** und die Arbeitsnotiz in der Spalte In **VerarbeitungUnknown**an.

2. Klicken Sie nach Abschluss der Verarbeitung eines Scans auf einen Datensatz in der Warteschlange, um Details für die Scan-Anforderung anzuzeigen.

### Aktivieren Sie den Basissystemfilter für bestätigte Erkennungsimporte

Aktivieren Sie einen Standardfilter mithilfe von Integrationsparametern, um nur bestätigte Erkennungen aus Qualys Cloud Platformzu importieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul_qualys.admin, sn_vul.vr_import_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Ein Instanzparameter für die Basissystemintegration „include_only_confirmed“ ist verfügbar, um eine gefilterte Liste von Erkennungen aus Qualys Cloud Platformzu importieren. Standardmäßig ist dieser Parameter auf *FALSE*festgelegt, und alle Erkennungen, ob potenziell, bestätigt oder informativ, werden importiert.

#### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.
2. Öffnen Sie die Qualys-Cloud-Plattformintegration aus der Liste der Integrationsinstanzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie in der Liste „Integrationsinstanzparameter“ den Parameter „*include_only_confirmed*“.
4. Aktualisieren Sie den Standardwert auf *True*.
5. Klicken Sie auf **Aktualisieren**.
   Sie haben den Filter aktiviert, um bestätigte Erkennungen aus der Qualys Cloud Platform -Integration zu importieren.

### Ergebnisse

Standardmäßig werden nur bestätigte Erkennungen aus der Qualys Cloud Platform -Integration importiert, wenn der nächste Qualys-Schwachstellenimport ausgeführt wird. Alle anderen Erkennungen wie „Information“ und „Potenziell“ werden ignoriert und nicht importiert. Weitere Informationen finden Sie unter Erkennungsdaten für angreifbare Elemente in Vulnerability Response anzeigen.

#### Initiieren Sie einen erneuten Scan für Qualys Vulnerability Integration

Vergewissern Sie sich, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie bei Bedarf erneute Scans im Produkt Qualys aus Ihrem Now Platform initiieren.

### Vorbereitungen

Sie können erneute Scans über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Informationen zum erneuten Scannen in der klassischen Umgebung finden Sie in den folgenden Abschnitten, in denen erläutert wird, wie Sie erneute Scans initiieren.

Erforderliches Setup für erneute Scans im Produkt Qualys, das von Ihrem Now Platforminitiiert wurde:

Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Qualys aus Ihrer Instanz von Now Platform® initiieren.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans im Produkt Qualys aus Datensätzen für angreifbare Elemente (VI), Korrekturaufgaben (RT), Drittanbietereinträgen (TPE) oder erkannten Elementen aus Ihrer Instanz von Now Platform initiieren.

Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Anwendungsfall

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde, erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformQualys auf angreifbare Elemente von [] initiieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können erneute Scans für AEs mit Qualys als Quelle in anderen Status als „Geschlossen“ initiieren. Siehe Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Vergewissern Sie sich, dass Sie das folgende Setup abgeschlossen haben, das für erneute Scans erforderlich ist. Weitere Informationen finden Sie in den Schritten ab Konfigurieren und Verwalten von Qualys Schwachstellenscannern und Scans, die in den vorherigen Abschnitten aufgeführt sind.

Erforderliche Rolle: sn_vul_manually_initiate_rescan

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   **Hinweis:**
   Sie können erneute Scans nur für AEs mit Qualys als Quelle initiieren. Vergewissern Sie sich, dass Qualys in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle nicht in der VI-Listenansicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol „**Liste personalisieren** “ (Zahnradsymbol), und verwenden Sie den Slushbucket, um **Quelle** von **Verfügbar** zu **Ausgewählt**zu verschieben.

3. Navigieren Sie alternativ zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**, **Vulnerability Response** > **Bibliotheken** > **Drittpartei**, oder zu **erkannten Elemente** für die Datensätze der Korrekturaufgabe, des Drittanbietereintrags oder der erkannten Elemente, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss die VI aus dem Produkt Qualys stammen und sich in einem anderen Status als **Geschlossen**befinden. Für mehrere VI-Datensätze müssen alle VIs Qualys als Quelle haben und sich in einem anderen Status als **Geschlossen**befinden.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als „ **Geschlossen**“ befinden, und alle zugeordneten AEs müssen Qualys als Quelle haben.
   - In einem TPE-Datensatz muss mindestens ein zugeordneter VI-Datensatz in einem anderen Status als **Geschlossen** mit Qualys als Quelle vorhanden sein.
   - In einem Datensatz eines erkannten Elements ist dem Konfigurationselement mindestens ein VI mit Qualys als Quelle in einem anderen Status als **Geschlossen**zugeordnet.

4. Klicken Sie oben rechts im ausgewählten Datensatz auf **Erneut scannen**.
   Wählen Sie im angezeigten Dialogfeld eines aus, um fortzufahren.

| Option | Beschreibung |
|---|---|
| Aktivieren Sie das Kontrollkästchen **Optionsprofile angeben**. | Wählen Sie in der Liste das Optionsprofil für den Scanner Qualys aus, den Sie für den erneuten Scan verwenden möchten. Dies sind |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | die Geräte (Scanner), die Sie konfiguriert und unter aufgelistet haben **Qualys Schwachstellenintegration** > **Scannergeräte**. |
| Deaktivieren Sie das Kontrollkästchen **Optionsprofile angeben** (nicht ausgewählt). | Das Optionsprofil Qualys für den Scanner, den Sie in der Liste der Scannergeräte als Standardscanner festgelegt haben, wird für den Scan verwendet.<br><br>Um weitere Informationen zum Festlegen der Standardscanner zu erhalten, die Sie über Now Platforminitiieren, richten Sie die im vorherigen Abschnitt aufgeführten Scanner-Appliances ein. |

5. Klicken Sie **auf Scan anfordern**.

Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den Datensätzen für VI, RT, TPE und erkannte Elemente gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Details** anzeigen, um den Status des erneuten Scans anzuzeigen und alle anderen erneuten Scans anzuzeigen, die von einem bestimmten Datensatz aus gestartet wurden.

Ihre Instanz verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt. Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens.

Nachdem der erneute Scan erfolgreich abgeschlossen wurde, wird die Qualys Host Detection Integration automatisch initiiert, um Ihre angreifbaren Elemente zu aktualisieren. Je nachdem, wie viele VIs Sie haben, werden Ihre Erkennungen, VIs und RTs nach Abschluss des Qualys Host Detection Integration-Scans aktualisiert. Navigieren Sie zu diesen Datensätzen, um die Updates anzuzeigen, nachdem die Integration der Hosterkennung abgeschlossen ist.

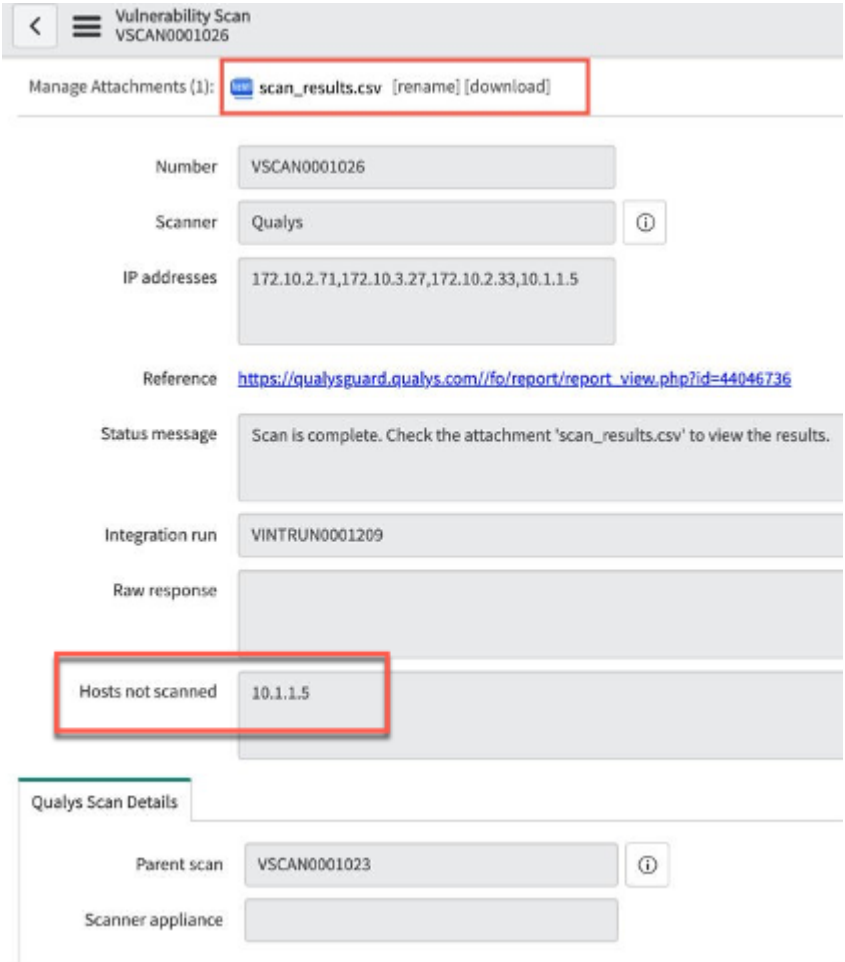
Dieser Scan ist instanzspezifisch und kann deaktiviert werden. Weitere Informationen zu den Qualys -Integrationen und zur Anzeige der Integrationen finden Sie unter Qualys Vulnerability Integration verstehen.

### Nächste Maßnahme

Sie können einen CSV-Anhang im Scan-Datensatz anzeigen, um Details zu den erneuten Scans anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wie in der vorherigen Abbildung gezeigt, werden während des erneuten Scans, wenn Hosts (Konfigurationselemente) in Ihrer Umgebung nicht zugänglich sind, Erkennungen und VIs, die diesen Assets zugeordnet sind, nicht aktualisiert, wenn der erneute Scan abgeschlossen ist. Damit Sie verstehen, warum sie nicht enthalten sind, werden die Asset-IP-Adressen für diese CIs nach Abschluss des erneuten Scans in den Schwachstellendatensätzen im Feld Nicht gescannte Hosts aufgelistet.

### Qualys -Metadaten für Schwachstellen

Die Qualys Host-Erkennungsintegration wurde erweitert und enthält nun weitere Felder aus Qualys. Diese Felder helfen beim Filtern der nicht ausnutzbaren Linux Schwachstellen. Diese Erweiterung verbessert die Integration auf Erkennungsebene und auf Ebene des angreifbaren Elements (AE).

### Importieren Sie zusätzliche Metadaten aus Qualys

Importieren Sie zusätzliche Metadaten für angreifbare Elemente (VI), um Schwachstellen basierend auf den Auswirkungen auf einen Kernel oder Service zu filtern.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.
2. Klicken Sie unter Integrationskonfiguration auf **Scanner-Integrationen**.
3. Klicken Sie unter Installierte Anwendung auf **Bearbeiten** für die Anwendung Qualys.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie **auf Hosterkennungskonfiguration**.
5. Navigieren zu **Weitere Metadaten für Erkennungen importieren**.
6. Um zusätzliche Metadaten aus Qualyszu importieren, aktivieren Sie manuell eines der folgenden Kontrollkästchen.
   - **Kernel-Metadaten**: Identifiziert Schwachstellen, die in ausgeführten oder nicht ausgeführten Linux-Kerneln gefunden wurden.

     Wenn der Wert der zurückgegebenen Metadaten **No**ist, bedeutet dies, dass die Schwachstelle aufgrund eines nicht ausgeführten Kernels nicht ausgenutzt werden kann. Weitere Informationen zu den abgerufenen Werten finden Sie unter Qualys -Metadatenwerte für Schwachstellen.
   - **Service-Metadaten**: Identifiziert Schwachstellen, die an ausgeführten oder nicht ausgeführten Ports oder Services gefunden wurden.
   - **Metadaten der ausnutzbaren Konfiguration**: Identifiziert Schwachstellen, die aufgrund der aktuellen Hostkonfiguration ausgenutzt werden können oder nicht.

   **Hinweis:**
   Standardmäßig sind diese Kontrollkästchen nicht aktiviert.
7. Führen Sie die Qualys Host-Erkennungsintegration mit einem rückwirkenden Datum aus.
   Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.

### Ergebnisse
Die Metadaten wurden importiert.

### Nächste Maßnahme
Geben Sie zum Anzeigen der importierten Metadaten `sn_vul_detection.list` in die Filternavigation ein. Die Liste „Erkennungen angreifbarer Elemente“ wird angezeigt. Weitere Informationen zu den in den neu hinzugefügten Spalten angezeigten Werten finden Sie unter Qualys -Metadatenwerte für Schwachstellen.

#### Qualys -Metadatenwerte für Schwachstellen

Wenn die Kernel-Metadaten, Service-Metadaten und Konfigurationsmetadaten importiert werden, werden auch einige Werte abgerufen. Die Werte **0**, **1** und **Nicht verfügbar** werden im Back-End verarbeitet und in **No**, **Yes** bzw. **Leer** konvertiert.

Diese Werte werden in die folgenden Spalten in der Liste „Erkennungen von angreifbaren Elementen“ und „Angreifbare Elemente“ eingetragen:

- Spalte „Wirkt ausgeführter Service“
- Betrifft die ausnutzbare Konfigurationsspalte
- Betrifft die Ausführung von Kernelspalten

**Hinweis:**

- Diese Spalten sind standardmäßig nicht sichtbar. Weitere Informationen zum Konfigurieren des Formularlayouts finden Sie unter Formularlayout konfigurieren
- Bei älteren Erkennungen können die Werte für diese Spalten leer sein. Um die Daten zu aktualisieren, führen Sie eine zurückdatierte Qualys Host Detection Integration aus. Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt die abgerufenen Werte und ihre Bedeutung.

**Abgerufene Feldwerte und ihre Bedeutung**

| Feld | Wert | Bedeutung |
|---|---|---|
| AUSWIRKUNG_AUSFÜHREN_KERN | 0 | Die Schwachstelle wurde in einem nicht ausgeführten Kernel gefunden. Die Schwachstelle kann nicht ausgenutzt werden. |
| AUSWIRKUNG_AUSFÜHREN_KERN | 1 | Schwachstelle wurde in einem ausgeführten Kernel gefunden. Die Schwachstelle ist ausnutzbar. |
| AUSWIRKUNG_AUSFÜHREN_KERN | Nicht verfügbar | Schwachstelle ist keine Kernel-bezogene Schwachstelle. |
| AFFECT_RUNNING_SERVICE | 1 | Schwachstelle wurde an nicht ausgeführten Ports oder Services gefunden. Die Schwachstelle kann nicht ausgenutzt werden. |
| AFFECT_RUNNING_SERVICE | 0 | Schwachstelle wurde bei ausgeführten Ports oder Services gefunden. Die Schwachstelle ist ausnutzbar. |
| AFFECT_RUNNING_SERVICE | Nicht verfügbar | Schwachstelle ist keine zugehörige Schwachstelle. |
| AUSWIRKUNG_AUSWIRKUNG_KONFIG | 1 | Schwachstelle kann aufgrund der Hostkonfiguration nicht ausgenutzt werden. |
| AUSWIRKUNG_AUSWIRKUNG_KONFIG | 0 | Schwachstelle ist aufgrund der Hostkonfiguration ausnutzbar. |
| AUSWIRKUNG_AUSWIRKUNG_KONFIG | Nicht verfügbar | Schwachstelle ist keine zugehörige Schwachstelle. |

### Legen Sie zusätzliche Filterparameter für Qualys Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Qualys Vulnerability Integration an, damit Sie die Schwachstellendaten, die Sie mit den unterstützten Qualys -Integrationen importieren, weiter verfeinern können.

**Vorbereitungen**
Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert werden. Oder Sie möchten nur Computer importieren, die sich in Ihrem Bereich befinden, z. B. nur Computer innerhalb Ihres Unternehmensnetzwerks, die keine externen Geräte sind.

Um die Erfassung dieser Daten zu erleichtern, können Sie Parameter Qualys hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Parametern Qualys in Ihrem Now Platformanpassen. Sie ändern oder fügen diese Werte in Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützten Qualys -Integrationen von Qualys Vulnerability Integrationhinzu.

Erforderliche Rolle: sn_vul.vulnerability_admin

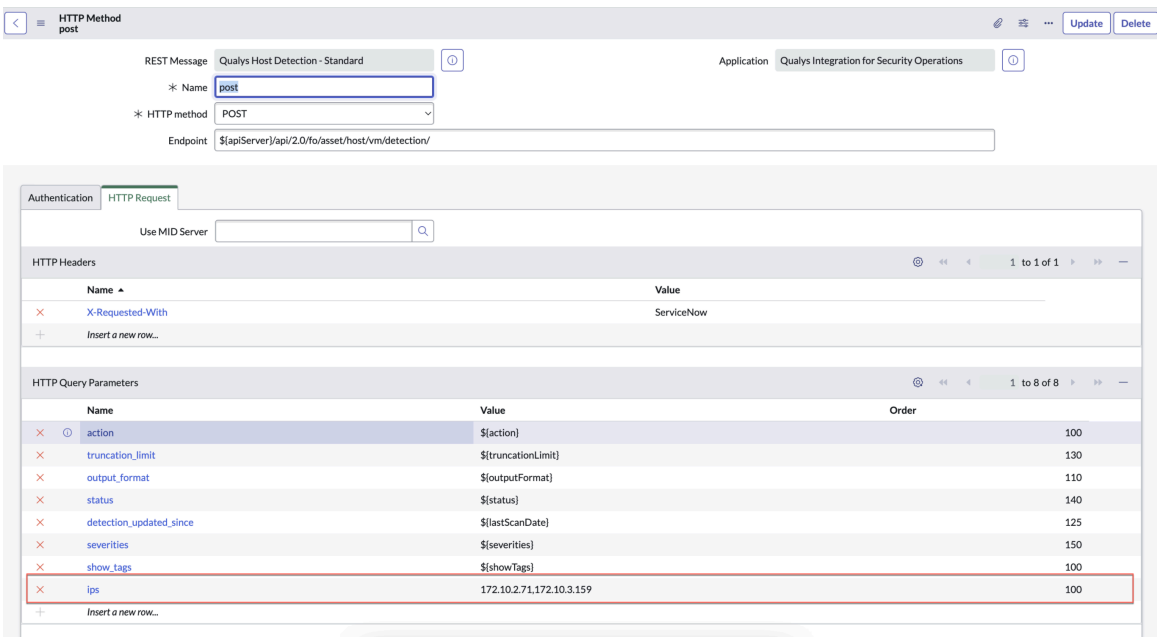


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Suchen Sie die vom Produkt Qualys unterstützten Parameter auf der Entwickler-Website, die Sie zum Filtern verwenden möchten.
   Parameter und Werte, die Sie aus dem Produkt Qualys eingeben, werden nur auf der Ebene der Integrationsinstanz in Now Platformunterstützt. Alle Qualys -Integrationen unterstützen die Filterung mithilfe von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
3. Klicken Sie auf der Listenseite Qualys Integrationen auf den Datensatz für die Integration, für die Sie den Datensatz öffnen möchten.
4. Suchen Sie auf der Registerkarte Qualys REST-Details das Informationssymbol (I) für die REST-Methode, gefolgt von **Datensatz** öffnen, um den HTTP-Methodendatensatz zu öffnen.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von der Entwickler-Website Qualys erhalten haben.

   In der folgenden Abbildung wurde beispielsweise der Parameter, der nur bestimmte IP-Adressen/Bereiche erfasst, `ips={value}` hinzugefügt. In diesem Fall ist der **Wert** eine oder mehrere von Ihnen angegebene IPs/Bereiche. Mehrere Einträge sind durch Kommas getrennt, `172.10.2.71, 172.10.3.159`, und ein Bereich wird mit einem Bindestrich angegeben, `10.10.10.1-10.10.10.100`. Weitere Informationen finden Sie auf der Entwickler-Website Qualys.




   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Qualys weitere Informationen zum Trennen der einzelnen Werte.

   **Hinweis:**
   Sie sollten Ihre API-Anforderungen kennen. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textinhalt hinzufügen.

   Einige andere Parameter, die Sie auf der Entwickler-Website Qualys nützlich finden könnten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `ag_ids` Abzurufende Asset-Gruppenlisten-IDs. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich übernommen werden.
- `qids` Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in Tabelle „Drittpartei-Eintrag“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überschwemmt wird.

7. Klicken Sie auf **Aktualisieren**.

### Behebung von Problemen bei der Qualys Vulnerability-Integration

Einige häufig auftretende Probleme werden zusammen mit Problemumgehungen besprochen.

### Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge für Datenquellen oder bei einem Security Incident nach dem Import von Drittanbieterintegrationen nicht wie erwartet angezeigt werden, überprüfen Sie Ihre IP-Beschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge angezeigt werden, es sei denn, Sie sind über eine sichere IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies dazu führen, dass Sie Duplikate entfernen müssen.

Wenn Sie beispielsweise beim Ausführen einer Hostimportintegration einer Drittpartei keine Anhänge in Ihren Datenquellen sehen, überprüfen Sie Ihre IP-Beschränkungen, und fügen Sie der sicheren Liste Benutzer vor dem Import hinzu.

### Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und reichen in der Regel aus. Sie können Transformationszuordnungen entsprechend den Anforderungen Ihrer Organisation ändern.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + import_admin

#### Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** , um die REST-Nachrichten anzuzeigen.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf die Anwendung **Qualys Vulnerability Integration**.
3. Ändern Sie die Transformationszuordnungen gemäß den Kundenanforderungen.

   Weitere Informationen zu den von der Qualys-API bereitgestellten Daten finden Sie in der Qualys-API-Dokumentation .

### Überprüfen Sie die Größe der XML-Anhangeigenschaft

Überprüft, ob die XML-Anhangeigenschaft für große Dateien ausreichend ist.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**.
2. Scrollen Sie nach unten zu **Eigenschaften importieren** > **XML-Format** am Ende der Seite.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie ggf. den Wert in 250, und klicken Sie auf **Speichern**.

**Zugehörige Informationen**

Verfügbare Systemeigenschaften

### Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen dafür, wie Daten aus Qualys abgerufen werden. Viele Datensätze können mit Schwachstellen mit geringem Schweregrad verknüpft werden, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/-Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder welcher geeignete Schweregrad auch immer gewünscht wird)

### Fehler bei der Qualys Knowledge Base-Integration wird behoben

Beheben Sie den Fehler bei der Knowledge Base-Integration von [ Qualys, indem Sie die von Qualys empfangene Nutzlast-Anhanggröße auf das angegebene Limit reduzieren.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

## Prozedur

1. Stellen Sie sicher, dass die Größe des Nutzlastanhangs innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.
   b. Wechseln Sie zur Registerkarte „ **Integrationsinstanzparameter“**.
   c. Wählen **Sie max_delta_days aus,** und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**.
   b. Wählen Sie **Qualys Knowledge Base aus**.
   c. Wechseln Sie zur Registerkarte **Integrationsdetails**.
   d. Wählen Sie im Feld **Startzeit** das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wechseln Sie zur Registerkarte „ **Integrationsinstanzparameter“**.

g. Wählen **Sie kb_backfill_full_import aus,** und ändern Sie den Standardwert in true.

**Ergebnisse**
Durch die Ausführung der Qualys Knowledge Base-Auffüllungsintegration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Während die Qualys-Hosterkennungsintegration einen Platzhaltereintrag erstellt, wird dieser durch die Qualys Knowledge Base-Auffüllungsintegration aktualisiert.

### Qualys Vulnerability Integration Berichterstellung

Die Qualys Cloud Platform -Übersicht ist eine Ausführungsansicht der Schwachstellenaktivität. Durch die Bereitstellung von Trends, Berichten und Drilldowns in bestimmte Daten kann ein Administrator oder Analyst Problembereiche schnell erkennen. Die Diagramme werden mit Daten ausgefüllt, nachdem angreifbare Elemente und die Knowledge Base-Daten Qualys abgerufen wurden.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

## Frühere Versionen von Vulnerability Response

Schwachstellenanalysten können auch die Standard-Dashboards in der klassischen Umgebung verwenden, um Schwachstellendaten zu überwachen. Weitere Informationen finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.

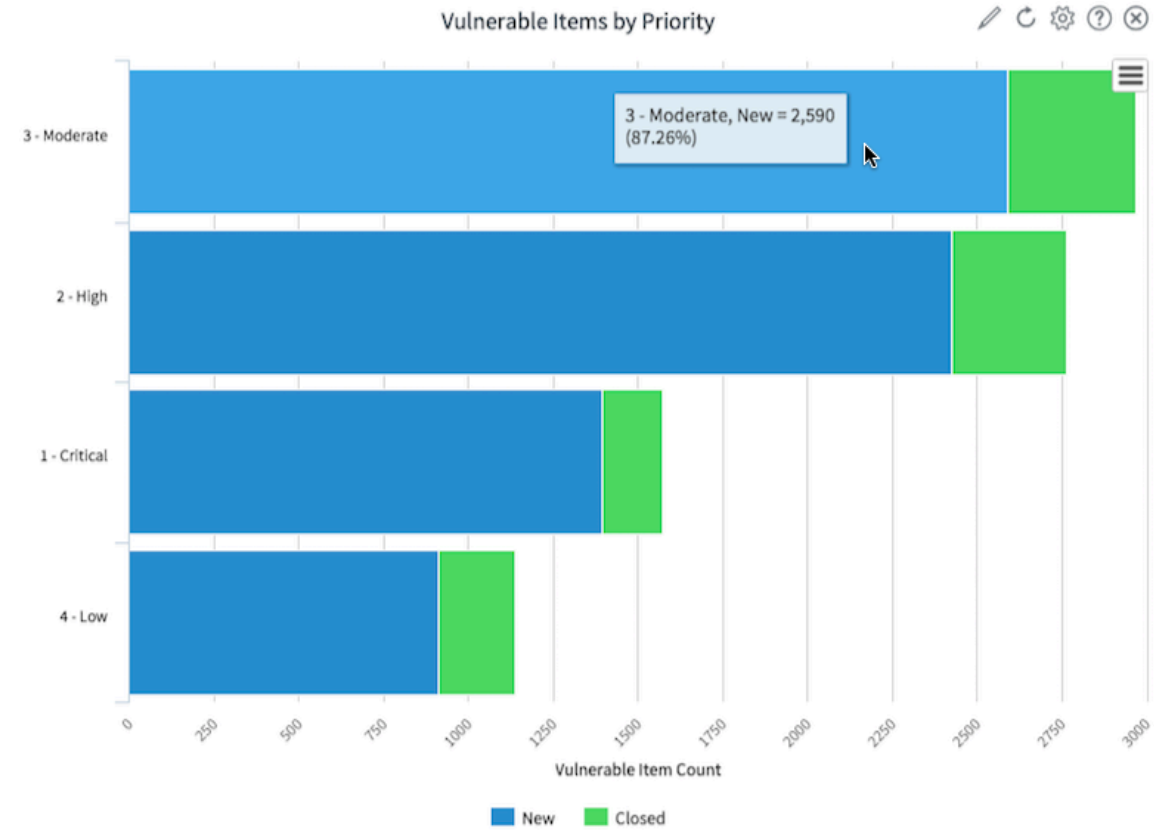
**Hinweis:**
Bei der Verwendung der Qualys Cloud Platform Vulnerability-Integration wird davon ausgegangen, dass Optimierung, Tests und Bereitstellung in Ihrer Instanz erfolgt sind. Diese Funktionen gehen über den Umfang der Produktdokumentation hinaus. Wenden Sie sich an Kundenservice und Support, um Unterstützung zu erhalten.

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt usw.) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Beispieldiagramm Qualys Vulnerability Integration .**




Die folgenden Berichte sind auf der Homepage Qualys Cloud Platform verfügbar.

**Qualys Vulnerability Integration Übersichtsberichte**

| Name | Visuell | Beschreibung |
|---|---|---|
| Mit Qualys synchronisierte CIs | Balkendiagramm | Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes CI aufgezeichnet wurden, von den meisten bis zu den wenigsten. |
| Offene angreifbare Qualys-Elemente | Balkendiagramm | Zeigt die Anzahl der offenen angreifbaren Elemente an, die Schwachstellen zugeordnet sind (CVE-Datensätze), von den meisten bis zu den wenigsten. |
| Angreifbare Qualys-Elemente insgesamt | Balkendiagramm | Zeigt die Anzahl der ignorierten angreifbaren Elemente an, deren Ablauf innerhalb von 7 Tagen geplant ist. |
| Angreifbare Elemente nach Priorität | Trend | Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an. |
| QID-Verbreitung | Balkendiagramm | Zeigt die Anzahl der für jedes Modell aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten. |
| Offene angreifbare Qualys-Elemente | Liste | Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Qualys Statusdiagramm der Integrationsausführung

Das Modul Qualys „ Integrationsausführungsstatus“ ist eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status der Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

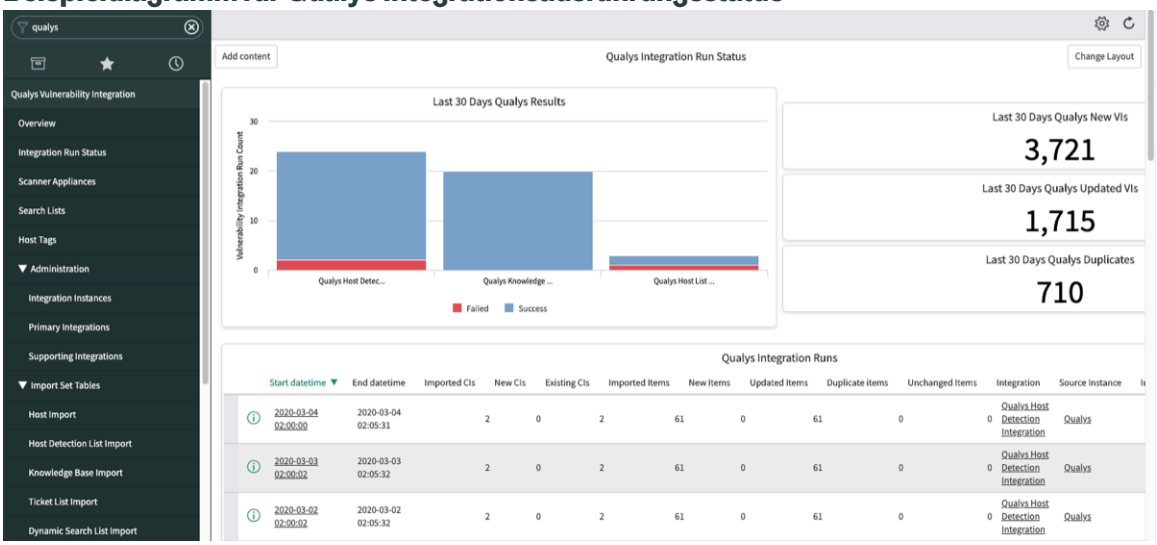
**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Der Integrationsausführungsstatus Qualys zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die von Qualys [qualys] aktualisierte VIs-Anzahl gibt die Anzahl für eindeutige Erkennungen im selben Asset an. Die VI wird dann mit der neuen Erkennung aktualisiert.

**Hinweis:**
Die Ausführungsanzahl der Schwachstellenintegrationen wird nur für die Integrationen angezeigt, die auf den Status „Aktiv“ gesetzt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** und legen Sie den Status auf „Aktiv“ fest.

### Beispieldiagramm für Qualys Integrationsausführungsstatus




- Die Werte in der Spalte „Importierte Elemente“ stellen die Gesamtzahl der Datensätze dar, die aus einer Integrationsausführung erstellt werden.
- Die Spalte Neue Elemente zeigt die Anzahl der Datensätze an, die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- Die Spalte Aktualisierte Elemente zeigt an, wie oft Datensätze während einer Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eindeutigen Datensätze, die aktualisiert werden. Wenn beispielsweise ein Datensatz während der Integrationsausführung zweimal aktualisiert wird, wird er zweimal gezählt und als 2 aktualisierte Elemente angezeigt.

- Die Spalte Unveränderte Elemente zeigt Datensätze an, die während der Integrationsausführung gefunden wurden und bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

**Hinweis:**
Die Integration wird mit null Ergebnissen für alle vier der folgenden Werte ausgeführt: **Neue CIs**, **vorhandene CIs**, **neue Elemente**und **aktualisierte Elemente** werden aus der Liste der **Qualys-Integrationsausführungen** herausgefiltert.

### Qualys Statusdiagrammberichte der Integrationsausführung

| Name | Beschreibung |
|---|---|
| Ergebnisse der letzten 30 Tage Qualys . | Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Führen Sie in einer visuellen Leiste aus. |
| Letzte 30 Tage Qualys Neue AEs | Die Anzahl der neuen Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Aktualisierte AEs der letzten 30 Tage Qualys . | Die Anzahl der aktualisierten Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Duplikate der letzten 30 Tage Qualys . | Die Anzahl der doppelten Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Qualys Integrationsausführungen | Die Datensätze der Integrationsausführung werden in einer Liste angezeigt.<br>**Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |
| Angreifbares Element – Erfassungsleistungsmetriken der letzten 30 Tage Qualys . | Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage. |
| Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Qualys . | Täglicher Durchsatz bei der Erfassung angreifbarer Elemente, gemessen für die Integration der Qualys -Hosterkennung in den letzten 30 Tagen. |

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

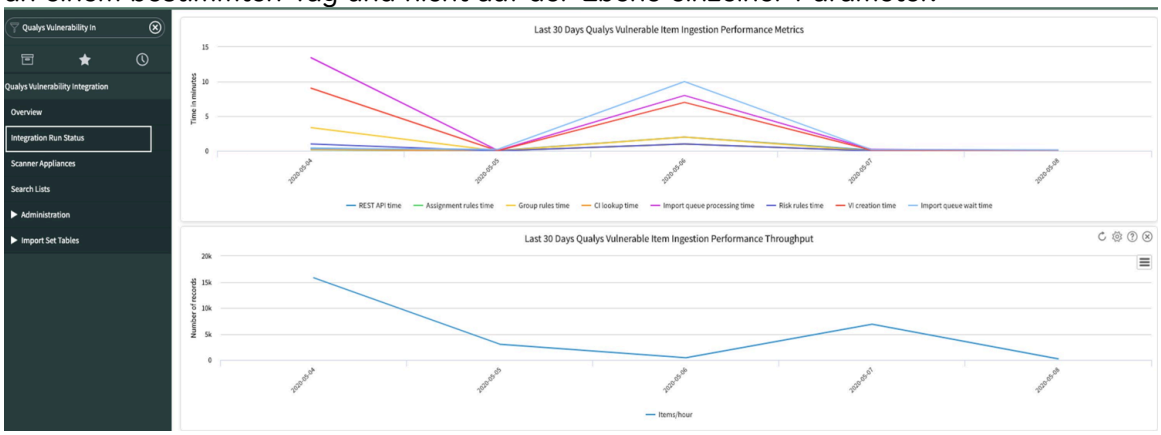
- Qualys Leistungsmetriken der Erfassung angreifbarer Elemente: Vergleichen Sie die täglichen Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu ermitteln. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf der Ebene der Integrationsausführung berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.

- Qualys Leistungsdurchsatz bei der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Durchsatz bei der Erfassung angreifbarer Elemente für die Qualys Host-Erkennungsintegration. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf der Ebene einzelner Parameter.




### Qualys-Datentransformation

Die aus Qualys abgerufenen Daten werden über eine Reihe von Datenquellen und Transformationen verarbeitet.

Die meisten Transformationen für Qualys Vulnerability Integration werden mithilfe von Transformationsskripts durchgeführt. Diese Skripts sind für den internen Gebrauch bestimmt. Das Löschen wird nicht empfohlen. Änderungen erfordern Codierung oder fortgeschrittene ServiceNow - oder Qualys Vulnerability Integration -Kenntnisse. Die verbleibenden Zuordnungen werden in diesem Abschnitt aufgelistet und verwenden Feldzuordnungen.

**Hinweis:**
Während der Installation werden im Modul Vulnerability Response Normalisierte Schweregradzuordnung normalisierte Schweregradzuordnungen installiert, die importierte Qualys Cloud Platform Schweregradstufen in standardmäßige ServiceNow Schweregradstufen umwandeln. Weitere Informationen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung.

### Import dynamische Suchliste

Die Transformationszuordnung für dynamische Qualys-Suchlisten wird zum Transformieren und Importieren von dynamischen Qualys-Suchlisten verwendet. Änderungen an dieser Transformation ändern, wie dynamische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Dynamische Suchlistenimport**.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

#### Qualys Dynamische Suchliste Transformationszuordnungsfelder

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Wird als Bezeichner für die dynamische Qualys-Suchliste verwendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Qualys Dynamische Suchliste Transformationszuordnungsfelder (Fortsetzung)**

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| [Skript] | list_type | Der Typ der Suchliste. Dynamisch ist der Standardwert für die Transformation der dynamischen Suchliste. |
| u_title | Titel | Der Name in Qualys für diese Suchliste. |

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

**Qualys Dynamische Suchliste Transformationszuordnungsskript Timing und Zweck**

| Wann das Skript ausgeführt wird | Zweck des Skripts |
|---|---|
| onAfter (nachdem die Transformation eines Importsatzes abgeschlossen wurde). | Erstellt die Beziehungen zwischen Suchlisten und den zugehörigen Schwachstellen.<br><br>Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Import statische Suchliste

Die Transformationszuordnung für statische Qualys-Suchlisten wird zum Transformieren und Importieren von statischen Qualys-Suchlisten verwendet. Änderungen an dieser Transformation ändern, wie statische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Import statische Suchliste**.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

**Qualys statische Suchliste Transformationszuordnungsfelder**

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Wird als Bezeichner für die statische Qualys-Suchliste verwendet. |
| u_title | Titel | Der Name in Qualys für diese Suchliste. |
| [Skript] | list_type | Der Typ der Suchliste. „Statisch“ ist der Standardwert für die Transformation der statischen Suchliste. |

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Qualys statische Suchliste Transformationszuordnungsskript Timing und Zweck

| Wann das Skript ausgeführt wird | Zweck des Skripts |
|---|---|
| onAfter (nachdem die Transformation eines Importsatzes abgeschlossen wurde). | Erstellt die Beziehungen zwischen Suchlisten und den zugehörigen Schwachstellen.<br><br>Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Assetgruppenimport

Die Transformationszuordnung für Qualys-Asset-Gruppengeräte wird verwendet, um Qualys-Asset-Gruppendaten zu transformieren, um Datensätze für Scanner-Geräte zu erstellen. Änderungen an dieser Transformation ändern, wie Scanner-Geräte erstellt und geändert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Assetgruppenimport**.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

### Qualys-Asset-Gruppen-Transformationszuordnungsfelder

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Wird als Bezeichner für die Qualys-Asset-Gruppe verwendet. |
| [Skript] | Manuell | Geskripteter Wert, um zu bestimmen, wie der Zieldatensatz erstellt wurde. Wenn es durch Transformationen erstellt wird, ist dieses Feld immer „false“. |
| [Skript] | ips | Die IP-Adressen, die der zu transformierenden Asset-Gruppe zugeordnet sind. |
| u_default_appliance_id | Appliance_ID | Der Qualys-Gerätebezeichner für das Standardgerät in dieser Asset-Gruppe. |
| u_title | asset_group_name | Name der Qualys-Asset-Gruppe |

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

### Timing und Zweck des Skripts für Qualys-Asset-Transformationszuordnungen

| Wann das Skript ausgeführt wird | Zweck des Skripts |
|---|---|
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Das Skript, das die Asset-Gruppe einschränkt, importiert nur Asset-Gruppen mit einer Standard-Appliance und einem Satz zugeordneter IP-Adressen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Timing und Zweck des Skripts für Qualys-Asset-Transformationszuordnungen (Fortsetzung)**

| Wann das Skript ausgeführt wird | Zweck des Skripts |
|---|---|
| | Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Appliance-Import

Die Qualys-Appliance-Transformationszuordnung wird verwendet, um Qualys-Appliance-Daten in Appliance-Datensätze umzuwandeln. Dies wird verwendet, um die Gerätedatensätze zu aktualisieren, die anfänglich aus dem Asset-Gruppenimport erstellt werden. Änderungen an dieser Transformation ändern, wie Gerätedatensätze mit Gerätedetails aktualisiert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Appliance-Import**.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

**Felder der Qualys-Appliance-Transformationszuordnung**

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_name | Appliance_name | Der Name der Qualys-Scanner-Appliance |
| u_status | Appliance_status | Der letzte gemeldete Status der Qualys-Scanner-Appliance. |
| u_id | Appliance_ID | Der Bezeichner des Qualys-Geräts. |

Zusätzlich zu den Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

**Timing und Zweck des Qualys-Appliance-Transformationszuordnungsskripts**

| Wann das Skript ausgeführt wird | Zweck des Skripts |
|---|---|
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Wird verwendet, um Gerätenamen und -status für die angegebene ID zu aktualisieren.<br><br>Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Qualys-REST-Nachrichten

Qualys-REST-Nachrichten werden für Aufrufe an die Qualys-API verwendet.

Ab Version 12.9.2 von Qualyshaben Sie die Möglichkeit, zwischen Standardauthentifizierung und OAuth zu wählen. Die Qualys-Cloud-Authentifizierungsmethode für Instanzparameter ist für Standardauthentifizierung vorkonfiguriert. Wenn Sie OAuth verwenden möchten, müssen Sie den Parameter der Integrationsinstanz ändern und dann die REST-Nachricht direkt für OAuth einrichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## REST-Nachricht für Qualys-Hosterkennung

Die REST-Nachricht der Qualys-Hosterkennung führt den ersten Aufruf der Hostlisten-Erkennungs-API für die Integration der Qualys-Hosterkennung durch.

### REST-Nachrichtenparameter der Qualys-Hosterkennung

| Parametername | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. Änderungen sind nicht erforderlich. |
| output_format | XML | Legt das Format des von Qualys zurückgegebenen Berichts fest.<br><br>Die verschiedenen Skripts und Transformationen setzen XML voraus, daher werden Änderungen am Wert nicht empfohlen. |
| discovery_processed_after | ${lastScanDate} | Zeigt nur Erkennungen an, deren Erkennungsstatus sich nach einem bestimmten Datum und einer bestimmten Uhrzeit geändert hat. Bei Erkennungen, die sich nie geändert haben, wird das Datum auf das Datum der letzten Erkennung angewendet. |
| truncation_limit | 500 | Die Anzahl der Hosts, von denen Daten laut Anforderung abgerufen werden sollen. Dieser Parameter wird für Paginierungszwecke verwendet.<br><br>Der Standardwert ist 500, es können jedoch höhere oder niedrigere Werte verwendet werden. Legen Sie keinen Wert unter 100 fest, da dies die Systemlast erheblich erhöht.<br><br>Kleinere Werte erfordern mehr Aufrufe der Qualys-API, und größere Werte führen zu größeren zu verarbeitenden Ergebnismengen und potenziellen Zeitüberschreitungen beim Datenabruf/-verarbeitung. |
| Status | Neu, Repariert, Aktiv, Erneut geöffnet | Erkennungsstatus, die aus Qualys abgerufen werden sollen.<br><br>Standardmäßig werden alle Status abgerufen. Bei großen Datenabrufen (häufig beim anfänglichen Abrufen von Daten) kann es von Vorteil sein, feste Status aus dieser Liste auszuschließen.<br><br>Es ist wichtig, den Status Repariert einzubeziehen, wenn bereits im System vorhandene Schwachstellen aktualisiert werden. |

## REST-Nachricht zur Paginierung der Qualys-Hosterkennung

Die REST-Nachricht zur Paginierung der Hosterkennung verarbeitet Paginierungsanforderungen an die Hosterkennungs-API.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die primäre Hosterkennung ausgeführt wird und die Qualys-API eine URL zum Abrufen der nächsten Datenseite bereitstellt, ruft diese REST-Nachricht diese zusätzlichen Daten ab. Diese Daten werden vom Host-Erkennungs-Paginierungs-Handler verwendet.

Hosterkennungspaginierung REST ist eine spezialisierte REST-Nachricht und soll nicht geändert werden.

## REST-Nachricht der Qualys-Knowledge Base (Auffüllung).

Die REST-Nachricht „Qualys Knowledge Base (Auffüllung)“ ruft Qualys-Knowledge Base-Daten basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten für die Qualys Knowledge Base-Integration ab.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys zum Abrufen von Knowledge Base-Informationen aus.

Die folgende Tabelle zeigt die gesendeten Anforderungsparameter.

**REST-Nachrichtenparameter der Qualys-Knowledge Base (Auffüllung).**

| Parameter | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. Änderungen werden nicht empfohlen. |
| details | Alle | Gibt die Detailebene an, die für abgerufene Schwachstellen angezeigt wird.<br><br>Kann bei Bedarf sicher geändert werden. |
| ids | ${qids} | Gibt an, welche QIDs aus Qualys abgerufen werden sollen.<br><br>In Code referenziert. Änderungen werden nicht empfohlen. |

## REST-Nachricht der Qualys-Knowledge Base (datumsbasiert).

Die REST-Nachricht der Qualys-Knowledge Base (datumsbasiert) wird verwendet, um Qualys-Knowledge Base-Daten basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten abzurufen. Diese Nachricht wird von der Qualys Knowledge Base-Integration verwendet.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys zum Abrufen von Knowledge Base-Informationen aus.

Die folgende Tabelle zeigt die gesendeten Anforderungsparameter.

**REST-Nachrichtenparameter der Qualys-Knowledge Base (datumsbasiert).**

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. Änderungen werden nicht empfohlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**REST-Nachrichtenparameter der Qualys-Knowledge Base (datumsbasiert). (Fortsetzung)**

| Quellfeld | Zielfeld | Beschreibung |
|---|---|---|
| details | Alle | Gibt die Detailebene an, die für abgerufene Schwachstellen angezeigt wird.<br><br>Kann bei Bedarf sicher geändert werden. |
| last_modified_after | ${DatumStart} | Gibt an, wann mit dem Abrufen von Verlaufsdaten begonnen werden soll.<br><br>Wird vom Code verwendet, um sowohl die Startzeit zu bestimmen als auch die Paginierung zu unterstützen.<br><br>Änderungen oder Entfernung werden nicht empfohlen. |
| last_modifiedbefore | ${DatumEnde} | Gibt an, wann das Abrufen von Verlaufsdaten enden soll. Wird vom Code verwendet, um die Endzeit zu bestimmen und die Paginierung zu unterstützen.<br><br>Änderungen oder Entfernung werden nicht empfohlen. |

## REST-Nachricht für Qualys-Tickets

Die REST-Nachricht für Qualys-Tickets ruft Qualys-Ticketinformationen für die Qualys-Ticket-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Qualys zum Abrufen von Ticketinformationen aus.

Die Tabelle zeigt die gesendeten Anforderungsparameter.

**REST-Nachrichtenparameter für Qualys-Tickets**

| Parametername | Wert | Beschreibung |
|---|---|---|
| modifiziert_seit_Datum/Uhrzeit | ${lastRunDatetime} | Gibt das letzte Ausführungsdatum der Integration und das Datum an, nach dem Daten abgerufen werden sollen.<br><br>Von Code verwendet. Änderungen werden nicht empfohlen. |
| seit_ticket_number | ${letzteTicketNummer} | Gibt an, welches Ticket zuletzt aus Qualys abgerufen wurde.<br><br>Wird für die Paginierung verwendet. Änderungen werden nicht empfohlen. |
| show_vuln_details | 1 | Gibt an, ob die Schwachstellendetails abgerufen werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Rapid7 Vulnerability Integration verstehen

ServiceNow® Rapid7 Vulnerability Integration verwendet Daten, die aus dem Data Warehouse von Rapid7 oder den Produkten von Rapid7 InsightVM ] importiert wurden, um die Auswirkungen und Priorität potenziell böswilliger Bedrohungen zu bestimmen.

Sensoren vonRapid7 Nexpose erfassen Daten und senden sie automatisch an die Produkte von Rapid7 Data Warehouse (lokal) oder Rapid7 InsightVM (cloud-basiert), die die Informationen kontinuierlich analysieren und korrelieren. Die Lösung lässt sich problemlos in ServiceNow® Vulnerability Response integrieren, um Schwachstellen in CIs und Services zuzuordnen. Rapid7 Vulnerability Integration erweitert die Schwachstellendaten in Ihrer Instanz.

Rapid7 -Integrationen sind Einstiegspunkte, die mit dem Data Warehouse oder den Produkten von Rapid7 InsightVMRapid7 interagieren und als regelmäßige Aufgaben aufgerufen werden. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Die geplanten Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen.

**Hinweis:**

Wenn Sie sowohl Rapid7 Data Warehouse als auch Rapid7 InsightVM als Quellen für Ihre Daten verwenden, besteht die Gefahr doppelter Schwachstellendatensätze.

**Hinweis:**

Bei der Migration vom **Data Warehouse** -Integrationstyp zum **InsightVM-** Typ können Sie Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Sie Rapid7 Vulnerability Integration Data Warehouse-Datensätze.

Wenn Sie mehrere Bereitstellungen der Schwachstellenintegration Rapid7 InsightVM haben, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen und ihre Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen mehreren Bereitstellungen überschneiden. Daten aus jeder Bereitstellung werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

**Hinweis:**

Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber Sie können sie deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

## Verfügbare Versionen

| **Release-Version für** Washington DC | **Releasehinweise** |
|---|---|
| Rapid7 Vulnerability Integration v13.6, 13.7 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Rollen

Rapid7 Aufgaben zur Integration von Schwachstellen umfassen die folgenden Rollen.

- sn_vul_r7.admin: Kann Datensätze lesen, schreiben und löschen.
- sn_vul_r7.user: Kann Datensätze lesen und schreiben.
- sn_vul_r7.read: Kann Datensätze lesen.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Rapid7 Vulnerability Integration-Integrationen

Um Rapid7 Vulnerability Integrationanzuzeigen, navigieren Sie zu **Rapid7** > **Administration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

### Rapid7 Data Warehouse-Integrationen

| Integration | Beschreibung |
|---|---|
| Rapid7 Vulnerability Integration | Ruft Schwachstellendaten von Rapid7 Nexpose ab und verarbeitet sie in Ihrer Instanz. |
| Rapid7 Integration von Asset-Listen | Ruft Scan-Daten einmal pro Woche aus Rapid7 Nexpose Data Warehouse ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums des **letzten Scans**. Zeigen Sie die Zeit des **letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responsean. |
| Rapid7 Kategorieintegration | Ruft Kategorieinformationen aus Rapid7 Nexposeab. Kategorien bieten eine allgemeine Klassifizierung für Schwachstellen. |
| Rapid7 Exploit-Integration | Ruft Exploit-Informationen von Rapid7 Nexposeab. |
| Rapid7 Malware-Kit-Integration | Ruft Malware-Kit-Informationen von Rapid7 Nexposeab. |
| Rapid7 Referenzintegration | Ruft Verweise auf externe regulatorische Dokumente wie CVEs oder herstellerspezifische Schwachstellenreferenzen ab. |
| Rapid7 Lösungsintegration | Ruft Lösungsdaten aus Rapid7 Nexposeab, die empfohlene Lösungen für bestimmte Schwachstellen bereitstellen. |
| Rapid7 Lösungsintegration ersetzen | Ruft Informationen darüber ab, welche Lösungen durch andere Lösungen ersetzt werden. |
| Rapid7 Erforderliche Lösungsintegration | Ruft Informationen zu den Lösungen ab, die Voraussetzungen für andere Lösungen sind. Wenn diese Integration ausgeführt wird, wird die Zuordnung von Lösungen und erforderlichen Lösungen aus dem Data Warehouse Rapid7 abgerufen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Rapid7 Data Warehouse-Integrationen (Fortsetzung)

| Integration | Beschreibung |
|---|---|
| | **Hinweis:**<br>Diese Integration funktioniert nur, wenn das Plugin Vulnerability Solution Management aktiviert ist. |
| Rapid7 Integration der Schwachstellen-Lösungszuordnung | Ruft die Zuordnung ab, um Lösungen mit Schwachstellen zu verknüpfen. |
| Rapid7 Integration von angreifbaren Elementen | Ruft Daten zu angreifbaren Elementen aus Rapid7 Nexpose ab und verarbeitet sie in Ihrer Instanz.<br>Die Ausgaben dieser Integration sind angreifbare Elemente. |
| Rapid7 Integration der Lösung angreifbarer Elemente | Ruft Informationen darüber ab, welche angreifbaren Elemente in Rapid7 Nexpose als geschlossen markiert sind, und schließt die entsprechenden angreifbaren Elemente in Vulnerability Response. |
| Rapid7 Site-Integration | Ruft Site-Daten aus Rapid7 Nexposeab. Eine Site ist eine Sammlung von Assets, die gescannt werden sollen. |
| Rapid7 Integration von Asset-Listen | Ruft Host-Tags und Scan-Daten einmal pro Woche aus dem Data Warehouse Rapid7 ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums des **letzten Scans**. Zeit des **letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responseanzeigen |
| Rapid7 Umfassende Integration von angreifbaren Elementen | Importiert alle Rapid7-Erkennungen für alle Konfigurationselemente, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuellen importierten Daten werden angreifbare Elemente, die kürzlich bei Scans nicht gefunden wurden, automatisch auf „Geschlossen“ gesetzt, wenn das Modul „Veraltete angreifbare Elemente automatisch schließen“ aktiviert ist. |

### Rapid7 InsightVM-Integrationen

| Integration | Beschreibung |
|---|---|
| Rapid7 Integration von angreifbaren Elementen – API | Ruft Daten zu angreifbaren Elementen von Rapid7 InsightVM ab und verarbeitet sie in Ihrer Instanz. |
| Rapid7 Vulnerability Integration -API | Ruft Referenz-, Kategorie-, Exploit-, Malware-Kit- und Schwachstellendaten von Rapid7 InsightVM ab und verarbeitet sie in Ihrer Instanz. |
| Rapid7 Asset-Listen-Integration – API | Ruft Host-Tags und Scan-Daten einmal pro Woche von Rapid7 InsightVM ab und speichert sie im Modul „Erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden, anhand des Datums des **letzten Scans**. Zeigen Sie die Zeit des **letzten Scans** in der Liste „Erkannte Elemente“ in Vulnerability Responsean. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Rapid7 InsightVM-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| Rapid7 Umfassende Integration von angreifbaren Elementen – API | Importiert alle Rapid7-Erkennungen für alle Konfigurationselemente, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuellen importierten Daten werden angreifbare Elemente, die kürzlich bei Scans nicht gefunden wurden, automatisch auf „Geschlossen“ gesetzt, wenn das Modul „Veraltete angreifbare Elemente automatisch schließen“ aktiviert ist. |
| Rapid7 Site-Integration | Ruft Site-Daten aus dem Produkt Rapid7 InsightVM ab. Diese Integration wird wöchentlich um 00:00:00 Uhr ausgeführt. |

Während des Imports werden noch nicht vorhandene CVE-Datensätze als NVD-Datensätze erstellt und standardmäßig in Einträgen von Drittanbietern für Rapid7 referenziert. Die Vorlagenintegration für Rapid7 kann nicht gelöscht werden. Deaktivieren Sie sie stattdessen.

## Der Service Graph Connector für Rapid7

Ab Version 2.0 ist Service Graph Connector für Rapid7 über den ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Service Graph Connector for Rapid7 .

## CI-Suchregeln

CI-Suchregeln bestimmen, wie das Feld **Configuration Item** in einem Datensatz für angreifbare Elemente ausgefüllt wird.

Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

Informationen zum Erstellen oder Bearbeiten von Suchregeln finden Sie unter Erstellen Sie eine Vulnerability Response-CI-Suchregel.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie, wenn Sie neue Regeln erstellen.

## Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus Rapid7 Integrationen angreifbarer Elemente (Data Warehouse oder InsightVM-API) und der Rapid7 Asset List Integration-API erkannt wurden. Die Rapid7 Asset List Integration – API importiert alle Rapid7-Assets, die seit der letzten Integrationsausführung auf Schwachstellen gescannt wurden. Die Rapid7 Data Warehouse-Asset-Listen-Integration ist enthalten.

**Hinweis:**
Der Standardfilter für diese Liste ist auf **Nicht abgeglichen**festgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente in Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Host-Tags

Host-Tags werden als Teil der Rapid7 Asset-Listen-Integration – API-Integration für Rapid7 InsightVMimportiert. Sie werden hauptsächlich zum Filtern in Vulnerability Response Zuweisungs- und Korrekturaufgabenregeln in Rapid7 InsightVMverwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

Host-Tags

**Hinweis:**
Die API-Integration von Rapid7 Asset List integration sollte vor dem Erstellen von Zuweisungs- oder Korrekturaufgabenregeln in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag hat den Vorzug.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags gesteuert**. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Wenn Sie Tags deaktivieren, werden sie in allen Instanzen deaktiviert.

## Sites

Eine Site ist eine Sammlung von Assets, die gescannt werden sollen. Eine Site besteht aus Ziel-Assets, einer Scan-Vorlage, einer oder mehreren Scan Engines und anderen scanbezogenen Einstellungen wie Zeitplänen oder Warnungen. Sites werden von Rapid7 -Anwendungen verwaltet.

Rapid7 Vulnerability Integration Mit der Site-Filterung während der Konfiguration können Sie Assets während des Imports nach Site kategorisieren und anfordern. Weitere Informationen zum Filtern von Importen finden Sie unter Filtern nach Rapid7 Sites.

Die Integrationen von Rapid7 Data Warehouse und Rapid7 InsightVM Sites importieren Sites als wöchentliche geplante Aufgabe.

Um die importierten Sites in einer Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Sites**.

## Öffnen Sie aufgelöste angreifbare Elemente erneut, die nicht durch Scans geschlossen wurden

Angreifbare Elemente, die in Ihrer Instanz Now Platform auf „Gelöst“ festgelegt, aber durch die nachfolgenden Integrationsausführungen nicht in „Geschlossen/Korrigiert“ geändert wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Erkennungen von Rapid7 ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um aufgelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIs, die auf „Gelöst“ gesetzt sind, aber dann nicht durch nachfolgende Scans auf „Geschlossen/Korrigiert“ gesetzt wurden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder auf „Offen“ gesetzt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## CIs mit der Identification and Reconciliation Engine (IRE) erstellen

Sie können die Identification and Reconciliation Engine verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Drittanbieter-Scanner importiert wurde. Aktivieren Sie das Plugin „CMDB CI Class Models“, um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.. Weitere Informationen zum Konfigurieren der Kategorisierung nicht abgeglichener Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

## Scannen Sie angreifbare Elemente erneut

Initiieren Sie erneute Scans auf der Rapid7 -Plattform, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen geplanten Scan-Zyklen korrigiert wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für die Rapid7 Schwachstellenintegration.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Rapid7 Lösungsmanagement

Wenn Sie das Plugin Rapid7Vulnerability Solution Management aktiviert haben, werden die Lösungen Rapid7 sowohl für das Data Warehouse von [] als auch für [ Rapid7 InsightVM in die Tabelle „Lösungen für Schwachstellen“ [sn_vul_solution] gefüllt. Wenn Sie jedoch das Plugin Rapid7 Vulnerability IntegrationVulnerability Solution Management nicht aktiviert haben, funktioniert [] unverändert und importiert die Lösungen in die benutzerdefinierte Tabelle [sn_vul_r7_solution]. Weitere Informationen finden Sie unter Rapid7 Lösungsmanagement.

### wird vorbereitet Rapid7 Vulnerability Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Rapid7 Vulnerability Integration setzt voraus, dass Sie mit Rapid7 Data Warehouse- oder Rapid7 InsightVM Produktscans in Ihrer Umgebung vertraut sind und diese ausführen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Warum und wann dieser Vorgang ausgeführt wird**
Die Scanner Rapid7 sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

Bevor Sie die Anwendung Rapid7 Vulnerability Integration aus dem ServiceNow® Store herunterladen und in Ihrer Instanz installieren, überprüfen Sie die folgenden Informationen zu den Integrationstypen und Setup-Informationen:

In [] sind zwei Arten von Integrationen enthalten, die in ServiceNow® StoreRapid7 Vulnerability Integration verfügbar sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rapid7 InsightVM
- Rapid7 Data Warehouse

Der Data Warehouse-Typ Rapid7 :

- Erfordert die URL Ihres Rapid7 Data Warehouse-Servers und Ihre Anmeldeinformationen für die Authentifizierung
- Erfordert einen MID-Server
- Verwendet einen PostgresSQL-Treiber, um Abfragen im Data Warehouse auszuführen
- Unterstützt nicht mehrere Instanzen

Der Integrationstyp Rapid7 InsightVM :

- Ist cloudbasiert und verwendet eine REST-API. Diese Integration erfordert einen API-Schlüssel aus Ihrem Rapid7 Insight-Konto.
- Unterstützt mehrere Instanzen.

Weitere Informationen zu den Setup-Anforderungen für diese Integrationstypen finden Sie unter Richten Sie für die Data Warehouse-Integration Rapid7 ein (Data Warehouse) und Richten Sie für die Rapid7 InsightVM -Integration ein.

### Richten Sie für die Data Warehouse-Integration Rapid7 ein

Die Rapid7 Data Warehouse-Integration ist einer der Integrationstypen, die in Rapid7 Vulnerability Integration Rapid7 Vulnerability Integrationenthalten sind.

**Vorbereitungen**
Bevor Sie die Data Warehouse-Integration von Rapid7 ausführen, führen Sie die folgenden Setup-Aufgaben durch:

- Ruft das Data Warehouse-Add-on Rapid7 ab. Informationen zum Erwerben und Installieren dieses Add-on finden Sie auf der Rapid7 Website und in der Dokumentation.
- Ruft den aktuellen PostgresSQL-Treiber ab. Wechseln Sie zu https://jdbc.postgresql.org/ , und laden Sie den neuesten Treiber herunter.
- Einen MID Server zum Ausführen von Abfragen an das Data Warehouse. Weitere Informationen zum Einrichten eines MID Servers finden Sie unter MID Server.

  Notieren Sie den Data Warehouse-Namen. Der Data Warehouse-Integrationstyp Rapid7 unterstützt nur eigenständige MID Server. Geclusterete MID Server werden nicht unterstützt.

- Rufen Sie die URL Ihres Rapid7 Data Warehouse-Servers und die Anmeldeinformationen für die Authentifizierung ab, und machen Sie sie zugänglich.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Melden Sie sich bei der Instanz Now Platform an, in der Sie die Anwendung Rapid7 Vulnerability Integration installieren möchten.
2. Installieren Sie die PostgreSQL-JAR-Datei, die Sie in den zuvor aufgeführten Setupaufgaben heruntergeladen haben.
   a. Navigieren Sie in Ihrer Instanz Now Platform zu **Alle** > **MID-Server** > **JAR-Dateien**.
   b. Klicken Sie auf **Neu**.
   c. Geben Sie den Namen des PostgresSQL-Treibers ein, den Sie zuvor heruntergeladen haben.

      Geben Sie optional die Informationen zu **Version**, **Quelle**und **Beschreibung** ein. Lassen Sie das Kontrollkästchen **Aktiv** aktiviert.

   d. Hängen Sie die heruntergeladene JAR-Datei mithilfe des Büroklammersymbols im Header an.
   e. Klicken Sie auf **Absenden**.

Sie haben das Setup für die Data Warehouse-Integration von Rapid7 abgeschlossen. Wenn Sie die Anforderungen für die Rapid7 InsightVM -Integration nicht überprüft haben, lesen Sie vor der Installation von Rapid7 Vulnerability IntegrationRichten Sie für die Rapid7 InsightVM -Integration ein und wird vorbereitet Rapid7 Vulnerability Integration.

Schritte zum Abrufen von -Berechtigungen, zum Herunterladen und Installieren von Rapid7 Vulnerability Integrationfinden Sie unter Rapid7 Vulnerability Integration installieren.

### Richten Sie für die Rapid7 InsightVM -Integration ein

Die Rapid7 InsightVM -Integration ist einer der Integrationstypen, die in Rapid7 Vulnerability Integration Rapid7 Vulnerability Integrationenthalten sind.

## Vorbereitungen

Führen Sie die folgenden Setup-Aufgaben aus, bevor Sie die Rapid7 InsightVM -Integration ausführen.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

## Prozedur

1. Halten Sie für den Integrationstyp Rapid7 InsightVM Ihre Region und Ihren API-Schlüssel bereit.
   Wenden Sie sich an Rapid7, um die entsprechende Region und den API-Schlüssel zu erhalten.
   Sie haben das Setup für die Rapid7 InsightVM -Integration abgeschlossen. Wenn Sie die Anforderungen für die Data Warehouse-Integration von Rapid7 nicht überprüft haben, lesen Sie vor der Installation von Rapid7 Vulnerability IntegrationRichten Sie für die Data Warehouse-Integration Rapid7 ein und wird vorbereitet Rapid7 Vulnerability Integration.
2. Schritte zum Abrufen von -Berechtigungen, zum Herunterladen und Installieren von Rapid7 Vulnerability Integrationfinden Sie unter Rapid7 Vulnerability Integration installieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Rapid7 Vulnerability Integration installieren

Nachdem Sie die Setup-Schritte für die -Integration abgeschlossen haben, damit sie ordnungsgemäß in Vulnerability Responseintegriert wird, rufen Sie Berechtigungen ab, laden Sie die Anwendung herunter und installieren Sie sie in Ihrer Now Platform® -Instanz.

#### Vorbereitungen

Erforderliche Rollen: admin für Download und Installation, sn_vuln.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

1. Weitere Informationen zu den Integrationstypen und Setup-Anforderungen für Rapid7 Vulnerability Integrationfinden Sie unter wird vorbereitet Rapid7 Vulnerability Integration, Richten Sie für die Data Warehouse-Integration Rapid7 ein und Richten Sie für die Rapid7 InsightVM -Integration ein ].
2. Führen Sie vor dem Herunterladen und der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.
3. Nachdem die Anwendung aktiviert wurde, führen Sie die unten aufgeführten Schritte aus, um Rapid7 Vulnerability Integrationzu konfigurieren.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen Now Platform für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich.<br><br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| | unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.<br>• Der Systemadministrator [admin] installiert die App. Falls noch nicht zugewiesen, weist der Administrator die Rolle „Schwachstellenadministrator“ [sn_vul.vulnerability_admin oder sn_vul.admin] zu.<br>• Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.<br>Die Administratorrolle Rapid7 wird geerbt, wenn Ihnen eine Administratorrolle in der Anwendung Vulnerability Response (VR) zugewiesen wird. |
| Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren. | Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support. |
| Richten Sie die Filterung ein | Verwenden Sie die Filterung, um die Anzahl der Elemente für den anfänglichen Import zu begrenzen, und stufen Sie Ihre Bereitstellung ein, indem Sie die Filter in nachfolgenden Importen anpassen. |
| Schwachstellenrechner deaktivieren | Wenn Sie keine Schwachstellenrechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird, zusätzlich zu den anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die anfängliche Importleistung auswirken. |
| Behalten Sie den Standardwert für „run-as“-Benutzer bei | Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht. |
| Verwenden von Host-Tags | Wenn Sie Host-Tags in Vulnerability Response Zuweisungs- oder Korrekturaufgabenregeln verwenden möchten, führen Sie die Rapid7 Asset List-Integration aus, bevor Sie Regeln erstellen. |
| Deduplizieren vorhandener Datensätze | Bei der Migration vom **Data Warehouse** -Integrationstyp zum **InsightVM-** Typ können Sie Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Sie Rapid7 Vulnerability Integration Data Warehouse-Datensätze. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie die Anwendung Rapid7 Vulnerability Integration installieren möchten.
2. Navigieren Sie zu ServiceNow Store, und melden Sie sich an.
3. Suchen Sie in [ ServiceNow Storenach der Anwendung Rapid7 Vulnerability Integration.

   **Hinweis:**
   In ServiceNow Storeheißt die Anwendung Rapid7 Integration for Security Operations. Diese Anwendung erfordert ein -Abonnement.

4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren Sie in Ihrer Instanz Now Platform zu **Systemanwendungen** > **Alle Anwendungen** > **Alle**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Im Dialogfeld „Installieren“ wird Ihr Abhängigkeitsstatus angezeigt. Wenn Sie eine Abhängigkeitsanwendung benötigen, wird die benötigte Anwendung angezeigt. Befolgen Sie die Anweisungen im Dialogfeld, um die Anwendung Rapid7 Vulnerability Integration in Ihrer Instanz zu installieren.

    **Hinweis:**
    Der Schwachstellenadministrator kann jetzt die Konfiguration der Anwendung abschließen. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability Integration.

#### Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability Integration

Konfigurieren Sie Rapid7 Vulnerability Integration, nachdem die Anwendung auf Ihrem Now Platform®installiert und aktiviert wurde.

### Vorbereitungen

Erforderliche Rolle: Der Administrator [admin] lädt die App herunter und installiert sie. sn_vul.vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

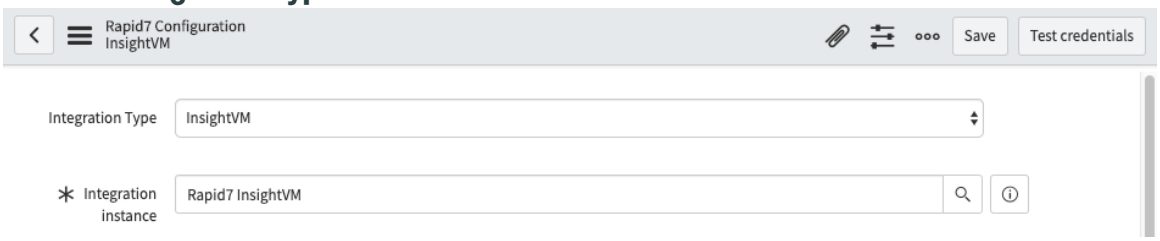
### Prozedur

1. Nachdem die Anwendung aktiviert (installiert) wurde, navigieren Sie zu **Rapid7 Vulnerability Integration** > **Administration** > **Konfiguration**.
2. Wählen Sie einen Integrationstyp aus der Liste aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Liste der Integrationstypen**




3. Wählen Sie eine Integrationsinstanz aus.
   Die Standardintegrationsinstanz Rapid7 InsightVM ist standardmäßig ausgewählt. Wenn dies der gewünschte Integrationstyp ist, führen Sie die folgenden Schritte aus. Wenn Sie den Data Warehouse-Integrationstyp Rapid7 konfigurieren möchten, fahren Sie mit Schritt 4 fort.

   a. Wählen Sie im angezeigten Formular die Registerkarte **Integration Setup** (Integrationseinrichtung) aus und füllen Sie die folgenden Felder aus:

**Registerkarte „Integrationseinrichtung“ für den Integrationstyp „InsightVM“.**

| Feld | Beschreibung |
|---|---|
| InsightVM-Region | Die Server-URL, die Sie von der Website Rapid7 abgerufen haben. |
| API-Schlüssel | Der API-Schlüssel, den Sie von Ihrem Rapid7 Insight-Konto erhalten haben. |
| Validierungsstatus | Nur Lesen: Status des Validierungsprozesses für Anmeldeinformationen. |

   b. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.

   c. Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

   d. Klicken Sie auf die Registerkarte **Importkonfiguration**.

   Füllen Sie die Felder des angezeigten Formulars aus.

**Registerkarte „Importkonfiguration“ für InsightVM**

| Feld | Beschreibung |
|---|---|
| CVSS-Mindestpunktzahl | Minimale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird. |
| Max. CVSS-Punktzahl | Maximale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird. |
| Standortfilter | Begrenzt die Daten auf die Rapid7 InsightVM Sites, die in der Sites-Liste ausgewählt wurden. Weitere Informationen finden Sie unter Filtern nach Rapid7 Sites. Sie können mehr als einen Standort auswählen. Standardmäßig (leer) werden alle Sites einbezogen. Um die Sites-Liste vorab auszufüllen, führen Sie die Rapid7 Site Integration - API aus, bevor Sie dieses Feld festlegen.<br><br>Weitere Informationen zur Verwendung der Websitefilterung finden Sie unter Filtern nach Rapid7 Sites. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| CVE-Eintrag automatisch erstellen | Die Systemeigenschaft zum Erstellen eines CVE-Eintrags ist standardmäßig aktiv (wahr). CVE-Platzhalter werden automatisch mit der Rapid7-Wissenserfassung erstellt, wenn die CVE-ID nicht vorhanden ist.<br><br>Wenn diese Funktion deaktiviert werden soll, deaktivieren Sie die Eigenschaft [sn_vul_r7.create_cve_for_vulnerabilities] in der Liste „Systemeigenschaften“. |
| Gelöste nach Alter erneut öffnen | Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die sie gelöst, aber nicht geschlossen haben, mit dem im Feld **Reopen resolve after (Aufgelöste Elemente erneut öffnen nach) übereinstimmen**. |

**e.** Klicken Sie auf **Speichern**.

Für mehrere Bereitstellungen des Integrationstyps Rapid7 InsightVM :

**f.** Öffnen Sie im Feld **Integrationsinstanz** das Suchsymbol der , und wählen Sie eine vorhandene Integrationsinstanz aus, oder klicken Sie im Popup-Menü auf **Neu**.

**g.** Geben Sie für **Neu**einen **Namen** für die Integrationsinstanz ein, und klicken Sie auf **Absenden**.
Der Integrationstyp wird im Konfigurationsformular Rapid7 angezeigt.

**Hinweis:**
Sie können jede Integrationsinstanz mit Ausnahme der Standardinstanz löschen. Durch das Löschen einer Instanz wird Folgendes gelöscht (mit Ausnahme von VIs):

- Integrationen
- Instanzparameter
- Integrationsausführungen
- Integrationsprozesse
- Instanzspalte im VI ist als leer markiert

**h.** Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken.

**i.** Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

**4.** Erweitern Sie im Feld Integrationstyp die Liste, und klicken Sie auf **Data Warehouse**.

**a.** Wechseln Sie zur Registerkarte **Integration Setup** (Integrationseinrichtung).

Füllen Sie die Felder des angezeigten Formulars aus.

**Registerkarte „Integrationseinrichtung“ für den Data Warehouse-Integrationstyp**

| Feld | Beschreibung |
|---|---|
| JDBC-Anmeldeinformationsname | Name Ihrer Data Warehouse-Anmeldeinformationen. |
| Benutzernamen | Rapid7 Data Warehouse-Benutzername. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Passwort | Rapid7 Data Warehouse-Passwort. |
| Validierungsstatus | Nur Lesen: Status des Validierungsprozesses für Anmeldeinformationen. |
| Validierungsdetail | Nur Lesen: Nur Data Warehouse. Zeigt zusätzliche Informationen zur Validierungsprüfung an, nachdem Sie mindestens einmal auf Anmeldeinformationen testen geklickt haben. Dies kann beim Debuggen Ihres Setups nützlich sein (z. B. beim Validieren, ob Ihr MID-Server falsch konfiguriert ist oder ob Sie einfach die falschen Anmeldeinformationen haben). |
| DNS/IP des Datenbankservers | DNS- oder IP-Adresse für Ihr Data Warehouse. |
| Datenbankanschluss | Port für Ihre Data Warehouse-Integration. |
| Datenbankname | Name des Data Warehouse. |
| Offset der Datenverzögerung (in Tagen) | Der Datenverzögerungs-Offset berücksichtigt die Verzögerung zwischen den Echtzeitdaten im Scanner Rapid7 Nexpose und den Daten im Data Warehouse. |
| MID-Server | Zu verwendender MID-Server. Es werden nur eigenständige MID-Server unterstützt. Geclusterete MID-Server werden nicht unterstützt. |
| Timeout für MID-Server (Min.) | Anzahl der Minuten, die auf die Antwort des MID-Servers gewartet werden soll, bevor die Integrationsausführung abgebrochen wird. |

**b.** Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken.

**c.** Klicken Sie nach einem erfolgreichen Test auf **Speichern**.

**d.** Klicken Sie auf die Registerkarte **Importkonfiguration**.

Füllen Sie die Felder des angezeigten Formulars aus.

### Registerkarte „Importkonfiguration“ für Data Warehouse

| Feld | Beschreibung |
|---|---|
| Vor v12.0: Kontrollkästchen CVE-Eintrag erstellen | Wenn diese Option aktiviert ist, werden Platzhalter für CVEs, die noch nicht vorhanden sind, als NVD-Datensätze erstellt und im Drittparteieintrag für Rapid7 referenziert. Wenn diese Option deaktiviert ist, werden diese CVEs ignoriert. |
| CVSS-Mindestpunktzahl | Minimale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird. |
| Max. CVSS-Punktzahl | Maximale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird. |
| Standortfilter | Begrenzt die importierten Sites Integration-Daten auf die ausgewählten Sites. Sie können mehrere auswählen.<br>**Hinweis:**<br>Da die Standardeinstellung darin besteht, Daten von allen Sites zu importieren, müssen Sie den Filter nicht verwenden, wenn Sie alle Sites anzeigen möchten. Dadurch wird die Anforderung verlangsamt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Gelöste nach Alter erneut öffnen | Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die sie gelöst, aber nicht geschlossen haben, mit dem im Feld **Reopen resolve after (Aufgelöste Elemente erneut öffnen nach) übereinstimmen**. |

5. Klicken Sie auf **Speichern**.
6. **Wahlweise:** Wenn Sie ein Startdatum in den Integrationsdatensätzen der Rapid7 Vulnerability Integration - API und der Rapid7 Vulnerable Item Integration - API-Integration festlegen möchten, um Verlaufsdaten während des ersten Imports aus dem Rapid7 -Scan abzurufen, führen Sie die folgenden Schritte aus.
   Sie können diese Daten für Veraltete Erkennungen in werden geschlossen Vulnerability Responseverwenden.

   a. Navigieren zu **Rapid7 Vulnerability Integration** > **Administration** > **Integrationen**.
   Die Liste Rapid7 Integrations (Integrationen) wird angezeigt.

   b. Klicken Sie auf einen der Integrationsdatensätze, um ihn zu öffnen.

   (Optional) Klicken Sie oben im Formular auf den Link **hier**, um den Datensatz zu bearbeiten.

   Das Feld **Importieren seit** Datum in den Rapid7 -Integrationen ist standardmäßig leer, mit Ausnahme der Rapid7 Vulnerability-Integration – API und der Rapid7-Integration von angreifbaren Elementen – API. Für diese Integrationen werden diese Felder auf 1998-12-31 oder 1999-01-01 festgelegt.

   Um Verlaufsdaten während des ersten Imports aus dem Scan Rapid7 abzurufen, legen Sie in den entsprechenden Integrationsdatensätzen ein Startdatum fest. Dieser Prozess funktioniert für jede Rapid7 -Integration mit den folgenden Ausnahmen:

   - Für die Integrationen von Rapid7 Exploit und Malware Kit wird das Feld „ **Importieren seit** “ nicht angezeigt, da sie keine Delta-Updates durchführen und daher dieses Feld nicht verwenden.
   - Die Rapid7 Asset-Listen-Integration ignoriert das Feld, da alle Daten abgerufen werden sollen.
   - Für die erste Ausführung der Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API, wenn das Modul „Veraltete angreifbare Elemente automatisch schließen“ aktiviert und das Feld „ **Importieren seit** “ leer gelassen wird.

     Wenn Sie die Funktion zum automatischen Schließen aktivieren, ist eine erfolgreiche Ausführung von Rapid7 Comprehensive Vulnerable Item Integration oder Rapid7 Comprehensive Vulnerable Item Integration – API erforderlich. Diese Integrationen sind standardmäßig deaktiviert.

     Wenn Sie Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API aktivieren und das Feld **Importieren seit** auf der Integrationskonfigurationsseite leer lassen, wird der Wert im Feld vor **Tagen** des Formulars „Veraltete angreifbare Elemente automatisch schließen“ auch für **Importieren seit** verwendet Datum der ersten Integrationsausführung. Der Standardwert für Veraltete angreifbare Elemente automatisch schließen ist (90 Tage).

     Beispiel: Wenn das Feld „ **vor Tagen** “ im Formular „Veraltete angreifbare Elemente automatisch schließen“ 90 ist und das Feld „ **Importieren seit** “ auf der Konfigurationsseite „Rapid7 Comprehensive Vulnerable Item Integration – API“ leer



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ist, werden bei der ersten Integrationsausführung die Daten für die letzten 90 Tage importiert Tage.

Diese Beziehung zwischen den Feldern „ **Importieren seit“** und **„Vor Tagen“** gilt nur für die erste Integrationsausführung. Danach wirkt sich eine Änderung des Felds „ **Vor Tagen** “ im Formular „Veraltete angreifbare Elemente automatisch schließen“ nicht auf das Feld **Importieren seit** auf der Konfigurationsseite „Rapid7 Comprehensive Vulnerable Item Integration“ (Integration von Rapid7 Comprehensive Vulnerable Item Integration – API) aus. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass bei nachfolgenden Integrationsausführungen nur die Delta-Informationen importiert werden

Das Feld **Importieren seit** kann bearbeitet werden, und Sie können für jede der Integrationen beliebige Werte eingeben.

7. Navigieren zu **Alle** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

   a. Der Parameter der Integrationsinstanz **import_starttime_buffer_comprehensive** legt eine Pufferzeit von 24 Stunden vor der im Feld **Importieren seit** angegebenen Zeit fest, sodass die Assets, die aus dieser Pufferzeit gescannt werden, während der Integration von **Rapid7 Comprehensive Vulnerable Item Integration – API** abgerufen werden.
   Sie können diese Pufferzeit Ihren Anforderungen entsprechend ändern.

   b. **Wahlweise:** Legen Sie den Parameter **close_stale_detections** auf *true* fest, um die veralteten Erkennungen zu schließen, die nicht mehr über die Rapid7-API für die Assets eingehen, die gescannt und über die Rapid7-API über die **Rapid7 Comprehensive Vulnerable Item Integration - API**abgerufen werden.

Sie haben die Setup-, Installations- und Konfigurationsschritte für Rapid7 Vulnerability Integrationerfolgreich abgeschlossen. Sie sind jetzt bereit, importierte Daten zu überprüfen und zu verifizieren.

### Nächste Maßnahme

Die Scanner Rapid7 und Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

So aktivieren Sie diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erstellen oder Verfeinern Ihrer Suchregeln vor dem Import finden Sie unter Erstellen Sie eine Vulnerability Response-CI-Suchregel.

### Filtern nach Rapid7 Sites

Filtern Sie nach Site für Rapid7 InsightVM Integrationstypen sowie Rapid7 Nexpose Data Warehouse-Integrationstypen.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Hinweis:**
Die Verwendung der Website-Filterung kann Auswirkungen auf die Leistung haben. Informationen zur Leistung und zu anderen Aspekten vor der Verwendung der Standortfilterung finden Sie unter KB0789221 .

## Warum und wann dieser Vorgang ausgeführt wird

## Prozedur

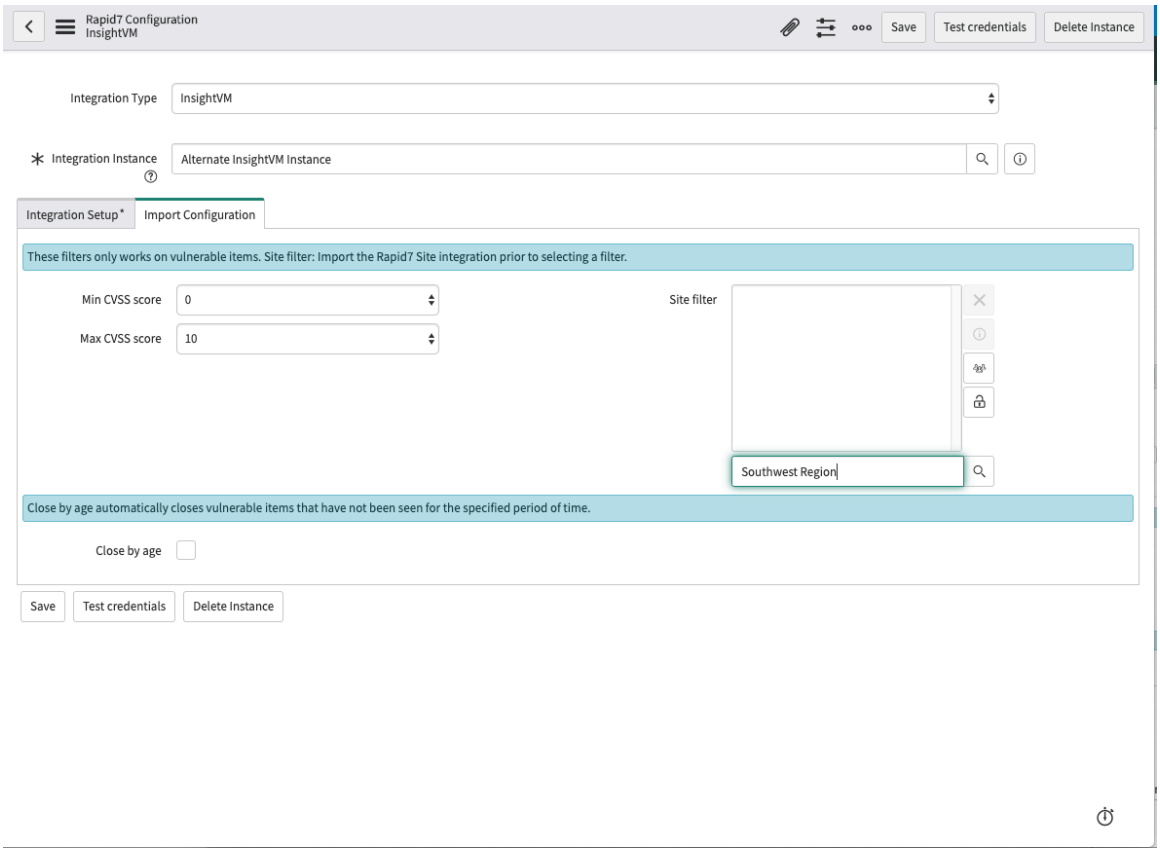
1. Navigieren zu **Alle** > **Rapid7 Vulnerability Integration** > **Konfiguration**.
2. Wählen Sie eine Integrationsinstanz aus.
3. Klicken Sie auf die Registerkarte **Konfiguration** importieren.

   **Hinweis:**
   Wenn Sie alle Sites anzeigen möchten, lassen Sie das Site-Filterfeld leer. Kein Site-Filter ist gleichbedeutend mit dem Hinzufügen aller Sites.

   Sites sind spezifisch für Integrationsinstanzen. In der Nachschlageliste für die Standortfilterung werden die Instanzstandorte Rapid7 InsightVM und Rapid7 Nexpose der Data Warehouse-Integration angezeigt. Stellen Sie sicher, dass die ausgewählte Site mit der ausgewählten Integrationsinstanz übereinstimmt. Wenn Sie beispielsweise versehentlich eine Data Warehouse-Site auswählen, funktioniert diese Site nicht für die Site-Filterung nach Rapid7 InsightVM.
4. Klicken Sie auf die Nachschlageliste, um die Site-Datensätze für die aktuelle Integrationsinstanz anzuzeigen.
5. Fügen Sie eine Site aus der Liste hinzu, um sie dem Site-Filter hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Wiederholen Sie die Auswahl, um weitere Sites hinzuzufügen.
7. Klicken Sie auf **Speichern**.
   Diese Sites werden verwendet, um beim nächsten Import nach Site zu filtern. Informationen zum Hinzufügen des Präfix SITE zu Ihren Site-Daten finden Sie unter Stellen Sie SITE Ihren Rapid7 InsightVM-Website-Tags voran.

### Stellen Sie SITE Ihren Rapid7 InsightVM-Website-Tags voran

Fügen Sie das Präfix SITE zu Ihren Rapid7 InsightVM -Website-Tags hinzu, um sie in Ihrer Tag-Liste hervorzuheben.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

**Hinweis:**
Wechseln Sie bei Bedarf Ihren Bereich zu Rapid7 Integration for Security Operations.

#### Prozedur

1. Geben Sie im linken Navigationsfeld Folgendes ein: `sys_properties.list`.
2. Suchen Sie unter **Name**nach: `sn_vul_r7.prefix_site_to_rapid7_tags`.
3. Öffnen Sie `sn_vul_r7.prefix_site_to_rapid7_tags`.
4. Ändern Sie den **Wert** in **true**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Neue und vorhandene Website-Tags werden beim nächsten Import von Rapid7 InsightVMmit dem Präfix versehen.

### Deduplizieren Sie Rapid7 Vulnerability Integration Data Warehouse-Datensätze

Wenn Sie vom Integrationstyp **Data Warehouse** zum Integrationstyp **InsightVM** migrieren, können Sie vorhandene angreifbare Data Warehouse-Elemente deduplizieren, solange sie zu denselben Quelldaten wie Ihre Rapid7 InsightVM -Daten gehören.

#### Vorbereitungen

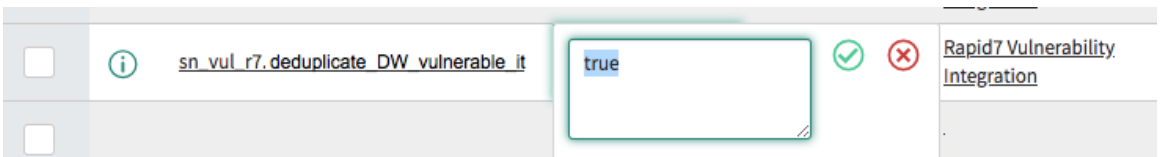
Erforderliche Rolle: sn_vul_r7.admin oder, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Diese Deduplizierung funktioniert nur bei der Migration von Rapid7 Nexpose Data Warehouse zur Integration von Rapid7 InsightVM angreifbaren Elementen.

#### Prozedur

1. Navigieren zu **Alle** > **Rapid 7** > **Integrationen**.
2. Legen Sie alle **aktiven** Spalteneinstellungen für Data Warehouse-Integrationen von Rapid7 Nexpose auf **False**fest, wodurch die Integrationen deaktiviert werden.
3. Geben Sie im linken Navigationsbereich sys_properties.list ein.
4. Suchen Sie nach dem **Namen**: sn_vul_r7.deduplizieren_DW_vulnerable_item.
5. Ändern Sie das Feld **Wert** in **True**.




6. Klicken Sie auf das grüne Häkchensymbol .
   Beim nächsten Rapid7 InsightVM Import der Integration angreifbarer Elemente verhindert eine Übereinstimmung mit vorhandenen Data Warehouse-Datensätzen, dass ein doppeltes angreifbares Element erstellt wird.

### Rapid7 Vulnerability Integration Ausführungsstatusdiagramm

Sensoren vonRapid7 Nexpose erfassen die Daten und senden sie automatisch an die Produkte von Rapid7 Nexpose oder Rapid7 InsightVM, die die Informationen kontinuierlich analysieren und korrelieren.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

Rapid7 Vulnerability Integration arbeitet problemlos mit Vulnerability Response zusammen, um Schwachstellen in CIs und Business Services zuzuordnen, um die Auswirkungen und Prioritäten potenziell böswilliger Bedrohungen zu bestimmen. Das Modul Rapid7 Vulnerability Integration „ Ausführungsstatus“ ist eine grafische Ansicht des Status von Rapid7 Vulnerability Integration -Ausführungen.

Um diese Daten in der veralteten Ansicht anzuzeigen, navigieren Sie zu **Alle** > **Integration aller Rapid7-Schwachstellen** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

## Vorherige Versionen von Vulnerability Response

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei neue Diagramme wurden hinzugefügt, um die Leistungsmetriken zu vergleichen:

- Rapid7 Leistungsmetriken der Erfassung angreifbarer Elemente: Vergleichen Sie die täglichen Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen zu ermitteln.
- Rapid7 Leistungsdurchsatz der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Durchsatz bei der Erfassung angreifbarer Elemente für die Rapid7 Integration angreifbarer Elemente – API. Der Durchsatz wird in Elementen pro Stunde gemessen.

**Hinweis:**
In Rapid7werden diese Diagramme nur für die Insight VM-Integration unterstützt.

### Ausführungsstatus der Rapid7-Integration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Beispiel für Rapid7 Vulnerability Integration Ausführungsstatusdiagramm

- Der Wert in der Spalte „Importierte Elemente“ stellt die Gesamtzahl der angreifbaren Elemente dar, die aus einer Integrationsausführung erstellt werden.
- Die Spalte Neue Elemente zeigt die Anzahl der angreifbaren Elemente an, die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- Die Spalte Aktualisierte Elemente zeigt an, wie oft angreifbare Elemente während einer Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- In der Spalte Unveränderte Elemente werden während der Integrationsausführung gefundene angreifbare Elemente angezeigt, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

**Hinweis:**
Die Integration wird mit null Ergebnissen für alle vier der folgenden Werte ausgeführt: **„Neue CIs“**, „ **Bestehende CIs**“, „ **Neue**Elemente“ und „ **Aktualisierte** Elemente“ werden aus der Liste der **Rapid7-Integrationsausführungen** herausgefiltert.

### Rapid7 Vulnerability Integration Statusdiagrammberichte ausführen

| Name | Beschreibung |
|---|---|
| Ergebnisse der letzten 30 Tage Rapid7 . | Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Führen Sie in einer visuellen Leiste aus. |
| Letzte 30 Tage Rapid7 Neue AEs | Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Aktualisierte AEs der letzten 30 Tage Rapid7 . | Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Duplikate der letzten 30 Tage Rapid7 . | Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Rapid7 Integrationsausführungen | Die Datensätze der Integrationsausführung werden in einer Liste angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Rapid7 Vulnerability Integration Statusdiagrammberichte ausführen (Fortsetzung)**

| Name | Beschreibung |
|---|---|
| | **Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br><br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |
| Angreifbares Element – Erfassungsleistungsmetriken der letzten 30 Tage Rapid7 . | Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage. |
| Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Rapid7 . | Täglicher Durchsatz bei der Erfassung angreifbarer Elemente für die Rapid7 Integration angreifbarer Elemente – API, gemessen für die letzten 30 Tage. |

## Zeigen Sie das Status-Dashboard für Importausführungen Rapid7 Vulnerability Integration an

Verwenden Sie das Rapid7 Schwachstellen-Importausführungsstatus-Dashboard, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu treffen.

### Vorbereitungen

Erforderliche Rolle: sn_vuln.admin

### Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren geht von den folgenden Annahmen aus.

- Sie haben Vulnerability Response und Rapid7 Vulnerability Integration installiert und konfiguriert.
- Rapid7 Vulnerability Integration Importe sind geplant und werden ausgeführt.
- Rapid7 Statusdiagramme der Integrationsausführung werden verwendet.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 19.0 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Rapid7** > **Status der Integrationsausführung**.

   Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

   **Hinweis:**
   Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

2. Wenn Sie das Statusdiagramm der Integrationsausführung Rapid7 nicht verwenden, navigieren Sie zu **Rapid7** > **Integrationen**.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf die zugehörige Liste Ausführungen der **Schwachstellenintegration**.
3. Vergewissern Sie sich, dass alle Importe erfolgreich waren.

   **Trouble?**

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung:
   - Netzwerkunterbrechung
   - Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt

   Klicken Sie für alle diese Bedingungen auf **Jetzt** ausführen, und führen Sie die Integration erneut aus.

## Initiieren Sie einen erneuten Scan für die Rapid7 Schwachstellenintegration

Initiieren Sie erneute Scans auf der Rapid7 -Plattform, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen geplanten Scan-Zyklen korrigiert wurden.

### Vorbereitungen

**Hinweis:**
Erneute Scans für Rapid7 angreifbare Data Warehouse-Elemente werden nicht unterstützt.

Sie können erneute Scans über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.

Erforderliche Rollen: Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Informationen zum erneuten Scannen in der klassischen Umgebung finden Sie in den folgenden Abschnitten.

Erneute Scans werden unterstützt. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente initiieren, die aus Rapid7 InsightVM -Integrationen aus Ihrer Now Platform® -Instanz importiert wurden.

**Hinweis:**
Der Scanner Rapid7 ist in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die die Anwendung Rapid7 als Quelle haben, ist die Schaltfläche Erneut scannen nicht verfügbar.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans von angreifbaren Elementen (AEs), Korrekturaufgaben (RTs), Drittanbietereinträgen (TPE) oder Datensätzen erkannter Elemente aus Ihrer Now Platform® -Instanz initiieren.

Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Beispiel: Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde, erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformRapid7 auf angreifbare Elemente von [] initiieren. Sie können aktualisierte Ergebnisse für Ihre angreifbaren Elemente beim nächsten geplanten Import von Rapid7 InsightVM Schwachstelle und Integrationen angreifbarer Elemente anzeigen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

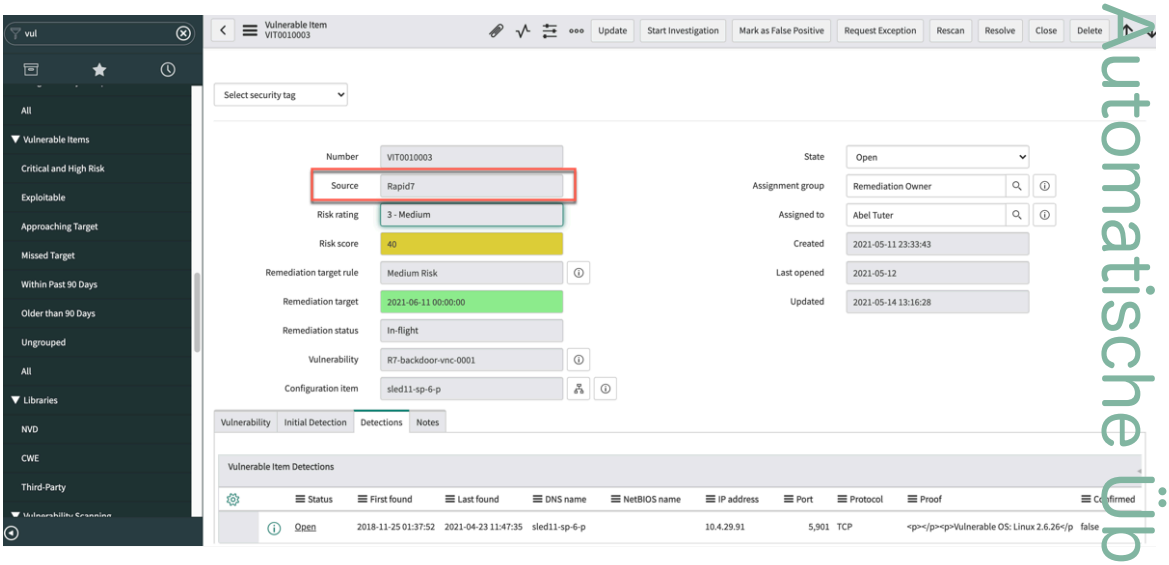


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Initiieren Sie erneute Scans für AEs mit Rapid7 als Quelle. Vergewissern Sie sich, dass Rapid7 in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte **Quelle** in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf das Zahnradsymbol, und verschieben Sie **Quelle** von **Verfügbar** zu **Ausgewählt**.

Wenn Sie erneute Scans initiieren, vermeiden Sie es, gleichzeitig Scans für eine Quell-ID aus mehreren Quellen auszulösen. Die letzte Scan-Anforderung weist einen Fehler auf.

Wenn Sie beispielsweise einen erneuten Scan für einen VI aus einem VI-Datensatz initiieren und einen weiteren erneuten Scan aus einem Korrekturaufgaben-Datensatz anfordern, der denselben VI enthält, schlägt die zweite Anforderung wahrscheinlich fehl.




3. Navigieren Sie alternativ zu **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen AE-Datensatz muss der AE aus dem Produkt Rapid7 stammen und sich in einem anderen Status als „Geschlossen“ befinden. Bei mehreren VI-Datensätzen müssen alle VIs, die Sie in der Listenansicht auswählen, aus dem Produkt Rapid7 stammen und sich in einem anderen Status als Geschlossen befinden.
   - In einem Korrekturaufgabendatensatz kann sich die Korrekturaufgabe in einem anderen Status als „Geschlossen“ befinden, und alle zugehörigen AEs müssen aus dem Produkt Rapid7 stammen.
   - In einem TPE-Datensatz (Third Party Entry) muss dem Datensatz mindestens ein zugeordneter VI-Datensatz aus dem Produkt Rapid7 in einem anderen Status als „Geschlossen“ zugeordnet sein.
   - In einem Datensatz eines erkannten Elements muss der VI aus dem Produkt Rapid7 stammen und sich in einem anderen Status als **Geschlossen**befinden.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie für Listenansichten die AEs aus der Liste aus, die Sie erneut scannen möchten, und wählen Sie in der Liste **Aktion für ausgewählte Zeilen** die **Option Erneut scannen aus**.

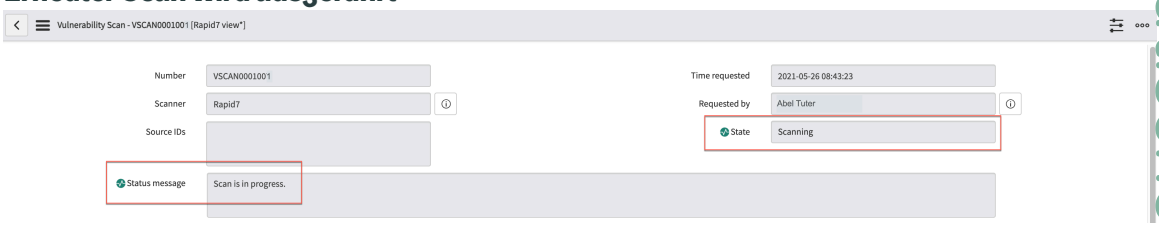
5. Bestätigen Sie im angezeigten Popup den erneuten Scan.
   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird (In der**Warteschlange**). Klicken Sie in der Nachricht auf den Link **Details** anzeigen, um den Status des erneuten Scans (untergeordneter Scan) zu überprüfen und alle anderen aus dem Datensatz gestarteten erneuten Scans anzuzeigen. Der Status für alle erneuten Scans kann jederzeit unter der zugehörigen Liste „Scans“ am unteren Rand der Datensätze für VI, Korrekturaufgabe, TPE und erkannte Elemente gefunden werden, die Sie zum Starten der erneuten Scans verwenden.

Wenn der Scanvorgang läuft, ändert sich das Feld Status in Scanning ( **Scanning**), und im Feld Statusmeldung wird **Scan is in progress**(Scan wird ausgeführt) angezeigt.

**Hinweis:**
Jeder erneute Scan unterstützt 500 Assets pro Scan. Wenn Ihre Anforderung mehr als 500 Assets umfasst, werden weitere untergeordnete Scans angefordert.

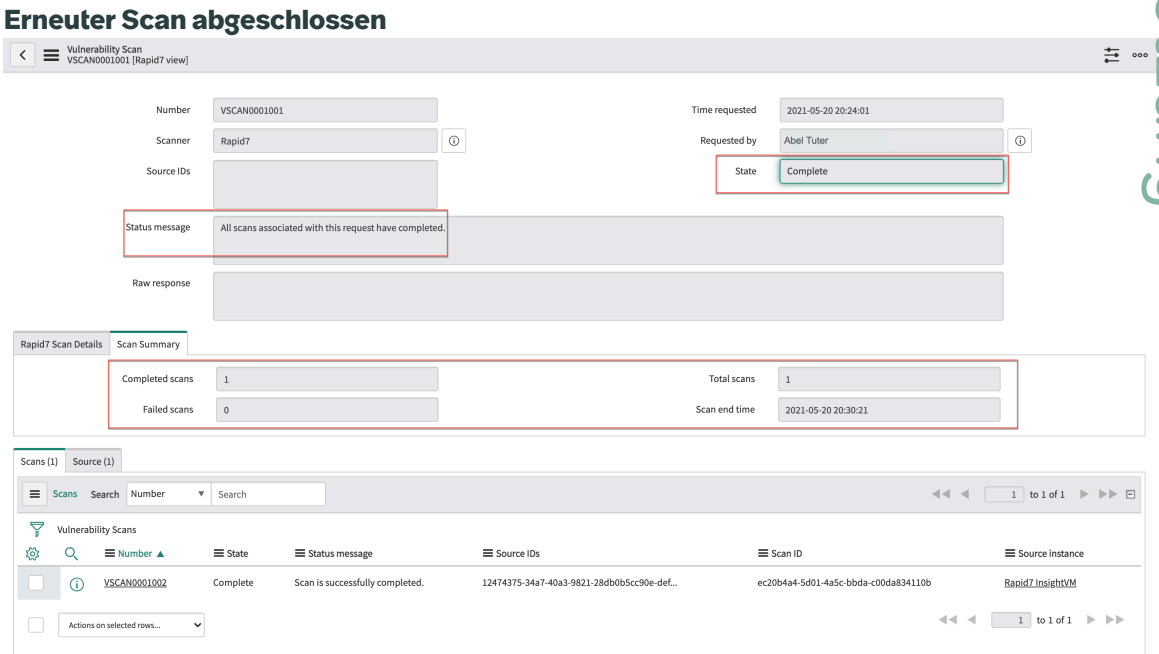
Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt.

**Erneuter Scan wird ausgeführt**




Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens. Alle AEs, die in den Status „Geschlossen/Korrigiert“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Rapid7 -Integrationen importiert.

**Erneuter Scan abgeschlossen**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

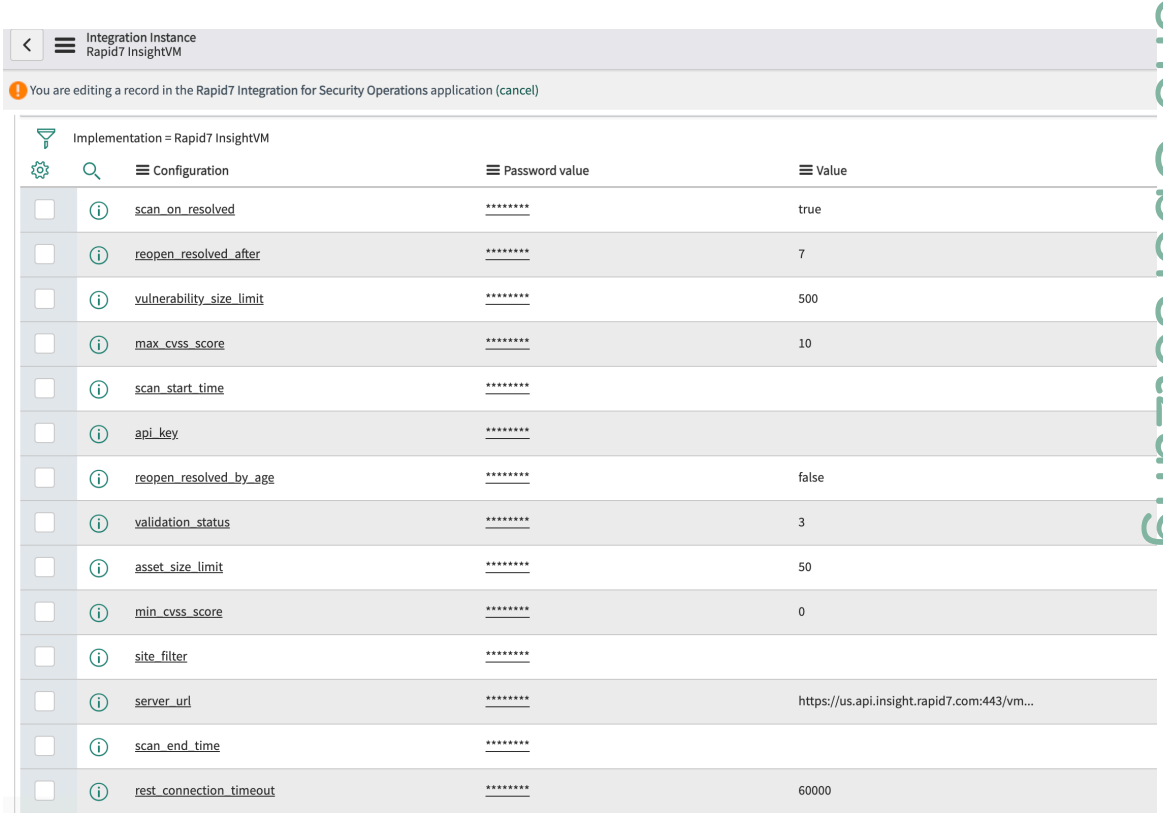
Alternativ können Sie bei Bedarf einen erneuten Scan für eine bestimmte Schwachstelle in einem bestimmten Asset initiieren. Sie können die Ergebnisse dieser Scans anzeigen, sobald der Scan für die aktualisierten AE-, Korrekturaufgaben-, TPE- und erkannten Elementdatensätze abgeschlossen ist, von denen aus Sie den Scan gestartet haben.

Der Wert des Felds Status in Datensätzen von Schwachstellen Scan wird aus Rapid7importiert. Wenn der Scan erfolgreich abgeschlossen wurde, wird der Status auf Abgeschlossen gesetzt. Wenn der Scan nicht erfolgreich abgeschlossen wird, wird ein Fehlerwert angezeigt.

**Automatische Scans und geplante Scans**

Als Schwachstellenmanager oder Analyst können Sie angeben und planen, wann erneute Scans für VIs und RTs initiiert werden. Sie können auch automatische Scans für VIs und Korrekturaufgaben aktivieren, die auf „Auflösen“ festgelegt sind.

6. Um die Integrationsparameter für die Integrationsinstanz zu ändern, navigieren Sie zu **Rapid7 Vulnerability Integration** > **Administration** > **Konfiguration**.
7. Wenn diese Option im Rapid7-Konfigurationsdatensatz in der Liste „ **Integrationstyp** “ nicht ausgewählt ist, wählen **Sie Rapid7 InsightVM aus**.
8. Klicken Sie rechts neben dem Feld **Integrationsinstanz** auf das Informationssymbol, gefolgt von **Datensatz öffnen**.
9. Suchen Sie im Datensatz der Integrationsinstanz Rapid7 InsightVM nach den Parametern für die Planung von Scans, und bearbeiten Sie sie nach Bedarf.




*scan_on_resolved* gibt an, ob der Scan initiiert wird, wenn eine Schwachstelle behoben wird. Der Standardwert ist „ **false** “ (deaktiviert).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn dieser Parameter auf „ true“ festgelegt ist und ein VI oder eine RT auf „Gelöst“ festgelegt wird, wird der Workflow zum erneuten Scannen des entsprechenden VI und der Korrekturaufgabe automatisch ausgelöst.

**scan_start_time**

Legen Sie die Scan-Startzeit in **HH:mm** (24-Stunden-Format) in der UTC-Zeitzone für die Startzeit des Fensters fest, in dem erneute Scans verfügbar sein sollen.

Der Standardwert ist 00:00.

**scan_end_time**

Legen Sie die Scan-Endzeit in **HH:mm** (24-Stunden-Format) in der UTC-Zeitzone für die Endzeit des verfügbaren Scan-Fensters fest.

Der Standardwert ist 23:59.

Wenn ein Scan innerhalb des geplanten Zeitfensters initiiert wird, wird er sofort gestartet. Wenn der Scan außerhalb des Fensters initiiert wird, wird er für das nächste geplante Fenster in die Warteschlange gestellt.

Wenn Sie beispielsweise eine Startzeit von 00:00 für den Parameter *scan_start_time* und eine *scan_end_time* von 10:00 Uhr desselben Morgens eingeben, werden Scans, die außerhalb des Zeitfensters von Mitternacht bis 10 Uhr geplant oder manuell gestartet wurden, in die Warteschlange gestellt und gestartet zur Startzeit des Zeitfensters des folgenden Tages um 00:00 Uhr.

Wenn Sie im selben Beispiel einen erneuten Scan um 11:00 Uhr manuell initiieren, wird der erneute Scan nicht sofort gestartet, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange, in diesem Beispiel 00:00.

### Legen Sie zusätzliche Filterparameter für Rapid7 InsightVM Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Integration von Rapid7 für Security Operations an, um die mit dem Produkt Rapid7 InsightVM importierten Schwachstellendaten weiter zu verfeinern.

#### Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen filtern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Beispielsweise möchten Sie möglicherweise nur importierte Schwachstellen anzeigen, die Kritisch und Schwerwiegendsind.

Um Sie beim Sammeln dieser Daten zu unterstützen, fügen Sie Parameter Rapid7 hinzu, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie ab Version 13.4 mit der Funktion Ihre HTTP-Anforderungsinformationen mit Parametern Rapid7 InsightVM in Ihrem Now Platformanpassen. Die folgenden Rapid7 InsightVM -Integrationen unterstützen die Filterung durch Hinzufügen von JSON-Inhalten im Anforderungstext:

- Rapid7 InsightVM Integrations-API für angreifbare Elemente
- Rapid7 InsightVM API für Schwachstellenintegration
- Rapid7 InsightVM

Sie sollten wissen, wie JSON Zeichenfolgen für diese Funktion verwendet werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vul.vulnerability_admin

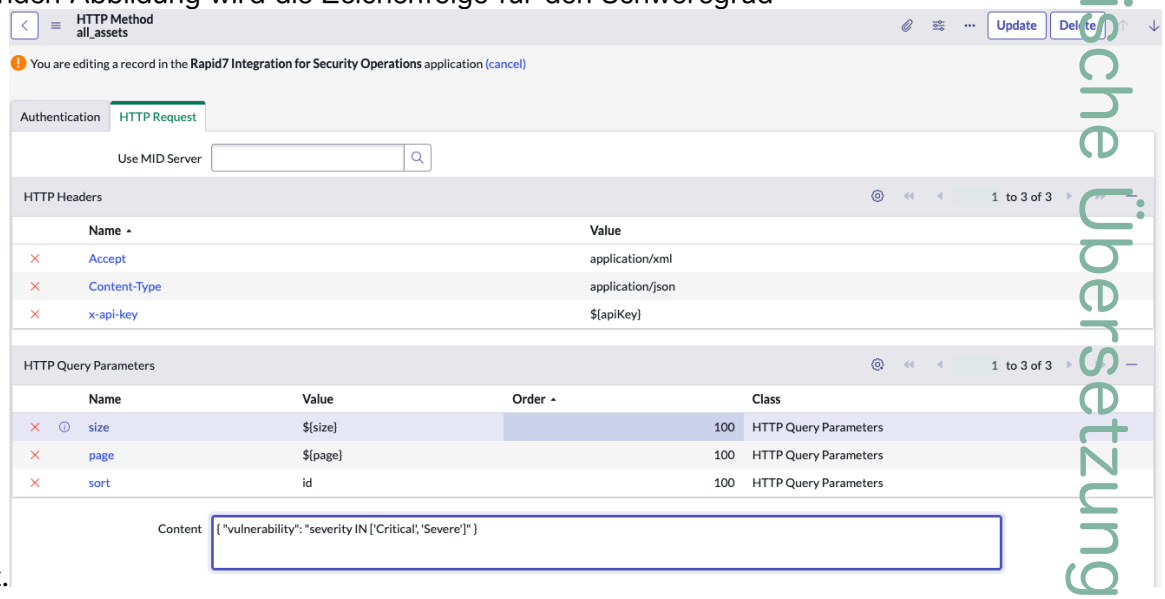
### Prozedur

1. Suchen Sie die vom Produkt Rapid7Rapid7 InsightVM unterstützten Parameter auf der Entwickler-Website von [], die Sie zum Filtern verwenden möchten.

   Sie können die Parameter für den Anforderungstext anhand der Rapid7 -Dokumentation erstellen. Parameter und Werte, die Sie aus dem Produkt Rapid7 InsightVM eingeben, werden nur auf der Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Rapid7 Vulnerability Integration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite Rapid7 Integrations (Rapid7-Integrationen) auf den Datensatz für die Rapid7 InsightVM -Integration, die Sie öffnen möchten.
4. Klicken Sie rechts auf der Seite auf das Informationssymbol (I) für die REST-Nachricht, gefolgt von **Datensatz öffnen**.
5. Klicken Sie bei ausgewählter Registerkarte HTTP-Anforderung unter HTTP-Methoden in der Spalte Name auf ein Element, um dessen HTTP-Abfrageparameter zu öffnen.
6. Geben Sie unter HTTP-Methodendatensatz unter HTTP-Abfrageparameter im Feld Inhalt die Parameterwerte ein, die Sie auf der Entwickler-Website Rapid7 gefunden haben.

   In der folgenden Abbildung wird die Zeichenfolge für den Schweregrad hinzugefügt.




   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Rapid7 weitere Informationen zum Trennen der einzelnen Werte.

7. Klicken Sie auf **Aktualisieren**.

## Die Shodan Exploit-Integration verstehen

Die Anwendung ServiceNow® Shodan Exploit Integration verwendet Daten, die aus der Suchmaschine Shodan importiert wurden, um die Auswirkungen und Prioritäten potenziell schädlicher Exploits zu bestimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Shodan Exploit Integration

Die Suchmaschine Shodan sammelt Exploit-Daten, und die Shodan-API stellt diese Datenbank Now Platform®zur Verfügung. Sie lässt sich problemlos in die Anwendung ServiceNow® Vulnerability Response integrieren, um Schwachstellen von Drittparteien Exploits zuzuordnen und die Exploit-Daten in Ihrer Instanz anzureichern.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Regelmäßige Aufgaben rufen die Integrationen jeden Tag automatisch in der Reihenfolge auf, in der sie aufgelistet sind. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

## Verfügbare Versionen

| Release-Version für Washington DC | Releasehinweise |
|---|---|
| Shodan Exploit Integration v10.6, 10.7 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Rollen

Shodan Exploit-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_shodan.admin: Benutzer mit dieser Rolle können Datensätze lesen, schreiben und löschen.
- sn_vul_shodan.user: Benutzer mit dieser Rolle können Datensätze lesen und schreiben.
- sn_vul_shodan.read: Benutzer mit dieser Rolle können Datensätze lesen.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

## Shodan-Exploit-Integrationen

Um die Exploit-Integrationen von Shodan anzuzeigen, navigieren Sie zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig aktiv.

**Shodan-Exploit-Integrationen**

| Integration | Beschreibung |
|---|---|
| Shodan ExploitDB-Integration | Ruft ExploitDB-Daten aus Shodan ab und erweitert Ihre Drittpartei-Schwachstellendaten. Diese Integration wird täglich um 03:15:00 Uhr ausgeführt. |
| Shodan Metasploit-Integration | Ruft Metasploit-Informationen aus Shodan ab und erweitert Ihre Drittpartei-Schwachstellendaten. Diese Integration wird täglich um 01:15:00 Uhr ausgeführt. |

Informationen zum Ändern der Standardstartzeit für geplante Integrationsimporte finden Sie unter Legen Sie die Importzeit für Shodan Exploit-Integration fest.

Informationen zum Anzeigen von Exploit-Daten in Schwachstellen von Drittparteien finden Sie unter Zeigen Sie Vulnerability Response Schwachstellenbibliotheken an.

Das Ändern anderer Einstellungen für die Exploit-Integration von [ Shodan erfordert fortgeschrittene Kenntnisse von ServiceNow und Vulnerability Response und geht über den Umfang der Produktdokumentation hinaus.

### Vorbereitung auf die Shodan Exploit-Integration

Eine erfolgreiche Shodan Exploit-Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Shodan Exploit-Integration setzt voraus, dass Sie mit der Suchmaschine und API von Shodan vertraut sind.

#### Vorbereitungen

Die Shodan Exploit-Integration erfordert einen API-Schlüssel. Registrieren Sie sich auf der Shodan Website, um ein kostenlose Abonnement für den Erwerb dieses Schlüssels zu erhalten.

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

- Wenn Sie keine NVD-Daten (NIST Vulnerability Database) in Vulnerability Responseimportiert haben, müssen Sie dies vor der Installation der Exploit-Integration von Shodan ] tun. Durch den Import der NVD-Daten wird sichergestellt, dass die Exploit-Datensätze automatisch mit Ihren CVE-Daten (Common Vulnerability and Exposure) gefüllt werden.

  Ohne NVD-Daten wird im Exploit-Datensatz ein Platzhalter erstellt und erst beim nächsten NVD-Update eingetragen. Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

- Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Shodan Exploit Integration für Security Operationsinstallieren und konfigurieren

Bevor Sie Shodan Exploit Integration in Ihrer Instanz ausführen können, müssen Sie sie aus dem ServiceNow Storeherunterladen und installieren. Diese Anwendung ist als separates Abonnement verfügbar.

## Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie gültige ServiceNow -Berechtigungen für die Anwendung Vulnerability Response und die Anwendung Shodan Exploit Integration für Security Operations haben. | Um Berechtigungen zu überprüfen, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Weitere Informationen zum Abrufen von Berechtigungen für eine Security Operations -Anwendung von ServiceNow Storefinden Sie unter Rufen Sie eine Berechtigung für ein Produkt oder eine Anwendung von Security Operations ab. |
| (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren. | Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. |
| Halten Sie den API-Schlüssel Shodan Exploit Integration bereit. | Weitere Informationen finden Sie unter Vorbereitung auf die Shodan Exploit-Integration. |

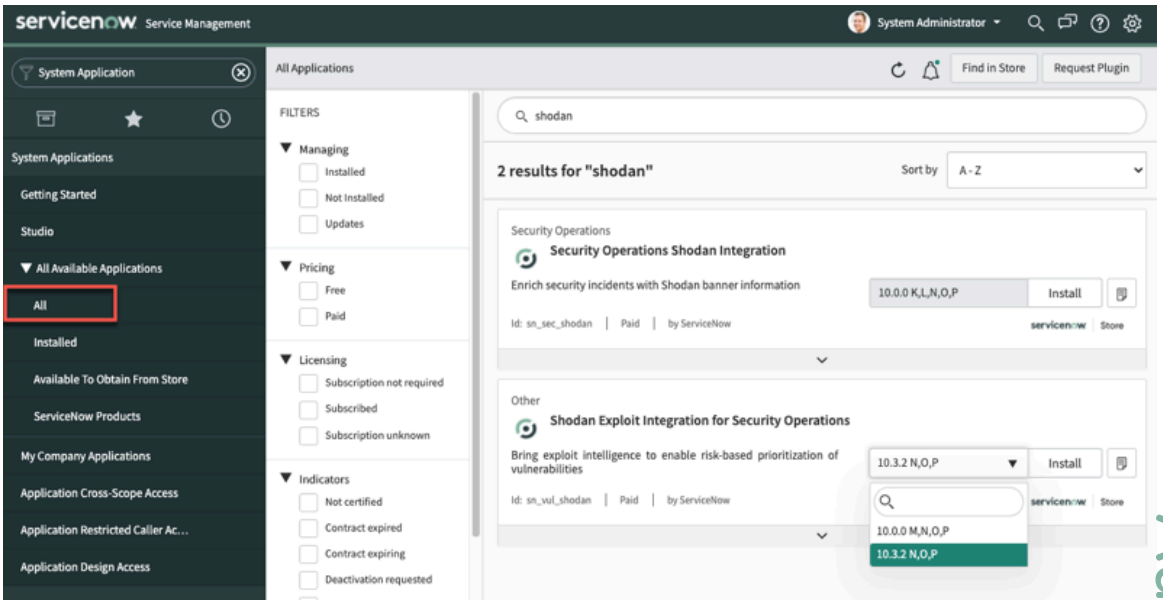
Erforderliche Rolle: admin

## Prozedur

1. Melden Sie sich bei der Instanz Now Platform an, in der Sie die Anwendung Shodan Exploit Integration installieren möchten.
2. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
3. Suchen Sie die Anwendung Shodan Exploit Integration für Security Operations, wählen Sie die gewünschte Version aus, und klicken Sie auf **Installieren**.



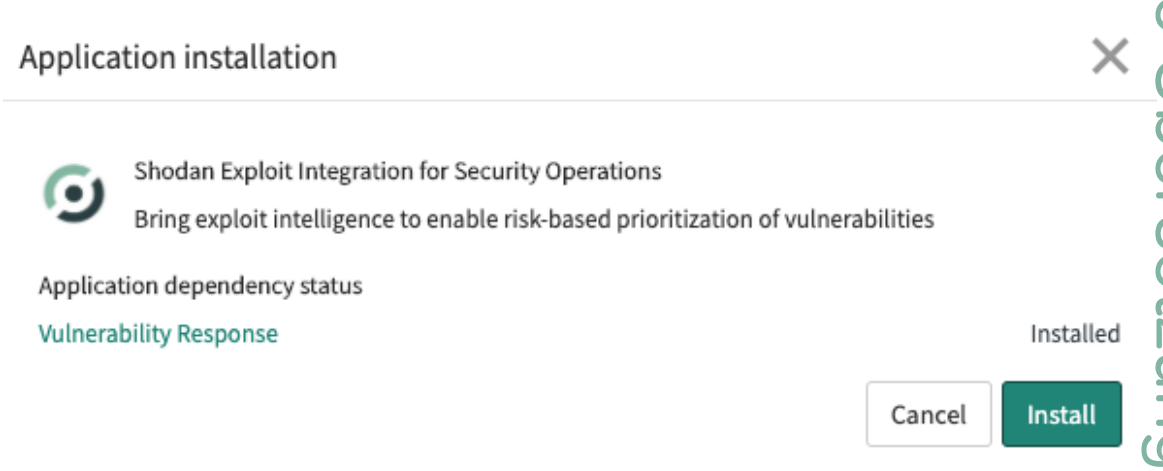
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wenn Sie Anspruch auf ein Update für diese Anwendung haben, wird die Schaltfläche **Aktualisieren** angezeigt.

Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld auf **Installieren**.

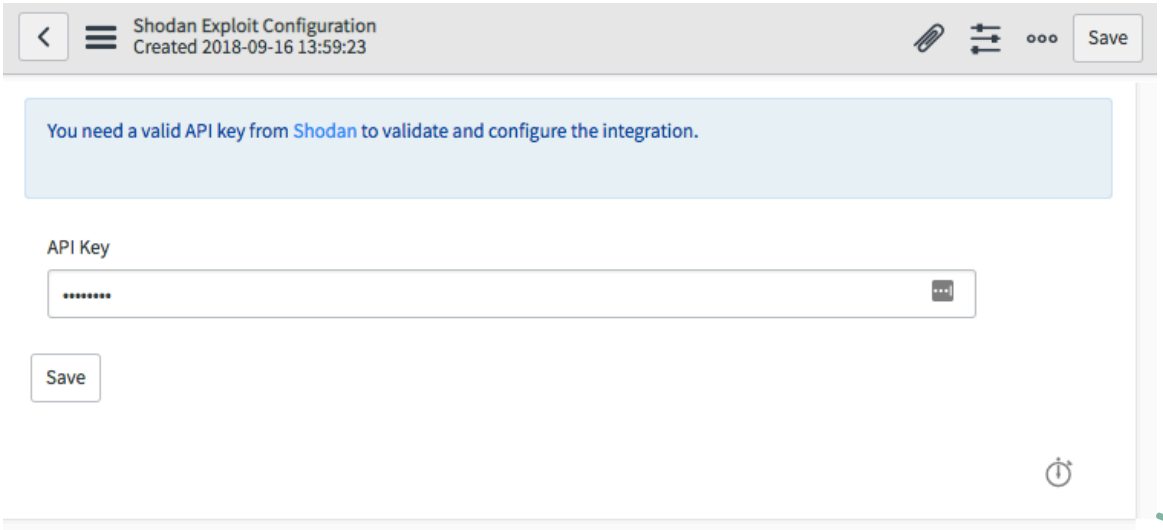



Im Dialogfeld „Installieren“ wird angezeigt, wenn die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Installationsdialogfeld.
6. Navigieren zu **Shodan Exploit Integration** > **Konfiguration**.
7. Geben Sie Ihren Shodan API-Schlüssel ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




8. Klicken Sie auf **Speichern**.
   Ihre Shodan Exploit Integration Konfiguration ist abgeschlossen.

### Legen Sie die Importzeit für Shodan Exploit-Integration fest

Sie können die Startzeit für die Exploit-Integrationen von Shodan zurücksetzen.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import übernehmen Shodan Exploit-Integrationen Delta-Daten, sofern kein vollständiger Import angefordert wird. Weitere Informationen zu vollständigen Importen finden Sie unter Führen Sie einen manuellen Shodan -Exploit-Import durch.

#### Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf den Link, um den Datensatz zu bearbeiten.
4. Legen Sie die neuen Optionen für **Ausführen** und **Zeit** fest.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für den Import des Exploits Shodan ist 03:15:00.
5. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

### Führen Sie einen manuellen Shodan -Exploit-Import durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie einen vollständigen Datenimport unabhängig von der täglichen geplanten Aufgabe durchführen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Aktivieren Sie das Kontrollkästchen **Vollständiger Datenimport**.
4. Klicken Sie auf **Jetzt ausführen**.
   Sobald der Import abgeschlossen ist, wird das Kontrollkästchen deaktiviert, und die Delta-Importe werden fortgesetzt.

## Zeigen Sie den Importausführungsstatus der Shodan Exploit-Integration an

Verwenden Sie die zugehörige Liste „Ausführungen von Schwachstellenintegrationen“, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, nach Problemen, zu suchen und Ihre Korrekturentscheidungen zu treffen.

### Vorbereitungen

So zeigen Sie den Status der Shodan-Importausführung an:

- Die Anwendung Vulnerability Response und die Shodan Exploit-Integration müssen installiert und konfiguriert sein.
- Die Importe von Shodan Exploit Integration müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: sn_vuln.admin

### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste Ausführungen der **Schwachstellenintegration**.
4. Vergewissern Sie sich, dass alle Importe erfolgreich waren.

**Trouble?**

Zu den häufigsten Ursachen für eine fehlgeschlagene Ausführung gehören:

- Netzwerkunterbrechung
- Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt

Wenn eine dieser Bedingungen auftritt, aktivieren Sie das Kontrollkästchen **Vollständiger Datenimport**, klicken Sie auf **Jetzt ausführen**, und führen Sie die Integration erneut aus.

## Die Tenable Vulnerability-Integration verstehen

Die Anwendung Vulnerability Response Integration with Tenable, die von ServiceNow Engineering für die Integration von Tenable Vulnerability entwickelt wurde, verwendet Daten, die aus den Produkten Tenable.io und Tenable.sc importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement von ServiceNow® Storeverfügbar.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die Tenable Vulnerability-Integration verwendet zwei Tenable-Integrationen, Tenable.io und Tenable.sc, um Scanner-Daten von Drittanbietern über Ihre Assets und Schwachstellen zu importieren. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.

- Tenable.io ist eine cloudbasierte Unternehmensintegration.
- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden.

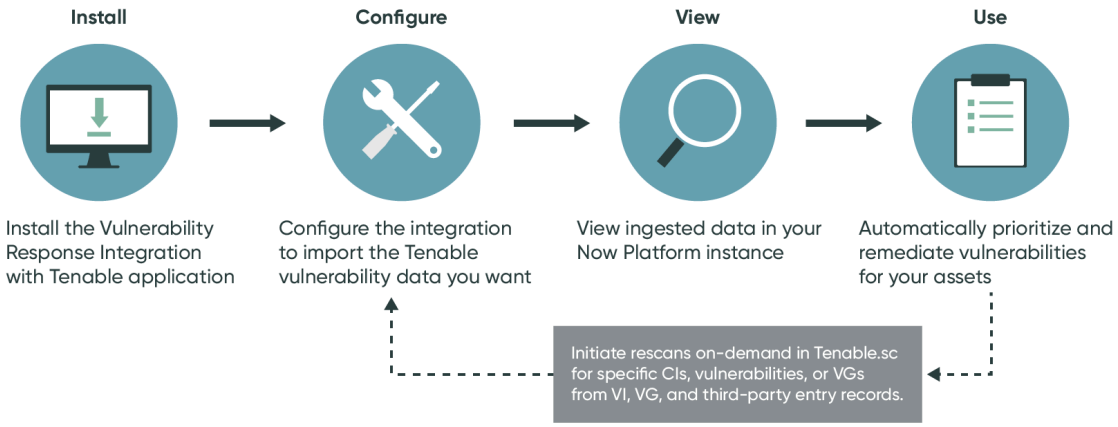
Die Anwendung Vulnerability Response Integration with Tenable ist im ServiceNow Store mit einem separaten Abonnement verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integrationfinden Sie unter Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance . und Integrationen vonTenable.sc mit der Anwendung Vulnerability Response ..

**Vertretbare Schwachstellenintegration**




## Verfügbare Versionen für Washington DC

| Release-Version | Versionsinformationen |
|---|---|
| Vulnerability Response Integration with Tenable v3.5, v3.6 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Begriffe und Hauptfunktionen der Integrationen

### Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle aus einem Scanner einer Drittpartei wird mit einem vorhandenen Asset (einem Konfigurationselement in CMDB) abgeglichen. Das Tenable-Produkt bezeichnet diese Übereinstimmungen als **Schwachstellen**.
- Eine importierte Schwachstelle von einem Drittanbieter-Scanner stimmt nicht mit einem vorhandenen Asset in Ihrem CMDBüberein. In diesem Fall wird zusammen mit einem angreifbaren Element auch ein nicht abgeglichenes CI erstellt.

  Für nicht abgeglichene CIs können Sie auch die Identification and Reconciliation Engine (IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“..

### Schwachstelleneinträge und Plugins von Drittparteien

Schwachstelleneinträge von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in Ihrer Now Platform -Instanz

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aufgelistet. Drittpartei-Schwachstelleneinträge von Tenable werden in Vulnerability Response erfasst und mit vorhandenen Assets abgeglichen, die in Ihrem CMDBaufgeführt sind. Tenable bezieht sich auf Schwachstelleneinträge von Drittparteien als **Plugins**.

**Konfigurationselement (Configuration Item, CI)**

Konfigurationselemente sind die vorhandenen Assets, die in Ihrem CMDBaufgeführt sind.

**Erkanntes Element**

Assets, die aus dem Tenable-Asset-Import erfasst wurden, werden mit vorhandenen Konfigurationselementen in CMDBabgeglichen. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse Nicht abgeglichen von CMDBerstellt. Wenn das Plugin „CMDB CI Class Models“ aktiviert ist, erstellt die Identification and Reconciliation Engine (IRE) neue CIs mit neuen Klassen. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die Datensätze der erkannten Elemente entsprechend dem Status aktualisiert. Erkannte Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

**CI-Suchregeln**

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten (Asset-Daten), um nach Übereinstimmungen in der Configuration Management Database (CMDB) zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden, um Sie bei der Korrektur zu unterstützen.

**Erneuter Scan und Korrekturscan**

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Schwachstellengruppe oder einen Drittanbietereintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Drittanbieter-Schwachstelleneinträge in Ihrer Now Platform -Instanz initiieren. Tenable bezeichnet diesen erneuten Scan als Korrektur **-Scan**.

**Ältere AEs automatisch schließen**

Mit dem Modul „Veraltete angreifbare Elemente automatisch schließen“ in Ihrem Now Platformkönnen Sie ältere, veraltete angreifbare Elemente (AEs) bereinigen, die von Ihren Drittanbieterintegrationen nicht kürzlich gefunden wurden. Wenn Sie diese AEs in den Status „ **Geschlossen** “ verschieben, können Sie die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben reduzieren und Assets in Ihrem CMDBabgleichen . Sie können alle Integrationen mit Vulnerability Response Integration with Tenable verwenden, um veraltete VIs automatisch zu schließen.

**Instanz**

Dieser Begriff bezieht sich auf ein eindeutiges Vorkommen Ihrer Now Platform® -Anwendung.

**Integration**

Eine Integration ist ein produktspezifischer Verweis auf eine Integration, z. B. die Tenable.io Assets-Integration oder die Tenable.sc Plugin-Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable Vulnerability-Integration in Ihrer Instanz gehören.

**Integrationsinstanz**

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach ihren Produkten Tenable.io und Tenable.sc aufgelistet sind.

**Bereitstellung**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff wird verwendet, um sich auf die Integrationen und Produkte in Ihrer Umgebung zu beziehen. Beispielsweise können Sie mehrere Bereitstellungen verschiedener Integrationen der Produkte Tenable.io und Tenable.sc in Ihrer Umgebung haben.

Die Integrationen Tenable.io und Tenable.sc umfassen auch die folgenden wichtigen Funktionen:

- Ergebnisse der Konfigurationsbewertung, d. h. Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit maßgeblichen Quellen, können mit dem Produkt Tenable.ioConfiguration Compliance in die Anwendung [] importiert werden. Weitere Informationen zur Funktionsweise dieser Integration mit der Anwendung Configuration Compliance ] finden Sie unter Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance . und Configuration Compliance erkunden.
- Erstellen Sie ab Version 2.1 von Tenable Vulnerability Integrationeindeutige Konfigurationselemente (CIs), die verschiedene Netzwerkpartitionsbezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufträge für alle Tenable.io - und Tenable.sc -Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben bei Bedarf auch manuell ausführen.
- Für Asset-Importe mit Tenable.iokönnen Sie Asset-Tags aktivieren, um die in Ihrem CMDB in der Tenable.io -Umgebung aufgeführten Assets zu organisieren und nachzuverfolgen.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie CI-Suchregeln konfigurieren, um zu definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Konfigurationselementen (Configuration Items, CIs) in Now Platform CMDBverwendet werden.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie Importfilter für den Import von Schwachstellen festlegen, sodass Sie nur die gewünschten Schwachstellen aus Tenable importieren. Für Tenable.iohaben Sie die Möglichkeit, mit dem Import von Schwachstellen behobene Schwachstellen aus **Tenable** zu importieren.
- Für Tenable.schaben Sie die Möglichkeit, erneute Scans bei Bedarf direkt aus Datensätzen für angreifbare Elemente, Korrekturaufgaben und Drittparteieinträgen in Ihrer Instanz Now Platform zu initiieren. Wenn AEs auf „ **Geschlossen"/** „Korrigiert" gesetzt wurden, aber in Ihrer Instanz noch nicht aktualisiert wurden, können Sie überprüfen, ob Schwachstellen in bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für die Tenable.sc -Integration.

In den folgenden Abschnitten werden weitere Details zu Tenable-Integrationen aufgeführt.

## Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

**Administrator**

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.

**sn_vul.vulnerability_admin**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und -Regeln für installierte Drittanbieterintegrationen.

**sn_vul_tenable.configure_integration**

Diese Rolle enthält die granulare Rolle „sn_vul_tenable.read_integration“. Benutzer mit dieser Rolle können die Anwendung Vulnerability Response Integration with Tenable konfigurieren.

**sn_vul_tenable.read_integration**

Benutzer mit diesen Rollen können Datensätze der Anwendung Vulnerability Response Integration with Tenable anzeigen (lesen), aber nicht bearbeiten.

**Vulnerability Response-Gruppe**

Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.

## Angreifbare Elemente

Angreifbare Elemente werden gemäß Gruppenregeln in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Vulnerability Response Übersicht über Zuweisungsregeln.

## Konfigurationselement-Suchregeln (CI).

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Die folgenden Suchregeln Tenable.io werden mit dem Basissystem geliefert.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Die folgenden Suchregeln Tenable.sc werden mit dem Basissystem geliefert.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Mehrere Werte für ip_address, mac_address, fqdns und network_interfaces werden für ein Asset verwendet. Alle Werte werden in den CI-Suchregeln für den Abgleich berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.

Weitere Informationen zum Konfigurieren der Kategorisierung nicht abgeglichener Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

## Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.iosind zwei Eigenschaften verfügbar, wenn Sie mehrere IP-Adressen oder mehrere MAC-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

**ignoreIPAddress**

Eine Liste der IP-Adressen, die für die CI-Suche und CI-Erstellung ignoriert werden sollen.

**ignoreMacAddress**

Eine Liste der MAC-Adressen, die für die CI-Suche oder CI-Erstellung ignoriert werden sollen.

## Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Integrationen von Tenable Vulnerable Items und Tenable Asset erkannt wurden.

**Hinweis:**
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente.

## Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den zu scannenden Assets zugeordnet sind. Mit dem Modul „Asset-Tags“ können Sie Asset-Tag-Daten aus Tenable.io nach Zeitplan in Ihre Instanz herunterladen. Asset-Daten, die Asset-Tags enthalten, werden aus Tenable.io abgerufen und mithilfe der Transformationszuordnungen der Tenable.io Asset Transform- Integration transformiert.

Alle Asset-Tags werden als Teil der Tenable.io Asset-Integration importiert. Asset-Tags werden im Allgemeinen zum Filtern in Vulnerability Response Zuweisungsregeln und Korrekturaufgabenregeln verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Führen Sie die Tenable.io Asset-Integration aus, bevor Sie Vulnerability Response Zuweisungsregeln oder Regeln für Korrekturaufgaben in der Anwendung Vulnerability Response erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise ein Tag erstellen, um Assets an Ihrem Standort San Diego zu beschreiben, und Sie das San Diego -Tag erstellen, können Sie nicht auch ein SAN DIEGO -Tag erstellen und in der Asset-Tag-Tabelle speichern. San Diego und SAN DIEGO werden vom System als dasselbe Asset-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das in Zukunft gespeichert und erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.import_asset_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „ true “ festgelegt. Durch das Deaktivieren von Tags werden sie in allen Now Platform® Instanzen deaktiviert.

## Datenabruffilter

Mit den Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in Ihre Now Platform® -Instanz importieren möchten. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable Vulnerability-Integration.

## Schwachstellenprioritätsbewertung (VPR)

Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable Risk-Regel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Die Aktivierung dieser Tenable Risk Calculator-Regel kann Auswirkungen auf die Leistung der Datenerfassung haben. Weitere Informationen zu Vulnerability Response -Rechnern und der Tenable-Risiko-Rechnerregel finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.

## Installation und Konfiguration

Nachdem Sie Vulnerability Response Integration with Tenable aus dem ServiceNow® Storeheruntergeladen haben, werden Installation und Konfiguration durch den Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

### Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance .

Die Tenable.io -Integrationen in der Anwendung Vulnerability Response Integration with Tenable sind in den Anwendungen Vulnerability Response und Configuration Compliance verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Liste der Tenable.io Integrationen

Mehrere Quellen werden für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in Vulnerability Responsehinzufügen und bereitstellen. Sie installieren und konfigurieren die Anwendung Vulnerability Response Integration with Tenable auch über den Setup-Assistenten.

Tenable.io ist eine cloudbasierte Unternehmensintegration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für das Produkt Tenable.io.

Tenable.io Integration von Compliance-Ergebnissen und Tenable.io Integration von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste Tenable Integrations (Vertretbare Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen können.

### Tenable.io-Integrationen

| Integration | Beschreibung |
|---|---|
| Tenable.io Assets-Integration | • Ruft alle Asset-Daten, einschließlich Asset-Tags, aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz.<br>• Ab v3.0 können Sie, wenn Tenable.io Compliance-Ergebnisse-Integration aktiviert ist, sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Asset-API.<br>• Die Ausgabe dieser Integration sind erkannte Elemente.<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br>• Ab v2.2 wird `Last Scan Time` nur für Assets mit Schwachstellen importiert und aktualisiert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| Tenable.io Integration von Compliance-Ergebnissen | • Ab v3.0 können Sie importierte sichere Konfigurationsbewertungsdaten aus der Compliance-Ergebnisintegration zusammen mit importierten Daten aus der Asset-Integration dabei unterstützen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.<br>• Wenn diese Option aktiviert ist, werden allgemeine sichere Konfigurationsbewertungsdaten abgerufen und in Ihrer Now Platform -Instanz verarbeitet. Importierte Daten umfassen Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen.<br>• Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert.<br>• Wenn ein Testergebnis importiert wird und das entsprechende Asset in Ihrer Instanz nicht abgeglichen werden kann, wird das Testergebnis ignoriert und die ID für das fehlende Asset in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_asset] gespeichert.<br>• Der Gesamtwert der ignorierten (fehlenden) Assets wird im Feld **Ignorierte CIs** auf der Registerkarte **Konfiguration** des Integrationsausführungsdatensatzes für diese Integration aufgelistet. |
| Tenable.io Integration von Compliance-Ergebnisauffüllung | • Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Assets-Integration im Rahmen einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration gleicht Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_tenable_missing_asset] aufgeführt sind.<br>• Importiert bis zu 200 Asset-IDs für fehlende Assets, die erkannt wurden oder in der Instanz vorhanden sind, nachdem der Import der Assets-Integration erfolgreich abgeschlossen wurde.<br>• Entfernt die temporären Datensätze aus der Tabelle [sn_vul_tenable_missing_asset], wenn Assets mit den entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können. |
| Tenable.io Integration von Scan-Anmeldeinformationen | • Diese Integration ruft die in Tenable.iokonfigurierten Scan-Anmeldeinformationen ab.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | • Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential] ausgefüllt sind.<br>• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scan-Anforderungen von Now Platforminitiiert werden.<br>• Diese Integration ist so geplant, dass sie wöchentlich ausgeführt wird. |
| Tenable.io Vorlagenintegration | Während des erneuten Scannens wird ein Vorlagendatensatz an Tenable.io gesendet. Diese Integration ruft verfügbare Tenable.io Anmeldeinformationen ab, die für erneute Scans verwendet werden sollen. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und sicher vorübergehend in der Tabelle [sn_vul_tenable_io_template] gespeichert. |
| Tenable.io Plugin-Integration | • Ruft die Plugin-Daten aus dem Produkt Tenable.io ab. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt durch eine Tenable.io Integrationsausführung aktualisiert wurden.<br>• Dieser Import stellt sicher, dass die Tenable.io Bezeichner (10 IDs) aktuell sind.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API.<br>• Das Ergebnis dieser Integration sind Schwachstellen von Drittparteien. |
| Tenable.io Integration behobener Schwachstellen | • Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status „ **Offen** “ und **„Erneut geöffnet“** befinden, da diese Datensätze korrigiert werden müssen. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen **behoben**sind, aber angreifbare Elemente werden standardmäßig nicht für **feste** Erkennungen erstellt, da **Tenablefeste**Schwachstellen als verringert betrachtet.<br>• Wenn im Setup-Assistenten die Kennzeichnung **„Angreifbare Zeiten für Erkennungen von festen Schwachstellen erstellen** “ aktiviert ist, werden neue VIs im Status „ **Fest** “ erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann dies die Importleistung beeinträchtigen. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit bei **Erkennungen** mit Korrekturen nur die Status vorhandener angreifbarer Elemente aktualisiert werden.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **geschlossene/behobene** angreifbare Elemente (AEs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br><br>Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach dem erfolgreichen Abschluss einer Ausführung die unten beschriebene Integration offener Schwachstellen ausgelöst wird.<br><br>Ab Tenable v3.3 können Sie die folgenden Informationen für ausgeführte Schwachstellenintegrationen anzeigen:<br>• Blöcke**gesamt:** Gesamtzahl der von Tenable generierten Blöcke<br>• **Verfügbare Blöcke:** Anzahl der Blöcke, die für ServiceNow zum Download verfügbar sind. |
| Tenable.io Integration offener Schwachstellen | • Diese Integration wird nach erfolgreichem Abschluss der Tenable.io Integration behobener Schwachstellen ausgelöst.<br>• Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **neue/erneut geöffnete** angreifbare Elemente (AEs). Außerdem werden |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind. Tenable betrachtet aktive Schwachstellen **kumulativ** (aktuell).<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br><br>Ab Tenable v3.3 können Sie die folgenden Informationen für ausgeführte Schwachstellenintegrationen anzeigen:<br>• Blöcke**gesamt:** Gesamtzahl der von Tenable generierten Blöcke<br>• **Verfügbare Blöcke:** Anzahl der Blöcke, die für ServiceNow zum Download verfügbar sind. |

### Integrationen vonTenable.sc mit der Anwendung Vulnerability Response .

Die Tenable.sc -Integrationen in der Anwendung Vulnerability Response Integration with Tenable.

Wenn ab Vulnerability Response v20.0 ein Asset von einem Agent gescannt wird, wird in der Spalte „Agent vorhanden“ der Wert „true“ in der Liste „Erkannte Elemente“ angezeigt, der angibt, dass es sich um einen echten Scan handelt.

## Liste der Tenable.sc Integrationen

Mehrere Quellen werden für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in Vulnerability Responsehinzufügen und bereitstellen. Sie installieren und konfigurieren die Anwendung Vulnerability Response Integration with Tenable auch über den Setup-Assistenten.

- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden.

**Tenable.sc-Integrationen**

| Integration | Beschreibung |
|---|---|
| Tenable.sc Assets-Integration | Um zu vermeiden, dass doppelte erkannte Elemente mit importierten Asset-Daten erstellt werden, besteht die Asset-Integration des Produkts Tenable.sc aus zwei Integrationen.<br>**Die Tenable.sc Open Assets-Integration**<br>Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **kumulativ** (aktuell) oder **offen**betrachtet. Die angreifbaren Elemente (VIs), die |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | in Ihrer Instanz mit diesen importierten Asset-Daten erstellt werden, gelten als offen, d. h. im Status „ **Offen** “. Diese angreifbaren Elemente müssen untersucht und möglicherweise korrigiert werden.<br>**Die Tenable.sc Integration von Anlagegütern**<br>Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **verringert** (nicht mehr angreifbar) oder **behoben**ansieht. Die angreifbaren Elemente für diese Assets gehen in Ihrer Instanz vom Status „ **Offen** “ in den Status **„Geschlossen/ Korrigiert** “ über, da die Ergebnisse von Scans zeigen, dass sie nicht mehr angreifbar sind.<br>• Ruft alle Asset-Daten aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Assets-API.<br>• Die Ausgabe dieser Integration sind erkannte Elemente.<br>• Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets-Integration. Es werden nur die Assets mit den Schwachstellen importiert, die den Bedingungen des Abfragefilters entsprechen. |
| Tenable.sc Plugin-Integration | • Ruft die Plugin-Daten aus dem Produkt Tenable.sc ab. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt durch eine Tenable.sc Integrationsausführung aktualisiert wurden.<br>• Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (10 IDs) aktuell sind und nur aktive Schwachstellen importiert werden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API.<br>• Das Ergebnis dieser Integration sind Schwachstellen von Drittparteien. |
| Tenable.sc Integration behobener Schwachstellen | • Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status „ **Offen** “ und **„Erneut geöffnet“** befinden, da diese Datensätze korrigiert werden |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | müssen. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen **behoben**sind, aber angreifbare Elemente werden standardmäßig nicht für **feste** Erkennungen erstellt, da **Tenablefeste**Schwachstellen als verringert betrachtet.<br>• Wenn im Setup-Assistenten die Kennzeichnung **Schwachstellenzeiten für Erkennungen von festen Schwachstellen erstellen** aktiviert ist, werden neue VIs im Status „ **Fest** “ erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann dies die Importleistung beeinträchtigen. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit bei **Erkennungen** mit Korrekturen nur die Status vorhandener angreifbarer Elemente aktualisiert werden.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **geschlossene/ behobene** angreifbare Elemente (AEs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br><br>Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach einer erfolgreichen Ausführung die unten beschriebene Tenable.sc Integration offener Schwachstellen ausgelöst wird.<br><br>**Hinweis:**<br>Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen. |
| Tenable.sc Integration offener Schwachstellen | • Diese Integration wird nach erfolgreichem Abschluss der Tenable.sc Integration behobener Schwachstellen ausgelöst.<br>• Ruft Schwachstellendaten basierend auf den im Produkt Tenable.sc ausgewählten Abfragefiltern ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration lautet **Aktualisieren/ Neue angreifbare Elemente erstellen**, sofern sie nicht bereits vorhanden sind. Außerdem werden Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>**Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen. |
| Tenable.sc Integration von Scan-Anmeldeinformationen | • Diese Integration ruft die in Tenable.scKonfigurierten Scan-Anmeldeinformationen ab.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API.<br>• Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in die Tabelle [sn_vul_tenable_scan_credential] eingetragen werden.<br>• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scan-Anforderungen von Now Platforminitiiert werden.<br>• Diese Integration ist so geplant, dass sie wöchentlich ausgeführt wird. |
| Tenable.sc Integration von Auffüllung von Schwachstellen | • Diese Auffüllungsintegration importiert alle offenen und behobenen Schwachstellen, die während eines Imports möglicherweise übersehen wurden.<br>• Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren.<br>• Diese Integration kann sich auf Ihre Leistung auswirken.<br>• Diese Integration ist standardmäßig deaktiviert.<br>• Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, sollten Sie die Integrationen von Tenable.sc mit festen und offenen Schwachstellen so planen, dass sie ausgeführt werden, wenn keine anderen Scans ausgeführt werden.<br>• Die Ausgabe dieser Integration ist: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | ○ **Geschlossene/behobene** angreifbare Elemente (VIs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>○ zum **Aktualisieren/Erstellen neuer** angreifbarer Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind. |

## Benutzerauthentifizierung und Tenable.sc

Die Benutzerauthentifizierung wird von Ihrer Now Platform® -Instanz und Version 5.13 des Tenable.sc -Produkts unterstützt. Die Benutzerauthentifizierung ist erforderlich, wenn Sie Version 5.12 und früher des Produkts Tenable.sc verwenden.

Wenn Sie die Benutzerauthentifizierung für die Tenable.sc -Integrationen auswählen, laufen Token möglicherweise ab und müssen während der Integrationsausführungen ersetzt werden. In der Spalte Notizen im Datensatz der Ausführung der Schwachstelle-Integration (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen. Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

### Vorbereitung auf die Tenable Vulnerability-Integration

Bereiten Sie sich auf die Integration von ServiceNow® Tenable Vulnerability vor, indem Sie die folgenden Setup-Aufgaben ausführen.

## Bevor Sie beginnen

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Für eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Integration with Tenable sollten Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Now Platform® -Instanz importieren.

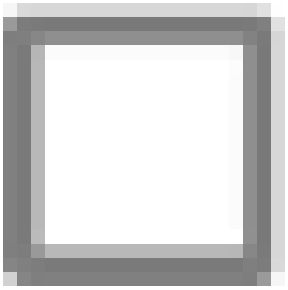
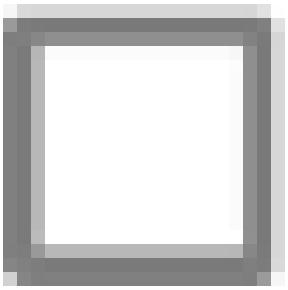
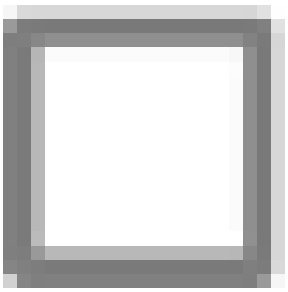
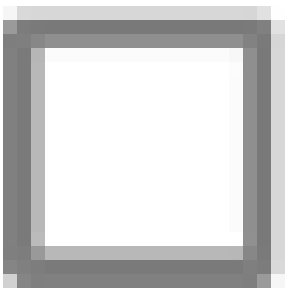
**Hinweis:**
Wenn Sie Daten mit der in Tenable erstellten Integration importiert haben und ServiceNow® Vulnerability Response Integration with Tenable verwenden möchten, finden Sie weitere Informationen unter

Aktuelle Informationen zur Datenbereinigung und Migration von der in Tenable erstellten Integration zur von ServiceNowerstellten Integration finden Sie im Artikel Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] .

Erforderliche Rolle: admin zum Herunterladen und Installieren der Anwendung.

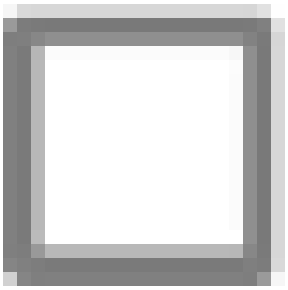
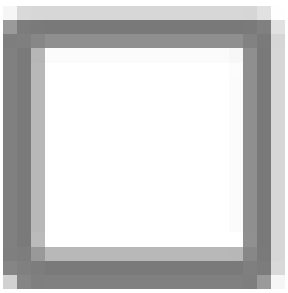


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
|  | (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 12.1 von Vulnerability Response oder höher. |
|  | Wenn Sie sie noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Tenable in Ihre Instanz Now Platform® ] herunter. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.<br><br>Weitere Informationen finden Sie unter . |
|  | Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren werden.<br><br>Vergewissern Sie sich, dass Ihre Instanz die Anzahl der zu importierenden angreifbaren Elemente akzeptieren kann. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support von ServiceNow®. |
|  | Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, die die Integrationen verwalten und angreifbare Elemente korrigieren.<br><br>**Administrator**<br><br>Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.<br><br>**sn_vul.vulnerability_admin**<br><br>Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittanbietern.<br><br>**sn_vul_tenable.configure_integration**<br><br>Kann die Tenable Vulnerability-Integration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration.<br><br>**sn_vul_tenable.read_integration** |

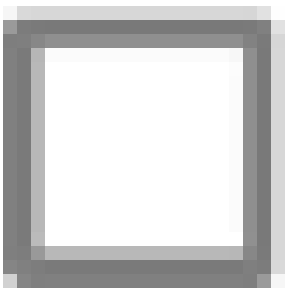


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | Kann Datensätze der Tenable Vulnerability-Integration anzeigen (lesen).<br>**Vulnerability Response-Gruppe**<br>Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.<br>Der Systemadministrator führt die anfängliche Zuweisung von Rollen zu Benutzern und Gruppen im Setup-Assistenten für die -Integration durch. Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Wenn dies noch nicht geschehen ist, ziehen Sie es möglicherweise vor, zusätzliche Gruppen zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen .<br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. |
|  | Um die Leistung beim ersten Import zu verbessern, sollten Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren.<br>• Deaktivieren Sie Schwachstellenrechner, wenn Sie sie nicht verwenden. Diese und die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Siehe Schwachstellenrechner deaktivieren.<br>• Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import möchten Sie möglicherweise benachrichtigungsbezogene Business Rules deaktivieren, wie in Importieren Sie Änderungen für die Integration von Tenable Vulnerabilitybeschrieben. |
|  | Vergewissern Sie sich, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Jobs in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind.<br>• Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Vulnerability Response Integration with Tenable und Ihre Instanz Now Platform in derselben Umgebung befinden. Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | Weitere Informationen zu MID Servern in Ihrer Instanz finden Sie unter MID Server .<br>• Vergewissern Sie sich, dass das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht Basissystemkomponenten den Aufruf externer Systeme mithilfe von Integrations-APIs und aktiviert Protokollschritte wie REST.<br>Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es. |
|  | Rufen Sie Tenable-Anmeldeinformationen ab.<br>Vergewissern Sie sich, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre Tenable-Produkte erforderlich sind, damit Sie darauf zugreifen können.<br>Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64. Tenable.sc erfordert Sicherheitsanalysten oder Managerzugriff.<br>**Hinweis:**<br>Ab Version 3.8 von Vulnerability Response Integration with Tenablesind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Basisbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen. |

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten.

### Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten

Bevor Sie ServiceNow® Tenable Vulnerability Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Tenable aus dem ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response ] installieren und konfigurieren.

#### Vorbereitungen

Vergewissern Sie sich vor der Installation der Tenable-Anwendung, dass Sie alle Elemente in der Prüfliste in Vorbereitung auf die Tenable Vulnerability-Integrationabgeschlossen haben.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Erforderliche Rollen: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) zur Konfiguration der Anwendung im Setup-Assistenten nach der Installation.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einiger Zeit werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie die Kachel **Tenable (Tenable-Plattform),** und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung Vulnerability Response Integration with Tenable installiert, die Sie aus dem ServiceNow Storeheruntergeladen haben.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.

### Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen**, um mit der Konfiguration fortzufahren. Weitere Informationen zu den Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten.

#### Datenabrufeinstellungen für die Tenable Vulnerability-Integration

Mit den folgenden Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der ServiceNow® Tenable Vulnerability-Integration in Ihre Now Platform® ]-Instanz importieren möchten.

Mit den in den folgenden Abschnitten beschriebenen Einstellungen können Sie die Daten steuern, die Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter in Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Integrationsinstanzen** und klicken Sie auf Ihre Integration, Tenable.io oder Tenable.sc.

Klicken Sie auf der angezeigten Seite „Integrationsinstanz“ auf Integrationsinstanzparameter, um eine Liste von Parametern anzuzeigen, oder auf die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

### Allgemeine Schweregrad- und Abrufeinstellungen und Filter für Tenable.io und Tenable.sc in Ihrer Now Platform -Instanz

Die folgenden Einstellungen sind für die Integrationen Tenable.io und Tenable.sc in Ihrer Instanz Now Platform ] verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Now Platform -Instanz angezeigt. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardwerten belassen.

Tenable.io

**insert_fixed**

Wenn Sie die **Kennzeichnung insert_fixed** im Setup-Assistenten für die Integration von Schwachstellenimport aktivieren, werden neue VIs für Erkennungen im Status „ **Fest** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

**Schweregrad_kritisch**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit kritischem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_hoch**

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit hohem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_mittel**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad aus den Integrationen Tenable.io offene Schwachstellen und Tenable.io feste Schwachstellen zu erhalten.

**Schweregrad_info**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Infoebene aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_niedrig**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad aus den Integrationen Tenable.io offene Schwachstellen und Tenable.io feste Schwachstellen zu erhalten.

**size**

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz aus der Tenable.io Plugin-Integration aufgenommen werden sollen. Muss im Format int32 vorliegen. Der Standardwert ist 1.000. Die maximale Größe beträgt 10.000.

**num_assets**

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus den Integrationen von Tenable.io Behobene Schwachstellen und Tenable.io Offene Schwachstellen. Der Standardwert ist 50.

**chunk_size**

Gibt die Anzahl der Assets pro exportiertem Block durch die Tenable.io Assets-Integration an. Der Standardwert ist 1.000.

Tenable.sc

**async_request**

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit Tenable.sc durchzuführen. Wenn bei synchronen Aufrufen eine Zeitüberschreitung bei 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box zu optimieren. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc. Für bestehende Kunden, die asynchrone Aufrufe verwenden, ist ein Korrekturskript verfügbar, das den vorhandenen Tenable.sc -Integrationsinstanzen einen neuen async_request-Parameter hinzufügt. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

**insert_fixed**

Wenn Sie die **Kennzeichnung insert_fixed** im Setup-Assistenten für die Integration von Schwachstellenimport aktivieren, werden neue VIs für Erkennungen im Status „ **Fest** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

**Offset**

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Abfragefilter**

Abfragefilter werden in der Tenable-Konsole konfiguriert. Diese Abfragefilter haben IDs, die im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in Ihrer Now Platform -Instanz ausgewählt werden können. Diese Filter werden beim Abrufen der Daten aus den Tenable.sc -Integrationen angewendet.

### REST-Nachrichten für die Integration von Tenable Vulnerability

Die REST-Nachrichten ServiceNow® Tenable Vulnerability Integration werden für Aufrufe an die Tenable-API verwendet.

## Tenable.io REST-Nachricht für Assets

Die REST-Nachricht Tenable.io Assets ruft Assets-Informationen für die Tenable.io Asset-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Asset-Informationen aus. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „is_deleted“: falsch
- „is_licensed“: wahr

## Tenable.io Plugins-REST-Nachricht

Die REST-Nachricht Tenable.io Plugins ruft Plugin-Informationen für die Tenable.io Plugin-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Plugin-Informationen aus.

## Tenable.io REST-Nachricht zu Schwachstellen

Die REST-Nachricht Tenable.io Schwachstellen ruft Schwachstelleninformationen für offene und geschlossene Schwachstellen aus der Schwachstellenintegration Tenable.io ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Informationen zu Schwachstellen aus.

## Tenable.sc Fragt die REST-Nachricht ab

Die REST-Nachricht „Tenable.sc-Abfragen“ ruft die Abfragefilterinformationen für die Tenable.sc-Asset-Integration und die Tenable.sc-Schwachstellenintegration ab, in der der Abfragefilter konfiguriert ist.

## Tenable.sc Plugins-REST-Nachricht

Die Tenable.sc Plugin-REST-Nachricht ruft Plugin-Informationen für die Tenable.sc Plugin-Integration ab. Änderungen am Methodendatensatz der REST-Nachricht „Plugins abrufen“ wirken sich auf die Anforderungen an Tenable.sc zum Abrufen von Plugin-Informationen aus.

| Parametername | Wert | Beschreibung |
|---|---|---|
| type | aktiv | Gibt an, aus welcher Quelle Tenable Daten abruft. Von Code verwendet. Änderungen werden nicht empfohlen. |
| Felder | ID, Beschreibung, cvssVector, cvssV3Vector, cvssV3TemporalVector, | Gibt die Liste der Felder an, die aus Tenable importiert wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Parametername | Wert | Beschreibung |
|---|---|---|
| | synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vpr, vprContext, PluginPubDate, PluginModDate, xrefs, Familie, RiskFactor, cpe, seeAlso, Lösung, ExploitFrameworkAvailable, ExploitFrameworkAvailable Typ, Copyright, Version, Quelldatei, Abhängigkeiten, erforderlichePorts, erforderlichUDPPorts, srcPort, dstPort,Protokoll, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifizierteZeit, md5 | |

## Tenable.sc REST-Nachricht zu Schwachstellen

Die REST-Nachricht Tenable.sc Schwachstellen ruft Schwachstelleninformationen aus der Tenable.sc -Integration ab. Änderungen an der REST-Nachricht „Schwachstellen abrufen“ oder „Gepatchte Schwachstellen abrufen“ oder, ab Version 14.0 Vulnerability Response und Version 2.2 der Tenable Vulnerability-Integration, am Datensatz „Schwachstellen für Auffüllung abrufen“ wirken sich auf die Anforderungen zum Abrufen von Informationen zu Schwachstellen an Tenable.sc aus.

## Tenable.sc REST-Nachricht „Anmeldeinformationen scannen“.

**Tenable.sc Richtlinien-REST-Nachricht**

Die POST-REST-Nachricht Tenable.sc policy fügt eine Richtlinie für angeforderte Plugins hinzu. Generierte Richtlinie wird in Tenable.sc Scan-Anforderungen verwendet.

**Tenable.sc REST-Nachricht scannen**

Die POST-REST-Nachricht Tenable.sc scan fügt einen Scan hinzu, der vom Zugriff und der Berechtigung abhängt, die im Anforderungstext der REST-Nachricht definiert sind. Im Anforderungstext für die Scan-Anforderung werden Richtlinie, Plugin-ID und IP(s) verwendet.

**Tenable.sc REST-Nachricht „Scan-Ergebnis“.**

Die GET-REST-Nachricht Tenable.sc Scan-Ergebnis enthält Scan-Details des Scans, der mit der Scan-REST-Nachricht generiert wurde. Er verwendet die scanResultId in der Antwort der Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

**Tenable.sc Anmeldeinformationen scannen**

Die REST-Nachricht Tenable.sc scan credentials ruft die Anmeldeinformationen aus Tenable.scab. Änderungen am Methodendatensatz der REST-Nachricht „Importieren“ wirken sich auf die Anforderungen an Tenable.sc zum Abrufen der Anmeldeinformationen aus.

| Parametername | Wert | Beschreibung |
|---|---|---|
| Felder | ID, Name, Beschreibung, Typ | Gibt die Liste der Felder an, die aus importiert wurden Tenable.sc |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Parametername | Wert | Beschreibung |
|---|---|---|
| filter | nutzbar | Gibt an, dass die Integration nur verwendbare Anmeldeinformationen von abruft Tenable.sc<br><br>Änderungen an einem der Parameter werden nicht empfohlen. |

### Datentransformation für die Integration von Tenable Vulnerability

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie aus dem Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen transformieren importierte Tenable-Schweregrade in Standardschweregrade für die Verarbeitung in Ihrer Instanz. Weitere Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Vulnerability Response-Schweregradzuordnungen erstellen in der Dokumentation Vulnerability Response.

## Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tenable.io-Asset-Importtabelle [sn_vul_tenable_io_asset_import] geladen.

Die Tenable.io Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach `Tenable.io Asset Transform`.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### Tenable.io Asset-Transformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Tenable stellt eine eindeutige ID für Assets bereit, ordnet sie dem Datensatz des erkannten Elements zu und wird für die CI-Suche verwendet. |
| u_ipv4s | ip_address | Ordnet den ersten IP-Wert dem Feld ip_address im Datensatz des erkannten Elements zu. |
| u_mac_addresses | mac_address | Ordnet den ersten mac_address-Wert dem MAC-Adressfeld im Datensatz des erkannten Elements zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io Asset-Transformationszuordnungsfelder (Fortsetzung)**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_fqdns | fqdn | Ordnet den ersten fqdn-Wert dem fqdn-Feld im Datensatz des erkannten Elements zu. |
| u_netBIOS_names | NetBIOS | Ordnet den ersten NetBIOS-Wert dem NetBIOS-Feld im Datensatz des erkannten Elements zu. |
| u_operating_systems | os | Ordnet den ersten BS-Wert dem BS-Feld im Datensatz des erkannten Elements zu. |
| (Vor Version 14.0 Vulnerability Response und Version 2.2 von Tenable Vulnerability Integration)u_last_scan_time | last_scan_date | Ordnet auf das Feld last_scan_date im Datensatz des erkannten Elements zu. |
| u_last_authenticated_scan_date | last_auth_scan_date | Ordnet auf das Feld last_auth_scan_date im Datensatz des erkannten Elements zu. |
| [Skript] | Name | Ordnet den Hostnamen mithilfe der Logik des Skripts zu. |
| u_tags | | Die Tags werden in sn_sec_cmn_host_tag gespeichert. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_tag gespeichert. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

## Timing und Zweck des Tenable.io Asset-Transformationszuordnungsskripts

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, die verwendet wird, um Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem import_set. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| | Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

## Integration von Tenable.io-Plugins

Die Transformationszuordnung für Tenable.io-Plugins wird verwendet, um aus Tenable.io importierte Plugins zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten verarbeitet werden, die von den Tenable-Plugins empfangen wurden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Tenable.io-Plugin-Transformation.

Die Nutzlast der Tenable.io-Plugins enthält alle Felder in der Spalte u_attributes der Tabelle sn_vul_tenable_io_plugin_import. Das Attributfeld wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| id | id | Ordnet die ID aus der Quelle zu und fügt das Präfix TEN hinzu. Beispiel: Wenn die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345. |
| Beschreibung | Zusammenfassung | Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu. |
| [Skript] | Quelle | Die Quelle für importierte TPE ist Tenable.io. |
| [Skript] | source_instance | Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert. |
| Familie | Kategorie | Ordnet die Familie des Plugins der Kategoriespalte zu |
| Plugin_Änderung_Datum | last_modified | Ordnet „plugin_modification_date“ dem Feld der letzten Änderung zu. |
| Plugin_Veröffentlichung_Datum | date_published | Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu. |
| has_patch | remediation_type | Ordnet den Korrekturtyp dem Wert has_patch zu. |
| synopsis | Bedrohung | Ordnet die Bedrohungsinformationen für diese Schwachstelle zu. |
| cvss_base__score | Punktzahl | Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| Lösung | Lösung | Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu. |
| Exploit_available | Exploit | Ordnet den vom Scanner bereitgestellten „ploit_available“ der Exploit-Spalte in der Drittpartei-Eintragstabelle zu |
| vpr.Punktzahl | source_risk_score | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| vpr.drivers.age_of_vuln | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.exploit_code_maturity | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.product_coverage | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.threat_sources_last28 | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittparteitabelle zu. |
| vpr.drivers.threat_intensity_last28 | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.threat_recency | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen von „scanner“ Threat_recency in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.cvss3_impact_score | v3_impact_subscore | Ordnet die cvss3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| cvss_temporal_score | cvss_temporal_score | Ordnet die temporäre Punktzahl für CVSS v2 zu. |
| cvss_v3_temporal_score | v3_temporal_score | Ordnet die temporäre Punktzahl für CVSS v3 zu. |
| risk_factor | source_severity | Ordnet auf den Quellschweregrad in der Drittpartei-Eintragstabelle zu. |
| Name | Name | Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu. |
| stig_severity | stig_severity | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| Plugin-Typ | check_type | Ordnet den Plugin-Typ check_type in der Drittpartei-Eintragstabelle zu. |
| unsupported_by_vendor | unsupported_by_vendor | Ordnet das Feld unsupported_by_vendor der Spalte unsupported_by_vendor zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve. |
| bid | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |
| see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| xrefs | Die X-REF-Liste wird als Referenz hinzugefügt. |
| [Skript] | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittparteieintrag. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

Die TenableIOPluginsImportProcessor-Skripteinbindung wird aus dem onBefore-Transformationsskript aufgerufen. Die Ausgabe der Tenable.io-Plugin-Integration wird in Now Platform Schwachstelleneinträge von Drittparteien umgewandelt. Alle Änderungen an dieser Skripteinbindung können die Transformation der Tenable.io-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

## Import von Tenable.io-Schwachstellen

Die Transformationszuordnung für angreifbare Tenable.io-Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Tenable-Schwachstellenimport verarbeitet werden.

Dieselbe Transformationszuordnung wird sowohl für die Integration von Tenable.io mit festen Schwachstellen als auch für die Integration mit Tenable.io Open Vulnerabilities verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Transformationszuordnung für angreifbares Tenable.io-Element.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_asset.uuid | id | Uuid wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.ipv4 | ip_address | Das ipv4-Feld wird dem ip-Adressfeld des cmdb_ci-Datensatzes zugeordnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_asset .last_authenticated_results | last_auth_scan_date | Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Auth-Scans des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.mac_addess | mac_address | MAC-Adresse wird dem Host-MAC-Adressfeld des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.netBIOS_name | NetBIOS | NetBIOS wird dem NetBIOS-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u._plugin.cvss3_base_score | v3_base_score | CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u._plugin.cvss3_temporal_score | v3_temporal_score | Die temporäre CVSS v3-Punktzahl wird der v3 temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u._plugin.cvss_base_score | Punktzahl | Die CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u._plugin.cvss_temporal_score | temporal_score | Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_plugin.description | Zusammenfassung | Die Beschreibung wird dem Zusammenfassungsfeld im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_plugin.familie | Kategorie | Ordnet die Plugin-Familie der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu. |
| u_plugin.modification_date | last_modified | Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittanbietereintrags zugeordnet. |
| u_plugin.publication_date | date_published | Das Veröffentlichungsdatum wird dem Feld |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | „Veröffentlichungsdatum“ des Datensatzes „Drittpartei-Eintrag“ zugeordnet. |
| u_plugin.risk_factor | source_severity | Der Risikofaktor wird dem Feld „source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_plugin.solution | Lösung | Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_plugin.synotsis | Bedrohung | Die Synopse wird dem Bedrohungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_severity_id | Priorität | Die Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5. |
| u_plugin.exploit_available | Exploit | Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu. |
| vpr.Punktzahl | source_risk_score | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_plugin.vpr.drivers.age_of_vuln | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.exploit_code_maturity | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_plugin.vpr.drivers.product_coverage | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_sources_last28 | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_intensity_last28 | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_recency | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.cvss3_impact_score | v3_impact_subscore | Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.type | check_type | Ordnet den Plugin-Typ check_type in der Drittpartei-Eintragstabelle zu. |
| u_plugin.unsupported_by_vendor | unsupported_by_vendor | Ordnet das Feld „unsupported_by_vendor“ im Plugin der Spalte „unsupported_by_vendor“ zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |
| u_plugin.family_id | Family_id | Ordnet die Familien-ID des Plugins der Spalte „family_id“ in der Drittpartei-Eintragstabelle zu. |
| port | port | Der Port wird dem Feld „Port“ des Datensatzes für angreifbare Elemente zugeordnet. |
| protocol | protocol | Das Protokoll wird dem Protokollfeld des Datensatzes |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | für angreifbare Elemente zugeordnet. |
| u_first_found | first_found | „Zuerst gefunden“ wird dem Feld „Zuerst gefunden“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_last_found | last_found | „Zuletzt gefunden“ wird dem Feld „Zuletzt gefunden“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_state | Status | Der Status wird dem Feld Status im Datensatz des angreifbaren Elements zugeordnet |
| [Skript] | Quelle | Die Quelle der Integration wird ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.io als Quelle. |
| [Skript] | integration_instance | integration_instance ist der Name der Instanz, aus der das angreifbare Element importiert wird. |
| u_plugin.name | Name | Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu. |
| u_plugin.stig_severity | stig_severity | Ordnet den STIG-Schweregrad des Plugins der Spalte „STIG-Schweregrad“ in der Drittpartei-Eintragstabelle zu |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve. |
| bid | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |
| see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| xrefs | Die X-REF-Liste wird als Referenz hinzugefügt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Beschreibung |
|---|---|
| [Skript] | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation löst TenableIOVulnerabilitiesProcessor aus, der Daten aus Tenable.io mithilfe des Importsatzes importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „Angreifbare Elemente“ und die Tabelle „Drittpartei-Schwachstelle“ lädt.Zur internen Verwendung. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, um zu überprüfen, ob der Drittpartei-Eintrag und die Erkennungen bereits vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Anzahl der aus Tenable.io importierten CIs, VIs und Erkennungen zu aktualisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Tenable.sc-Asset-Import

Aus Tenable.sc importierte Asset-Daten werden zuerst in die Tenable.sc-Asset-Importtabelle (sn_vul_tenable_sc_asset_import) geladen. Die Tenable.sc Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach `Tenable.sc Asset Transform`.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_uuid | id | Die UUID wird nicht über die Tenable-API ausgefüllt. Daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges UUID-Feld für Assets zu erstellen und dem cmdb_ci-Datensatz zuzuordnen. |
| u_ip | ip_address | Ordnet das IP-Feld der API dem Feld ip_address in einem cmdb_ci-Datensatz zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_macaddress | mac_address | Ordnet das Feld macaddress aus der API dem Adressfeld im cmdb_ci-Datensatz zu. |
| u_dnsname | fqdn | Ordnet das dnsname-Feld der API dem fqdn-Feld im cmdb_ci-Datensatz zu. |
| u_netBIOSName | NetBIOS | Ordnet das NetBIOS-Feld der API dem NetBIOS-Feld im cmdb_ci-Datensatz zu. |
| u_oscpe | os | Die BS-Informationen werden aus dem Attribut oscpe in der Nutzlast extrahiert und dem BS-Feld im cmdb_ci-Datensatz zugeordnet. |
| u_lastauthrun | last_auth_scan_date | Ordnet das Feld „lastauthrun“ der API dem Feld „last_auth_scan_date“ im Datensatz des erkannten Elements zu. |
| u_lastauthrun und u_lastunauthrun | last_scan_date | „lastauthrun“ wird aus der Tenable-API oder „lastunauthrun“ extrahiert. Basierend darauf, welcher Wert in der Nutzlast angezeigt wird, wird das Feld „last_scan_date“ im Datensatz des erkannten Elements ausgefüllt. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion zum Aktualisieren der Werte auf dem Host und Überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem import_set. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Import von Tenable.sc-Plugins

Aus Tenable.sc importierte Plugin-Daten werden zuerst in die Tenable.sc-Plugin-Importtabelle (sn_vul_tenable_sc_plugin_import) geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach Tenable.sc Plugin Transform Map.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Ordnet die ID der Quelle zu und fügt das Präfix TEN hinzu. Beispiel: Wenn die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345. |
| u_description | Zusammenfassung | Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu. |
| [Skript] | Quelle | Importiertes TPE aus dieser Integration hat Tenable.sc als Quelle. |
| [Skript] | source_instance | Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert. |
| u_familie | Kategorie | Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu. |
| u_plugin_modification_date | last_modified | Ordnet „plugin_modification_date“ dem Feld der letzten Änderung zu. |
| u_plugin_publication_date | date_published | Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu. |
| u_has_patch | remediation_type | Ordnet den Korrekturtyp dem Wert has_patch zu. |
| u_synosis | Bedrohung | Ordnet die Bedrohungsinformationen für diese Schwachstelle zu. |
| u_cvss_base_score | Punktzahl | Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu. |
| u_solution | Lösung | Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu. |
| u_cvss_temporal_score | cvss_temporal_score | Ordnet die temporäre Punktzahl für CVSS v2 zu. |
| u_cvss_v3_temporal_score | v3_temporal_score | Ordnet die temporäre Punktzahl für CVSS v3 zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_risk_factor | Quellschweregrad | Ordnet auf den Quellschweregrad in der Drittpartei-Eintragstabelle zu. |
| u_cvss_v3_base_score | v3_base_score | Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu. |
| u_exploit_available | Exploit | Ordnet das vom Scanner bereitgestellte ExploitAvailable der Exploit-Spalte in der Drittpartei-Eintragstabelle zu. |
| u_vpr_score | source_risk_score | Ordnet die VPR-Punktzahl vom Scanner der Quellrisikopunktzahl in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_vpr_context[id=age_of_vuln] | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = exploit_code_maturity] | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = product_coverage] | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = ”threat_sources_last_28] | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen von „scanner“ zu „thread_sources“ in der Drittparteitabelle zu. |
| u_vpr_context [id = ”threat_intensity_last_28] | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = „threat_recency“] | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = cvssV3_impactScore] | v3_impact_subscore | Ordnet die CVSS v3-Auswirkungspunktzahl des |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | Scanners v3_impact_subscore in der Drittpartei-Eintragstabelle zu. |
| u_name | Name | Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu. |
| u_stig_severity | stig_severity | Ordnet das Feld stig_severity im Plugin stig_severity in der Drittpartei-Eintragstabelle zu. |
| u_check_type | check_type | Ordnet den Prüfungstyp check_type in der Drittpartei-Eintragstabelle zu. |
| u_familie.id | familie_id | Ordnet das Plugin „family_id“ „family_id“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| u_cpe | Die Liste der CPEs wird als Referenz hinzugefügt. |
| u_see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| u_exploit_frameworks | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion zum Aktualisieren der Werte im Drittparteieintrag und zum Überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittparteieintrag. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte der erstellten und ignorierten Plugins festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

Die TenableSCPluginsImportProcessor-Skripteinbindung wird aus dem onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe der Tenable.sc-Plugin-Integration und wandelt sie in ServiceNow-Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Umwandlung von Tenable.sc-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

## Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung für Tenable.sc Open Vulnerabilities wird verwendet, um importierte Daten aus der Integration von Tenable.sc Open Vulnerabilities zu transformieren, und die Transformationszuordnung für Tenable.sc und feste Schwachstellen wird verwendet, um importierte Daten aus der Integration von Tenable.sc für feste Schwachstellen zu transformieren.

**Hinweis:**
Änderungen an diesen Transformationszuordnungen ändern, wie Daten aus dem Import von festen/offenen Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen für offene und feste Schwachstellen von Tenable.sc zuzugreifen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationsinstanzen** > **Tenable.sc – Integration von festen/offenen Schwachstellen** > **Datenquellen** > **Offene/behobene Schwachstellen von Tenable.sc** > **Transformationen**.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_pluginID | ID | Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_riskfactor | source_severity | Dieses Feld ist „source_severity“ im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_severity | Priorität | Das Prioritätsfeld wird dem Schweregrad zugeordnet. Der Standardwert ist 5. |
| u_hasbeenmitigated | Status | „Wurde verringert“ wird dem Statusfeld des Schwachstellendatensatzes zugeordnet. Bei der Integration behobener Schwachstellen befinden sich alle AEs im Status „Geschlossen“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_ip | ip_address | Die IP-Adresse wird dem Host-IP-Feld der Tabelle „cmdb_ci“ zugeordnet. |
| u_port | port | Der Port wird dem Feld „Port“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_protocol | protocol | Das Protokoll wird dem Port-Feld des Datensatzes für angreifbare Elemente zugeordnet. |
| u_firstSeen | first_found | Der erste gefundene Wert wird dem ersten gefundenen Feld des VI-Datensatzes zugeordnet. |
| u_lastSeen | last_found | Der zuletzt angezeigte Wert wird dem zuletzt gefundenen Feld des VI-Datensatzes zugeordnet. |
| u_exploitVerfügbar | Exploit | ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_synosis | Bedrohung | Die Synopse wird dem Bedrohungsfeld im Datensatz des Drittpartei-Eintrags zugeordnet. |
| u_description | Zusammenfassung | Die Beschreibung wird dem Zusammenfassungsfeld im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_solution | Lösung | Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_basescore | Punktzahl | BaseScore wird dem Punktzahlfeld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_temporalScore | temporal_score | Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_cvssv3basescore | v3_base_score | Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | Eintragsdatensatz zugeordnet. |
| u_cvsstemporalscore | v3_temporal_score | Cvssv3temporal score wird der zeitlichen v3-Punktzahl im Datensatz des Drittparteieintrags zugeordnet. |
| u_pluginpubdate | date_published | Das Plugin-Veröffentlichungsdatum wird dem Plugin-Veröffentlichungsdatum im Datensatz des Drittanbietereintrags zugeordnet. |
| u_pluginmoddate | last_modified | Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittanbietereintrags zugeordnet. |
| u_dnsname | fqdn | DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_macaddress | mac_address | MacAddress wird dem Feld mac_address des cmdb_ci-Datensatzes zugeordnet. |
| u_netBIOSName | NetBIOS | NetBIOSName wird dem NETBIOS-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_ip | ip | IP wird dem IP-Feld des cmdb_ci-Datensatzes zugeordnet. |
| hostUniqueness | uuid | Die Eindeutigkeit des Hosts wird keinem Feld zugeordnet, sondern verwendet, um die UUID für den Host zu bestimmen. |
| u_familie | Kategorie | Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu. |
| u_plugintext | Nachweis | Plugin-Text wird dem Nachweis im TPE-Datensatz zugeordnet. |
| [Skript] | Quelle | Die Quelle der Integration wird ausgefüllt. Die aus dieser Integration erstellten |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | angreifbaren Elemente haben Tenable.sc als Quelle. |
| [Skript] | integration_instance | integration_instance ist der Name der Instanz, aus der das angreifbare Element importiert wird. |
| u_vpr_score | source_risk_score | Ordnet die VPR-Punktzahl vom Scanner der Quellrisikopunktzahl in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_vpr_context[id=age_of_vuln] | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = exploit_code_maturity] | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = product_coverage] | product_coverage | Ordnet die Produktabdeckung vom Scanner „product_coverage“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = ”threat_sources_last_28] | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittparteitabelle zu. |
| u_vpr_context [id = ”threat_intensity_last_28] | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = „threat_recency“] | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = cvssV3_impactScore] | v3_impact_subscore | Ordnet die CVSS v3-Auswirkungspunktzahl des Scanners v3_impact_subscore in der Drittpartei-Eintragstabelle zu. |
| u_pluginname | Name | Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu. |
| u_stigseverity | stig_severity | Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Drittpartei-Eintragstabelle zu. |
| u_checktype | check_type | Ordnet den Prüfungstyp check_type in der Drittpartei-Eintragstabelle zu. |
| u_familie.id | familie_id | Ordnet das Plugin „family.id“ „family_id“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „plot_attack_vector“ in der Tabelle „dritter_party_entry“ wird basierend auf „ploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

| Quellenfeld | Beschreibung |
|---|---|
| u_cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung befindet sich in sn_vul_m2m_entry_cve. |
| u_BID | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Beschreibung |
|---|---|
| u_cpe | Die Liste der CPEs wird als Referenz hinzugefügt. |
| u_seealso | Die Liste der URLs wird als Referenz hinzugefügt. |
| u_xrefs | Die Liste der X-REFs wird als Referenz hinzugefügt. |
| u_exploitframeworks | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einer Tabelle mit angreifbaren Elementen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten AEs und AEs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Legen Sie zusätzliche Filterparameter für Tenable.io Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Tenable Vulnerability Integration an, um die mit dem Produkt Tenable.io importierten Schwachstellendaten weiter zu verfeinern.

#### Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach `cidr_range`, `num_assets`, `indexed_at`und `plugin_family`gefiltert werden. Angenommen, Sie möchten eine Tenable.io -Integration so ausführen, dass eine Ausführung nur kritische Schwachstellen alle vier Stunden importiert und eine andere alle 24 Stunden ausführt, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um die Erfassung dieser Daten zu erleichtern, können Sie von Tenable unterstützte Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in Ihrem Now Platformanpassen. Die folgenden Tenable.io -Integrationen unterstützen die Filterung durch Bereitstellung von JSON-Inhalten im Anforderungstext:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Assets-Integration
- Integration behobener Schwachstellen
- Integration offener Schwachstellen

Sie sollten wissen, wie JSON Zeichenfolgen für diese Funktion verwendet werden.

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Suchen Sie die vom Produkt Tenable.io unterstützten Parameter auf der Entwickler-Website, die Sie zum Filtern verwenden möchten.

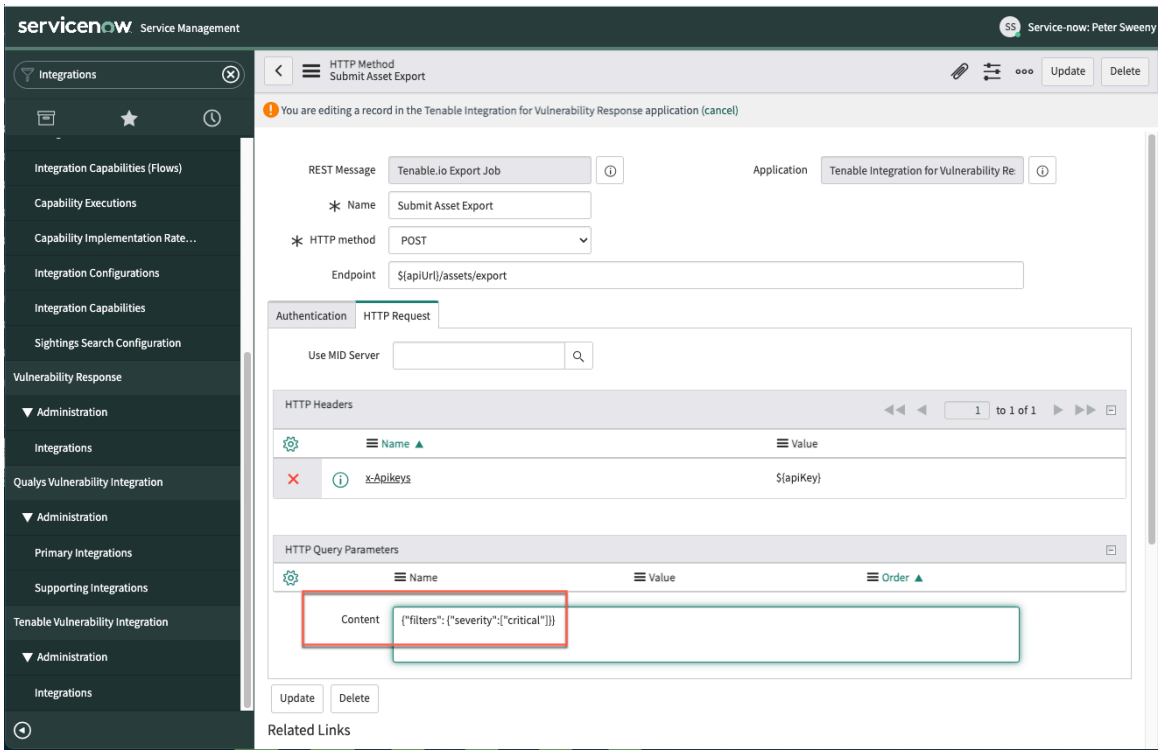
   Parameter und Werte, die Sie aus dem Produkt Tenable.io eingeben, werden nur auf der Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite Tenable Integrations auf den Datensatz für die Tenable.io -Integration, die Sie öffnen möchten.
4. Klicken Sie bei ausgewählter Registerkarte Vertretbare REST-Methoden auf das Informationssymbol (I) für die REST-Methode, gefolgt von **Datensatz öffnen**.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in. Um den Datensatz zu bearbeiten, klicken Sie **hier**.
7. Geben Sie im Datensatz „REST-Methode“ im Feld Inhalt den JSON-Inhalt ein, den Sie als Teil des Anforderungstexts verwenden möchten.

   In der folgenden Abbildung wurde beispielsweise der Schweregradparameter für importierte Schwachstellen `{"filters": {"severity": ["critical"]}}` [] für die Asset-Integration von Tenable.io angepasst . Dieser Wert importiert nur kritische Schwachstellen (CVSS-Punktzahl 10,0).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Tenable.io weitere Informationen zum Trennen der einzelnen Werte.

8. Klicken Sie auf **Aktualisieren**.

### Tenable Vulnerability Integration-Berichterstellung

Zeigen Sie Berichte über Schwachstellen und angreifbare Elemente in den Vulnerability Response -Dashboards an.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

## Vorherige Versionen von Vulnerability Response

Das Übersichts-Dashboard von Vulnerability Response (Vulnerability Management) bietet einen Überblick über Schwachstellen und angreifbare Elemente und hilft dem Schwachstellenadministrator, Problembereiche schnell zu erkennen. Das Vulnerability Response-Korrektur-Dashboard (Schwachstellenkorrektur) ermöglicht es einem Korrekturspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, die er besitzt.

Weitere Informationen finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Korrekturbesitzer.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um das Dashboard anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Korrekturübersicht**.

### Statusdiagramm der Integrationsausführung für die Tenable Vulnerability-Integration

Das Modul Tenable Integration Run Status bietet Ihnen eine grafische Ansicht des Status von Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein beliebiges Teil im Balkendiagramm klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

Erforderliche Rolle: Schwachstellenadministrator

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Vertretbare Schwachstellenintegration** > **Status der Integrationsausführung**.

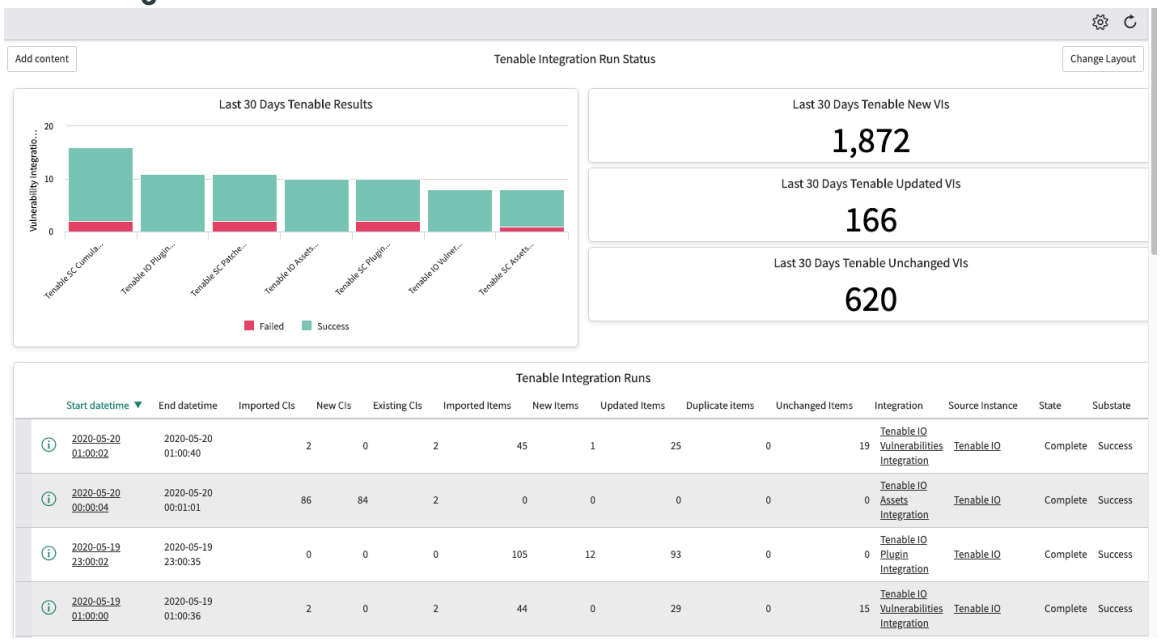
Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausführungsstatus




## Berichte über den Ausführungsstatus der Tenable-Integration

| Name | Beschreibung |
|---|---|
| Tenable-Ergebnisse der letzten 30 Tage | Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Jede Ausführung wird im Diagramm als Balken angezeigt. |
| Neue Tenable-VIs der letzten 30 Tage | Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Aktualisierte Tenable-VIs der letzten 30 Tage | Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Nicht geänderte Tenable-VIs der letzten 30 Tage | Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Tenable-Integrationsausführung | Die Datensätze der Integrationsausführung werden in einer Liste angezeigt.<br><br>**Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br><br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |

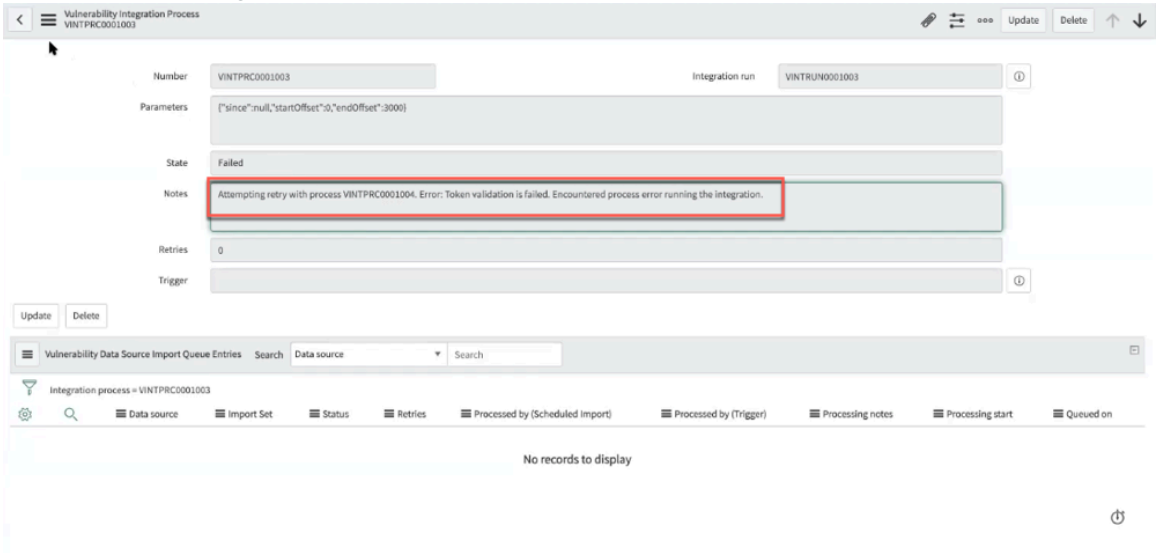


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ablauf der Tokenvalidierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und eine Nachricht wird im Datensatz des Integrationsprozesses für Schwachstellen angezeigt.

**Nachricht über abgelaufenes Token**




Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle fehlgeschlagenen und erfolgreichen Integrationsprozesse werden auf der Registerkarte „Schwachstellenintegrationsprozess“ im Datensatz „Schwachstellenintegrationsprozess“ angezeigt.

### Initiieren Sie einen erneuten Scan für die Tenable.sc -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen geplanten Scan-Zyklen korrigiert wurden, indem Sie erneute Scans in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Tenable.sc aus Ihrer Instanz von Now Platform® initiieren.

#### Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

**Hinweis:**
Tenable.sc unterstützt das erneute Scannen auf Agent-basierten Computern nicht.

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

#### Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Initiieren eines erneuten Scans aus den Arbeitsbereichen finden Sie unter Scannen Sie Tenable.io und Tenable.sc angreifbare Elemente aus den Vulnerability Response -Arbeitsbereichen erneut.

Befolgen Sie die unten aufgeführten Schritte, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbaren Elementen (AEs), Korrekturaufgaben (RTs), Drittanbietereinträgen (TPE) oder Datensätzen erkannter Elemente aus Ihrer Now Platform -Instanz initiieren.

Mit erneuten Scans können Ihre Korrekturbesitzer und Schwachstellenanalysten überprüfen, ob durch Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Beispiel: Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde, erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformTenable.sc auf angreifbare Elemente von [] initiieren.

**Hinweis:**
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen von Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.sc Scan Credential Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.sc -Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen wird automatisch im Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen von Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen) konfigurieren.

Notieren Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf in Ihrer Now Platform -Instanz anzeigen können:

- Mit der Administratorbenutzerrolle Tenable.sc erstellte Anmeldeinformationen stehen Benutzern in allen Ihren Organisationen zur Verfügung.
- Mit der Benutzerrolle der Organisation Tenable.sc erstellte Anmeldeinformationen sind nur für Benutzer innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in Now Platform importiert, es sei denn, sie werden mit dem Konto des Benutzers geteilt, der für die Verbindung mit der Instanz verwendet wird.

Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.sc.

Weitere Informationen zum Konfigurieren der Anwendung Tenable.scKonfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten finden Sie unter []. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Vertretbare Schwachstellenintegration** > **Integrationen** > **Tenable.sc-Integration von Scan-Anmeldeinformationen**.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   **Hinweis:**
   Sie können erneute Scans nur für AEs mit Tenable.sc als Quelle initiieren. Vergewissern Sie sich, dass Tenable.sc in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle nicht in der VI-Listenansicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol „ **Liste personalisieren** “ (Zahnradsymbol), und verwenden Sie den Slushbucket, um **Quelle** von **Verfügbar** zu **Ausgewählt**zu verschieben.

3. Navigieren Sie alternativ zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss die VI aus dem Produkt Tenable.sc stammen und sich in einem anderen Status als **Geschlossen**befinden. Für mehrere VI-Datensätze müssen alle VIs aus dem Tenable.sc-Produkt stammen und sich in einem anderen Status als **Geschlossen**befinden.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Tenable.sc stammen.
   - In einem TPE-Datensatz muss mindestens ein zugeordneter VI-Datensatz aus dem Produkt Tenable.sc einen anderen Status als **Geschlossen**aufweisen.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Scanner-Anmeldeinformationen für den Zugriff auf den Scanner auszuwählen. Dies sind die Anmeldeinformationen, die von der Tenable.sc Scan Credential Integration importiert werden.
5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie **auf Scan anfordern**.

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Details** anzeigen, um den Status des erneuten Scans anzuzeigen und alle anderen erneuten Scans anzuzeigen, die von einem bestimmten Datensatz aus gestartet wurden.

   Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Die untergeordneten Scans importieren Daten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt. Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens. Alle VIs, die in den Status „ **Geschlossen/** Behoben“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.sc-Integration mit festen Schwachstellen importiert.

### Initiieren Sie einen erneuten Scan für die Tenable.io -Integration

Vergewissern Sie sich, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneute Scans in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Tenable.io aus Ihrer Instanz von Now Platform® initiieren.

#### Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

#### Warum und wann dieser Vorgang ausgeführt wird

- Informationen zum Initiieren eines erneuten Scans in den Vulnerability Response-Arbeitsbereichen finden Sie unter und Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.
- Befolgen Sie die unten aufgeführten Schritte, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

**Hinweis:**
Tenable.io unterstützt das erneute Scannen auf Agent-basierten Computern nicht.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Korrekturbesitzer, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. können Sie nach bestimmten Schwachstellen in Assets (Konfigurationselementen) in Ihren Umgebungen suchen. Sie können erneute Scans aus Datensätzen für angreifbare Elemente (AEs), Korrekturaufgaben (VUL), Drittanbietereinträgen (TPE) oder erkannten Elementen (SDI) aus Ihrer Now Platform -Instanz initiieren. Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen von Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.io Scan Credential Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.io -Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Die folgenden Informationen beschreiben die Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf in Ihrer Now Platform -Instanz anzeigen können:

- Mit der Administratorbenutzerrolle Tenable.io erstellte Anmeldeinformationen stehen Benutzern in allen Ihren Organisationen zur Verfügung.
- Mit der Benutzerrolle der Organisation Tenable.io erstellte Anmeldeinformationen sind nur für Benutzer innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in Now Platform importiert, es sei denn, sie werden mit dem Konto des Benutzers geteilt, der für die Verbindung mit der Instanz verwendet wird.

  Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.io.

- Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen vor dem Initiieren von erneuten Scans aktiviert werden. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Integrationen** > **Tenable.io-Integration von Scan-Anmeldeinformationen**.

  Standardmäßig sind die Integrationen von Vorlagen und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io -Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
  2. Suchen Sie in der angezeigten Liste die gewünschten Tenable.io Integrationsdatensätze.
  3. Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

Weitere Informationen zum Konfigurieren der Produkte Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-AssistentenTenable.io und Tenable.sc finden Sie unter [].

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformTenable.io auf angreifbare Elemente von [] initiieren.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von festen Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   **Hinweis:**
   Wenn Sie den Scanner Tenable.io verwenden, können Sie erneute Scans für VIs nur mit Tenable.io als Quelle initiieren. Vergewissern Sie sich, dass Tenable.io in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle nicht in der VI-Listenansicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol „ **Liste personalisieren** “ (Zahnradsymbol), und verwenden Sie den Slushbucket, um **Quelle** von **Verfügbar** zu **Ausgewählt**zu verschieben.

3. Navigieren Sie alternativ zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:



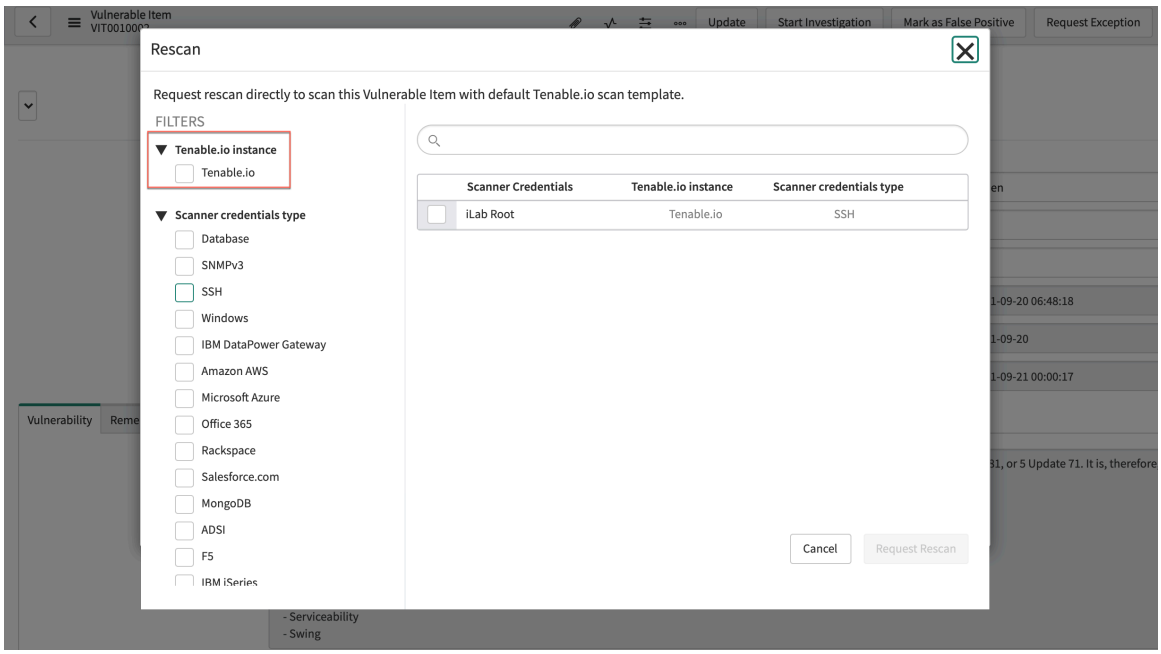
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In einem einzelnen VI-Datensatz muss sich die VI in einem anderen Status als **Geschlossen**befinden. Für mehrere VI-Datensätze müssen alle VIs aus dem Produkt Tenable.io stammen und sich in einem anderen Status als **Geschlossen**befinden.
- Für Korrekturaufgabendatensätze werden nur Korrekturaufgaben in einem anderen Status als **„Geschlossen"** unterstützt. Alle zugeordneten AEs müssen sich in einem anderen Status als „ **Geschlossen** " befinden und Tenable.io als Quelle verwenden.
- In einem TPE-Datensatz muss mindestens ein zugeordneter VI-Datensatz aus dem Produkt Tenable.io einen anderen Status als **Geschlossen**aufweisen.
- Bei Datensätzen für erkannte Elemente muss der Datensatz mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **Geschlossen**haben.
- In der Liste „Angreifbare Elemente" können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen links unten auf dem Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind die, die von der Tenable.io Scan Credential Integration importiert wurden.

5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   In der folgenden Abbildung wird eine Integrationsinstanz, Tenable.io, angezeigt. Wenn Sie mehr als eine Instanz Tenable.io haben, werden sie alle im Abschnitt Tenable.io im Formular angezeigt.




6. Klicken Sie **auf Erneutes Scannen anfordern**.

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird, und ein übergeordneter Scan-Datensatz wird erstellt. Der Status für alle untergeordneten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgaben-,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Details** anzeigen, um den Status des erneuten Scans anzuzeigen und alle anderen erneuten Scans anzuzeigen, die von einem bestimmten Datensatz aus gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Die untergeordneten Scans importieren Daten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden mehrere untergeordnete Scans in einem übergeordneten Scan-Datensatz angezeigt. Zum Beispiel beträgt die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, 1000. Wenn 1002 IPs für ein angreifbares Element vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt. Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens. Alle VIs, die in den Status „ **Geschlossen/** Behoben“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.io Integration behobener Schwachstellen importiert.

Bei Scans, bei denen ein Fehler auftritt, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von festen Schwachstellen initiiert haben.

### Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Tenable Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Sie Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, sie werden jedoch als ein CI in Ihrer CMDB gespeichert.

Beispielsweise können, wie in den folgenden Tabellen gezeigt, mehrere Assets (CIs) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche als einzelnes CI (CI 1) identifiziert und gespeichert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Standardmäßige IP-Suche und CI-Erstellung**

| Quelle | IP-Adresse | Netzwerk-ID | Konfigurationselement |
|---|---|---|---|
| Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 |

| Quelle | IP-Adresse | Repository_id | Konfigurationselement |
|---|---|---|---|
| Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 |

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse haben, damit Sie sie als unterschiedliche Assets identifizieren können. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die regelmäßige Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] vorhandenen CI-Datensätzen aus importierten Daten hinzu. Vorhandene von der IRE erstellte CIs werden ebenfalls aktualisiert. Die regelmäßige Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie die Aufgabe bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

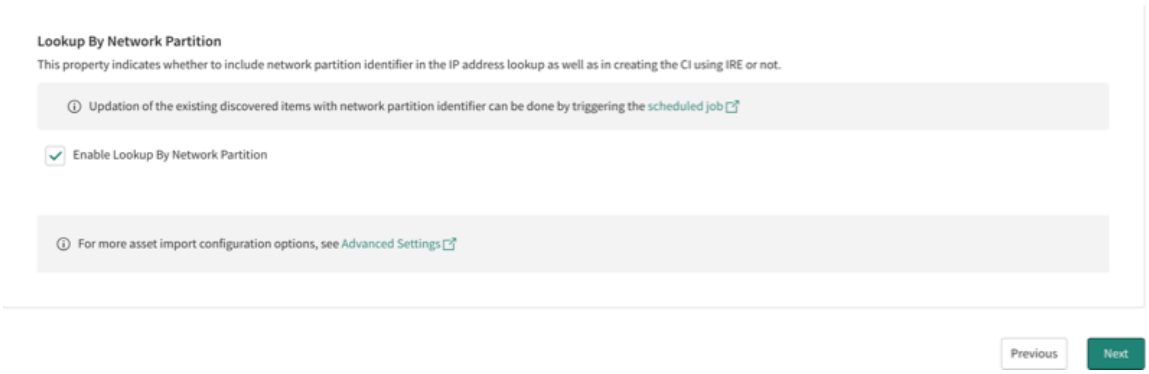
Wenn Sie ein Upgrade ab Version 14.0 von Vulnerability Response und Version 2.2 von Tenable Vulnerability Integration durchführen, wird CMDB CI Class Models (1.0.21.) unterstützt. Die Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Tenable.io Integrationen oder Tenable.sc Integrationen aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Checkbox aus dem **Suche nach Netzwerkpartition aktivieren** Abschnitt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Next (Weiter)**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID sind enthalten und aktualisieren vorhandene CIs oder erstellen CIs mit der nächsten geplanten Aufgabe.

**Attribut für Netzwerkpartitionsbezeichner, das in die IP-Suche und CI-Erstellung einbezogen wird**

| Quelle | IP-Adresse | NETWORK_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 | CI 2 |

| Quelle | IP-Adresse | REPOSITORY_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 | CI 2 |

Mit der nächsten geplanten Aufgabe beziehen die Suchregeln für IP-Adresse und unvollständige IP-Adressen-CI-Identifizierung das Attribut „Netzwerkpartitionsbezeichner“ automatisch für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc ein.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

### Importieren Sie Änderungen für die Integration von Tenable Vulnerability

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration von Tenable-Schwachstellen in der ServiceNow® Integration von Tenable-Schwachstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Aufgabensatz erfordert Codierung und fortgeschrittene Kenntnisse über Now Platform.

Befolgen Sie diese Schritte, um domänengetrennte Importe für die Integrationen von Tenable Vulnerabilities zu erstellen. Das folgende Beispiel bezieht sich auf die Tenable.io Open Vulnerabilities-Integration, aber dieser Inhalt gilt auch für die anderen Tenable-Integrationen.

### Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede Domäne, die Sie erstellen, einen Benutzer, und weisen Sie den Benutzer dieser Domäne zu.

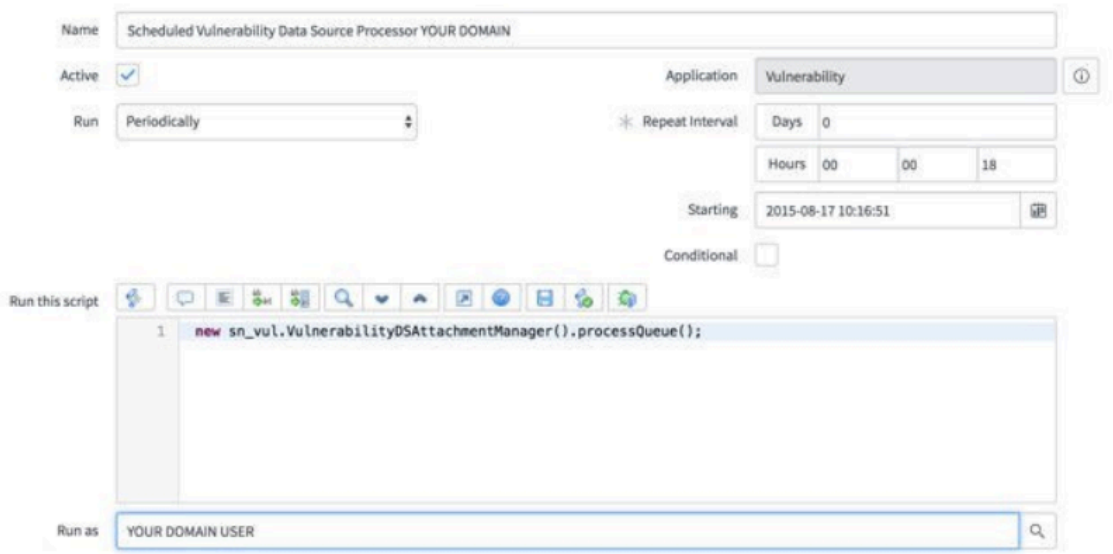
   Stellen Sie sich diesen Benutzer als run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration offener Schwachstellen
   Der Benutzer entspricht dem VR.System-Benutzer in der globalen Domäne und muss die folgenden Rollen haben: sn_vul.tenable_configure_integration, import_admin und sn_vul.vulnerability_write. Dieser Benutzer benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   **Hinweis:**
   Betrachten Sie diesen Benutzer als spezifisch für diese Rolle. Der Benutzer sollte keinen anderen Zweck haben
4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den Datenquellenprozessor für geplante Schwachstellen kopieren, der sich unter befindet **Systemdefinition** > **Geplante Aufgaben**.
5. Hängen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Benutzer run_as in den Benutzer, den Sie im vorherigen Schritt erstellt haben.

   **Hinweis:**
   Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Bearbeiten Sie die UI-Aktion Jetzt ausführen in der Tenable.io Open Vulnerabilities-Integration, um diesen Codeblock am Anfang der Datei hinzuzufügen.
   `//sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }`

   **Hinweis:**
   Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.

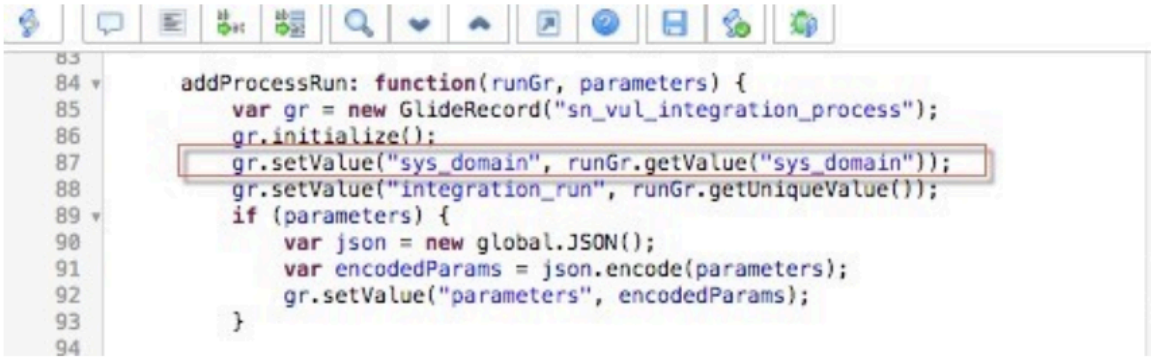
8. Bearbeiten Sie die VulnerabilityIntegrationUtils-Skripteinbindungsmethode addIntegrationRun, um den hervorgehobenen Code hinzuzufügen.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Bearbeiten Sie die VulnerabilityIntegrationUtils-Skripteinbindungsmethode addProcessRun, um den hervorgehobenen Code hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um den ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in Bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die VulnerabilityDSAttachmentManager-Skripteinbindungsmethode queueItem, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen queueItem, _getNext, _processQueueEntry-Funktion.

Sie sind bereit für domänengetrennte Hosterkennungsimporte.

Deaktivieren Sie Rechner vor dem Import

Befolgen Sie diese Schritte, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellenrechner verwenden, deaktivieren Sie am besten die Standardrechner zusätzlich zu den anderen, die Sie definiert haben. Schwachstellenrechner werden bei jedem Zugriff auf einen Datensatz eines angreifbaren Elements ausgeführt und können sich auf die Instanzleistung auswirken.

Erforderliche Rolle: sn_vul.vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Sicherheitsrisiko-Rechner**.
13. Öffnen Sie die Gruppe Schwachstellenauswirkung.
14. Öffnen Sie den Rechner für Punktzahl und servicebasierte Auswirkung.
15. Deaktivieren Sie das Feld Aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie vor dem ersten Import benachrichtigungsbasierte Business Rules

Befolgen Sie diese Schritte, um Benachrichtigungsbezogene Geschäftsregeln deaktivieren vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Business Rules viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Geschäftsregeln müssen geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
18. Suchen Sie nach Benachrichtigungen über betroffene CIs.
19. Öffnen Sie die Geschäftsregel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
    - Betroffene Kostenstellenbenachrichtigungen
    - Betroffene Gruppenbenachrichtigungen
    - Betroffene Standortbenachrichtigungen

**Hinweis:**
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Geschäftsregeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und die Leistung Ihrer Instanz beeinträchtigen.

Ändern Sie ein anfängliches Startdatum

Befolgen Sie diese Schritte, um ein anfängliches Startdatum zu ändern. Während der Installation mit dem Setup-Assistenten legen Sie ein anfängliches Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle gescannten und erkannten Schwachstellen seit diesem Zeitpunkt erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, ist das Feld Startzeit vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass eine große Datenmenge die Ratenbeschränkungen der Tenable-API überschreitet und Ausführungszeitüberschreitungen auslöst.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie auf **Jetzt** ausführen, um den Vorgang sofort auszuführen.

## Informationen zur Integration von [ Atlassian Jira mit Vulnerability Response

Die Integration von [ Atlassian Jira mit Vulnerability Response ermöglicht Ihnen die Nutzung verschiedener Tools für Problemnachverfolgung und agiles Management für die Nachverfolgung von Behebungsmaßnahmen für Schwachstellen.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Übersicht

ServiceNow® Vulnerability Response ist in Atlassian Jira integriert, um Probleme zu erstellen, die Schwachstellen entsprechen, und synchronisiert die Problementität in Jira und die Entität für angreifbare Elemente in Vulnerability Response bidirektional, um die neuesten Updates widerzuspiegeln. Schwachstellenmanager erfordern, dass in ServiceNow Vulnerability



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Response vorhandene angreifbare Elemente erstellt und Korrekturbenutzern (Entwicklern im Fall von Application Vulnerability Response) in ihrem bevorzugten Erfassungssystem und Problemverwaltungstool wie Atlassian Jirazugewiesen werden. Jeder Fortschritt, der für die Schwachstellen im Problemmanagement-Tool erzielt wird, sollte in ServiceNow Vulnerability Response aktualisiert werden, um für Schwachstellenmanager sichtbar zu sein. Darüber hinaus müssen alle Aktualisierungen, die von Schwachstellenmanagern in Vulnerability Response für angreifbare Elemente vorgenommen werden, auch an das Problemverwaltungstool weitergeleitet werden, um für Korrekturbenutzer transparent zu sein.

## Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Vulnerability Response | Versionshinweise zur Vulnerability Response-Integration |
| Vulnerability Response und Configuration Compliance für Container | Versionshinweise zu Container Vulnerability Response |
| Jira-Spoke | Versionshinweise zur Jira-Spoke |

## Jira Schwachstellenintegrationen

Um die Jira Schwachstellenintegration anzuzeigen, navigieren Sie zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren** .

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

### Vorbereitung der Jira Vulnerability Response -Integration

Eine erfolgreiche Jira Schwachstellenintegration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Jira Vulnerability Response -Integration setzt voraus, dass Sie mit dem Produkt und der API von Jira vertraut sind.

## Mit Agile Integration for Vulnerability Response und Jira Integration for Vulnerability Response installierte Komponenten

Bei Aktivierung der Plugins „Agile Integration for Vulnerability Response“ und „Jira Integration for Vulnerability Response“ werden mehrere Arten von Komponenten installiert, darunter Tabellen und Benutzerrollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Installierte Rollen

| Rollentitel [name] | Beschreibung |
|---|---|
| Agile-Tool-Administrator [sn_vul_agile.agile_tool_admin] | Ermöglicht das Erstellen einer Konfigurationsregel für Agile Management zum Erstellen oder Aktualisieren von Problemen. Erstellen Sie Regelkonfigurationen für Agile Management. |
| JIRA-Administrator [sn_vul_jira.admin] | Ermöglicht die Auswahl des Agile-Tools zum Erstellen von Problemen für die ausgewählte Entitätstabelle. |

### Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Agile-Tool-Konfiguration [sn_vul_agile_tool_rule_config] | Enthält Konfigurationsregeln zum Erstellen von Problemen auf der Agile-Plattform. |
| Agile-Tool-Feldzuordnung [sn_vul_agile_tool_field_mapping] | Enthält die Feldzuordnung der Konfigurationsregel. |
| Agile-Tool-Statuszuordnung [sn_vul_agile_tool_state_mapping] | Enthält die Statuszuordnung des Jira-Problemstatus mit dem Status „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“. |
| Agile-Tool-Manifest [sn_vul_agile_tool_manifest] | Enthält die Nutzlast für die Problemerstellung. |
| Agile-Tool-Datenressource [sn_vul_agile_tool_data_resource] | Enthält die Informationen zum erstellten Jira-Problem. |
| JIRA-Administrator [sn_vul_jira.admin] | Ermöglicht die Auswahl des Agile-Tools zum Erstellen von Problemen für die ausgewählte Entitätstabelle. |

### Installieren Sie Vulnerability Response Integration with Jira

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Jira ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Erforderliche Rolle: admin.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | • Jira Integration for Vulnerability Response erfordert die Anwendung Vulnerability Response.<br>• Stellen Sie für die aktuelle Version von Jira Integration for Vulnerability Response sicher, dass Sie die aktuelle Version von Vulnerability Response installiert haben. Weitere Informationen finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix und Release Schema Changes .<br>• Wenn die Anwendung nicht installiert und aktiviert ist, lesen Sie Vulnerability Response installieren. |
| Vergewissern Sie sich, dass das Plugin „Integration Hub“ installiert ist. | • Jira-Spoke erfordert Integration Hub.<br>• Informationen zur Installation von Integration Hub finden Sie unter KB1112383 .<br>• Weitere Informationen finden Sie unter Gesetzliche Zeitpläne – IntegrationHub – Übersicht . |
| Vergewissern Sie sich, dass die neueste Version von Jira Spoke installiert ist. | Weitere Informationen zur Installation von Jira-Spoke finden Sie unter KB0792632 . |
| Vergewissern Sie sich, dass Vulnerability Response Integration with Agile Management installiert ist. | Vulnerability Response Integration with Atlassian Jira erfordert diese Integration. |

## Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie die Jira Vulnerability Response -Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in [ ServiceNow Storenach der Anwendung Vulnerability Response integration with Jira.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Konfigurieren Sie Regeln in der Agile-Tool-Konfiguration

Jira Probleme werden auf der Plattform Jira erstellt, wenn die Datensätze, die im angreifbaren Anwendungselement, im angreifbaren Containerelement, in der Anwendungskorrekturaufgabe und in der Containerkorrekturaufgabe erstellt wurden, mit den in der Agile-Tool-Konfiguration erstellten Regeln übereinstimmen.

#### Vorbereitungen

Erforderliche Rollen: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin.

#### Prozedur

1. Navigieren zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren**.
2. Um eine neue Konfigurationsregel in der Agile Tool-Konfiguration zu erstellen, wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

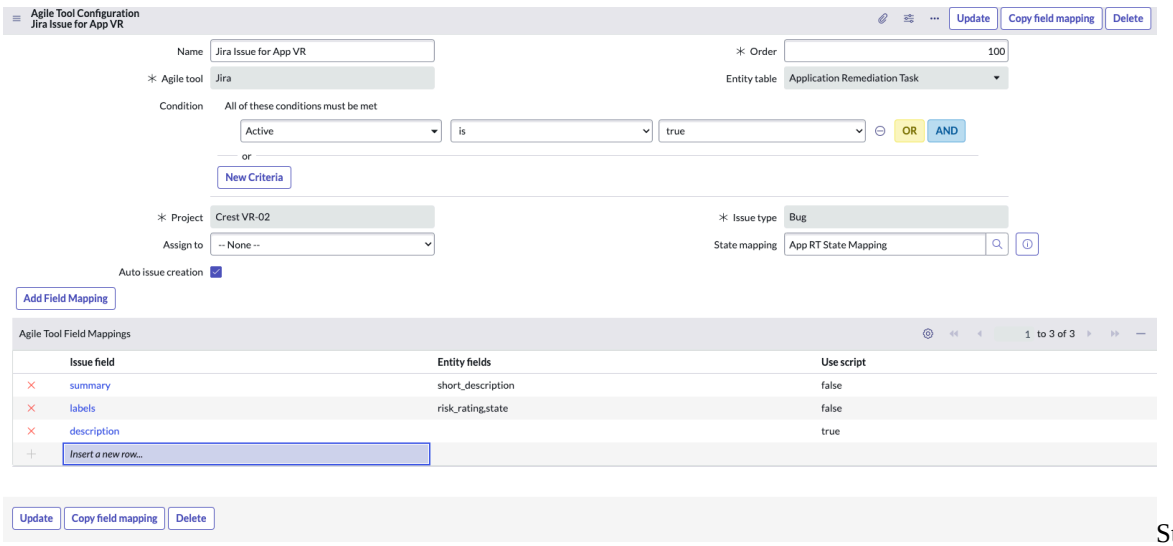
**Formular „Agile Tool-Konfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Agile-Tool-Konfiguration. |
| Reihenfolge | Reihenfolge der Agile-Tool-Konfiguration. |
| Agile-Tool | Das agile Tool zum Erstellen von Problemen auf der spezifischen agilen Plattform. |
| Entitätstabelle | Tabelle, auf die die Konfigurationsregel angewendet werden soll. |
| Bedingung | Filterbedingung für die ausgewählte Entitätstabelle, um Probleme auf der Agile-Plattform zu erstellen. |
| Automatische Problemerstellung | Die Konfigurationsregel wird nur abgefragt, wenn ein neuer Datensatz in der ausgewählten Entitätstabelle erstellt wird, wenn das Kontrollkästchen aktiviert ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Der Benutzer muss die Listenaktion verwenden, um Probleme für vorhandene Entitätsdatensätze zu erstellen. |
| Projekt | Projekt, in dem das Jira-Problem erstellt wird. |
| Problemtyp | Der Typ des Problems, das in einem bestimmten Projekt erstellt werden soll. |
| Zuweisen an | Der Beauftragte, dem das Problem bei der Erstellung des Problems zugewiesen werden soll. Um die Zuweisung der erstellten Probleme aufzuheben, wählen Sie „Keine“ aus. |
| Statuszuordnung | Die vorhandenen Statuszuordnungen aus der Tabelle „Agile Tool-Statuszuordnung“ oder Erstellen einer neuen Statuszuordnung zwischen dem Problemstatus in Agile Platform und den Status der ServiceNow -Entitätstabelle. |




werden bei der Installation der Anwendung Anwendungskorrekturaufgabe und Container-Korrekturaufgabe im Feld Entitätstabelle des Formulars „Konfiguration des Agile-Tools“ angezeigt.

4. Um das angreifbare Anwendungselement und das angreifbare Container-Element in der Auswahlliste Entitätstabelle hinzuzufügen, navigieren Sie zu **Systemeigenschaften** > **sn_vul_agile.tablesToShow**, und fügen Sie alle im Feld Wert hinzu.

### Formular für Systemeigenschaften

| Feld | Beschreibung |
|---|---|
| Auswahlmöglichkeiten | Durch Kommas getrennte Werte für eine Auswahlliste. |
| Wert | Legen Sie den gewünschten Wert für die Eigenschaft fest. Alle Eigenschaftswerte werden als Zeichenfolgen gespeichert. Behandeln Sie die Ergebnisse beim Abrufen von Eigenschaften über die gs.getProperty()-Methode als Zeichenfolgen. |

Automatische Übersetzung
Standardmäßig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Zum Beispiel gibt eine true\|false-Eigenschaft „true“ oder „false“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent. |

5. Wählen Sie den vorhandenen Statuszuordnungsdatensatz aus, oder erstellen Sie eine neue Statuszuordnung in der Agile Tool-Statuszuordnung.

**Formular „Agile-Tool-Statuszuordnung“.**

| Feld | Beschreibung |
|---|---|
| Name | Fügen Sie den eindeutigen Namen der Statuszuordnung ein. |
| Agile-Tool | Wählen Sie das Agile-Tool aus. |
| Entitätstabelle | Wählen Sie die Quelltabelle aus, für die die Statuszuordnung erstellt wird. |
| Projekt | Wählen Sie das Projekt aus, in dem der Status zugeordnet wird. |
| ServiceNow-Entitätsstatus | Wählen Sie den Status aus, den Sie dem Agile-Tool-Status zuordnen möchten. |
| Agile-Tool-Status | Wählen Sie aus den Status der angreifbaren Elemente den Status aus, den Sie zuordnen möchten. |

6. Klicken Sie auf „ **Speichern und Projekte abrufen** “, um die Projekte im Feld „Projekt“ Konfigurationsregel abzurufen und die Anmeldeinformationen des Agile-Tools zu validieren.

**Tipp:**
Sie können die Systemeigenschaft **projectsPageSize** festlegen, um eine bestimmte Anzahl von Projekten pro Seite abzurufen.

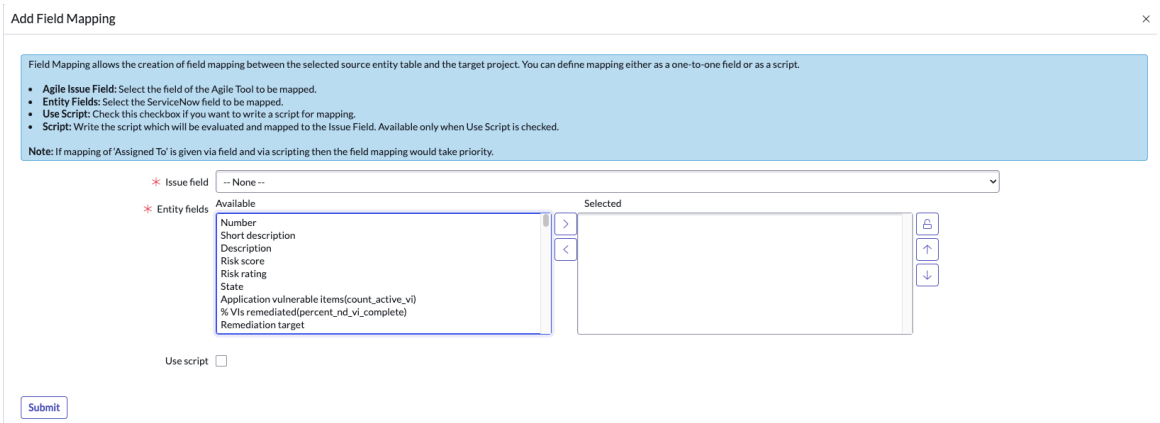
7. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.projectsPageSize**, und fügen Sie die Anzahl der Projekte hinzu, die pro Seite im Feld Wert für Jira Cloud abgerufen werden sollen.
8. Wählen Sie Projekt, Problemtyp und Zuweisen zu in der Konfigurationsregel aus, nachdem die Projekte abgerufen wurden.

   Die Standardfeldzuordnung wird in der eingebetteten Liste der Agile-Tool-Feldzuordnungen ausgefüllt. Standardmäßig werden die Felder Zusammenfassung und Beschreibung von Problemen zugeordnet.

9. Um andere Problemfelder den Feldern ServiceNow zuzuordnen, klicken Sie auf **Feldzuordnung hinzufügen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**

- Sie müssen nur Felder des Typs „Zeichenfolge“ und „Auswahl“ zuordnen.
- Stellen Sie sicher, dass alle Problem-Pflichtfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

**Formular „Agile-Tool-Statuszuordnung“.**

| Feld | Beschreibung |
|---|---|
| Problemfeld | Enthält die Problemfelder des aktuell ausgewählten Projekt- und Problemtyps in der Konfigurationsregel. |
| Entitätsfelder | Enthält die Felder der in der Konfigurationsregel ausgewählten Entitätstabelle. |
| Verwenden Sie das Skript | Wählen Sie diese Option aus, um das Skript für die Zuordnung der Problemfelder zu Entitätsfeldern zu verwenden. |
| Skript | Skript zum Zuordnen des Problemfelds zu Entitätsfeldern. |

10. Klicken Sie im Glide-Dialogfeld auf Absenden, um den **Feldzuordnungsdatensatz** in der Tabelle „Agile Tool-Feldzuordnungen“ zu übermitteln.

    **Hinweis:**
    Wenn Sie die Pflichtfelder nicht zuordnen, werden für diese Konfigurationsregel keine Probleme erstellt.

    Pflichtfelder werden oben im Formular „Agile Tool-Konfiguration“ angezeigt.
    Alle Feldzuordnungen für eine bestimmte Konfigurationsregel werden in der eingebetteten Liste der Tabelle „Agile Tool-Feldzuordnung“ in der Tabelle „Agile Tool-Konfiguration“ angezeigt.

11. Klicken Sie mit der rechten Maustaste in den Header, um Ihre Änderungen zu speichern.
    Der gespeicherte Datensatz ist in der Agile Tool-Konfigurationstabelle sichtbar. Wenn ein Datensatz im angreifbaren Anwendungselement erstellt wird, das angreifbare Container-Element, die Anwendungskorrekturaufgabe und die Container-Korrekturaufgabe mit einer Konfigurationsregel übereinstimmen, wird das Problem für den Datensatz gemäß der Zuordnung in der Konfigurationsregel erstellt.

12. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.cloudBulkSize**, und legen Sie die Anzahl der pro Batch zu erstellenden Probleme im Feld Wert fest.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Die maximale Anzahl von Problemen, die pro Batch in Jira Cloud erstellt werden können, beträgt 50.

Sie können die Batch-Größe für die Erstellung von Problemen in Jira Server festlegen.

13. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.onPremBulkIssue**, und legen Sie die Anzahl der pro Batch zu erstellenden Probleme im Feld **Wert** fest.
Sie können die Fehleranzahl auch im Feld Wert in der Systemeigenschaft festlegen, um die Datensätze in der Manifesttabelle zu verarbeiten und Jira-Probleme bis zu einer bestimmten Fehleranzahl zu erstellen.
14. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_agile.ManifestErrorCount**, und legen Sie die maximale Anzahl von Malen fest, bis zu der das Manifest mit Fehler verarbeitet werden soll.

### Erstellen Sie ein Agile-Problem manuell mithilfe der Listenaktion

Wenn eine Listenaktion „Jira-Problem erstellen“ ausgelöst wird, sollten Datensätze, die den Regelkonfigurationskriterien entsprechen, für „Jira-Problem erstellen“ berücksichtigt werden. Diese Datensätze sollten in die Tabelle „sn_vul_agile_tool_manifest“ mit der in der Konfigurationsregel ausgewählten Zuordnung erfasst werden.

#### Vorbereitungen
Erforderliche Rolle: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **Jira-**Problem erstellen.
Die ausgewählten Datensätze sollten die Feldzuordnung und Statuszuordnung des zugeordneten Agile-Tools berücksichtigen.
Die ausgewählten Datensätze, die die Konfigurationsregelbedingung erfüllen, sollten für die Erstellung von Jira-Problemen geeignet sein, und diese Datensätze sollten der Tabelle `sn_vul_agile_tool_manifest` hinzugefügt werden.

### Erstellen Sie ein Agile-Problem manuell mithilfe einer Formularaktion

Erstellen Sie ein Agile-Problem manuell mithilfe einer Formularaktion. Wenn der Datensatz mit einer Konfigurationsregelbedingung abgeglichen wird, wird ein Popup-Fenster mit Werten ausgefüllt, die in der Konfigurationsregel ausgewählt sind. Wenn keine Kriterien erfüllt sind, kann der Benutzer Werte für vordefinierte auswählen Felder.

#### Vorbereitungen
Stellen Sie sicher, dass alle obligatorischen Problemfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

Erforderliche Rollen: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie einen beliebigen Datensatz aus, um manuell ein Agile-Problem zu erstellen.
3. Wählen **Sie Agile-Problem erstellen aus**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Fügen Sie gültige Details für die genannten Felder ein.

   Wenn der Datensatz die Bedingung einer Konfigurationsregel erfüllt, müssen die folgenden Felder mit dem konfigurierten Wert ausgefüllt werden, und der Benutzer kann die Feldwerte ändern.

| Feld | Beschreibung |
|---|---|
| Projekt | Wählen Sie das Projekt aus, in dem das Jira-Problem erstellt wird. |
| Problemtyp | Wählen Sie den Typ des Problems aus, das in einem bestimmten Projekt erstellt werden soll. |
| Zuweisen an | Wählen Sie den Beauftragten aus, dem das Problem bei der Erstellung des Problems zugewiesen werden soll. |
| Feldzuordnung | Wählen Sie die Problemtypfelder des Agile-Tools aus, und fügen Sie die direkten Werte für das ausgewählte Feld ein. |

5. Wählen **Sie Agile-Problem erstellen** aus, um den Datensatz zu übermitteln.
   Nach dem Absenden des Datensatzes wird der Datensatzeintrag in der Tabelle „sn_vul_agile_tool_manifest“ erstellt.

### Synchronisieren Sie den Status des Problems Jira manuell

Aktualisieren Sie den Status des einzelnen Datensatzes, indem Sie im Kontextmenü des Formulars auf die Schaltfläche **„Agile-Status** synchronisieren“ klicken, und aktualisieren Sie den Status mehrerer Datensätze, indem Sie auf die **Listenaktion „Agile-Status** synchronisieren“ der Tabellen „Angreifbares Anwendungselement“, „Angreifbares Container-Element“ und „Korrekturaufgabe“ klicken Arbeitsbereich des Schwachstellenmanagers.

#### Vorbereitungen

Erforderliche Rollen: sn_vul_agile.agile_tool_admin oder sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

#### Warum und wann dieser Vorgang ausgeführt wird

Der Status wird von ServiceNow mit dem Agile-Tool synchronisiert, wenn der Entitätsstatus in ServiceNow geschlossen wird oder wenn eine Entität erneut geöffnet wird (z. B. Status ist „Offen“). Alle anderen Status werden vom Agile-Tool zu ServiceNowübertragen. Der Benutzer darf den Status nicht für die Datensätze synchronisieren, deren zugeordnete konfigurierte Regel keine Statuszuordnung hat, oder für die Probleme, die direkt aus der Formularaktion erstellt werden.

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Containerelemente**.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **Sync Agile Status**(Agile-Status synchronisieren).
   Status der Datensätze, für die bereits Probleme erstellt wurden, werden aktualisiert, wenn sich der Datensatz nicht im Status „Geschlossen“ befindet und die Statuszuordnung für die ausgewählten Datensätze in der Konfigurationsregel vorhanden ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie einen Datensatz, und der **Agile-Status synchronisieren** wird im Kontextmenü des Formulars angezeigt, wenn die folgenden Bedingungen erfüllt sind.
   - Für den Datensatz wird ein Problem erstellt, und der Datensatz befindet sich nicht im Status „Geschlossen“.
   - Statuszuordnung für den Datensatz vorhanden
4. Klicken Sie auf **Agile-Status** synchronisieren, um den Agile-Status mit dem zugeordneten Status zu synchronisieren.
   Sie können die Systemeigenschaft festlegen, um die Batch-Größe zum Abrufen des Problemstatus aus Jira festzulegen.
5. Navigieren Sie zu **Systemeigenschaft** > **sn_vul_jira.bulkIssueStatusSize**.
   - Für Jira Server die maximale Anzahl der zurückzugebenden Probleme (standardmäßig 50). Der maximal zulässige Wert wird durch die Jira-Eigenschaft „jira.search.views.default.max“ vorgegeben. Wenn Sie einen höheren Wert als diese Zahl angeben, werden Ihre Suchergebnisse abgeschnitten.
   - Wenn das Problem aus einer Formularaktion erstellt wird oder die konfigurierte Regel keine Statuszuordnung aufweist, werden diese Datensätze nicht für die Statussynchronisierung berücksichtigt.

### Konfigurieren Sie den Planer so, dass Probleme automatisch erstellt werden

Konfigurieren Sie den Scheduler so, dass er ausgeführt wird und automatisch die Probleme Jira für die Datensätze erstellt, die in der Tabelle sn_vul_agile_tool_manifest erstellt wurden.

#### Vorbereitungen
Erforderliche Rolle: admin oder schedule_admin.

#### Warum und wann dieser Vorgang ausgeführt wird
Alle Datensätze des angreifbaren Anwendungselements, des angreifbaren Container-Elements, der Anwendungskorrekturaufgabe und der Container-Korrekturaufgabe, die in der Tabelle „sn_vul_agile_manifest“ erstellt werden, werden bei der Problemerstellung Jira berücksichtigt.

#### Prozedur
1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Erstellt Jira-Probleme**.
2. Sie können die Felder Ausführen, Zeitzone und Zeit im geplanten Skript ändern.

**Formular „Geplante Skript-Ausführung“**

| Feld | Beschreibung |
|---|---|
| Run-Kosten | Zeitintervall für die Ausführung der geplanten Aufgabe:<br>○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt.<br>○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag ausgeführt.<br>○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag im Monat ausgeführt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Regelmäßig: Wird in einem festgelegten Wiederholungsintervall ausgeführt.<br>○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt.<br>○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt.<br>○ Geschäftskalender: Eintragsbeginn: Wird am Anfangseintrag für den im Feld ausgewählten Geschäftskalender ausgeführt. Eine regelmäßige Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt.<br>○ Geschäftskalender: Eintragsende – Wird für das Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge.<br>**Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset.<br>Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter Create a business calendar und Define business calendar entries . |
| Tag | Tag, an dem die geplante Aufgabe ausgeführt werden soll<br>○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus.<br><br>Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen. |
| Wiederholungsintervall | Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel:<br><br>○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein.<br>○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein.<br>○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein. |
| Zeit | Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag. |
| Zeitzone | Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus:<br><br>○ **Keine**: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die geplante Aufgabe erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben.<br>○ **Zeitzone des Systems verwenden**: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | wird. Die regelmäßige Aufgabe wird beispielsweise um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist und Sie 22:15 in das Feld Zeit eingeben.<br>○ Tatsächliche Zeitzone.<br>○ Beispielsweise wird die regelmäßige Aufgabe um 13:30 Uhr in der Zeitzone USA /Ost ausgeführt, wenn Sie USA/ Osten auswählen und 13:30 in das Feld Zeit eingeben. |
| run_as | Standardmäßig sollte „run_ as“ Feldwert leer sein. Der Benutzer kann den Wert als Domänenbenutzerwert festlegen, um ein Problem für eine bestimmte Domäne zu erstellen. |

### Konfigurieren Sie den Planer so, dass Probleme automatisch aktualisiert werden

Konfigurieren Sie den Scheduler so, dass die Probleme Jira für die Datensätze, die in der Tabelle sn_vul_agile_tool_manifest hinzugefügt wurden, automatisch aktualisiert werden.

**Vorbereitungen**
Erforderliche Rolle: admin oder schedule_admin.

**Warum und wann dieser Vorgang ausgeführt wird**
Alle Datensätze des angreifbaren Anwendungselements, des angreifbaren Container-Elements, der Anwendungskorrekturaufgabe und der Container-Korrekturaufgabe, die in der Tabelle „sn_vul_agile_manifest“ erstellt werden, werden für die Problemaktualisierung Jira berücksichtigt. Wenn der Datensatz geschlossen wird und Kommentare hinzugefügt werden, sollten diese Werte auch auf das zugehörige Problem Jira aktualisiert werden.

**Hinweis:**

- Die regelmäßige Aufgabe „Probleme aktualisieren“ aktualisiert den Status Jira nicht, wenn der Workflow für das ausgewählte Agile-Problemprojekt einen Benutzer daran hindert, den Status direkt aus einem anderen Status zu ändern.
- Wenn Sie einen Entitätsdatensatz mit zusätzlichen Kommentaren schließen, wird nur der letzte Kommentar zum Zeitpunkt der Aktualisierung berücksichtigt. Bei der nächsten Aktualisierung werden alle Kommentare dem zugehörigen Jirahinzugefügt.

**Prozedur**

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Aktualisiert Jira-Probleme**.
2. Sie können die Felder **Ausführen**, **Zeitzone**und **Zeit** im geplanten Skript ändern.

**Formular „Geplante Skript-Ausführung“**

| Feld | Beschreibung |
|---|---|
| Run-Kosten | Zeitintervall für die Ausführung der geplanten Aufgabe: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt<br>○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag ausgeführt.<br>○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag im Monat ausgeführt.<br>○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt<br>○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt<br>○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt<br>○ Geschäftskalender: Eintragsbeginn: Wird am Anfangseintrag für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Eine regelmäßige Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt.<br>○ Geschäftskalender: Eintragsende: Wird am Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge.<br>**Hinweis:**<br>Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset.<br>Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | unter und Create a business calendar Define business calendar entries . |
| Tag | Tag, an dem die geplante Aufgabe ausgeführt werden soll<br>○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus.<br>○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus.<br>Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen. |
| Wiederholungsintervall | Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel:<br>○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein.<br>○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein.<br>○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein. |
| Zeit | Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag. |
| Zeitzone | Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus:<br>○ Keine: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die geplante Aufgabe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | erstellt. Beispiel: Die regelmäßige Aufgabe wird um 16:45 Uhr ausgeführt. US/Pazifik-Zeit, wenn es sich um die zugewiesene Zeitzone des Benutzers handelt und Sie 16:45 in das Feld Zeit eingeben.<br>○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Beispiel: Die regelmäßige Aufgabe wird um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist und Sie 22:15 in das Feld Zeit eingeben.<br>○ Tatsächliche Zeitzone.<br>○ Beispiel: Die regelmäßige Aufgabe wird um 13:30 Uhr in der Zeitzone USA/Osten ausgeführt, wenn Sie USA/Osten auswählen und 13:30 in das Feld Zeit eingeben. |
| run_as | Standardmäßig ist der **Feldwert run_as** leer. Sie können den Wert auf einen Domänenbenutzer festlegen, um ein Problem für eine bestimmte Domäne zu erstellen. |

### Konfigurieren Sie den Planer, um den Status ServiceNow® automatisch mit [ Jira zu synchronisieren

Konfigurieren Sie den Scheduler, um den Status von Jira Problemen mit Anwendungsschwachstellenelementen, Container-Schwachstellenelementen und Aufgaben in der Tabelle „sn_vul_agile_manifest“ zu synchronisieren.

#### Vorbereitungen
Erforderliche Rolle: schedule_admin oder admin

#### Warum und wann dieser Vorgang ausgeführt wird
Der Planer wird automatisch gemäß dem konfigurierten Zeitplan ausgeführt. Der Status der Datensätze, die in den Tabellen „Angreifbares Element in Anwendung“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“ erstellt wurden und in Jira erstellte Probleme aufweisen, wird basierend auf dem aktuellen Status des Problems in der Plattform Jira ] aktualisiert Statuszuordnung in der Konfigurationsregel.

Alle in der Tabelle „sn_vul_agile_manifest“ erstellten Datensätze für angreifbares Anwendungselement, angreifbares Container-Element, Anwendungskorrekturaufgabe und Container-Korrektur werden bei der Problemerstellung Jira berücksichtigt.

#### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Synchronisierungsstatus**.
2. Sie können die Felder Ausführen, Zeitzone und Zeit im geplanten Skript ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Geplante Skript-Ausführung“

| Feld | Beschreibung |
|---|---|
| Run-Kosten | Zeitintervall für die Ausführung der geplanten Aufgabe:<br>○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt<br>○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag ausgeführt.<br>○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und an einem bestimmten Tag im Monat ausgeführt.<br>○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt<br>○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt<br>○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt<br>○ Geschäftskalender: Eintragsbeginn: Wird am Anfangseintrag für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Eine regelmäßige Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt.<br>○ Geschäftskalender: Eintragsende: Wird am Enddatum für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offsettyp und Offset.<br><br>Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter Create a business calendar und Define business calendar entries . |
| Tag | Tag, an dem die geplante Aufgabe ausgeführt werden soll<br><br>○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus.<br>○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus.<br><br>Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen. |
| Wiederholungsintervall | Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel:<br><br>○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein.<br>○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein.<br>○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Zeit | Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag. |
| Zeitzone | Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus:<br>○ -Keine-: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die regelmäßige Aufgabe erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben.<br>○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Beispiel: Die regelmäßige Aufgabe wird um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist und Sie 22:15 in das Feld Zeit eingeben.<br>○ Tatsächliche Zeitzone.<br>○ Beispiel: Die regelmäßige Aufgabe wird um 13:30 Uhr in der Zeitzone USA/Osten ausgeführt, wenn Sie USA/Osten auswählen und 13:30 in das Feld Zeit eingeben. |
| run_as | Standardmäßig ist der Feldwert run_as leer. Sie können den Wert als erforderlichen Wert des Domänenbenutzers festlegen, um ein Problem für eine bestimmte Domäne zu erstellen. |



## Erstellen Sie manuell eine Schwachstellenintegration

Schwachstellenintegrationen bieten Kunden und Lieferanten die Möglichkeit, die Schwachstellendaten in ihrer Instanz durch Abrufen von Daten aus externen Systemen und Lieferanten zu ergänzen. Diese Fähigkeit kann den Lebenszyklus der Schwachstellenkorrektur vereinfachen, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Ausführliche Anweisungen zum Erstellen von Integrationen finden Sie unter Definieren Sie eine neue Schwachstellenintegration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definieren Sie eine neue Schwachstellenintegration

Eine Schwachstellenintegration ruft Berichtsdaten aus einem Drittanbietersystem ab, im Allgemeinen, um Schwachstellendaten abzurufen und diese Berichtsdaten mithilfe von Datenquellen oder einem benutzerdefinierten Prozessor zu verarbeiten.

## Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

## Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

#### Schwachstellenintegration

| Feld | Beschreibung |
|---|---|
| Name | Ein beschreibender Name für die Integration. |
| Aktiv | Gibt an, ob die Integration aktiv ist. Wenn er für einen bestimmten Zeitraum nicht ausgeführt werden soll, können Sie die Parameter einrichten, die Sie verwenden möchten, und den Job deaktivieren. |
| Run-Kosten | Die Häufigkeit, mit der die Integration ausgeführt werden soll: Täglich, Wöchentlich, Regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf Ihrer Einstellung in diesem Feld angezeigt. |
| Tag | Der Tag, an dem die Integration ausgeführt werden soll.<br>○ Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, werden in diesem Feld die Wochentage angezeigt.<br>○ Wenn Sie im Feld **Ausführen** die Option **Monatlich** ausgewählt haben, werden in diesem Feld die Tage des Monats angezeigt. |
| Zeit | Zeitpunkt, zu dem die Integration beginnen soll. Dieses Feld wird nur angezeigt, wenn Sie im Feld **Ausführen**die Option **Täglich**, **Wöchentlich** oder **Monatlich** ausgewählt haben. |
| Anwendung | [Nur lesen] Der Name der Anwendung, für die diese Integration erstellt wurde. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Wiederholungsintervall | Wenn Sie **Regelmäßig** im Feld **Ausführen** ausgewählt haben, wird in diesem Feld die Anzahl der Tage und Stunden angezeigt, bevor die Integration erneut ausgeführt wird. |
| Wird gestartet | Wenn Sie **Regelmäßig** im Feld **Ausführen** ausgewählt haben, werden in diesem Feld die Datums- und Uhrzeitangaben angezeigt, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen. |
| Bedingt | Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten. |
| Bedingung | Wenn Sie das Kontrollkästchen Bedingt aktiviert haben, geben Sie hier die **Bedingungen** ein. |
| **Integrationsdetails** | |
| Integrationsskript | Wählen Sie die Skripteinbindung aus, die die VulnerabilityIntegrationBase erweitert, die ausgeführt werden soll, wenn die Integration ausgeführt wird. Dieses Skript definiert, wie Daten aus einem Drittanbietersystem abgerufen werden. |
| Integrationswerksskript | Geben Sie ein Skript ein, das definiert, wie die für das **Integrationsskript ausgewählte Skripteinbindung erstellt**wird. Weitere Informationen finden Sie unter Felder des Integrationswerksskripts.<br>**Hinweis:**<br>Skripts erfordern sowohl ServiceNow als auch Vulnerability Response. |
| Berichtsprozessorstrategie | Wählen Sie die Strategie aus, die Sie für die Verarbeitung der vom Integrationsskript zurückgegebenen Daten verwenden möchten, wenn die Integration ausgeführt wird.<br>○ Wählen Sie **Datenquellenanhang** aus, wenn Sie Daten mithilfe einer Datenquelle verarbeiten möchten.<br>○ Wählen Sie **Benutzerdefinierter Berichtsprozessor** aus, um einen benutzerdefinierten Prozessor auszuwählen. |
| Berichtsprozessor-Skript | Wenn Sie **Benutzerdefinierter Berichtsprozessor** im Feld **Berichtsprozessorstrategie** ausgewählt haben, wählen Sie die Skripteinbindung aus, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert, die ausgeführt werden soll, wenn die Integration ausgeführt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Dieses Skript definiert, wie die vom Integrationsskript zurückgegebenen Daten verarbeitet werden. |
| Prozessorwerksskript | Geben Sie ein Skript ein, das definiert, wie die für den **Berichtsprozessor ausgewählte Skripteinbindung erstellt**wird. |

4. Klicken Sie auf **Absenden**.

**Zugehörige Informationen**

Schwachstellenintegrationsskript

Berichtsprozessorstrategien

Felder des Integrationswerksskripts

Führen Sie eine Schwachstellenintegration manuell aus

### Schwachstellenintegrationsskript

Im Formular „Schwachstellenintegration“ verweist das Integrationsskript auf eine Skripteinbindung, die die VulnerabilityIntegrationBase-Skripteinbindung erweitert.

Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen, um die Mittel zu verwalten, mit denen Daten aus einer externen Datenquelle abgerufen werden. Jede Unterklasse von VulnerabilityIntegrationBase hat Zugriff auf kontextbezogene Informationen zum aufrufenden Prozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- integrationGr – ein GlideRecord des Schwachstellenintegrationsdatensatzes, der die Ausführung der Integration angefordert hat.
- integrationProcessGr – ein GlideRecord, der kontextbezogene Informationen für den aktuellen Prozess einer Integration bereitstellt.

Der Schwachstellenprozess enthält spezielle Parameter, die innerhalb einer Integration verwendet werden sollen, im Allgemeinen für Paginierungszwecke. Jeder Ausführung einer Schwachstellenintegration (als Schwachstellenintegrationsausführung bezeichnet) ist mindestens ein Schwachstellenintegrationsprozess zugeordnet. Für Multi-Call-Integrationen gibt es einen oder mehrere Schwachstellenintegrationsprozess-Datensätze für jede Schwachstellenintegrationsausführung.

Die Skripteinbindung muss eine Implementierung für die Methode `abrufenData()` bereitstellen und ein Objekt zurückgeben, das vom Berichtsprozessorskript verarbeitet wird. Das von abrufenData zurückgegebene Objekt ist ein einfaches Objekt mit Eigenschaften für Inhalt, Inhaltstyp und Erweiterung.

Hier ist ein Screenshot von VulnerabilityIntegrationBase.retrieveData():

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

Die Logik in abrufenData() hängt von der Schnittstelle ab, die zum Abrufen der Daten erforderlich ist. Wenn die Quelle der abgerufenen Daten beispielsweise eine REST-API hat, kann der Textkörper dieser Methode den REST-Endpunkt aufrufen, wahrscheinlich über RESTMessageV2. Die Antwort des Aufrufs kann dann analysiert oder in einen Anhang eingefügt werden, und die Details können zum Erstellen des Rückgabeobjekts verwendet werden.

### Einzelanruf-Integrationen

Einzelaufruf-Integrationsskripts (einzelne Seite) sind die einfachsten Arten von Integrationen. Sie benötigen einen Aufruf, häufig an eine externe Datenquelle, um Daten abzurufen. Nur abrufenData() muss für Einzelseiten-/Einzelaufruf-Integrationen implementiert werden.

Es folgt ein Beispiel, das ein einfaches Einzelaufruf-Integrationsskript veranschaulicht. Er erstellt eine RESTMessageV2 und führt sie aus. Anschließend wird ein Objekt zurückgegeben, das den Antworttext als Inhalt verwendet, zusammen mit einem angenommenen contentType und einer Erweiterung.

### Einzelaufruf-Integrationsskript

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

### Integrationen mit mehreren Anrufen

Integrationsskripts mit mehreren Aufrufen (oder mehreren Seiten) sind etwas komplizierter. Sie erfordern mehrere Aufrufe einer Datenquelle, um Daten abzurufen.

Wie bei einer Einzelaufruf-Integration muss auch bei einer Mehrfachaufruf-Integration „retrieData()“ implementiert sein. Im Textkörper von abrufenData() verwendet die Integration die Methoden hasMoreData() und setNextRunParameters(), die von VulnerabilityIntegrationBase bereitgestellt werden.

Die Methode hasMoreData() akzeptiert einen einzelnen booleschen Wert, der den VulnerabilityIntegrationController anweist, weitere Prozesse einzufügen, um weitere Daten



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abzurufen. Bei der Übergabe von „true“ an hasMoreData() wird setNextRunParameters() aufgerufen, um den Kontext für den nächsten Prozess bereitzustellen.

Die setNextRunParameters()-Methode akzeptiert ein einzelnes Objekt, das Kontextinformationen bereitstellt, die beim nächsten Aufruf von abrufenData() verwendet werden sollen. Dieses Objekt wird verwendet, um den Status an nachfolgende Aufrufe von abrufenData() zu übergeben. Ein Beispiel für einen Anwendungsfall ist die Übergabe eines Objekts, das die aktuelle Seitenzahl und Seitengröße angibt, an einen Webservice.

Bei Integrationen mit mehreren Aufrufen überprüft jeder Aufruf von abrufenData() zuerst die aktuellen Prozessparameter. Die Methode _getProcessParameters() wird für alle VulnerabilityIntegrationBase bereitgestellt, um die vom vorherigen Prozess festgelegten Parameter abzurufen. Wenn keine Parameter vorhanden sind, weist dies darauf hin, dass es sich um den ersten Prozess handelt.

Nachfolgend sehen Sie einen Screenshot eines Beispielskripts für die Integration mehrerer Anrufe. Dieses Skript erweitert das Beispiel der Einzelaufruf-Integration und demonstriert Aufrufe an einen REST-Endpunkt mit grundlegender Paginierungsunterstützung. Es zeigt, wie Sie eine einzelne Seite mit Daten abrufen, erkennen, dass weitere Daten abzurufen sind, und dann dem nächsten Prozess mitteilen, welche Seite abgerufen werden soll.

**Skript für Mehrfachaufruf-Integration**

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

### Anhänge als abrufenData()- Rückgabewerte

Manchmal ist es vorzuziehen, einen Anhang von abrufenData() zurückzugeben. Die Logik zum Erstellen und/oder Abrufen eines Anhangs ist spezifisch für die Implementierung, aber nachdem der Anhang bekannt ist, können seine Informationen zurückgegeben werden.

Um einen Anhang bereitzustellen, gibt abrufenData() ein Objekt zurück wie:

```
{
    contents: "attachment-sys-id",
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    contentType: "sys_attachment"
}
```

Es folgt ein Beispiel, das das vorherige Beispielerweitert, aber den Antworttext der REST-Nachricht im Datensatz des Integrationsprozesses speichert. Anschließend wird dieser Anhangsbezeichner als Inhalt des Rückgabeobjekts zurückgegeben.

**Anhang von abrufenData zurückgeben**

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

### Berichtsprozessorstrategien

Das Feld **Berichtsprozessorstrategie** im Formular „Schwachstellenintegration“ wird verwendet, um die Methode zur Verarbeitung der vom Schwachstellenintegrationsskript zurückgegebenen Daten auszuwählen, wenn der Schwachstellenintegrationsprozess ausgeführt wird.

Der Standardwert ist **Datenquellenanhang**. Diese Methode ist die Baselineimplementierung, die die abgerufenen Daten an eine Datenquelle weiterleitet, die in das System importiert werden soll. Wenn Sie **Benutzerdefinierter Berichtsprozessor** auswählen, können Sie ein benutzerdefiniertes Prozessorskript für die Verarbeitung der Daten auswählen.

### Verwenden Sie die Berichtsprozessorstrategie für Datenquellenanhänge

Die Berichtsprozessorstrategie „Datenquellenanhang“ wird verwendet, um vom Integrationsskript abgerufene Daten an konfigurierte Datenquellen zu übergeben.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen** und erstellen Sie eine neue Integration.
2. **Wählen Sie im Feld Berichtsprozessorstrategie** die Option **Datenquellenanhang**aus.
3. Klicken Sie mit der rechten Maustaste in den Formular-Header, und klicken Sie auf **Speichern**.
4. Klicken Sie in der zugehörigen Liste **„Datenquellen für Schwachstellenintegration** “ auf **Neu**.
5. Definieren Sie die zu verwendende Datenquelle.
6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 4 bis 6, wenn Sie weitere Datenquellen benötigen.
   Stellen Sie sicher, dass Sie die Reihenfolge, in der die mehreren Datenquellen Informationen senden, im Feld **Reihenfolge** angeben.
8. Klicken Sie auf **Aktualisieren**.

### Über benutzerdefinierte Berichtsprozessorskripts

Im Formular „Integration von Schwachstellen“ verweist der Berichtsprozessor auf eine Skripteinbindung, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert. Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen und definiert die Mittel, mit denen die vom Integrationsskript zurückgegebenen Daten verarbeitet werden.

Jede Unterklasse von VulnerabilityReportProcessorBase hat Zugriff auf kontextbezogene Informationen zum aufrufenden Prozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- integrationGr – ein GlideRecord des Datensatzes der Schwachstellenintegration, der die Ausführung der Integration angefordert hat.
- integrationProcessGr – GlideRecord des Schwachstellenprozesses, der kontextbezogene Informationen für den aktuellen Prozess einer Integration bereitstellt.

Die Skripteinbindung muss eine Implementierung für die `processReport()`- Methode bereitstellen. Das an processReport() übergebene Objekt ist das von abrufenData zurückgegebene Objekt und als solches ein einfaches Objekt mit Eigenschaften für Inhalt, Inhaltstyp und Erweiterung. Die tatsächliche Logik in processReport() ist spezifisch für die Implementierung und abhängig von den bereitgestellten Berichtsdaten.

Hier ist ein Screenshot von VulnerabilityReportProcessorBase.processReport():

#### Benutzerdefiniertes Berichtsprozessorskript

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Felder des Integrationswerksskripts

Das Formular „Integration von Schwachstellen“ enthält das Integration Factory-Skript und, wenn die **Berichtsprozessorstrategie Benutzerdefinierter Berichtsprozessor** ausgewählt ist, das Factory-Skript Prozessor. Diese Felder werden verwendet, um die Logik bereitzustellen, um das durch die Skripteinbindungsreferenzfelder, das Integrationsskript und den Berichtsprozessor definierte Objekt tatsächlich zu instanziieren.

Wenn die Skripteinbindung ausgewählt ist, werden beide Felder vorab mit einem Konstruktoraufruf ohne Argumente ausgefüllt. Oft reicht dies aus, aber es kann Fälle geben, in denen mehr Logik erforderlich ist, um das Skriptobjekt zu instanziieren.

Der integrationProcessGr-Datensatz ist für die werkseitigen Skriptfelder verfügbar, sodass prozessspezifische Informationen nach Bedarf verwendet werden können.

### Führen Sie eine Schwachstellenintegration manuell aus

Eine Schwachstellenintegration ist so konfiguriert, dass sie nach Zeitplan ausgeführt wird. Sie können sie jedoch bei Bedarf manuell ausführen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen**.
2. Öffnen Sie die Integration, die Sie ausführen möchten.
3. Klicken Sie auf **Jetzt ausführen**.

## Manuelle Erfassung von Schwachstellen

Erfassen Sie Schwachstellen manuell in der Anwendung Vulnerability Response, damit Sie sie schnell beheben können, ohne auf die Scanner-Ergebnisse warten zu müssen.

Scanner von Drittanbietern wie Rapid7 helfen beim Importieren von Schwachstellendaten in Vulnerability Response und verarbeiten die Daten, um die Ergebnisse zu melden. Mit der Integration der manuellen Erfassung können Sie die Schwachstellen proaktiv erfassen und beheben, anstatt darauf zu warten, dass Scanner die gefährdeten Assets melden. Die manuelle Erfassung von Schwachstellen schützt die Assets effektiv vor unbekannten Bedrohungen wie Zero-Day-Exploits.

## Manuelle Erfassung von Schwachstellen

Sie können die Schwachstellendaten importieren, indem Sie eine Vorlage in den folgenden Dateiformaten hochladen:

- Excel
- Kommagetrennter Wert (CSV)

Um auf die Vorlage zuzugreifen und sie herunterzuladen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung angreifbarer Elemente** > **Datei hochladen – UI**.

Stellen Sie sicher, dass Sie beim Ausfüllen der Datensätze in der Vorlage die folgenden wichtigen Punkte beachten:

- Machen Sie keine Tippfehler in den Datensätzen der Spalte „Schweregrad/Status“. Bei einem Tippfehler wird der Datensatz übersprungen.
- Ändern Sie die Spaltennamen nicht.
- Platzieren Sie Spaltennamen nur in der ersten Zeile.
- Ändern Sie nicht die Reihenfolge der Blätter in der Excel-Vorlage. Die Schwachstellendaten müssen immer im zweiten Blatt vorhanden sein.
- Fügen Sie Schwachstellendetails nur dem Blatt „Manuelle Erkennungen eingeben“ hinzu.
- Verwenden Sie keine anderen Zeichen als alphanumerische Zeichen und Sonderzeichen wie Bindestrich (-), Punkt (.), Pluszeichen (+), Unterstrich (_), Leerzeichen, Klammern „(“ „)“ und At-Symbol (@). Dateiname.

Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.

## Integrationen der manuellen Erfassung

Die Integration wird ausgelöst, wenn eine Datei hochgeladen wird. Basierend auf dem Typ der hochgeladenen Datei wird die zugehörige Integration ausgelöst.

Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung angreifbarer Elemente** > **Integrationen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Basissystem-Integrationen für die manuelle Erfassung sind standardmäßig verfügbar.

### Integrationen

| Integrationstyp | Beschreibung |
|---|---|
| Manuelle Erfassung Excel-Integration | Ruft Daten ab, indem die neueste Excel-Datei aus der Tabelle „Schwachstellen-Erfassungs-Push-Warteschlange“ abgerufen wird, und kopiert den Anhang in die entsprechende Integrationsausführung. |
| CSV-Integration für manuelle Erfassung | Ruft Daten ab, indem die neueste CSV-Datei aus der Tabelle „Schwachstellen-Erfassungs-Push-Warteschlange“ abgerufen wird, und kopiert den Anhang in die entsprechende Integrationsausführung. |

Die Drittparteiintegration „Manuelle Erfassung“ erstellt standardmäßig eine Integrationsinstanz mit den folgenden beiden Integrationsinstanzparametern:

- max_input_records: Definiert die Anzahl der Datensätze, die in der Vorlage erstellt werden können. Wenn Sie mehr Datensätze hinzufügen, als in diesem Parameter angegeben sind, werden die zusätzlichen Datensätze übersprungen. Die Anzahl der Datensätze kann in der Spalte Wert aktualisiert werden. Die empfohlene Anzahl von Datensatzerstellungen in der Vorlage beträgt 1000. Alles über diesem Wert kann zu Leistungsproblemen führen.
- insert_fixed: Importiert behobene Schwachstellenerkennungen.

Um die Parameter der Integrationsinstanz anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung angreifbarer Elemente** > **Integrationen** und klicken Sie auf die Quellinstanz einer beliebigen Integration. Alternativ können Sie zu navigieren **Alle** > **Vulnerability Response** > **Integrationsinstanzen** und klicken Sie auf **Manuelle Erfassung**.

### Erfassen Sie Schwachstellen manuell

Erfassen Sie Schwachstellen manuell, indem Sie eine Vorlage mit Schwachstellendaten hochladen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**.
2. Klicken Sie auf die Excel- oder CSV-Links, und laden Sie die Vorlage im entsprechenden Format herunter.
3. Geben Sie in der Vorlage die Schwachstellendaten in die Datensätze ein.
   Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.
4. Klicken Sie **auf Datei importieren**, und laden Sie die aktualisierte Vorlage hoch.
5. Klicken Sie auf **Absenden**.
   Die Seite Push-Warteschlangen für Schwachstellenintegration wird angezeigt. Sie können die Liste der Integrationsinstanzen, den Status der Integrationsausführungen und Protokollnotizen nach Abschluss der Integrationsausführung anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Navigieren Sie nach dem Hochladen der Datei zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**. Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist.

#### Überprüfen Sie die Ausführung der manuellen Integration

Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist. Zeigen Sie die Anzahl der einzelnen Erkennungen und der angreifbaren Elemente (VIs) an, die aufgrund der Integrationsausführung erstellt oder aktualisiert wurden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**.
2. Klicken Sie auf den Namen der Integration basierend auf dem hochgeladenen Dateityp.
3. Klicken Sie auf die Registerkarte Ausführungen der **Schwachstellenintegration**.
4. Klicken Sie auf die Ausführungsnummer der Integration.
5. **Klicken** Sie auf die Registerkarte Elemente.
6. Überprüfen Sie die Informationen auf der **Registerkarte** Elemente.

#### Registerkarte „Elemente“.

| Registerkarte/Feld | Beschreibung |
|---|---|
| Registerkarte „Elemente“. | Zeigt die Gesamtzahl der importierten VIs an. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte „Erkennungen“ aufgeführten Zahlen hinzufügen. |
| Neue Elemente | Zeigt die Anzahl der angreifbaren Elemente an, die aus dieser Integrationsausführung erstellt wurden. |
| Importierte Elemente | Zeigt die Summe aller Felder in diesem Abschnitt an. |
| Doppelte Einträge | Zeigt doppelte Elemente an. Dieses Feld wird nicht mehr ausgefüllt. |
| Aktualisierte Elemente | Zeigt an, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt. |
| Unveränderte Elemente | Zeigt während der Integrationsausführung gefundene angreifbare Elemente an, die in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Nachdem Sie sich vergewissert haben, dass die Integrationsausführung erfolgreich ist, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**. Überprüfen Sie, ob fehlerhafte Datensätze aus den Notizen vorhanden sind.

## Konfigurieren Sie manuelle Erkennungen für automatisches Schließen

Aktivieren Sie das automatische Schließen manueller Erkennungen, um veraltete manuelle Erkennungen automatisch zu schließen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**.
2. Klicken Sie **auf Konfiguration für automatisches Schließen ändern**.
3. Klicken Sie auf die Registerkarte **Manuelle Erkennungen**.
4. Stellen Sie sicher, dass das Kontrollkästchen **Manuelle Erkennungen automatisch schließen aktiviert** ist.
5. Geben Sie im Feld **Zuletzt gefundene manuelle Erkennungen (vor Tagen)** die Anzahl der Tage ein, nach denen die manuellen Erkennungen geschlossen werden sollen.
   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben.

## Überprüfen Sie den Upload-Status

Überprüfen Sie, ob die Ausführung der Schwachstellenintegration erfolgreich oder teilweise erfolgreich war oder fehlgeschlagen ist.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**.
2. Überprüfen Sie in der Tabelle „Schwachstellenintegration – Veröffentlichungswarteschlangen“ die Uhrzeit des Uploads und den Status des Uploads in den Spalten Erstellt und Status.
3. **Wahlweise:** Zeigen Sie im Feld **Notizen** den Grund für den Fehler an.

## Vorlage für die manuelle Erfassung von Schwachstellen

Die Vorlage enthält Spalten, die mit Schwachstellen- und Konfigurationselementdaten (CI) gefüllt werden müssen. Nachdem die Vorlage ausgefüllt und hochgeladen wurde, werden die Daten verarbeitet.

## Anweisungen zum Ausfüllen der Vorlage

Befolgen Sie die Anweisungen in der folgenden Tabelle, um die Details in die Vorlage einzugeben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorlagenanweisungen

| Spalte | Erforderlich/ optional? | Zeichenfolgenlänge (max.)/ Gültige Werte | Beschreibung |
|---|---|---|---|
| Asset-ID | Optional | 255 | Universally Unique Identifier (UUID) oder Asset-ID. Dies kann der von einem Scanner generierte Wert sein. |
| Geben Sie Informationen in mindestens eine der folgenden fünf Spalten ein: | | | |
| MAC-Adresse | Erforderlich | 24 | Host- oder Asset-Informationen. Die Kombination aller angegebenen Werte muss für ein Asset eindeutig sein. |
| FQDN | Erforderlich | 255 | |
| NETBIOS | Erforderlich | 255 | |
| IP-Adresse | Erforderlich | 255 | |
| Hostname | Erforderlich | 255 | |
| Die verbleibenden Spalten sind nicht voneinander abhängig. | | | |
| Schwachstellen-ID | Erforderlich | 255 | Stellt eine Schwachstelle in der National Vulnerability Database (NVD) oder eine ID dar, die von einem Drittanbieter-Scanner zurückgegeben wird. |
| Schwachstellenzusammenfassung | Optional | 512 | Kurze Beschreibung der Schwachstelle.<br><br>Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist. |
| Schweregrad | Optional | kritisch, hoch, mittel, niedrig, keine | Schweregrad der Schwachstelle.<br><br>Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist. Wenn der Datensatz leer ist, wird er standardmäßig als kritisch betrachtet. |
| Port | Optional | Nicht zutreffend | Port, an dem die Schwachstelle erkannt wird<br><br>Der Wert muss eine gültige Ganzzahl sein. Bei einer ungültigen Eingabe wird der Datensatz übersprungen. |
| Protokoll | Optional | 40 | Typ des verwendeten Netzwerkprotokolls. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vorlagenanweisungen (Fortsetzung)**

| Spalte | Erforderlich/ optional? | Zeichenfolgenlänge (max.)/ Gültige Werte | Beschreibung |
|---|---|---|---|
| Nachweis | Optional | 4000 | Stellt den Speicherort oder Systempfad der Schwachstelle dar. |
| Status | Optional | offen, behoben | Status der Erkennung.<br><br>Wenn der Datensatz leer ist, wird er standardmäßig als offen betrachtet. |

## Vulnerability Response Arbeitsbereiche

Vulnerability Response Workspaces bieten eine konsolidierte Ansicht der Funktionen, mit der Sie mehrere Aufgaben im selben Bereich ausführen können, um die Produktivität zu steigern und Zeit zu sparen. Vulnerability Manager und IT Remediation Workspaces unterstützen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Configuration Compliance.

### Die Arbeitsbereiche Schwachstellenmanager, IT-Korrektur und Schwachstellenbewertung

**Arbeitsbereich des Schwachstellenmanagers**

Schützen Sie als Schwachstellenanalyst oder Administrator die Assets Ihres Unternehmens vor Malware und böswilligen Angriffen. Von einem einzigen Arbeitsbereich in Ihrem Now Platform®aus können Sie mit der Anwendung Vulnerability Response zusammen mit aktuellen Schwachstellendaten, die aus Schwachstellenbibliotheken und Scanner-Datenanwendungen von Drittanbietern in Ihre Instanz importiert wurden, kritische Schwachstellen identifizieren, priorisieren und Listen von Korrekturaufgaben über senden an die IT, damit ihre Spezialisten darauf reagieren können.

**Arbeitsbereich für IT-Korrekturen**

Verwenden Sie als IT-Spezialist Listen oder Korrekturaufgaben (Remediation Tasks, RT), die von Schwachstellenmanagern gesendet werden, um kritische Schwachstellen zu überwachen und zu beheben, die Ihnen oder Ihren Gruppen zugewiesen sind. Reparieren Sie Gruppen angreifbarer Elemente mit Patches, Lösungen, erneuten Schwachstellenprüfungen, Change-Anforderungen, Ausnahmen und anderen Tools, um angreifbare Elemente von einem zentralen Ort aus zu beheben.

**Arbeitsbereich der Schwachstellenbewertung**

Führen Sie als Schwachstellen-Event-Manager eine Gefährdungsbewertung durch und verwalten Sie proaktiv kritische Schwachstellen-Events, insbesondere während kritischer Schwachstellen-Events wie Zero-Day-Events.

### Vulnerability Response Arbeitsbereiche suchen

Wenn Sie sich zum ersten Mal bei Ihrer Now Platform® -Instanz anmelden, wird die Homepage in der Next Experience-UI angezeigt. Navigieren Sie in Arbeitsbereichen zu **Vulnerability Manager Workspace**, **IT Remediation Workspace** und **Vulnerability AssessmentWorkspace**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen:

- Vulnerability Manager Workspace: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin
- IT-Korrekturarbeitsbereich: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

## Neue Funktionen

Die Arbeitsbereiche Vulnerability Response enthalten die folgenden Funktionen und Erweiterungen.

- Sie können die Dashboards „Schwachstellenmanagement“, „Schwachstellenmanagement (PA)“, „Schwachstellengenehmigungen“, „CISO“, „Container Vulnerability Management Übersicht“, „Anwendungsschwachstellenmanagement-Dashboard“, „Unified Vulnerability Response“ und „Integrität“ in der Next Experience-UI auf der Seite „Dashboards“ des Arbeitsbereichs „Schwachstellenmanager“ anzeigen. Weitere Informationen finden Sie unter Dashboardübersicht.
- Sie können das Dashboard „Schwachstellenkorrektur“ in der Next Experience-UI auf der Seite „Dashboards“ des IT-Korrekturarbeitsbereichs anzeigen. Weitere Informationen finden Sie unter Dashboardübersicht.
- Teilen Sie die Korrekturaufgaben der Testergebnisse in Vulnerability Manager Workspace und IT Remediation Workspace auf. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und Datensätze aus Vulnerability Manager Workspace an bzw. Teilen Sie eine Korrekturaufgabe in auf IT Remediation Workspace.
- Sie können die Richtlinienausnahmen für angreifbare Containerelemente (CVITs), Testergebnisgruppen aus dem Schwachstellenmanager und IT-Korrekturarbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und Datensätze aus Vulnerability Manager Workspace an bzw. Ausnahme mit GRC: Policy and Compliance Management in IT Remediation Workspaceanfordern.
- Sie können der Bibliothek für Ausgleichskontrollen Ausgleichskontrollen hinzufügen. Weitere Informationen finden Sie unter Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu.
- Sie können eine Risikominderung für ein angreifbares Host-Element und eine Korrekturaufgabe über den IT-Korrekturarbeitsbereich anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Risikominderung in an IT Remediation Workspace.

Weitere Informationen finden Sie unter Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

Weitere Informationen zur Versionskompatibilität mit den Familien-Releases finden Sie im Artikel KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes in der HI Knowledge Base.

## Bevor Sie beginnen

Bevor Sie die Arbeitsbereiche verwenden können:

- Sie müssen einige Konfigurationsaufgaben ausführen. Weitere Informationen finden Sie unter Konfigurieren Sie die Vulnerability Response Arbeitsbereiche.
- Überprüfen Sie wichtige Informationen zu Updates für Korrekturaufgaben, Regeln für Korrekturaufgaben sowie wichtige Begriffe und Konzepte zu den Arbeitsbereichen in Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Regeln für Korrekturaufgaben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Patchen Sie die Orchestration mit den Vulnerability Response -Arbeitsbereichen

Sie können Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets mit Patch-Orchestration mit Vulnerability Responseverwalten.

## Patchen Sie die Orchestration in den Arbeitsbereichen

Bei der Patch-Orchestrierung mit der Anwendung Vulnerability Response werden geplante Importe aus Lösungsintegrationen von Drittanbietern, Patch-Anbietern und Schwachstellenscannern verwendet.

Die Patch-Orchestration mit der Anwendung Vulnerability Response wird sowohl in der klassischen -Umgebung als auch in den Arbeitsbereichen von Vulnerability Response unterstützt. Korrelierte Daten werden zusammengefasst und sowohl in den Arbeitsbereichen als auch in der klassischen Umgebung angezeigt. Eine Übersicht über die Funktionen, Anforderungen und Informationen zur Patch-Orchestrierung in der klassischen Umgebung finden Sie unter Patch-Orchestration mit Vulnerability Response.

- Weitere Informationen zu den unterstützten Integrationen mit Patch-Anbietern finden Sie unter Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Response und Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM.
- Informationen zum Planen von Patches aus Datensätzen in den Arbeitsbereichen finden Sie unter Planen von Patches mit der Microsoft SCCM-Integration mit Vulnerability Response und Planen Sie Patches mit der Vulnerability Response Patch Orchestration-Integration HCL BigFix.

## Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch Orchestration-Integration erforderlich sind

Zum Anzeigen von Patch-Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Responsesind die folgenden Anwendungen erforderlich. Alle aufgeführten Anwendungen sind im ServiceNow® Storeverfügbar. Einige Anwendungen erfordern separate Abonnements. Weitere Informationen finden Sie unter Patch-Orchestration mit Vulnerability Response.

## Erforderliche Rollen

Zusätzlich zu den Rollen sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin, die für die Arbeitsbereiche Vulnerability Response erforderlich sind, benötigen Benutzer Rollen, die spezifisch für die Patch-Orchestration-Integrationen sind, die Sie zum Anzeigen von Daten und Planen von Patches verwenden. Weitere Informationen zu diesen Rollen finden Sie in den folgenden unterstützten Integrationen.

Siehe Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Response und Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM.

## Patchen Sie Daten in den Vulnerability Response -Arbeitsbereichen

Im IT-Korrekturarbeitsbereich können Sie Patchdaten in den folgenden Arbeitsbereichen anzeigen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie in der Ansicht „Home“ auf Bewertungslisten, um Datensätze für bevorzugte Lösungen für VIs, angreifbare CIs und bevorzugte Patches für VIs anzuzeigen.
- Zeigen Sie in der Listenansicht alle Patch-Update-Datensätze (VPUs) und die Ihnen zugewiesenen angreifbaren Elemente an, für die Patches aus den verfügbaren Links vorhanden sind.

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

In der Arbeitsbereich des Schwachstellenmanagers, können Sie Patches anzeigen:

- In der Ansicht „Homepage“ für Überwachungsthemen auf der Registerkarte „Angreifbare Elemente“ können Sie bevorzugte und potenzielle Patches, geplante Patch-Daten und andere Informationen anzeigen.
- In der Listenansicht für Datensätze zu Korrekturmaßnahmen können Sie Patch-Daten zu VIT-Datensätzen auf der Registerkarte „Angreifbare Elemente“ anzeigen.

## Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Regeln für Korrekturaufgaben

Korrekturaufgaben bündeln angreifbare Elemente in den Vulnerability Response Arbeitsbereichen.

## Wichtige Begriffe für die Vulnerability Response -Arbeitsbereiche

**Vulnerability Response-Arbeitsbereiche oder -Arbeitsbereiche**

Vulnerability Response unterstützt die Arbeitsbereiche Vulnerability Response. Sie können entweder die klassische Core-UI Experience oder die Arbeitsbereiche verwenden.

**Klassische (veraltete) UI**

Bezieht sich auf die Experience Core-UI. In der klassischen Umgebung führen Sie noch einige Aktionen aus und zeigen einige Listen an.

**Arbeitsbereich des Schwachstellenmanagers**

In diesem Arbeitsbereich überwachen Manager gezielte Schwachstellen und wählen die VIs und Testergebnisse aus, die ihnen am wichtigsten sind, um sie der IT zuzuweisen.

**Arbeitsbereich für IT-Korrekturen**

In diesem Arbeitsbereich können sich IT-Teams auf die wichtigsten Schwachstellen konzentrieren, die ihnen von der Sicherheitsabteilung zugewiesen wurden. IT-orientierte Informationen, einschließlich betroffener, unterschiedlicher Konfigurationselemente (CIs), Lösungen und Korrekturfortschritt, sind für Korrekturbesitzer in diesem Arbeitsbereich leicht verfügbar.

**Arbeitsbereich des Schwachstellenanalysten**

In diesem Arbeitsbereich können Schwachstellenanalysten während der Zero-Day-Schwachstellenanalyse eine Schwachstellenbewertung durchführen. Nachdem eine Zero-Day-Schwachstelle identifiziert wurde, können sie die potenziellen Auswirkungen und Risiken bewerten, die mit der Schwachstelle verbunden sind. Die Analysten können die betroffenen System-, Anwendungs- oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

**Überwachungsthema**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachungsthemen definieren ein Segment der angreifbaren Elemente, die Schwachstellenmanager und Analysten in Vulnerability Manager Workspace überwachen möchten. Beobachtungsthemen zeigen eine fokussierte Übersicht von Berichten, die sich auf ein Segment von VIs und Testergebnissen beziehen, mit Statistiken zu Trends, CIs und Schwachstellen. Die Dashboards zu diesen Themen können zur Überwachung von Trends verwendet werden. Die Dashboards können Manager auch unterstützen:

- Zeigen Sie den Fortschritt der Korrektur für kritische Elemente an
- Bestimmen Sie das Vorhandensein von Schwachstellen in kritischen Systemen
- Sehen Sie, wenn ein neuer Exploit veröffentlicht wird
- Erhöhen Sie die schnelle Reaktion auf die Behebung eines bestimmten Satzes von Schwachstellen

**Korrekturaufwand (RE)**

Korrekturmaßnahmen werden von Schwachstellenmanagern erstellt, wenn sie feststellen, dass es für die IT an der Zeit ist, die in einem Überwachungsthema aufgeführten Schwachstellen zu beheben. Schwachstellenmanager und Analysten können auswählen, wie sie Korrekturaufgaben erstellen möchten, z. B. nach Zuweisungsgruppe und Schwachstelle. Korrekturaufgaben sind in der Korrekturmaßnahme enthalten.

**Korrekturaufgabe (VUL)**

IT-Teams verwenden Korrekturaufgaben, um die ihnen von der Sicherheit zugewiesenen Schwachstellen zu beheben. Korrekturaufgaben sind Listen der Aktionen, die zum Beheben von Schwachstellen erforderlich sind. Korrekturaufgaben werden automatisch erstellt, wenn Sicherheitsmanager Korrekturmaßnahmen erstellen.

## Entwicklung der Arbeitsbereiche

In früheren Versionen von Vulnerability Responsehatten Sie zwei Optionen, um eine Reihe von angreifbaren Elementen (AEs) als Sicherheits- und Schwachstellenanalyst zu überwachen:

- Das Übersichts-Dashboard, das alle AEs zusammenfasst
- Korrekturaufgaben

Angreifbare Elemente wurden gemäß Ihren vordefinierten Regeln für Korrekturaufgaben automatisch in Korrekturaufgaben sortiert. Korrekturaufgaben wurden entwickelt, um IT-Teams bei der Korrektur verwaltbarer Blöcke angreifbarer Elemente zu unterstützen.

Diese Automatisierung ermöglichte die automatische Gruppierung einer sehr großen Anzahl von VIs für die Massenzuweisung und -korrektur. Schwachstellenanalysten und -manager empfanden es jedoch als schwierig, den gesamten Satz angreifbarer Elemente aus Korrekturaufgaben zu überwachen. Neben Leistungsproblemen bei großen Gruppen kann es schwierig sein, funktionale Regeln für Korrekturaufgaben [] zu erstellen, die nur die Schwachstellen herausfiltern, die Sie als am kritischsten eingestuft haben.

Die Vulnerability Response Arbeitsbereiche:

- Helfen Sie Sicherheitsmanagern, aktive VIs und Testergebnisse im Laufe der Zeit herauszufiltern, zu überwachen und die Behebung der von ihnen als am wichtigsten eingestuften Schwachstellen voranzutreiben.
- Stellen Sie IT-Teams IT-orientierte Informationen an einem Ort bereit, mit denen sie die ihnen von der Sicherheit zugewiesenen Schwachstellen beheben können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Updates für Korrekturaufgaben in den Arbeitsbereichen

Im Arbeitsbereich des Schwachstellenmanagers verwenden *Schwachstellenanalysten* und *-manager „* Überwachungsthemen“ und „Korrekturmaßnahmen“ als zwei neue Methoden für die Überwachung und Zuweisung von VIs zur Korrektur.

Schwachstellengruppen wurden in *Korrekturaufgaben*umbenannt. Diese Änderung gilt für Bezeichnungen in Listen, Datensätzen und Regeln sowohl in der veralteten Benutzeroberfläche als auch in den Arbeitsbereichen. Korrekturaufgaben werden so eingerichtet, dass IT-Teams im IT-Korrekturarbeitsbereich mit ihnen arbeiten können. Die folgende Liste zeigt, wie Sie als Schwachstellenmanager oder Schwachstellenanalyst Schwachstellen überwachen und Ergebnisse testen, filtern und zuweisen können:

1. Im Arbeitsbereich des Schwachstellenmanagers überwachen Manager importierte Schwachstellen in Überwachungsthemen. Manager und Analysten verwenden Überwachungsthemen, um einen dynamischen Satz gefilterter VIs im Laufe der Zeit zu überwachen, die ihrer Meinung nach am kritischsten sind.
2. Mit Überwachungsthemen können Sicherheitsmanager bestimmen, wann und welche Art von VIs in Korrekturmaßnahmen (Remediation Efforts, REs) an IT-Teams übergeben werden soll. Diese REs sind statische Listen der VIs, die die Sicherheitsabteilung von IT-Teams beheben möchte.

   Bei den Korrekturmaßnahmen haben Manager vier Optionen, um VIs in Korrekturaufgaben (VULs) zu bündeln. Korrekturaufgaben werden IT-Teams automatisch basierend auf den Zuweisungsgruppen zugewiesen, die ursprünglich den AEs zugeordnet sind.
3. IT-Teams arbeiten im IT-Korrekturarbeitsbereich an Korrekturaufgaben, ohne alle AEs sortieren zu müssen.

   Eine Korrekturaufgabe durchläuft dieselben Status wie die Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle VIs in einer Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen und auf **Inaktiv**gesetzt.

   Der Korrekturfortschritt wird in Datenvisualisierungen in den Überwachungsthemen und auf der IT-Korrektur-Homepage aktualisiert.

## Aktualisiert die Regeln für Korrekturaufgaben in den Arbeitsbereichen

Schwachstellengruppenregeln werden als *Korrekturaufgabenregeln*bezeichnet. Diese Änderung gilt für die Bezeichnungen in Listen, Datensätzen und Regeln sowohl in der veralteten Benutzeroberfläche als auch in den Arbeitsbereichen.

Tabellennamen, z. B. [sn_vul_m2m_vul_group_item], werden nicht geändert.

Wenn Sie Regeln für Schwachstellengruppen in früheren Versionen von Vulnerability Responseerstellt haben, stehen sie Ihnen weiterhin als Korrekturaufgabenregeln zur Verfügung.

In den Arbeitsbereichen werden Schwachstellengruppenregeln jedoch nicht mehr als primäre Methode zum Organisieren einer großen Menge angreifbarer Elemente in Schwachstellengruppen verwendet. Möglicherweise möchten Sie die Regeln für Korrekturaufgaben inaktiv lassen, wenn Sie sich an die Arbeitsbereiche vertraut gemacht haben.

Möglicherweise möchten Sie stattdessen schrittweise Vulnerability Response Arbeitsbereiche verwenden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Response durchführen, bleiben Ihre vorhandenen VG-Regeln erhalten. Sie stehen Ihnen weiterhin in den Arbeitsbereichen zur Verfügung. Die Standardgruppenregel, Schwachstelle, ist standardmäßig inaktiv.
2. Konfigurieren Sie Zuweisungsregeln und, falls gewünscht, Risikoregeln, und führen Sie dann einen Import durch.
3. Als Schwachstellenmanager oder Analyst können Sie zu überwachende Segmente aus den Überwachungsthemen im Arbeitsbereich des Schwachstellenmanagers auswählen. Sie können Überwachungsthemen als eigenständige Funktionen verwenden. Wählen Sie eine beliebige Teilmenge von VIs aus, und verwenden Sie das Dashboard, um Trends zu überwachen. Mit ihnen können Sie entscheiden, wo und wann Sie die Korrekturmaßnahmen konzentrieren möchten.
4. Als Schwachstellenmanager oder Analyst erstellen Sie Korrekturmaßnahmen aus Überwachungsthemen, wenn Sie entscheiden, dass es an der Zeit ist, eine Teilmenge angreifbarer Elemente zu korrigieren. Wenn Sie eine Korrekturmaßnahme erstellen, wird auch automatisch eine Korrekturaufgabe zur Übergabe an die IT erstellt.
5. Im Laufe der Zeit entdecken Sie als Schwachstellenmanager oder Analyst möglicherweise Routinemuster, die Sie automatisch mit Regeln für Korrekturaufgaben behandeln können.

Um die Regeln für Korrekturaufgaben anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**.

## Weitere Informationen zu Zuweisungsregeln, Regeln für Korrekturaufgaben, Korrekturbemühungen und angreifbaren Elementen finden Sie in den Vulnerability Response Arbeitsbereichen

- Korrekturaufgabendatensätze (VUL) werden in Listen und Datensätzen sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen angezeigt.
- Eine Korrekturaufgabe durchläuft dieselben Status wie eine Schwachstellengruppe. Wenn alle AEs in einer Korrekturaufgabe geschlossen sind, geht die Korrekturaufgabe in den Status „Inaktiv“ über.
- Um Ihre Teams bei der Korrektur zu unterstützen, darf ein angreifbares Element nur in einer Korrekturmaßnahme enthalten sein. Sobald es sich um eine Korrekturmaßnahme handelt, wird ein angreifbares Element keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt.
- Wenn Sie eine Korrekturmaßnahme löschen, wird die Korrekturmaßnahme inaktiv, und alle aktiven AEs sind für neue Korrekturmaßnahmen verfügbar.
- Ein angreifbares Element kann sich in mehreren Korrekturaufgaben befinden.
- Korrekturaufgaben werden IT-Teams automatisch basierend auf der Zuweisungsgruppe zugewiesen, die einem angreifbaren Element in einer Korrekturmaßnahme zugeordnet ist. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Zuweisungsgruppe aus.
- Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, wurden Ihre Zuweisungsregeln in der veralteten UI beibehalten.
- Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, werden Ihre aktuellen Benutzer und Gruppen geerbt und sind für Sie in den Arbeitsbereichen zugänglich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu den Lebenszyklen von Korrekturmaßnahmen finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in Vulnerability Response Workspaces.

## Konfiguration und Setup für Vulnerability Response Arbeitsbereiche

Weitere Informationen zu Zuweisungsregeln und Regeln für Korrekturaufgaben finden Sie unter Konfigurieren Sie die Vulnerability Response Arbeitsbereiche und Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn Sie Neukunde sind und sie noch nicht hinzugefügt haben, müssen Sie Benutzer und Gruppen so einrichten, dass angreifbare Elemente und Korrekturaufgaben den gewünschten Korrekturgruppen zugewiesen werden. Vulnerability Response-Zuweisungsregeln werden verwendet, um Arbeit an Gruppen zuzuweisen.

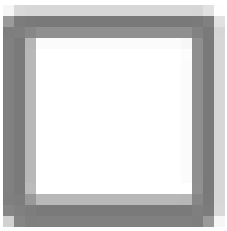
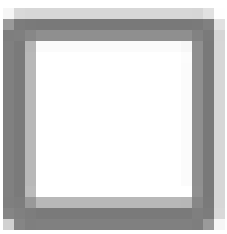
## Konfigurieren Sie die Vulnerability Response Arbeitsbereiche

Vergewissern Sie sich, dass Sie die folgenden Setupaufgaben abgeschlossen haben, bevor Sie die Arbeitsbereiche verwenden können.

**Vorbereitungen**
Erforderliche Rolle: admin für die Zuweisung von Rollen zu Benutzern und Gruppen und Benutzern zu Gruppen.

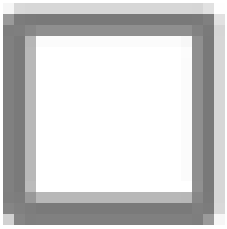
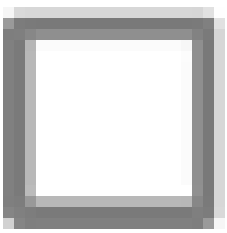
sn_vul.vulnerability_admin zum Bearbeiten, Erstellen von Regeln und Konfigurieren der Anwendung Vulnerability Response.

Bestätigen Sie, dass Sie die folgenden Setupaufgaben abgeschlossen haben. Weitere Informationen zum Ausführen dieser Aufgaben finden Sie in den Schritten nach der Liste.

| Aufgabe | Beschreibung |
|---|---|
|  | Wenn dies noch nicht geschehen ist, weisen Sie Benutzern und Gruppen die richtigen Rollen zu, damit sie Zugriff auf die Arbeitsbereiche haben.<br><br>Erforderliche Rolle: admin. Weitere Informationen finden Sie in den folgenden Schritten. |
|  | Richten Sie Zuweisungsregeln ein, damit angreifbare Elemente den richtigen Gruppen zur Korrektur zugewiesen werden.<br><br>Erforderliche Rolle: sn_vul.vulnerability_admin.<br><br>Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

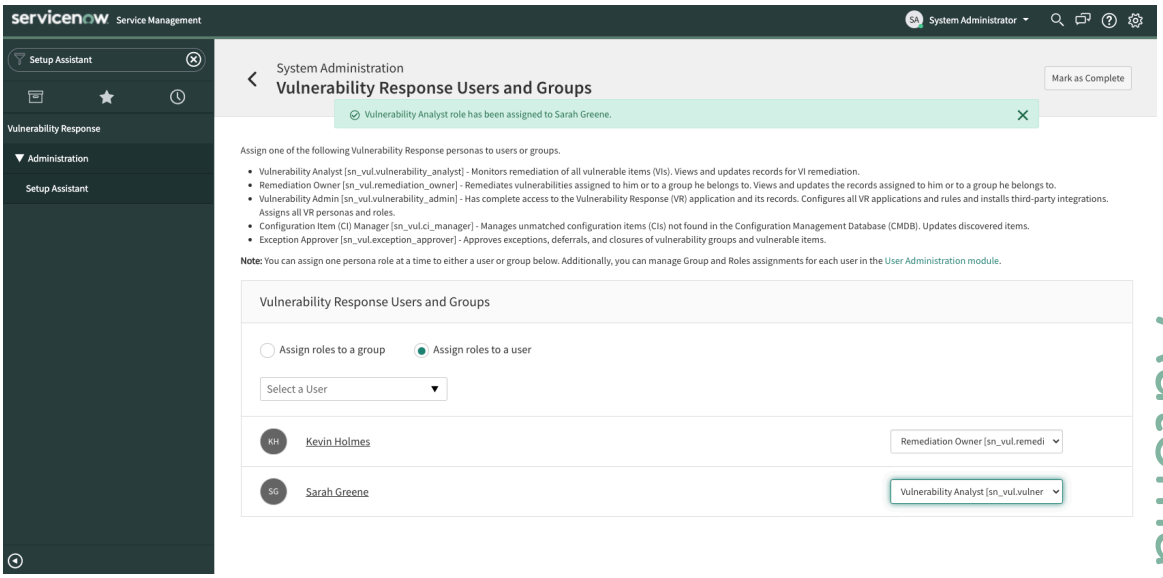
| Aufgabe | Beschreibung |
| --- | --- |
|  | (Optional): Bearbeiten oder erstellen Sie die Regeln für Korrekturaufgaben.<br><br>Erforderliche Rolle: sn_vul.vulnerability_admin.<br><br>**Hinweis:**<br><br>Funktional funktionieren Korrekturaufgabenregeln genauso wie Korrekturaufgabenregeln in früheren Versionen von Vulnerability Response. Im Gegensatz zu den Schwachstellengruppen, die automatisch aus den Regeln für Korrekturaufgaben erstellt wurden, werden jedoch Korrekturaufgaben erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben die folgenden Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln:<br><br>• Nach Zuweisungsgruppe<br>• Nach Zuweisungsgruppe und Konfigurationselement<br>• Nach Zuweisungsgruppe und Schwachstelle<br>• Keine: Verwenden Sie diese Option, wenn Sie VIs manuell zu einer Korrekturaufgabe hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe.<br><br>Weitere Informationen dazu, wie AEs automatisch gruppiert werden und wie die Gruppenregeln in der klassischen Umgebung erneut angewendet werden, finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln. |
|  | Bearbeiten Sie die Korrekturzielregeln.<br><br>Erforderliche Rolle: sn_vul.vulnerability_admin.<br><br>Fügen Sie Korrekturzielregeln in der klassischen Umgebung hinzu. Weitere Informationen zu Korrekturzielregeln finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Nachdem Sie die Anwendung Vulnerability Response installiert und aktiviert haben, navigieren Sie in der klassischen Umgebung als Benutzer mit der Administratorrolle zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**.




2. Weisen Sie im Setup-Assistenten Benutzer den folgenden Gruppen zu.

> **Hinweis:**
> 1000 ist der Grenzwert für die Anzahl der Benutzergruppen, denen ein Benutzer in Vulnerability Response Workspaces zugewiesen werden kann.

Die folgenden Gruppen werden mit der Anwendung Vulnerability Response bereitgestellt und in den Arbeitsbereichen verwendet. Sie können ihnen im Setup-Assistenten Benutzer zuweisen:

- Korrekturbesitzer: Diese Gruppe ist für IT-Korrekturbesitzer im IT-Korrekturarbeitsbereich vorgesehen. Benutzer mit dieser Rolle beheben Schwachstellen, die ihnen in Korrekturaufgaben zugewiesen wurden.

  > **Hinweis:**
  >
  > Wenn Sie möchten, dass Ihre Korrekturbesitzer Change-Anforderungen erstellen und anzeigen und Daten zu angreifbaren Konfigurationselementen (CIs) im IT-Korrekturarbeitsbereich und in der klassischen Umgebunganzeigen, weisen Sie ihnen die itil-Rolle zu. Möglicherweise möchten Sie die itil-Rolle einzelnen Benutzern anstatt allen Mitgliedern einer Gruppe zuweisen. Die Rolle cmdb_read ist auch eine Option für Benutzer, um CI-Daten in den Arbeitsbereichen anzuzeigen.

- Ab v16.1 können Sie E-Mail-Erinnerungen an Ihre IT-Korrekturbesitzer einrichten. Informationen zum Einrichten von E-Mail-Benachrichtigungen an die Arbeitsbereiche finden Sie unter Richten Sie E-Mail-Benachrichtigungen in den Vulnerability Response Arbeitsbereichen ein.
- Schwachstellenadministrator: Diese Gruppe ist für Schwachstellenmanager vorgesehen. Diese Rolle konfiguriert die Anwendung Vulnerability Response im Setup-Assistenten. Diese Rolle hat auch die Berechtigung zum Verarbeiten von Ausnahme- und falsch positiven Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schwachstellenanalyst: Diese Gruppe ist für Sicherheitsmanager, Schwachstellenmanager und Analysten im Arbeitsbereich „Schwachstellenmanager“ vorgesehen. Diese Rolle überwacht Schwachstellen, erstellt Überwachungsthemen und Korrekturmaßnahmen und überwacht den Fortschritt der Korrektur.
- Falsch positiver Genehmiger: Benutzer in dieser Gruppe verarbeiten falsch positive Anforderungen für angreifbare Elemente oder Korrekturaufgaben. Eine falsch positive Anforderung erfordert einen einstufigen Genehmigungsprozess. Sie können die Zuweisung von Benutzern zu dieser Gruppe außerhalb des Setup-Assistenten in der **Benutzeradministration verwalten**.
- Ausnahmegenehmiger – Eine Ausnahmeanforderung für ein angreifbares Element oder eine Korrekturaufgabe wird mit einem standardmäßigen zweistufigen Genehmigungsworkflow genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Fügen Sie Benutzer zu beiden Genehmigungsgruppen hinzu: „Ausnahmegenehmiger – Ebene 1“ und „Ausnahmegenehmiger – Ebene – 2“. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet. Sie verwalten die Zuweisung von Benutzern zu dieser Gruppe außerhalb des Setup-Assistenten in der **Benutzeradministration**.

**Hinweis:**
Fügen Sie den Genehmigungsgruppen Benutzer hinzu, bevor Sie falsch positive Meldungen und Ausnahmeanforderungen senden. Wenn Sie Anforderungen erstellen, bevor Sie Benutzer mit Genehmigungsberechtigung zuweisen, sind die Anforderungen für sie möglicherweise nicht sichtbar.

Klicken Sie alternativ auf den Link **Benutzeradministration**, um die folgenden granularen Rollen zu verwalten und Ihren Benutzern und vorhandenen Gruppen zuzuweisen. Mit diesen Rollen können Benutzer bestimmte Aktionen in der Anwendung Vulnerability Response und den Arbeitsbereichen ausführen.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Um Change-Anforderungen im IT-Korrekturarbeitsbereich und in der klassischen Umgebung zu erstellen und anzuzeigen, weisen Sie ihnen die itil-Rolle zu.

Weitere Informationen zum Zuweisen von Persona-Rollen zu Benutzern und Benutzern zu Gruppen finden Sie unter Vulnerability Response Personas und granulare Rollen und Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

3. Korrekturaufgaben werden bei ihrer Erstellung automatisch zur Verarbeitung an IT-Korrekturzuweisungsgruppen übergeben.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine: Verwenden Sie diese Option, wenn Sie VIs manuell zu einer Korrekturaufgabe hinzufügen möchten.

   **Hinweis:**
   Für Version 18.0 von Vulnerability Responseist die Option **Keine** nicht verfügbar.

   Wenn Sie ein Upgrade von einer früheren Version von Vulnerability Responsedurchführen, bleiben Ihre Zuweisungsgruppen erhalten. Möglicherweise möchten Sie diese Gruppen jedoch so bearbeiten, dass angreifbare Elemente bestimmten Zuweisungsgruppen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugeordnet werden, bis Sie sich mit der Funktionsweise von Überwachungsthemen und Korrekturmaßnahmen vertraut gemacht haben. Sie können beispielsweise Zuweisungsgruppen nach Produkt oder Region erstellen, aber Sie können beliebige Kriterien verwenden, die für Ihre Organisation am besten geeignet sind.

Sie können auch Zuweisungsregeln verwenden, um Gruppen Korrekturaufgaben zuzuweisen. Für die folgenden Elemente sollten Sie nur Regeln mit hoher Priorität ausführen:

- Artikel, die einer besonderen Behandlung bedürfen
- Elemente, bei denen das Risiko kritisch ist oder bei denen ein AEs die Einhaltung gesetzlicher Vorschriften erfordert

Die folgenden mit der Anwendung bereitgestellten Zuweisungsregeln sind standardmäßig aktiv:

- Außer Kraft gesetzte CI-Zuweisungsregel
- An CI-Supportgruppe zuweisen
- Zuweisungsregel für Arbeitsplatz-PCs
- Datenbankzuweisungsregel
- Zuweisungsregel für Webanwendungen
- Windows-Server-Zuweisungsregel
- Zuweisungsregel für Nicht-Windows-Server
- Zuweisungsregel „Alle erfassen“.

Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung.

4. **Wahlweise:** Bearbeiten oder erstellen Sie die Regeln für Korrekturaufgaben.

   (Optional) In den Arbeitsbereichen werden Korrekturaufgaben erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben die folgenden Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln:

   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine: Verwenden Sie diese Option, wenn Sie VIs manuell zu einer Korrekturaufgabe hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe.

   **Hinweis:**
   Für Version 18.0 von Vulnerability Responseist die Option **Keine** nicht verfügbar.

   Weitere Informationen dazu, wie AEs automatisch gruppiert werden und wie die Gruppenregeln in der klassischen Umgebung erneut angewendet werden, finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

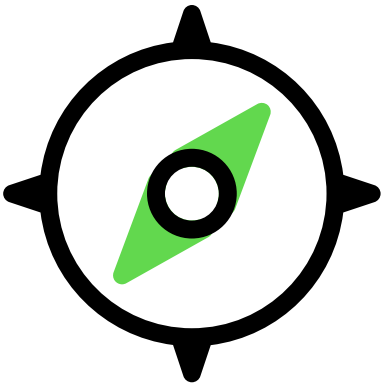
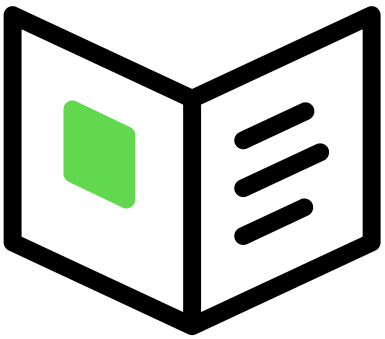
## Arbeitsbereich des Schwachstellenmanagers

Mit dem Vulnerability Manager Workspace können Schwachstellenmanager und Analysten die für sie wichtigsten Schwachstellen überwachen und strategisch entscheiden, welche Schwachstellen sie an IT-Teams zur Behebung senden.

## Übersicht

V18.0 V18.0 Vulnerability Manager Workspace-Demo

## Erste Schritte

| Erkunden | Verwenden | Referenz |
| --- | --- | --- |
|  | |  |
| Erfahren Sie mehr über die Funktionen in Vulnerability Manager Workspace | Erfahren Sie, wie Sie Vulnerability Manager Workspace zum Überwachen, Verwalten und Beheben von Schwachstellen verwenden | Erfahren Sie mehr über zusätzliche Informationen, die für die Verwendung von Vulnerability Manager Workspace erforderlich sind |

## Problembehandlung und Hilfe

- Security Operations in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Vulnerability Manager Workspace erkunden

Erhalten Sie als Schwachstellenmanager und -analyst eine einheitliche Ansicht aller Schwachstellentypen in Vulnerability Manager Workspace. Sie können Host-, Anwendungs- und Container-Schwachstellen und Konfigurationsprobleme anzeigen, Überwachungsthemen für diese Schwachstellen und Fehlkonfigurationen erstellen und Korrekturaufgaben erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

Sie können Vulnerability Manager Workspace anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.

Der Arbeitsbereich des Schwachstellenmanagers besteht aus den folgenden Seiten:

**Homepage**

Besteht aus vordefinierten Filtern, die zur Visualisierung der Zusammenfassung von Datensätzen verwendet werden.

Weitere Informationen zur Homepage finden Sie unter Homepage-Übersicht.

**Hinweis:**
Ab v21.0 von Vulnerability Responsewerden die Überwachungsthemen auf der Seite „Überwachungsthemen“ angezeigt.

**Seite „Überwachungsthemen“.**

Besteht aus einer Liste von Überwachungsthemen, die in vier Module unterteilt sind: Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Konfigurationstestergebnisse.

Weitere Informationen zu Überwachungsthemen finden Sie unter Übersicht über Überwachungsthemen.

**Seite „Dashboards“**

Besteht aus den Dashboards Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Übersicht, Application Vulnerability Management, Unified Vulnerability Response und Integrität.

Weitere Informationen finden Sie unter Dashboardübersicht.

**Hinweis:**
Die Seite „Dashboards“ wird ab Version 19.0 von Vulnerability Responseangezeigt.

**Listen-Seite**

Besteht aus den standardmäßigen und benutzerdefinierten Listenseiten für Korrekturbemühungen, Korrekturaufgaben, angreifbare Hostelemente, angreifbare Anwendungselemente, angreifbare Containerelemente, Konfigurationstestergebnisse, Ausnahmen, Genehmigungen und Bibliotheken.

Weitere Informationen finden Sie unter Listenübersicht.

## Schlüsselfunktionen

Vulnerability Manager Workspace bietet die folgenden Funktionen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vulnerability Manager Workspace unterstützt Application Vulnerability Response, Container Vulnerability Responseund Configuration Compliance.
- Ruft eine Zusammenfassung aller aktiven angreifbaren Hostelemente (VIs), angreifbaren Anwendungselemente (AVITs), angreifbaren Containerelemente (CVITs) und Konfigurationstestergebnisse in der Formularvisualisierung auf der Homepage ab.
- Die Überwachungsthemen werden nach dem Datensatztyp im Navigationsbereich auf der Seite „Überwachungsthemen“ kategorisiert. Das heißt, Sie können ein Überwachungsthema erstellen, das entweder angreifbare Hostelemente (VIs), angreifbare Anwendungselemente (AVITs), angreifbare Containerelemente (CVITs) oder Konfigurationstestergebnisse enthält.
- Sie können die Dashboards Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Übersicht, Application Vulnerability Management, Unified Vulnerability Response und Integrität im Vulnerability Manager Workspace anzeigen.

### Sehen Sie sich ein Workflow-Beispiel in Vulnerability Manager Workspace an

Sehen Sie sich ein Beispiel für einen End-to-End-Workflow in Vulnerability Manager Workspace an. Erfahren Sie, wie ein Schwachstellenmanager oder Analyst den Arbeitsbereich verwenden kann, um kritische Datensätze zu überwachen und Korrekturaufgaben zur Übergabe an die IT zu erstellen.

**Vorbereitungen**
Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

**Prozedur**

Klicken Sie auf das folgende Video, um die Schritte des Workflows anzuzeigen.
Vulnerability Manager Workspace-Demo

Das vorherige Video enthält die folgenden Aufgaben:

**a.** Klicken Sie in der **Startseite** des Arbeitsbereichs auf ein Überwachungsthema, um Daten in einem Dashboard für verschiedene Kategorien von Datensätzen anzuzeigen.

**b.** Erstellen Sie mithilfe von Filterbedingungen ein Überwachungsthema, und zeigen Sie eine Vorschau der übereinstimmenden Datensätze an. Weitere Informationen zum Erstellen eines Überwachungsthemas finden Sie unter Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema.

**c.** Zeigen Sie Daten zu Datensätzen und die zugehörigen Konfigurationselemente auf der Registerkarte „ **Angreifbare CIs** “ in einem Überwachungsthema an. Weitere Informationen zu den Visualisierungen finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

**d.** Zeigen Sie Daten zu Schwachstellen auf der Registerkarte **Eindeutige Schwachstellen** in einem Überwachungsthema an.

**e.** Zeigen Sie die dem Überwachungsthema zugeordneten Datensätze auf der Registerkarte **Angreifbare Elemente** für ein Überwachungsthema an. Scrollen Sie nach rechts, um in der Spalte Korrekturmaßnahme anzuzeigen, welche Datensätze sich bereits in einer Korrekturmaßnahme befinden.

**f.** Klicken **Sie in einem Überwachungsthema auf Korrekturmaßnahme erstellen**, wenn Sie bereit sind, Aufgaben für bestimmte Datensatztypen zu erstellen und der IT zur Korrektur



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zuzuweisen. Weitere Informationen zum Erstellen einer Korrekturmaßnahme finden Sie unter Erstellen Sie im Arbeitsbereich von Vulnerability Manager eine Korrekturmaßnahme.

g. Klicken Sie auf die Listenansicht, um **Listen** Ihrer Korrekturbemühungen, Korrekturaufgaben, Datensätze, Ausnahmen und Genehmigungen anzuzeigen. Weitere Informationen zur Seite „Listen“ finden Sie unter Listenübersicht.

h. Klicken Sie in der Listenansicht auf die Liste **Aktive** Korrekturmaßnahmen, um einen Datensatz für Korrekturmaßnahmen zu öffnen und den Status und Informationen zum Datensatz anzuzeigen. Weitere Informationen finden Sie unter Listenübersicht.

i. **Klicken** Sie im Datensatz der Korrekturmaßnahme auf die Registerkarte Korrekturaufgabe, um die mit dem Korrekturdatensatz verknüpften Korrekturaufgaben anzuzeigen. Weitere Informationen finden Sie unter Listenübersicht.

j. Klicken Sie im Datensatz der Korrekturmaßnahme auf die Registerkarte **Angreifbare** Elemente, um eine Liste der Datensätze anzuzeigen, die der Korrekturmaßnahme zugeordnet sind. Weitere Informationen finden Sie unter Listenübersicht.

k. Wenn Sie bei Bedarf eine neue Korrekturaufgabe aus der Korrekturmaßnahme für eine Teilmenge von Datensätzen erstellen möchten, wählen Sie die Datensätze aus, die Sie verschieben möchten, und klicken Sie auf **Korrekturaufgabe erstellen**.

**Hinweis:**
Da Sie in Version 18.0 von Vulnerability Response keine Korrekturaufgaben bei Bedarf erstellen können, wird die Schaltfläche **Korrekturaufgabe erstellen** aus der Liste der zugehörigen Elemente für angreifbare Elemente einer Korrekturmaßnahme entfernt.

### Homepage-Übersicht

Ab Vulnerability Response v21.0 bietet die Homepage in Vulnerability Manager Workspace eine Zusammenfassung der aktiven Datensätze, indem Visualisierungen von Risikobewertung, Korrekturfortschritt, Zuweisungen zu Zuweisungsgruppen, Datensätzen in Korrekturaufgaben und Schwachstellen aus Cloud-Ressourcen angezeigt werden.

**Tipp:**

Wenn Sie die Systemeigenschaft `sn_vul_cmn_ws.navigate_to_workspace` auf „true“ festlegen und die vordefinierten Filterlinks im Navigationsbereich auswählen, werden diese Links in Vulnerability Manager Workspace geöffnet, und der entsprechende gespeicherte Filter wird automatisch ausgewählt.

Zum Beispiel, wenn Sie **Hohes Risiko** auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente**, wird dieser Link zur Homepage in Vulnerability Manager Workspace mit automatischer Auswahl des Filters „ **Hohes Risiko** “ weitergeleitet.

Ab Version 21.0 von Vulnerability Response werden die Überwachungsthemen auf der Seite „Überwachungsthemen“ angezeigt. Weitere Informationen finden Sie unter Übersicht über Überwachungsthemen.

Auf der Homepage können Sie die Visualisierungen für die vorgefilterten Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen und Konfigurationstestergebnisse anzeigen. Sie können auch Visualisierungen für eine Reihe von gewünschten Datensätzen anzeigen, indem Sie Filter erstellen und anwenden. Weitere Informationen zum Erstellen, Aktualisieren und Löschen von Filtern finden Sie unter Erstellen Sie Filter, um die Zusammenfassung der aktiven Datensätze anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Host-Schwachstellen

Die Registerkarte **Host-Schwachstellen** enthält Visualisierungen, die eine allgemeine Übersicht über die aktiven Host-Schwachstellen bieten.

Erforderliche Rollen:

- sn_vul.vulnerability_analyst und sn_vul.vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

**Visualisierungen auf der Registerkarte Host-Schwachstellen auf der -Homepage**

| Visualisierung | Beschreibung |
|---|---|
| Nach Zuweisungsgruppe und Korrekturstatus | Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach dem Korrekturstatus gruppiert sind. |
| nach Status | Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“). |
| Nach Risikobewertung | Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine) |
| In Korrekturaufgabe | Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht. |
| Mit vorhandenen Exploits | Aktive Datensätze mit und ohne bekannte Exploits. |
| Nach außen gerichtet | Aktive r-Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet. |
| Nach CI-Klasse | Aktive Datensätze, kategorisiert nach CI-Klassen. |
| Nach Cloud-Ressource | Aktive r-Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen. |
| Zurückgestellte Elemente nach Grund | Aktive zurückgestellte Datensätze, gruppiert nach Grund. |

## Container-Schwachstellen

Die Registerkarte **Container-Schwachstellen** enthält Visualisierungen, die eine Gesamtübersicht der aktiven angreifbaren Containerelemente bieten.

Erforderliche Rollen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_analyst und sn_vul_container.vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul_container.read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

**Visualisierungen auf der Registerkarte „Container-Schwachstellen“ auf der -Homepage**

| Visualisierung | Beschreibung |
|---|---|
| Nach Zuweisungsgruppe und Korrekturstatus | Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach dem Korrekturstatus gruppiert sind. |
| nach Status | Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“). |
| Nach Risikobewertung | Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine) |
| In Korrekturaufgabe | Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht. |
| Mit vorhandenen Exploits | Aktive Datensätze mit und ohne bekannte Exploits. |
| Nach außen gerichtet | Aktive r-Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet. |
| Docker-Images | Anzahl der eindeutigen Docker-Images. |
| Nach Basis-Image | Aktive Datensätze, kategorisiert nach dem Typ des Image. |
| Zurückgestellte Elemente nach Grund | Aktive zurückgestellte Datensätze, gruppiert nach Grund. |

## Anwendungsschwachstellen

Die Registerkarte **Anwendungsschwachstellen** enthält Visualisierungen, die eine allgemeine Übersicht über die Anwendungsschwachstellen bieten.

Erforderliche Rollen:

- sn_vul.app_sec_manager, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.app_read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Visualisierungen auf der Registerkarte „Anwendungsschwachstellen“ auf der Homepage**

| Visualisierung | Beschreibung |
|---|---|
| Nach Zuweisungsgruppe und Korrekturstatus | Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach dem Korrekturstatus gruppiert sind. |
| nach Status | Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“). |
| Nach Risikobewertung | Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine) |
| In Korrekturaufgabe | Aktive Datensätze, die Teil der Korrekturaufgabe sind und nicht. |
| Mit vorhandenen Exploits | Aktive Datensätze mit und ohne bekannte Exploits. |
| Nach außen gerichtet | Aktive r-Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet. |
| Nach CI-Klasse | Aktive Datensätze, kategorisiert nach CI-Klassen. |
| Nach Cloud-Ressource | Aktive r-Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen. |
| Zurückgestellte Elemente nach Grund | Aktive zurückgestellte Datensätze, gruppiert nach Grund. |

## Konfigurationstestergebnisse

Die Registerkarte **Konfigurationstestergebnisse** enthält Visualisierungen, die eine allgemeine Übersicht über die aktiven Fehlkonfigurationen der Assets in Ihrer Organisation bieten.

Erforderliche Rollen:

- sn_vulc.admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vulc.read zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

In der folgenden Tabelle werden die Visualisierungen auf der Registerkarte „Konfigurationstestergebnisse“ auf der Homepage beschrieben. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze zu erhalten.

**Visualisierungen auf der Registerkarte „Konfigurationstestergebnisse“ auf der Homepage**

| Visualisierung | Beschreibung |
|---|---|
| Nach Zuweisungsgruppe und Korrekturstatus | Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach dem Korrekturstatus gruppiert sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Visualisierungen auf der Registerkarte „Konfigurationstestergebnisse“ auf der Homepage (Fortsetzung)**

| Visualisierung | Beschreibung |
|---|---|
| nach Status | Aktive Datensätze, kategorisiert nach verschiedenen Status („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „In Überprüfung“, „Gelöst“ und „Zurückgestellt“). |
| Nach Risikobewertung | Aktive Datensätze, kategorisiert nach Risikobewertung (1 – Kritisch, 2 – Hoch, 3 – Mittel, 4 – Niedrig und 5 – Keine) |
| Nach Technologie | Aktive Datensätze, kategorisiert nach Technologie. |
| Durch Test | Aktive Datensätze, kategorisiert nach Tests. |
| Nach außen gerichtet | Aktive r-Datensätze, kategorisiert nach Asset-Gefahrenpotenzial im Internet. |
| Nach CI-Klasse | Aktive Datensätze, kategorisiert nach CI-Klassen. |
| Nach Cloud-Ressource | Aktive r-Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen. |
| Zurückgestellte Elemente nach Grund | Aktive zurückgestellte Datensätze, gruppiert nach Grund. |

Sie können die neuesten Informationen anzeigen, indem Sie im Widget auf das Symbol **Aktualisieren** klicken.

### Übersicht über Überwachungsthemen

Ein *Beobachtungsthema* ist eine Reihe von Datenvisualisierungen, mit denen Sie eine gefilterte Gruppe von Datensätzen im Laufe der Zeit in einem Dashboard überwachen können, die für Ihre Organisation von besonderem Interesse oder Priorität sein könnten.

Ab Version 21.0 von Vulnerability Response werden die Überwachungsthemen auf der Seite „Überwachungsthemen“ angezeigt.

Die in den Datenvisualisierungen zu den Überwachungsthemen angezeigten Daten werden dynamisch aktualisiert, wenn sich die Schwachstellendaten beim Import ändern. Verwenden Sie die Dashboards, um Trends, Umfang und Typen von Schwachstellen und Ihre Konfigurationselemente für das ausgewählte Überwachungsthema zu überwachen. Anhand dieser Informationen können Sie ermitteln, wie sich die Schwachstellen in den einzelnen Überwachungsthemen auf Ihre Umgebung auswirken. Weitere Informationen zu den Registerkarten für zugehörige Elemente und ihren Visualisierungen in einem Überwachungsthema finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

Die folgenden Überwachungsthemen werden mit dem Basissystem im Modul „Hostschwachstellen“ bereitgestellt:

- Schwachstellen in nach außen gerichteten Assets
- Schwachstellen mit verfügbaren Exploits
- Schwachstellen auf Windows-Servern
- Schwachstellen auf LINUX-Servern



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kritische überfällige Schwachstellen
- Kritische Schwachstellen nicht in Korrekturaufgaben

**Hinweis:**
Wenn eine Datenvisualisierung zeigt, dass für diese Kategorie keine AEs vorhanden sind, Sie jedoch eine Liste der AEs sehen können, wenn Sie auf das Diagrammsymbol klicken, überprüfen Sie die Spalte mit dem Namen des Überwachungsthemas in der angezeigten Liste. Stellen Sie sicher, dass der Wert für alle VIs, die in der Spalte des Überwachungsthemas aufgeführt sind, z. B. mit Internetverbindung, `false`lautet. Dieser Wert in diesem Beispiel gibt an, dass für dieses Überwachungsthema keine VIs mit Internetverbindung vorhanden sind.

Um die Korrektur zu starten oder wenn ein kritischer Bedarf für die Datensätze besteht, die sich in einem Überwachungsthema befinden, können Sie eine *Korrekturmaßnahme* aus einem Überwachungsthema erstellen. Weitere Informationen finden Sie unter Erstellen Sie im Arbeitsbereich von Vulnerability Manager eine Korrekturmaßnahme.

**Zugehörige Informationen**

Verwenden Sie Überwachungsthemen in Vulnerability Manager Workspace

Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema

Bearbeiten oder löschen Sie ein Überwachungsthema

Deaktivieren oder aktivieren Sie ein Überwachungsthema

### Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema

Ab Version 18.0 können Sie Überwachungsthemen erstellen, die in vier Module kategorisiert sind: Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen und Konfigurationstestergebnisse. Die Registerkarten für zugehörige Elemente in einem Überwachungsthema unterscheiden sich für jedes Modul.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

Der Navigationsbereich auf der Zielseite enthält die folgenden Module:

- Host-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Host-Elemente enthalten.
- Container-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Containerelemente enthalten.
- Anwendungsschwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Anwendungselemente enthalten.
- Konfiguration Testergebnisse: Zeigt die Überwachungsthemen an, die die Konfigurationselemente enthalten.
- Inaktiv: Zeigt die inaktiven Überwachungsthemen aus allen vier Modulen an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt die Registerkarten für zugehörige Elemente, die für verschiedene Überwachungsthemenmodule verfügbar sind:

### Überwachungsthema und zugehörige Elemente

| Überwachungsthema | Registerkarten „Zugehörige Elemente“. |
|---|---|
| Host-Schwachstellen | Übersicht, betroffene CIs, bestimmte Schwachstellen und angreifbare Elemente |
| Container-Schwachstellen | Übersicht, betroffene CIs, bestimmte Schwachstellen und angreifbare Elemente |
| Anwendungsschwachstellen | Übersicht und angreifbare Elemente |
| Konfigurationstestergebnisse | Übersicht, betroffene CIs, eindeutige Konfigurationstests und Konfigurationstestergebnisse |

Die folgende Tabelle enthält eine Beschreibung der Registerkarten für zugehörige Elemente und der Visualisierungen in einem Überwachungsthema.

### Registerkarten und Visualisierungen für zugehörige Elemente in einem Überwachungsthema

| Registerkarte „Zugehörige Elemente“ und Visualisierung | Beschreibung |
|---|---|
| **Übersicht** | |
| Aktive angreifbare Elemente im Laufe der Zeit | Anzahl der aktiven angreifbaren Elemente (VIs) im Zeitverlauf. Sie können die Trends aus diesen Daten für die letzten 30 Tage überwachen. Sie können die Daten auch mithilfe der Filter Asset-Kategorie filtern. |
| VIs in Korrekturmaßnahmen | Anzahl der aktiven VIs aus der Gesamtzahl der VIs, die sich bereits in aktiven Korrekturmaßnahmen befinden. |
| Aktive Korrekturmaßnahmen | Liste der aktiven Korrekturmaßnahmen. |
| **Betroffene CIs** | |
| Eindeutige CIs | Anzahl der Konfigurationselemente (CIs) (Assets), die von diesen Schwachstellen betroffen sind. |
| AEs pro CI-Klasse | Anzahl der angreifbaren Elemente (AEs) für jede Configuration Management Database (CMDB) CI-Klasse.<br>**Hinweis:**<br>Dieses Widget wird nur für die Überwachungsthemen im Host-, Anwendungs- und Container-Schwachstellenmodul angezeigt. |
| Konfigurationsprobleme pro CI-Klasse | Anzahl der CIs für jede Configuration Management Database (CMDB) CI-Klasse. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarten und Visualisierungen für zugehörige Elemente in einem Überwachungsthema (Fortsetzung)**

| Registerkarte „Zugehörige Elemente“ und Visualisierung | Beschreibung |
|---|---|
| | **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul „Konfigurationsprobleme“ angezeigt. |
| VIs mit Internetzugriff | Anzahl der aktiven VIs aus der Gesamtzahl der VIs für Ihre Assets, die über das Internet verfügbar gemacht werden.<br>**Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Host-, Anwendungs- und Container-Schwachstellenmodul angezeigt. |
| Konfigurationsprobleme mit Internetverbindung | Anzahl der aktiven CIs aus der Gesamtzahl der CIs für Ihre Assets, die über das Internet verfügbar gemacht werden.<br>**Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul „Konfigurationsprobleme“ angezeigt. |
| **Eindeutige Schwachstellen** | |
| VIs mit vorhandenen Exploits | Aktive VIs mit bekannten Exploits. |
| Eindeutige Schwachstellen | Anzahl der einzelnen, unterschiedlichen Schwachstellen, die Ihren Assets zugeordnet sind. Die eindeutigen Schwachstellen können basierend auf dem Problemtyp gefiltert werden. |
| VIs mit PCI-Schwachstellen | Anzahl der einzelnen, unterschiedlichen Assets mit aktiven VIs mit PCI-Schwachstellen (Payment Card Industry). |
| **Angreifbare Elemente** | |
| Angreifbare Host-Elemente | Liste aller angreifbaren Hostelemente. Sie können diese Liste filtern, sodass nur die Datensätze angezeigt werden, die Sie anzeigen möchten.<br>**Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Host-Schwachstellen“ angezeigt. |
| Angreifbare Anwendungselemente | Liste aller angreifbaren Anwendungselemente. Sie können diese Liste filtern, sodass nur die Datensätze angezeigt werden, die Sie anzeigen möchten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarten und Visualisierungen für zugehörige Elemente in einem Überwachungsthema (Fortsetzung)**

| Registerkarte „Zugehörige Elemente“ und Visualisierung | Beschreibung |
|---|---|
| | **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Anwendungsschwachstellen“ angezeigt. |
| Angreifbare Container-Elemente | Liste aller angreifbaren Containerelemente. Sie können diese Liste so filtern, dass nur die Datensätze angezeigt werden, die Sie anzeigen möchten.<br>**Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Container-Schwachstellen“ angezeigt. |
| Registerkarte „**Übersicht** “ in einem Überwachungsthema unter dem Modul „Konfigurationstestergebnisse“ | |
| Aktive Konfigurationstestergebnisse im Zeitverlauf | Anzahl der aktiven Konfigurationstestergebnisse im Zeitverlauf. Sie können die Trends aus diesen Daten für die letzten 30 Tage überwachen. |
| Konfigurationstestergebnisse bei Korrekturmaßnahmen | Anzahl der aktiven Konfigurationstestergebnisse aus der Gesamtzahl der Datensätze, die sich bereits in aktiven Korrekturmaßnahmen befinden. |
| Aktive Korrekturmaßnahmen | Liste der aktiven Korrekturmaßnahmen. |
| Registerkarte „**Unterschiedliche Konfigurationstests** “ in einem Überwachungsthema unter dem Modul „Konfigurationstestergebnisse“. | |
| Konfigurationstestergebnisse über Testrelevanz | Konfigurationstestergebnisse, die auf der Relevanz der Probleme basieren. |
| Unterschiedliche Konfigurationstests | Anzahl der eindeutigen Konfigurationstests. |
| Registerkarte „**Konfigurationstestergebnisse** “ in einem Überwachungsthema unter dem Modul „Konfigurationstestergebnisse“. | Liste der Konfigurationstestergebnisse. |

Sie können die neuesten Details eines Überwachungsthemas abrufen, indem Sie auf die Schaltfläche **Aktualisieren** klicken. Der aktuelle Aktualisierungsstatus und der Zeitstempel werden unter dem Namen des Überwachungsthemas angezeigt. Wenn Sie ein Überwachungsthema aktualisieren, werden alle Details des Überwachungsthemas aktualisiert, einschließlich der Diagramme und Korrekturmaßnahmen. Ein Überwachungsthema wird automatisch aktualisiert, wenn es erstellt oder aktualisiert wird.

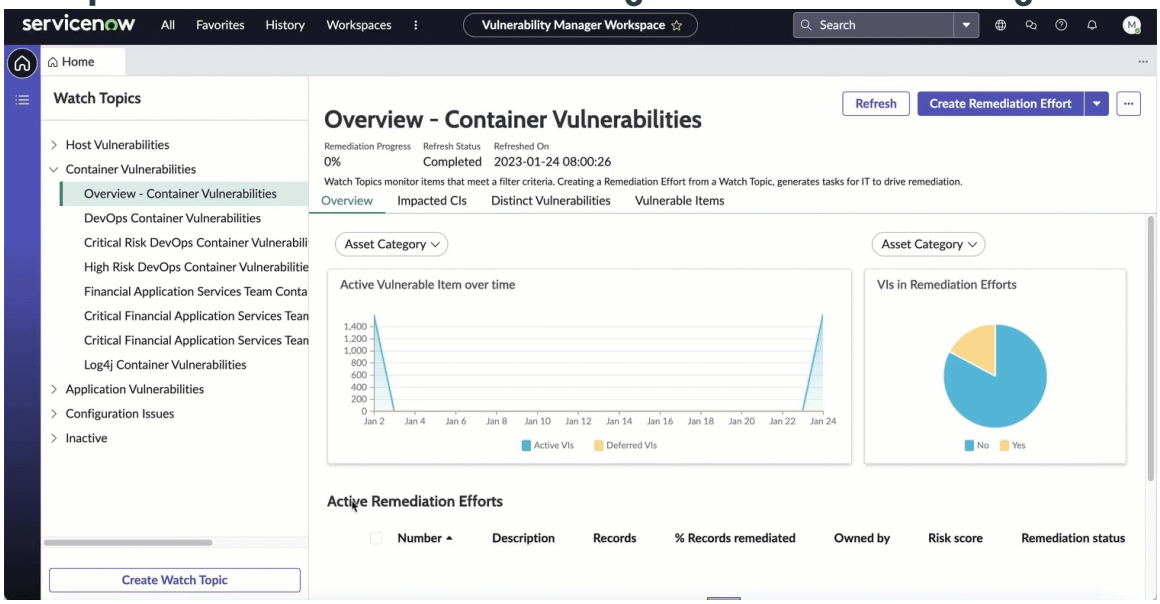
**Hinweis:**
Da Sie ein inaktives Überwachungsthema nicht aktualisieren können, ist die **Schaltfläche** Aktualisieren für ein inaktives Überwachungsthema inaktiv.

Klicken Sie in einem der Widgets auf eine Datenzeichnung, um zusätzliche Informationen zu den Datensätzen anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Example: Version 18.0 Datenvisualisierungen in einem Überwachungsthema




### Übersicht über die Korrekturmaßnahmen

Eine Korrekturmaßnahme ist eine Reihe von Datensätzen, die einem Überwachungsthema zugeordnet sind. Die in einer Korrekturmaßnahme aufgelisteten Datensätze sind statisch. Sie werden nicht durch neue Importdaten oder Änderungen aktualisiert, die Sie an Überwachungsthemen vornehmen.

Wählen Sie **Aktiv** in der Liste der **Korrekturmaßnahmen** aus, und klicken Sie auf den Link einer Korrekturmaßnahme, um sie zu öffnen.

Mit den zugehörigen Listenelementen im Datensatz der Korrekturmaßnahme können Sie den Gesamtfortschritt und Status der Korrektur in den zugehörigen Datensätzen anzeigen.

- Überwachen Sie auf der Registerkarte **Übersicht** die mit dieser Korrekturmaßnahme verknüpften Datensätze, die im Laufe der Zeit geschlossen wurden. Klicken Sie rechts neben dem Datensatz auf das Filtersymbol im Diagramm, um die auf die Datenvisualisierung angewendeten Filter anzuzeigen.
- Zeigen Sie auf der Registerkarte **Details** Details zur Korrekturmaßnahme an, einschließlich des zugehörigen Überwachungsthemas und Status (Aktiv oder Inaktiv). Sie können eine Korrekturmaßnahme auf dieser Seite deaktivieren. Wenn Sie die Korrekturmaßnahme deaktivieren, bevor alle Datensätze geschlossen sind, werden alle aktiven Datensätze verfügbar, die zu neuen Korrekturmaßnahmen hinzugefügt werden können.
- **Zeigen** Sie auf der Registerkarte Korrekturaufgaben die Korrekturaufgaben an, die dieser Korrekturmaßnahme zugeordnet sind. Zeigen Sie den Prozentsatz der dieser Aufgabe zugeordneten Datensätze an, die korrigiert wurden.
- Zeigen Sie auf der Registerkarte **„Angreifbare** Elemente“ die Datensätze an, die dieser Korrekturmaßnahme zugeordnet sind. Wenn alle Datensätze in einer Korrekturaufgabe abgeschlossen und geschlossen sind, wird die Korrekturmaßnahme in „Inaktiv“ geändert. Wenn eine Korrekturmaßnahme inaktiv ist, können nicht alle geschlossenen Datensätze, die der Korrekturmaßnahme zugeordnet sind, neuen Korrekturmaßnahmen hinzugefügt werden.

**Hinweis:**
Ab Version 18.0 wird die Registerkarte Angreifbare Elemente für die Korrekturmaßnahmen angezeigt, die Überwachungsthemen in den Modulen „ **Hostschwachstellen** “, „Anwendungsschwachstellen“ und „Containerschwachstellen“ zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zeigen Sie auf der Registerkarte Konfigurationstestergebnisse**die Konfigurationstestergebnisse an, die der Korrekturmaßnahme zugeordnet sind.

**Hinweis:**
Ab Version 18.0 wird die Registerkarte „ **Konfigurationstestergebnisse** “ für die Korrekturmaßnahmen angezeigt, die den Überwachungsthemen im Modul „Konfigurationstestergebnisse“ zugeordnet sind.

Weitere Details und UI-Aktionen, die Sie aus einer Korrekturmaßnahme ausführen können, finden Sie unter Verwenden Sie Datensätze der Korrekturmaßnahme.

### Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in Vulnerability Response Workspaces

Die Status von Datensätzen und die zugehörigen Korrekturaufgaben (RTs) werden beeinflusst, wenn Datensätze zurückgestellt, aufgelöst, erneut geöffnet und an andere Korrekturmaßnahmen (REs) übertragen werden.

Erforderliche Rollen: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin für Vulnerability Manager Workspace.

## Erstellen von Korrekturmaßnahmen

Wie die Status und Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen beeinflusst werden, hängt davon ab, wie eine Korrekturmaßnahme erstellt wird, wann sie erstellt wird und ob sie deaktiviert wird.

In der Liste oben rechts in einem Überwachungsthema können Sie eine Korrekturmaßnahme erstellen, indem Sie auf Korrekturmaßnahme erstellen oder **Wiederkehrende** Maßnahme **erstellen**klicken. Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen. Wenn Sie eine wiederkehrende Korrekturmaßnahme erstellen, werden nachfolgende Korrekturmaßnahmen für das zugehörige Überwachungsthema automatisch basierend auf den von Ihnen festgelegten Kriterien erstellt. In beiden Fällen:

- Um die Korrektur zu erleichtern, werden den Korrekturbemühungen nur aktive Datensätze hinzugefügt.
- Alle Datensätze in neuen Korrekturmaßnahmen werden in neue Korrekturaufgaben eingefügt. Datensätze können in mehreren Korrekturaufgaben vorhanden sein, aber nur ein Datensatz kann einer Korrekturmaßnahme zugeordnet werden.

**Hinweis:**
Eine Korrekturmaßnahme wird automatisch deaktiviert, wenn keine aktiven Datensätze vorhanden sind.

## Übertragen von Datensätzen oder Übertragen von Datensätzen

Sie können Datensätze von einer Korrekturmaßnahme in eine andere übertragen, wenn Sie eine Korrekturmaßnahme erstellen, indem Sie das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen übertragen** aktivieren. Weitere Informationen zum Übertragen der Datensätze finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen in den Vulnerability Response Arbeitsbereichen. Wenn Datensätze aus einer Korrekturmaßnahme übertragen oder in wiederkehrende Korrekturmaßnahmen übertragen werden:

**Zu einer neuen Korrekturmaßnahme im selben Überwachungsthema**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle Korrekturaufgaben aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben.
- Neue Korrekturaufgaben werden basierend auf den ausgewählten Gruppierungskriterien für die Datensätze erstellt, die zuvor nicht Teil einer Korrekturaufgabe waren.
- Die alte Korrekturmaßnahme ist deaktiviert.

**Zu einer neuen Korrekturmaßnahme in einem anderen Überwachungsthema**

Alle Datensätze aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben, und Korrekturaufgaben werden basierend auf den ausgewählten Gruppierungskriterien erstellt.

- Wenn alle Datensätze in den Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, übertragen werden, werden diese Korrekturaufgaben als abgebrochen geschlossen.
- Wenn nur eine Teilmenge der Datensätze übertragen wird, werden die der alten Korrekturmaßnahme zugeordneten Korrekturaufgaben aufgeteilt und bleiben aktiv.

Die geschlossenen Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, sind nicht betroffen.

**Hinweis:**
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen zum Übertragen von Datensätzen finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen in den Vulnerability Response Arbeitsbereichen.

### Dashboardübersicht

Sie können die Dashboards in der Benutzeroberfläche von Next Experience in Vulnerability Manager Workspace anzeigen und diese Dashboards zum Nachverfolgen und Analysieren der Schwachstellen verwenden.

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin oder sn_vulc.admin

Sie können die Dashboards in Vulnerability Manager Workspace anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**. Das Standard-Dashboard wird basierend auf Ihrer Rolle angezeigt.

Die folgende Tabelle zeigt das Standard-Dashboard, das für eine bestimmte Rolle angezeigt wird.

**Standard-Dashboard**

| Standard-Dashboard | Rolle |
|---|---|
| Einheitliches Dashboard | sn_vul_cmn_vulnerability_admin oder sn_vul_cmn_vulnerability_analyst |
| Schwachstellen-PA-Dashboard | sn_vul_vulnerability_admin oder sn_vul_vulnerability_analyst |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Standard-Dashboard (Fortsetzung)

| Standard-Dashboard | Rolle |
|---|---|
| Anwendungsübersicht | sn_vul_app_sec_manager |
| Containerübersicht | sn_vul_container_vulnerability_admin oder sn_vul_container_analyst |

Sie können die folgenden Dashboards für die Aufgaben anzeigen, die Sie ausführen möchten, indem Sie sie in der Dropdown-Liste auf der Seite „Dashboards“ auswählen.

### Dashboards in Vulnerability Manager Workspace

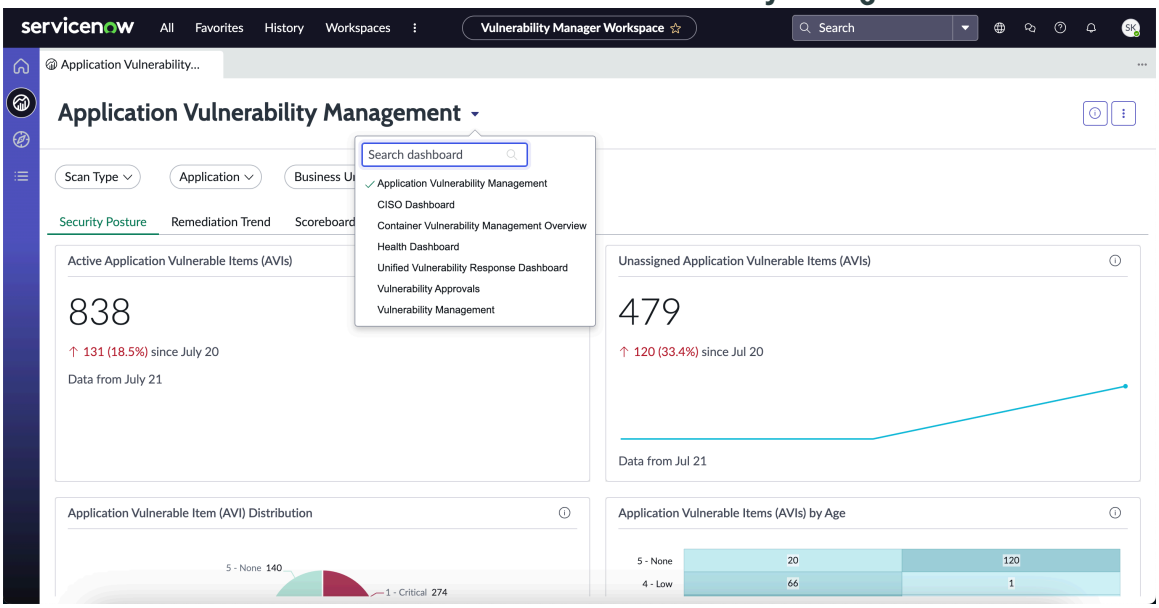
| Dashboard | Beschreibung |
|---|---|
| Schwachstellenmanagement (PA) | Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Host-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach. Weitere Informationen finden Sie unter Vulnerability Management (PA) -Dashboard. |
| Schwachstellengenehmigungen | Zeigen Sie die Anzahl der für Sie genehmigten, abgelehnten und ausstehenden Genehmigungsanforderungen an. Weitere Informationen finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet. |
| CISO-Dashboard | Zeigt die allgemeine Sicherheitslage Ihrer Organisation an, einschließlich Sicherheitsschwachstelle und Incidents. Weitere Informationen finden Sie unter CISO-Dashboard. |
| Container-Schwachstellenmanagement – Übersicht | Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Container-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach. Weitere Informationen finden Sie unter Container Vulnerability Response-Dashboard. |
| Dashboard für Anwendungsschwachstellenmanagement | Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Anwendungsschwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach.Application Vulnerability Management (PA)-Dashboard |
| Einheitliches Vulnerability Response-Dashboard | Bietet Transparenz aus mehreren Schwachstellenscannern und Sicherheitstools, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten. Weitere Informationen finden Sie unter Analytics- und Reporting-Lösungen für das Unified Vulnerability Response Dashboard. |
| Health Vulnerability Response Dashboard | Zeigt die Gesamtintegritätspunktzahl der Vulnerability Response-Anwendung an. |

Die folgende Abbildung zeigt die Seite „Dashboards“ in Vulnerability Manager Workspace.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Version 19.0 Dashboards im Arbeitsbereich von Vulnerability Manager




Sie können ein benutzerdefiniertes Dashboard erstellen, indem Sie das Symbol „ ⋮ auswählen und dann **Neues Dashboard erstellen**auswählen.

### Listenübersicht

Die Listenansicht im Arbeitsbereich von Vulnerability Manager ermöglicht es Schwachstellen- und Sicherheitsmanagern und Analysten, den Korrekturfortschritt für Datensätze anzuzeigen, Detailinformationen zu Vulnerability Response-Datensätzen anzuzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzuzeigen.

Diese Listen und Links bieten Ihnen einfachen Zugriff auf Datensätze und Aufgaben. Sie enthält zwei Registerkarten:

- Registerkarte**Listen** : Zeigt die Standardlisten für Korrekturbemühungen, Korrekturaufgaben, angreifbare Elemente, Lösungen, Ausnahmen und Konfigurationstestergebnisse an.
- Registerkarte**Meine Listen** : Zeigt alle Listen an, die Sie auf der Registerkarte Liste umbenannt haben, und alle Listen, die Sie erstellen.

  Sie können auch eine eigene Liste erstellen, um den Fortschritt der Fehlerkorrektur zu überwachen. Weitere Informationen finden Sie unter Erstellen Sie eine benutzerdefinierte Liste von Datensätzen.

## Registerkarte „Listen“.

Die folgenden Listen werden angezeigt:

- Korrekturaufwände (REs) – Zeigt aktive REs und alle REs an, die Ihren Gruppen zugewiesen sind.
- Korrekturaufgaben (VULs): Zeigt aktive Korrekturaufgaben und alle Korrekturaufgaben an, die Ihren Gruppen zugewiesen sind.

**Hinweis:**
Ab Version 18.0 werden in der Liste der Korrekturaufgaben die Korrekturaufgaben angezeigt, die in der klassischen Benutzeroberfläche und im Arbeitsbereich für Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Configuration Complianceerstellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbare Elemente – Zeigt aktive (offene) Datensätze und alle Datensätze an, die Ihren Gruppen zugewiesen sind.
- Lösungen: Zeigt alle Lösungen für angreifbare Elemente an.
- Ausnahmen: Zeigt Genehmigungsstatus für alle Ausnahme- und falsch positiven Anforderungen Ihrer Gruppen an.
- Genehmigungen: Zeigt Genehmigungsanforderungen an, die Ihnen zur Verarbeitung zugewiesen sind. Informationen zum Verarbeiten Ihrer Genehmigungen im Arbeitsbereich finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.
- Ab Version 18.0 werden die folgenden Listen auch in der Listenansicht angezeigt:
  - Angreifbare Host-Elemente: Zeigt aktive angreifbare Host-Elemente (VIs) und alle Host-VIs aus dem Modul „Host-Schwachstellen“ an.
  - Angreifbare Anwendungselemente: Zeigt aktive angreifbare Anwendungselemente (AVITs) und alle AVITs aus dem Modul „Anwendungsschwachstellen“ an.
  - Angreifbare Container-Elemente: Zeigt aktive angreifbare Container-Elemente (CVITs) und alle CVITs aus dem Modul „Container-Schwachstellen“ an.
  - Konfigurationstestergebnisse: Zeigt aktive Konfigurationstestergebnisse und alle Konfigurationstestergebnisse aus dem Modul „Konfigurationstestergebnisse“ an.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

  - Bibliotheken: Zeigt die folgenden Bibliotheken, Richtlinien und Tests an.
    - CVEs: Zeigt alle gemeinsamen Schwachstellen und Gefährdungen (CVEs) von Vulnerability Response, Application Vulnerability Responseund Container Vulnerability Responsean.
    - TPEs: Zeigt alle Drittpartei-Einträge (TPEs) von Vulnerability Responsean.
    - CWEs – Zeigt alle Common Weakness Enumerations (CWEs) von Vulnerability Response, Application Vulnerability Responseund Container Vulnerability Responsean.
    - App-Schwachstellen: Zeigt alle Anwendungsschwachstelleneinträge von Drittparteianwendungen an.
    - Richtlinien: Zeigt alle Configuration Compliance Richtlinien an.
    - Tests: Zeigt alle Tests von Configuration Compliancean.
    - Ausgleichskontrollen: Zeigt alle Ausgleichskontrollen an, die für Risikominderungsanforderungen verwendet werden. Sie können eine Ausgleichskontrolle hinzufügen, indem Sie auf **Neu**klicken. Weitere Informationen zum Hinzufügen einer Ausgleichskontrolle finden Sie unter Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu.

**Hinweis:**
Die Liste „Ausgleichskontrollen“ wird ab v20.0 von Vulnerability Responseangezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Ausgleichskontrollen sind die Maßnahmen, die ergriffen werden, um das Risiko von Schwachstellen zu reduzieren, die nicht sofort behoben werden können. Sie können verwendet werden, um die Wahrscheinlichkeit oder Auswirkung eines erfolgreichen Exploits zu verringern.

**Hinweis:**
Die Funktion „Ausgleichskontrollen“ ist nur für Host-Schwachstellen verfügbar.

Die Anwendung von Ausgleichskontrollen kann dazu beitragen, das Risiko einer Schwachstelle zu reduzieren.

Die folgende Tabelle zeigt die Anwendungsfälle für Ausgleichskontrollen:

**Anwendungsfälle für Ausgleichskontrollen**

| Anwendungsfall | Ausgleichskontrolle |
|---|---|
| Eine Schwachstelle in einem Webserver, die es Angreifern ermöglicht, beliebigen Code auszuführen. | Implementieren Sie eine Web Application Firewall (WAF), um schädliche Anforderungen an den Webserver zu blockieren. |
| Eine Schwachstelle in einem Betriebssystem, die es Angreifern ermöglicht, Berechtigungen auf den Stamm zu eskalieren. | Implementieren Sie die Anwendungssteuerung, um einzuschränken, welche Anwendungen auf dem Hostsystem ausgeführt werden können. |
| Eine Schwachstelle in einem Datenbankserver, die Angreifern den Zugriff auf vertrauliche Daten ermöglicht. | Implementieren Sie die Netzwerksegmentierung, um den Datenbankserver von anderen Hosts und kritischen Systemen zu isolieren. |

Weitere Informationen zu den Auswirkungen von Ausgleichskontrollen auf die Risikopunktzahl eines angreifbaren Elements und einer Korrekturaufgabe finden Sie unter Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum.

**Zugehörige Informationen**

Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

### Analytics- und Reporting-Lösungen für das Unified Vulnerability Response Dashboard

Platform Analytics-Lösungen enthalten vorverpackte Platform Analytics -Inhalte zur Verwendung mit anderen Now Platform -Produkten. Das Unified Vulnerability Response Dashboard ist ein zentralisiertes, zusammengefasstes Dashboard, das Einblicke in mehrere Schwachstellenscanner und Sicherheitstools bietet, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten.

## Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet. Sie sind zum Anzeigen und Freigeben der Berichte erforderlich:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

**Zugehörige Informationen**

Analytics- und Reporting-Lösungen

### Einheitliches Vulnerability Response-Dashboard

Das Dashboard „Unified Vulnerability Response“ bietet eine umfassende Ansicht der Schwachstellen und Risiken einer Organisation. Die Schwachstellen im Zusammenhang mit Infrastruktur, Cloud, Anwendungen und Containern können zur besseren Transparenz und Behebung in einem zentralen Dashboard angezeigt werden.

## Erforderliche Now Platform-Rollen

Die folgenden Rollen sind dieser Lösung zugeordnet. Sie sind zum Anzeigen, Bearbeiten und Freigeben der Berichte erforderlich:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

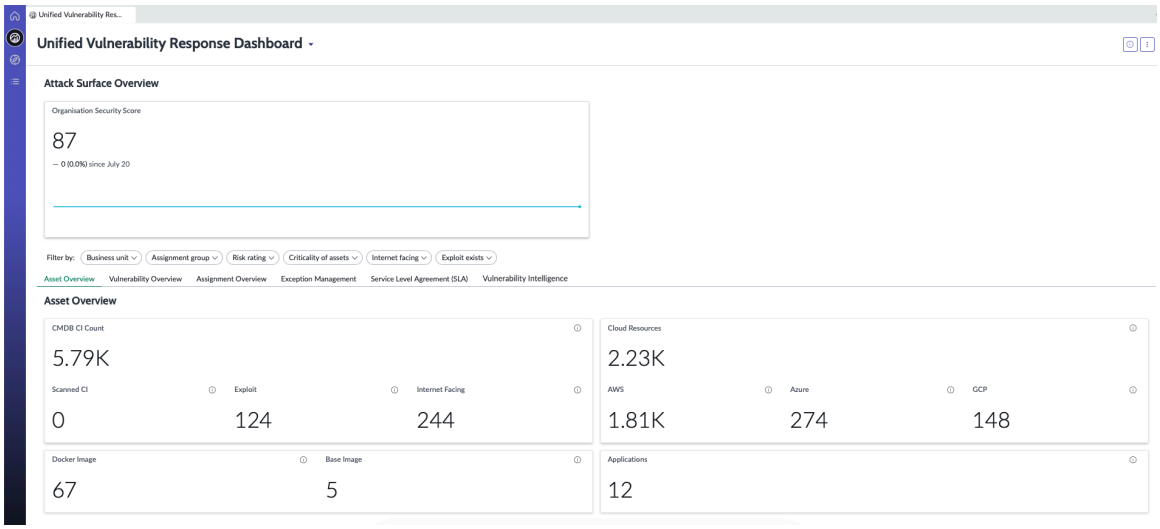
## Greifen Sie auf das Unified Vulnerability Response-Dashboard zu

Um das Dashboard zu öffnen, navigieren Sie zu einem der folgenden Elemente:

- **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** und wählen Sie das Symbol **Dashboards**. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um das Unified Vulnerability Response-Dashboard anzuzeigen, wählen Sie die Dropdown-Liste neben dem Dashboard-Namen aus.
- **Arbeitsbereiche** > **Platform Analytics-Arbeitsbereich** > **Dashboards** > **Einheitliches Vulnerability Response-Dashboard**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

| Anwender | Dashboard-Verwendung |
|---|---|
| • Schwachstellenmanager<br>• Schwachstellenanalysten | • Bietet Echtzeittransparenz der Risiken in Infrastruktur, Anwendungen, Konfigurationen und Containern. Eermöglicht ihnen, die Schwachstellen rechtzeitig zu priorisieren und zu beheben.<br>• Stellt eine Angriffsoberflächenübersicht von kritischen Assets bereit, die zur Nachverfolgung des Korrekturfortschritts und der Korrekturmaßnahmen verwendet werden kann.<br>• Bietet eine Übersicht über Risiken in Geschäftsbereichen (Business Units, BUs). Sie können Filter verwenden, um Geschäftsbereiche auszuwählen und den Fortschritt bei der Neuzuteilung von Ressourcen nach Bedarf zu vergleichen. Dem Geschäftsbereichsleiter muss Zugriff auf Rollenebene gewährt werden.<br>• Bietet Einblick in die potenziellen Auswirkungen nach Geschäftsbereichen. Sie können den CVE-Filter (Common Vulnerability and Exposure) verwenden, um Gefährdungen in der gesamten Organisation zu identifizieren.<br>• Bietet Einblick in die EPSS-Punktzahlen, die von angreifbaren |



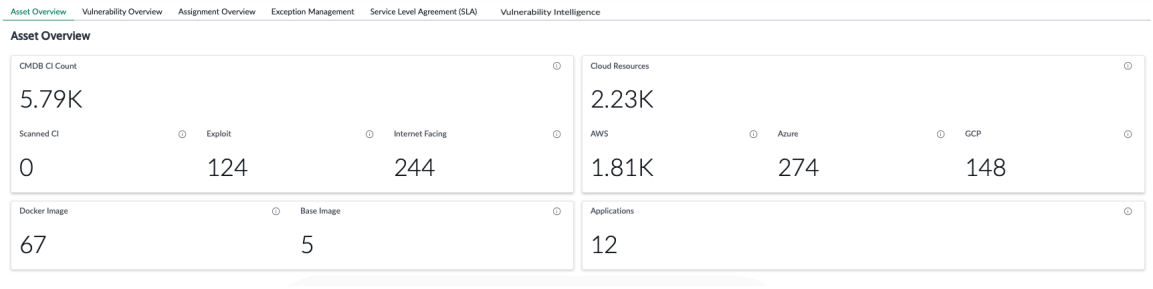
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwender | Dashboard-Verwendung |
| --- | --- |
| | Einträgen im CISA-KEV-Katalog für angreifbare Anwendungs-, Host- und Containerelemente erreicht werden. |

## Unified Vulnerability Response Dashboard-Registerkarten

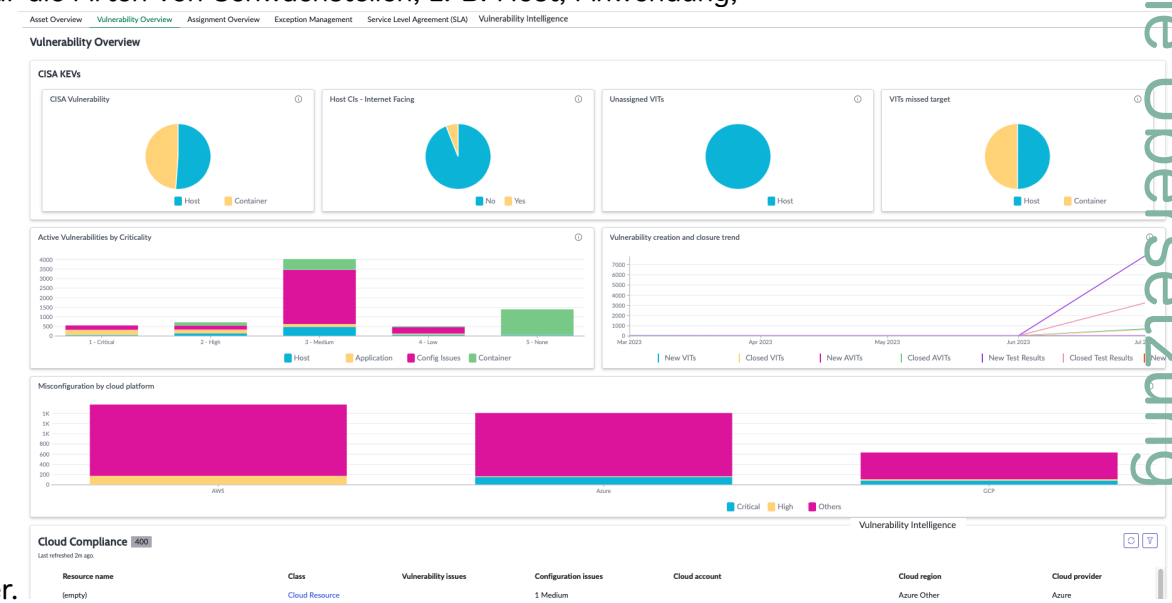
In diesem Dashboard können Sie die Schwachstellen oder Probleme anzeigen, die in Hosts, Cloud, Konfigurationen, Anwendungen und Containern vorhanden sind. Sie können die Schwachstellen basierend auf Geschäftsbereich, Zuweisungsgruppe, Risikobewertung, Relevanz und Exploit für die Schwachstellen anzeigen.

Die Registerkarte „ **Asset-Übersicht** “ zeigt den Gesamtstatus der Konfigurationselemente (CIs) im System




an.

Die Registerkarte „ **Schwachstellenübersicht** “ enthält einen Status für die Arten von Schwachstellen, z. B. Host, Anwendung,



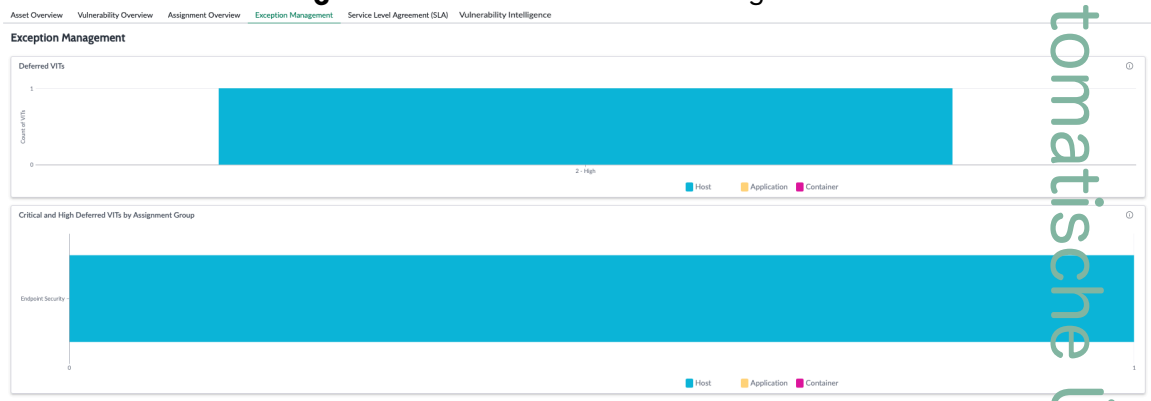

Container.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Registerkarte „ **Zuweisungsübersicht** “ enthält einen Status für die Zuweisung der Schwachstellen.

Die Registerkarte **Ausnahmenverwaltung** enthält einen Status der zurückgestellten Schwachstellen.



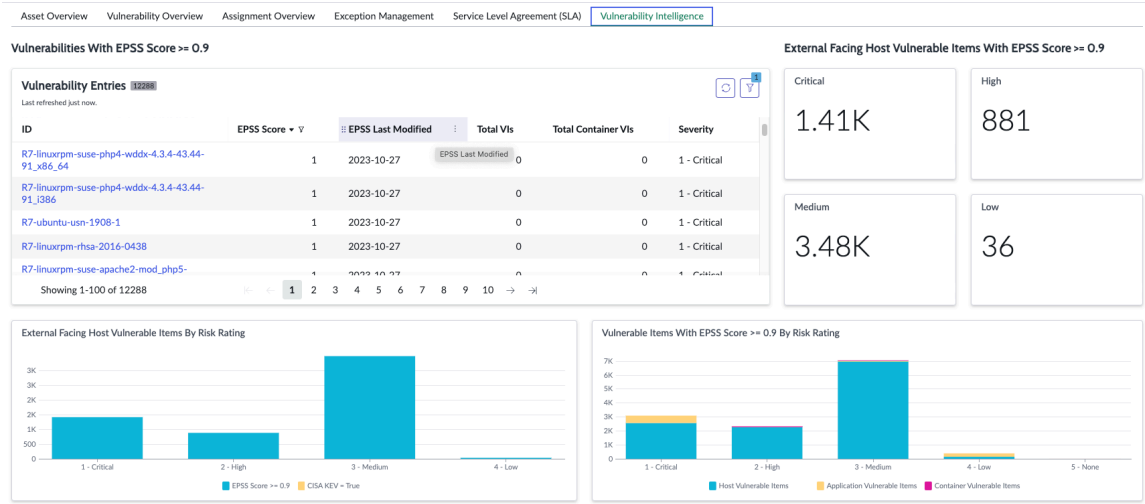

Die Registerkarte Servicelevel- **Vereinbarung (Service Level Agreement, SLA)** enthält einen Status der Servicelevel-Vereinbarung, die von verschiedenen Zuweisungsgruppen erreicht wurde.

Die Registerkarte „ **Vulnerability Intelligence** “ bietet einen Status für die EPSS-Punktzahlen, die von Schwachstellen mit der CISA-KEV-Kennzeichnung „true“ und einer EPSS-Punktzahl >= 0,9 für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbare Anwendungs-, Host- und Container-Elemente erreicht wurden.




## Filter

Sie können die Widgets nach Folgendem filtern:

- Geschäftsbereich
- Zuweisungsgruppe
- Risikobewertung
- Relevanz von Assets
- Mit Internetzugriff
- Exploit vorhanden

Wenn ein Filter ausgewählt wird, werden die Daten in allen Widgets aktualisiert. Wenn jedoch ein Filter für ein Widget nicht anwendbar ist, wird neben dem Filternamen ein Cross-Symbol angezeigt.

**Hinweis:**
In Tokyosind nur Filter für Geschäftsbereich und Zuweisungsgruppe verfügbar. Alle Filter sind ab Utah verfügbar.

## Indikatoren

**Gescannte Assets**

Formelindikator für in den letzten 60 Tagen gescannte Assets. Enthält gescannte erkannte Element-Assets, gescannte Anwendungs-Release-Assets und gescannte erkannte Container-Image-Assets als beitragende Indikatoren.

**Assets – Exploit vorhanden**

Formelindikator für Assets, bei denen Exploits in den Schwachstellen vorhanden sind. Enthält Host-Assets – Exploit vorhanden, Anwendungs-Assets – Exploit vorhanden, Container-Assets – Exploit vorhanden als beitragende Indikatoren

**Infra-Asset – mit Internetzugriff**

Indikator zum Abrufen der Anzahl der Assets, die mit dem Internet verbunden sind.

**Erkannte Elemente basierend auf Cloud-Ressourcentyp**

Indikator zum Abrufen der Anzahl von Assets mit einer Asset-Kategorie wie „Cloud“.

**Basis-Images**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indikator zum Abrufen der Anzahl der Basis-Images.

**CISA-KEVs-Asset-Typ**

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen die Kennzeichnung „CISA KEV (BOD 22-01)“ für die Schwachstelle auf „true“ gesetzt ist. Enthält „CISA vorhanden – CVR“ und „CISA vorhanden – Angreifbare Elemente“ als beitragende Indikatoren.

**CISA vorhanden – Angreifbare Elemente – Nicht zugewiesen**

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung „CISA KEV (BOD 22-01)“ auf „wahr“ gesetzt ist und die angreifbaren Elemente nicht zugewiesen sind. Enthält nicht zugewiesene angreifbare Container-Elemente und nicht zugewiesene angreifbare Host-Elemente als beitragende Indikatoren.

**CISA vorhanden – Angreifbare Elemente – Ziel verfehlt**

Formelindikator, der die Anzahl der angreifbaren Container- und Hostelemente angibt, bei denen die Kennzeichnung „CISA KEV (BOD 22-01)“ für die Schwachstelle auf „wahr“ gesetzt ist und die angreifbaren Elemente das Ziel verfehlt haben. Enthält „CISA vorhanden“ angreifbare Elemente, „CISA vorhanden“-CVR als beitragende Indikatoren.

**Aktive Host-VITs**

Anzahl der aktiven angreifbaren Hostelemente (VITs).

**Aktive Anwendungs-VITs**

Anzahl der aktiven angreifbaren Elemente in Anwendungen (AVITs).

**Aktive Container-VITs**

Anzahl der aktiven angreifbaren Containerelemente (CVITs).

**Neue VITs**

Anzahl der an einem Tag geöffneten VITs

**Neue AVITs**

Anzahl der AVITs, die an einem Tag geöffnet wurden.

**Neue CVITs**

Anzahl der CVITs, die an einem Tag geöffnet wurden.

**Neue Testergebnisse**

Anzahl der Testergebnisse (TRs), die an einem Tag erstellt wurden.

**Geschlossene AVITs**

Anzahl der an einem Tag geschlossenen VITs

**Geschlossene VITs**

Anzahl der an einem Tag geschlossenen AVITs

**Geschlossene CVITs**

Anzahl der an einem Tag geschlossenen CVITs

**Geschlossene Testergebnisse**

Anzahl der an einem Tag geschlossenen TRs.

**Offene Konfigurationsprobleme – Testergebnisse**

Anzahl aller offenen Testergebnisse, die sich im Status „Fehlgeschlagen“ befinden.

**Risikopunktzahl der Organisation**

Risikopunktzahl einer Organisation aus der Tabelle „Rollup-Anwendungsrisikopunktzahl“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Nicht zugewiesene angreifbare Anwendungselemente**

AVITs ohne Zuweisungsgruppe oder zugewiesen zu.

**Nicht zugewiesene angreifbare Host-Elemente**

VITs ohne Zuweisungsgruppe oder zugewiesen zu

**Nicht zugewiesene angreifbare Container-Elemente**

CVITs ohne Zuweisungsgruppe oder zugewiesen zu

**Nicht zugewiesene Konfigurationsprobleme**

TRs ohne Zuweisungsgruppe oder zugewiesen zu.

**Zurückgestellte VITs**

VITs im Status „Zurückgestellt“

**Zurückgestellte AVITs**

AVITs im Status „Zurückgestellt“

**Zurückgestellte CVITs**

CVITs im Status „Zurückgestellt“

**Host-SLA – Geschlossen**

Durchschnittliches Abschlussalter von geschlossenen VITs

**Anwendungs-SLA – Geschlossen**

Durchschnittliches Abschlussalter von geschlossenen AVITs

**Container-SLA – Geschlossen**

Durchschnittliches Abschlussalter von geschlossenen CVITs

**Testergebnis-SLA – Bestanden**

Durchschnittliches Abschlussalter von bestandenen TRs

**Host-SLA – Geschlossen (Kritisch und Hoch)**

Durchschnittliches Abschlussalter von geschlossenen VITs mit kritischen und hohen VITs.

**Anwendungs-SLA – Geschlossen (Kritisch und Hoch)**

Durchschnittliches Abschlussalter von kritischen AVITs und hohen AVITs

**Container-SLA – Geschlossen (Kritisch und Hoch)**

Durchschnittliches Abschlussalter von geschlossenen kritischen und hohen CVITs

**Testergebnis-SLA – Bestanden (Kritisch und Hoch)**

Durchschnittliches Abschlussalter von bestandenen kritischen und hohen TRs

**Aggregierte MTTR**

Durchschnittliches Abschlussalter von geschlossenen VITs, AVITs, CVITs und TRs

**SLA verfehlt**

Durchschnittliches Abschlussalter von geschlossenen VITs, AVITs, CVITs und TRs mit verfehltem Ziel.

**Schwachstellen mit EPSS-Punktzahlen >= 0,9**

Anzahl der Schwachstelleneinträge mit EPSS-Punktzahlen größer oder gleich 0,9.

## BreakdownsAufgliederungen

- VIT-Typ (einheitlich)
- Mit Internetzugriff (einheitlich)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Risikobewertung (einheitlich)
- Exploit vorhanden (einheitlich)
- Cloud-Ressourcentyp des erkannten Elements (einheitlich)
- CISA vorhanden (einheitlich)
- CMDB-Klasse (einheitlich)
- Geschäftsbereich (einheitlich)
- Business-Relevanz (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Zuweisungsgruppe (einheitlich)
- Korrekturstatus (einheitlich)

## Datenvisualisierungen

### Registerkarte „Asset-Übersicht“

| Titel | Typ | Beschreibung |
|---|---|---|
| Angriffsoberfläche – Übersicht | Einzelwert | Zahl, die die zusammengefasste Punktzahl der Sicherheit einer Organisation darstellt. |
| CMDB-CI-Anzahl | Einzelwert | Anzahl der CIs in der Organisation, die in Configuration Management Database (CMDB)registriert sind und nachverfolgt werden Stellt eine Aufgliederung der folgenden CIs bereit:<br>• Gescannte CIs: Anzahl der gescannten CIs<br>• Exploit: Anzahl der verfügbaren Exploits<br>• Mit Internetverbindung: Anzahl der CIs mit Internetzugriff |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Asset-Übersicht“ (Fortsetzung)

| Titel | Typ | Beschreibung |
|---|---|---|
| Cloud-Ressource | Einzelwert | Anzahl der CIs mit Asset-Kategorie wie „Cloud“. Stellt eine Aufgliederung der folgenden Cloud-Assets bereit:<br>• AWS<br>• Azure<br>• GCP |
| Docker-Bild | Einzelwert | Anzahl der Docker-Images einschließlich der Anzahl der Basis-Images. |
| Anwendungen | Einzelwert | Anzahl der Anwendungen in der Organisation. |

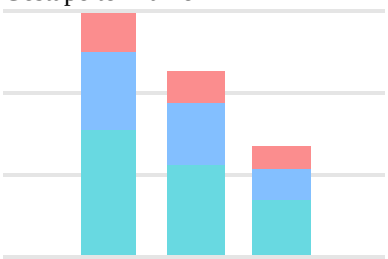
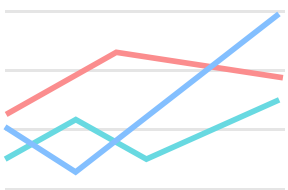
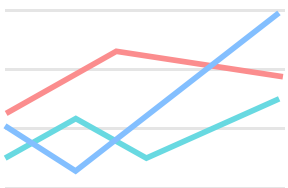
### Registerkarte „Schwachstellenübersicht“

| Titel | Typ | Beschreibung |
|---|---|---|
| CISA-KEVs | Kreisdiagramm | Anzahl der Schwachstellen, die mit dem Katalog CISA und der CISA-Kennzeichnung „wahr“ verknüpft sind.<br>Stellt eine Aufgliederung bereit, die auf Folgendem basiert:<br>• CISA-Schwachstelle: Arten von Schwachstellen mit „wahr“-CISA-Kennzeichnung<br>• Host-CIs – mit Internetverbindung: CIs mit Internetverbindung |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Schwachstellenübersicht“ (Fortsetzung)

| Titel | Typ | Beschreibung |
|---|---|---|
| | | • Nicht zugewiesene VITs: Nicht zugewiesene VITs mit CISA-Kennzeichnung „wahr“.<br>• VITs mit verfehltem Ziel: VITs, die das Ziel verfehlt haben und deren CISA-Kennzeichnung „wahr“ ist |
| Aktive Schwachstellen nach Relevanz | Gestapelter Balken  | Anzahl der aktiven VITs, AVITs und CVITs basierend auf Relevanz. |
| Trend bei der Erstellung und Schließung von Schwachstellen | Mehrere Leitungen  | Anzahl der neuen und geschlossenen Schwachstellen für alle Anwendungen. Stellt einen Trend für die letzten drei Monate bereit. |
| Falsche Konfiguration nach Cloud-Plattform | Mehrere Leitungen  | Anzahl der Konfigurationsprobleme basierend auf der Risikobewertung für jedes Cloud-Asset. |
| Cloud-Compliance | Tabelle | Liste der Ressourcen mit der Asset-Kategorie „Cloud“ mit den folgenden Details:<br>• Ressourcenname<br>• Klasse<br>• Schwachstellenprobleme: Anzahl der in der Ressource vorhandenen Probleme, die basierend |

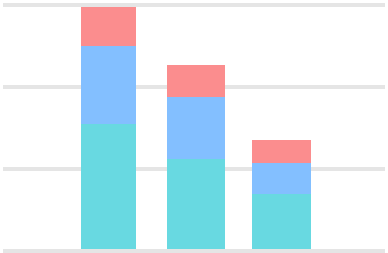
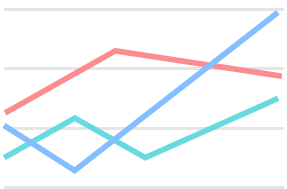
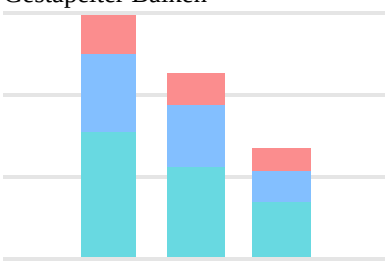
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Schwachstellenübersicht“ (Fortsetzung)

| Titel | Typ | Beschreibung |
|---|---|---|
| | | auf der Risikobewertung zusammengefasst werden.<br>• Konfigurationsprobleme: Anzahl der Ressourcen mit Konfigurationsproblemen zusammen mit Risikobewertung.<br>• Cloud-Konto: ID des Cloud-Kontos.<br>• Cloud-Region: Speicherort der Cloud-Ressourcen.<br>• Cloud-Provider: Name des Cloud-Providers. |

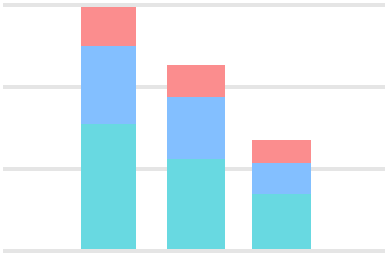
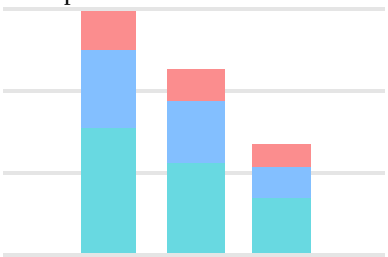
### Registerkarte „Zuweisungsübersicht“.

| Titel | Typ | Beschreibung |
|---|---|---|
| Nicht zugewiesene VITs | Gestapelter Balken  | Anzahl der Schwachstellen, die keiner Gruppe oder Einzelperson zugewiesen sind, zusammen mit Risikobewertung. |
| MTTR nach Zuweisungsgruppe – Top 10 | Mehrere Leitungen  | Durchschnittliche Zeit, die eine Zuweisungsgruppe benötigt, um die Sicherheitsschwachstellen oder -probleme zu identifizieren und zu beheben. Die 10 wichtigsten Zuweisungsgruppen mit der höchsten durchschnittlichen Zeit für die Korrektur werden angezeigt. |
| Top-10-Zuweisungsgruppen ohne SLA (als „kritisch“ und „hoch“ eingestufte Schwachstelle) | Gestapelter Balken  | Top-10-Zuweisungsgruppen, die das Zieldatum der Korrektur von kritischen und hohen Schwachstellen verfehlt haben. |

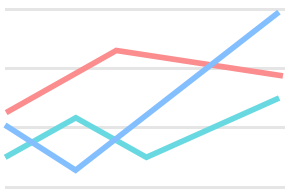
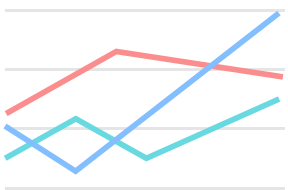


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Exception Management“

| Titel | Typ | Beschreibung |
|---|---|---|
| Zurückgestellte VITs | Gestapelter Balken  | Anzahl der Schwachstellen im Status „Zurückgestellt“ basierend auf der Risikobewertung. |
| Als „kritisch“ und „hoch“ eingestufte zurückgestellte VITs nach Zuweisungsgruppe | Gestapelter Balken  | Anzahl der Schwachstellen mit kritischen und hohen Risikobewertungen im Status „Zurückgestellt“, die basierend auf den Zuweisungsgruppen kategorisiert werden. |

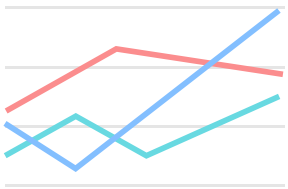
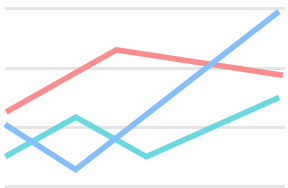
### Registerkarte Servicelevel-Vereinbarung (SLA).

| Titel | Typ | Beschreibung |
|---|---|---|
| Host-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe | Mehrere Leitungen  | Zeit, die eine Zuweisungsgruppe für die Behebung von Host-Schwachstellen benötigt hat. Stellt einen Trend für die letzten 10 Monate bereit. |
| Compliance-Probleme: SLA-Erreichung nach Zuweisungsgruppe | Mehrere Leitungen  | Zeit, die eine Zuweisungsgruppe für die Behebung von Compliance-Problemen benötigt hat. Stellt einen Trend für die letzten 10 Monate bereit. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte Servicelevel-Vereinbarung (SLA). (Fortsetzung)

| Titel | Typ | Beschreibung |
|---|---|---|
| Anwendungsschwachstelle: SLA-Erreichung nach Zuweisungsgruppe | Mehrere Leitungen  | Zeit, die eine Zuweisungsgruppe für die Korrektur von Anwendungsschwachstellen benötigt hat. Stellt einen Trend für die letzten 10 Monate bereit. |
| Container-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe | Mehrere Leitungen  | Zeit, die eine Zuweisungsgruppe für die Korrektur von Container-Schwachstellen benötigt hat. Stellt einen Trend für die letzten 10 Monate bereit. |

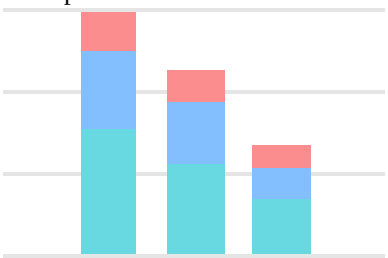
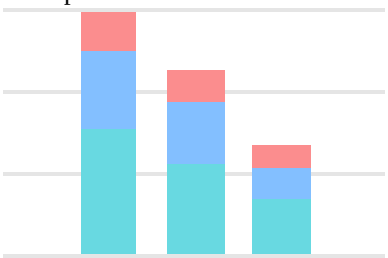
### Registerkarte „Schwachstellen-Intelligenz“.

| Titel | Typ | Beschreibung |
|---|---|---|
| Schwachstellen mit einer EPSS-Punktzahl >= 0,9 | Tabelle | Vollständige Listenansicht aller angreifbaren Einträge (CVEs oder TPEs), deren EPSS-Punktzahl größer oder gleich 0,9 ist, zusammen mit den folgenden Details.<br>• ID: CVE-ID der Schwachstelle<br>• EPSS-Punktzahl<br>• EPSS – Zuletzt geändert<br>• CISA KEV BOD 22-01: Gibt an, ob der Eintrag im CISA KEV BOD vorhanden ist (Binding Operational Direktive 22-01)<br>• AEs insgesamt: Gesamtanzahl der AEs, die für diesen Schwachstelleneintrag vorhanden sind.<br>• Container-VIs insgesamt: Gesamtanzahl |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Schwachstellen-Intelligenz“. (Fortsetzung)**

| Titel | Typ | Beschreibung |
|---|---|---|
| | | der Container-VIs, die für diesen Schwachstelleneintrag vorhanden sind.<br>• Schweregrad |
| Nach außen gerichtete angreifbare Host-Elemente mit einer EPSS-Punktzahl >= 0,9 | Einzelwert | Zahl, die die Gesamtanzahl der nach außen gerichteten angreifbaren Hostelemente mit einer EPSS-Punktzahl größer oder gleich 0,9 angibt. Stellt Einzelpunktzahlen bereit, sortiert nach Schweregrad der Risikobewertung. |
| Nach außen gerichtete angreifbare Host-Elemente nach Risikobewertung | Gestapelter Balken  | Anzahl der nach außen gerichteten angreifbaren Hostelemente nach Risikobewertung. Die Stapelleisten werden nach EPSS-Punktzahl >=0,9 und CISA KEV = True kategorisiert. |
| Angreifbare Elemente mit EPSS-Punktzahl >= 0,9 nach Risikobewertung | Gestapelter Balken  | Anzahl der Schwachstellen mit einer EPSS-Punktzahl größer oder gleich 0,9, sortiert nach Risikobewertung. Stellt eine Aufgliederung nach angreifbaren Hostelementen, angreifbaren Anwendungselementen und angreifbaren Containerelementen bereit. |

## Geplante Aufgaben für die Datenerfassung

Datensammlungsaufträge sammeln automatisch Punkte für automatisierte Indikatoren und Aufgliederungen. Die folgenden geplanten Aufgaben werden ausgeführt, um automatisch Punktzahlen für neue Daten zu sammeln.

**Warnung:**
Standardmäßig sind die folgenden Datenerfassungsaufgaben im Basissystem deaktiviert:

- Tägliche Datensammlung im einheitlichen Dashboard
- Wöchentliche Datensammlung im einheitlichen Dashboard
- Historische Datensammlung im einheitlichen Dashboard

Bevor Sie die Aufträge aktivieren, lesen Sie die KB .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Häufigkeit | Beschreibung |
|---|---|---|
| Historische Datensammlung im einheitlichen Dashboard | Einmal | Sammelt Punktzahlen und Snapshots für vorhandene Datensätze. |
| Wöchentliche Datensammlung im einheitlichen Dashboard | Wöchentlich | Erfasst Daten wöchentlich. |
| Tägliche Datensammlung im einheitlichen Dashboard | Täglich | Erfasst täglich Daten. |
| Rollup der Risikopunktzahlen zur Organisation | Täglich | Erfasst die zusammengefasste Risikopunktzahl für eine Organisation. |
| Füllen Sie die täglichen Cloud-Compliance-Anzahlen aus | Täglich | Sammelt Daten für Cloud-Compliance |
| Täglicher EPSS-Auftrag | Täglich | Sammelt EPSS-Daten von First.org |

Eine neue Tabelle „Rollup-Anwendungsrisikopunktzahl“ [sn_vul_cmn_rollup_app_risk_score] wird im allgemeinen Bereich der Schwachstelle erstellt. Diese Tabelle wird täglich mit den folgenden Rollup-Rechnern über die regelmäßigen Aufgaben ausgefüllt.

| Name des Rollup-Rechners | Beschreibung |
|---|---|
| Rollup für Risikopunktzahl der Organisation | Fasst die Risikopunktzahlen für alle angreifbaren Elemente und Konfigurationsprobleme in einer Organisation zusammen. Sie stellt eine Gesamtrisikopunktzahl für eine Organisation bereit. |
| Rollup für angreifbare Elemente | Fasst die Risikopunktzahlen für alle angreifbaren Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen. |
| Rollup für angreifbare Anwendungselemente | Fasst die Risikopunktzahlen für alle angreifbaren Anwendungselemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen. |
| Rollup für angreifbare Container-Elemente | Fasst die Risikopunktzahlen für alle angreifbaren Container-Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen. |
| Testergebnis-Rollup | Fasst die Risikopunktzahlen für alle Testergebnisse in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen. |
| Rollup von EPSS-Punktzahlen von NVDs zu TPEs | Rollup der EPSS-Punktzahlen von NVDs zu TPEs, um zur Gesamtrisikopunktzahl einer Organisation beizutragen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vulnerability Manager Workspace verwenden

In Vulnerability Manager Workspacekönnen Sie eine Reihe von Schwachstellen in einem Überwachungsthema gruppieren, indem Sie eine Bedingung definieren, und Sie können ihren Korrekturfortschritt nachverfolgen, indem Sie Korrekturmaßnahmen erstellen.

### Erstellen Sie Filter, um die Zusammenfassung der aktiven Datensätze anzuzeigen

Als Schwachstellenmanager und Analyst können Sie Filter erstellen, um die Zusammenfassung der gewünschten Datensätze im Vulnerability Manager Workspaceanzuzeigen .

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Homepage**.
2. Wählen Sie auf der Homepage auf einer der Registerkarten „ “, „Containerschwachstellen“, „Anwendungsschwachstellen“ oder „Konfigurationstestergebnisse“ das Zahnradsymbol Zahnradsymbol aus.
3. Füllen Sie im Dialogfeld „Gespeicherte Filter“ die Felder aus.

**Modales Fenster für gespeicherte Filter**

| Feld | Beschreibung |
|---|---|
| Filtername | Name für den Filter |
| Bedingungen | Bedingung für die kurze Liste der Datensätze, für die Sie die Visualisierungen anzeigen möchten. |

4. Wählen Sie **Speichern**.
   Der erstellte Filter wird in der **Dropdown** -Liste Anzeigen nach angezeigt.
5. Wählen Sie den **Filter** im Feld Anzeigen nach aus, um die Visualisierungen für die gefilterten Datensätze anzuzeigen.
   Weitere Informationen zu den Widgets finden Sie unter Homepage-Übersicht.
6. So aktualisieren oder löschen Sie einen Filter:
   a. Wählen Sie das Zahnradsymbol .
   b. Wählen Sie im Formular „Gespeicherte Filter“ die **Option Vorhandene Filter verwenden** aus, füllen Sie die Felder aus, und wählen Sie **Aktualisieren**.

**Formular „Gespeicherte Filter“**

| Feld | Beschreibung |
|---|---|
| Filter auswählen | Liste der vorhandenen Filter. |
| Filtername | Beschreibender Name für den Filter. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Bedingungen | Die Bedingungen des vorhandenen Filters. Bearbeiten Sie die Bedingung für eine neue Gruppe von Datensätzen. |

**c.** Um einen Filter zu löschen, wählen Sie **Löschen**.

### Verwenden Sie Überwachungsthemen in Vulnerability Manager Workspace

Verwenden Sie Überwachungsthemen im Arbeitsbereich von Vulnerability Manager, um Schwachstellen anzuzeigen, die aus Ihren importierten Daten anhand von von Ihnen festgelegten Kriterien gefiltert werden. Verwenden Sie diese Informationen, um zu bestimmen, wie sich die Schwachstellen in jedem Überwachungsthema auf Ihre Umgebung auswirken können.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

#### Warum und wann dieser Vorgang ausgeführt wird

Über die Überwachungsthemen können Sie die folgenden Aufgaben ausführen:

- Überwachen Sie die Anzahl der Korrekturbemühungen und Datensätze angreifbarer Elemente, um den Fortschritt der Schwachstellenkorrektur anzuzeigen.
- Bearbeiten oder löschen Sie vorhandene Überwachungsthemen, und erstellen Sie Themen.
- Erstellen Sie die Korrekturmaßnahmen, und übergeben Sie die Korrekturaufgaben automatisch an Ihre IT-Teams nur für die Schwachstellen, die Sie beheben möchten.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie ein Überwachungsthema aus.

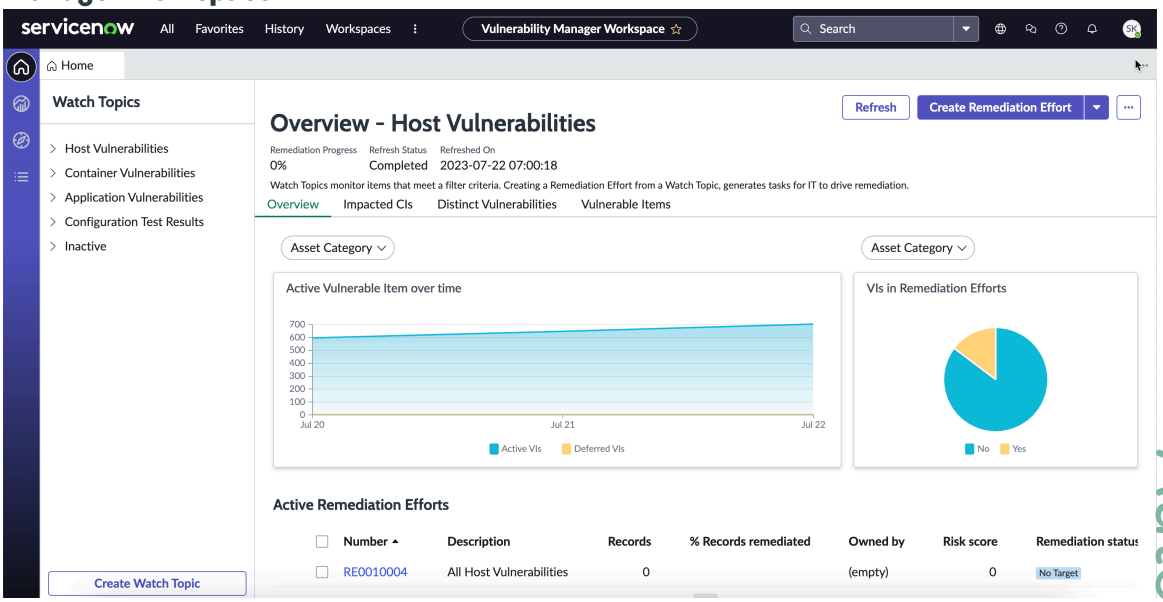
   Wenn Sie ein Überwachungsthema auswählen, wird standardmäßig die Registerkarte **Übersicht** angezeigt.

   Weitere Informationen zu den Überwachungsthemen finden Sie unter Übersicht über Überwachungsthemen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Version 19.0 Registerkarte „Übersicht“ auf der Homepage von Vulnerability Manager Workspace**




Die Dashboards sind dynamisch und neue Schwachstellendaten werden beim Import aktualisiert.

3. Wählen Sie eine **Registerkarte Zugehörige Elemente** aus, um weitere Daten anzuzeigen.

   Informationen zu Aktualisierungen in der Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema ab Version 18.0 finden Sie unter Liste zugehöriger Elemente und Visualisierungen in einem Überwachungsthema.

4. Führen Sie die UI-Aktionen auf der Seite „Überwachungsthemen“ aus.

5. **Wahlweise:** Wählen Sie einen Datensatz aus, um weitere Details anzuzeigen.

## Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema

Schwachstellenmanager und Analysten können Überwachungsthemen mithilfe einer Reihe von Bedingungen erstellen, um Teilmengen angreifbarer Elemente herauszufiltern, die sie überwachen möchten.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Auf der Registerkarte Übersicht der Überwachungsthemen zeigt ein Trendbericht, der jede Nacht aktualisiert wird, zusammen mit anderen Berichten den aktuellen Status der Datensätze für dieses Überwachungsthema an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
   Die Startseite (Zielseite) wird mit den aktuellen Überwachungsthemen angezeigt.
2. **Wahlweise:** Alternativ können Sie rechts neben der Schaltfläche Korrekturmaßnahme erstellen auf die drei Punkte klicken und anschließend auf Bearbeiten klicken, um ein vorhandenes Überwachungsthema zu ändern.

   **Hinweis:**
   Möglicherweise stellen Sie eine Verzögerung fest, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

3. Klicken Sie links unten auf der Seite auf Überwachungsthema **erstellen**.
4. Füllen Sie im angezeigten Modal die Felder aus.
   Weitere Informationen zu den modalen Feldern für Überwachungsthemen erstellen finden Sie unterFelder im Formular „Überwachungsthema erstellen“.
5. Ab Version 18.0 können Sie Bedingungen für die ausgewählte Datensatzkategorie definieren.

   **Hinweis:**
   Wenn Sie in Ihrem Überwachungsthema keine Bedingungen festlegen, werden keine Daten in das Dashboard abgerufen.

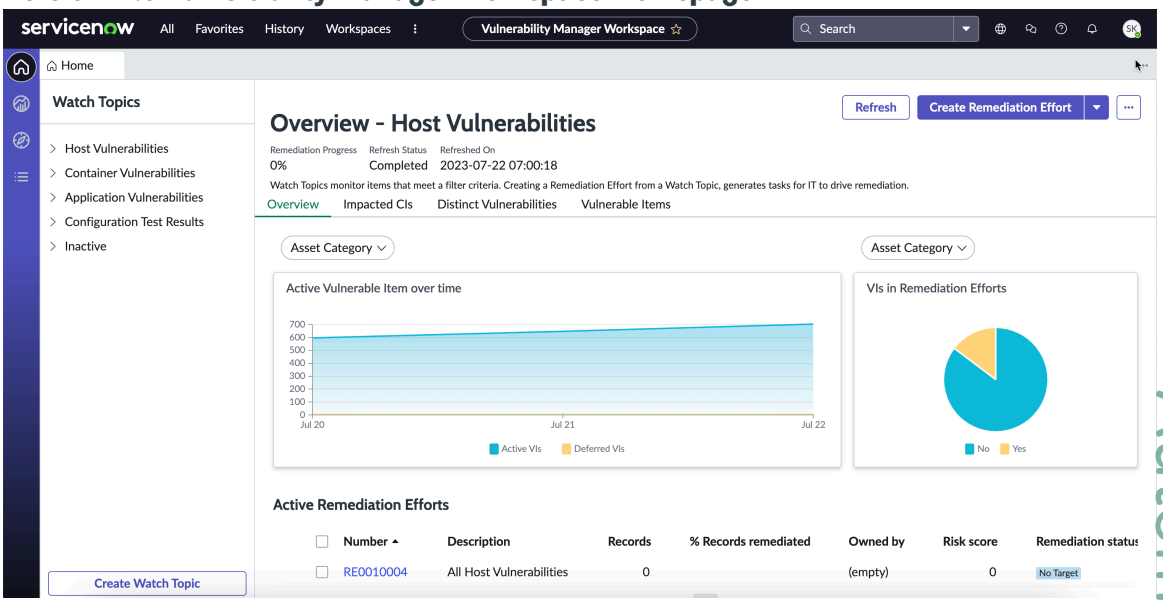
6. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihr neues Überwachungsthema wird auf der Zielseite der Startseite angezeigt. Ab Version 18.0 werden die Überwachungsthemen im Navigationsbereich nach Datensatztyp kategorisiert.

**Version 19.0 Vulnerability Manager Workspace-Homepage**




## Nächste Maßnahme

Erstellen Sie eine Korrekturmaßnahme.

### Bearbeiten oder löschen Sie ein Überwachungsthema

Als Schwachstellenadministrator oder -analyst können Sie ein vorhandenes Überwachungsthema bearbeiten oder löschen.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

## Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein vorhandenes Überwachungsthema bearbeiten:

- Die Daten im Dashboard werden entsprechend Ihren Änderungen aktualisiert.
- Die Datensätze, die sich derzeit in den vorhandenen Korrekturmaßnahmen befinden, bleiben unverändert.
- Die Datensätze, die sich derzeit nicht in Korrekturmaßnahmen befinden, werden basierend auf den Kriterien angezeigt, die Sie im Bedingungsgenerator eingeben.

Wenn Sie ein Überwachungsthema löschen, bevor alle zugehörigen Datensätze korrigiert werden, sind die Datensätze, die mit diesem Überwachungsthema angezeigt werden, nicht betroffen.

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
   Die Startseite (Zielseite) wird mit den aktuellen Überwachungsthemen angezeigt.
2. Öffnen Sie das Überwachungsthema, das Sie bearbeiten möchten.
3. Klicken Sie auf die drei Punkte, und klicken Sie auf **Bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können ein inaktives Überwachungsthema nicht bearbeiten.

4. Ändern Sie im modalen Fenster „Überwachungsthema bearbeiten“ die Felder.
5. Klicken Sie auf **Absenden**.

**Hinweis:**
Möglicherweise stellen Sie eine Verzögerung fest, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten. Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, ist Wiederkehrende Maßnahme **bearbeiten** im Menü verfügbar. Wählen Sie diese Option aus, um den wiederkehrenden Aufwand zu bearbeiten.

Alle Änderungen, die Sie vornehmen und im Datensatz der Korrekturmaßnahme speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. **Wahlweise:** Um ein Überwachungsthema zu löschen, wählen Sie im Überwachungsthema das Drei-Punkte-Menü und dann **Löschen**aus.

### Deaktivieren oder aktivieren Sie ein Überwachungsthema

Ab Version 18.0 können Sie ein Überwachungsthema deaktivieren oder aktivieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

#### Warum und wann dieser Vorgang ausgeführt wird

- Alle inaktiven Überwachungsthemen werden im Modul „ **Inaktiv** “ im Navigationsbereich angezeigt.
- Sie können keine Korrekturmaßnahme oder eine wiederkehrende Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen.
- Sie können ein inaktives Überwachungsthema nicht aktualisieren.
- Die Details eines inaktiven Überwachungsthemas und die zugehörigen Korrekturmaßnahmen werden nicht aktualisiert.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
   Die Startseite (Zielseite) wird mit den aktuellen Überwachungsthemen angezeigt.
2. Öffnen Sie das Überwachungsthema, das Sie deaktivieren möchten.
3. Klicken Sie auf die drei Punkte, und klicken Sie auf **Deaktivieren**.
   Das Überwachungsthema wird im Modul „Inaktiv“ angezeigt.
4. Um ein Überwachungsthema zu aktivieren, wählen Sie im Modul „Inaktiv“ ein Überwachungsthema aus, wählen Sie das Menü mit den drei Punkten aus, und wählen Sie **Aktivieren**aus.
   Das aktivierte Überwachungsthema wird in das entsprechende Modul im Navigationsbereich verschoben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verwenden Sie Datensätze der Korrekturmaßnahme

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen (REs) erstellen, werden den IT-Teams automatisch Korrekturaufgaben (VUL) zur Korrektur zugewiesen.

## Vorbereitungen

Sie müssen eine Korrekturmaßnahme erstellen, bevor Sie sie zur Überwachung des Korrekturfortschritts für Korrekturaufgaben verwenden können.

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

## Prozedur

1. Wenn diese Option nicht ausgewählt ist, klicken Sie oben links auf das Listensymbol.

   Die Listenansicht mit aktiven Datensätzen der Korrekturmaßnahme wird angezeigt.

2. Klicken Sie auf der Zielseite der Listenansicht mit Aktive Korrekturmaßnahmen in den gefilterten Listen auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt. Sie können die Korrekturaufgaben und Datensätze anzeigen, die der ausgewählten Korrekturmaßnahme zugeordnet sind.

3. In der folgenden Tabelle finden Sie die Aktionen, die Sie für den Datensatz der Korrekturmaßnahme ausführen können.

   Nachdem Sie einen Datensatz erstellt haben, kann es einige Minuten dauern, bis die Korrekturaufgaben und eine große Anzahl von Datensätzen angezeigt werden.

| UI-Aktion | Beschreibung |
|---|---|
| Fügen Sie ein Tag hinzu | Klicken Sie rechts neben der Kopfzeile auf das kleine Tag-Symbol. Sie können Text hinzufügen, der Ihnen bei der Identifizierung dieses Datensatzes hilft. Beispielsweise möchten Sie möglicherweise ein Tag hinzufügen, das angibt, dass dieser Datensatz PCI oder andere kritische Daten enthält. |
| Fügen Sie dem Datensatz eine Arbeitsnotiz hinzu | Klicken Sie ganz rechts auf dem Bildschirm auf das **Aktivitätssymbol** (helles Symbol), und geben Sie eine Arbeitsnotiz ein. Klicken Sie auf das Symbol, um den Bereich umzuschalten. |
| Datensatz aktualisieren | Klicken Sie auf der Registerkarte **Details** für alle bearbeitbaren Felder auf ein Feld, um es auszuwählen, nehmen Sie Ihre Änderungen vor, und klicken Sie auf **Speichern**, um den Datensatz zu aktualisieren. |
| Klicken Sie bei der Anzeige auf das Filtersymbol, um die Daten auf der angezeigten Seite einzugrenzen | Wenn eine der Registerkarten Korrekturaufgaben, angreifbare Elemente oderr Konfigurationstestergebnisse ausgewählt ist, klicken Sie ganz rechts auf das Filtersymbol, um die Filter anzuzeigen, die für die Registerkarte gelten.<br><br>Klicken Sie im angezeigten Bereich auf **Erweiterte Ansicht**, um Filterbedingungen für die Elemente auf der Seite |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| UI-Aktion | Beschreibung |
|---|---|
| | hinzuzufügen oder zu ändern. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.<br><br>Beispielsweise können Sie auf der Registerkarte „ **Angreifbare** Elemente“ das Feld Alter hinzufügen und einen Bereich eingeben, um nur Datensätze aus einem bestimmten Zeitraum anzuzeigen. Datensätze, die den von Ihnen festgelegten Bedingungen entsprechen, werden in der Liste angezeigt. |
| Filter für Elemente in einer Spalte verfeinern | Wählen Sie eine Spalte aus, klicken Sie auf das Menü mit den drei vertikalen Punkten, erweitern Sie es, und geben Sie Bedingungen ein, um die Daten in der Spalte zu verfeinern und zu gruppieren. |
| Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab | Angenommen, Sie möchten nur Datensätze anzeigen, die eine bestimmte Schwachstelle aufweisen. Wählen Sie in der Liste der Datensätze die Zeile des Datensatzes in der Spalte **Zusammenfassung** aus. Klicken Sie auf das angezeigte vertikale Punktmenü, und wählen Sie eine der folgenden Optionen aus:<br>○ **Übereinstimmungen anzeigen: Zeigt** alle anderen Datensätze an, die diese Schwachstelle aufweisen.<br>○ **Herausfiltern** : Zeigt alle Datensätze an, die diese Schwachstelle nicht aufweisen. |

4. Auf den Registerkarten „Korrekturaufgaben“, „Angreifbare Elemente“ und „Konfigurationstestergebnisse“ können Sie Detailinformationen für einzelne Korrekturaufgaben (VUL), angreifbare Elemente (VIT) und Testergebnisse (CTR) anzeigen.

## Nächste Maßnahme

Informationen zum Erstellen einer Korrekturaufgabe bei Bedarf aus einer Korrekturmaßnahme finden Sie unter Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe. Sie können auch Erstellen Sie eine benutzerdefinierte Liste von Datensätzen verwenden, um den Fortschritt der Fehlerkorrektur zu überwachen.

### Erstellen Sie im Arbeitsbereich von Vulnerability Manager eine Korrekturmaßnahme

Ein Datensatz für eine Korrekturmaßnahme ist eine statische Liste von Datensätzen, die Sie aus einem Überwachungsthema im Arbeitsbereich von Vulnerability Manager erstellen.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Sie verwenden Korrekturmaßnahmen, um die Aufgaben zu übergeben, die IT-Teams zur Behebung von Schwachstellen verwenden. Ab v16.1:

- Sie können vorhandene Korrekturmaßnahmen bearbeiten.
- Erstellen Sie Korrekturmaßnahmen, die automatisch zu den von Ihnen festgelegten Daten und Uhrzeiten erstellt werden.
- Übertragen Sie Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme.

Ab Version 18.0 ist die Schaltfläche **Korrekturmaßnahme erstellen** inaktiv, da Sie keine Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen können.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Zielseite (Homepage) ein Überwachungsthema aus, für das Sie eine Korrekturmaßnahme erstellen möchten.
3. Um die Datensätze anzuzeigen, die dem ausgewählten Überwachungsthema zugeordnet sind, klicken Sie unter der Datensatzkopfzeile auf . **Angreifbare Elemente** Registerkarte.

   Die Datensätze werden angezeigt.

   Im Header unter der Registerkarte „Angreifbare Elemente“ können Sie die Gesamtzahl der Datensätze anzeigen, die dieses Überwachungsthema aufweist.

   Die folgenden Spalten und Daten werden angezeigt:

**Spalten auf der Registerkarte „Angreifbare Elemente“.**

| Spalte | Beschreibung |
|---|---|
| Nummer | Die Datensatznummer. |
| Zusammenfassung | Beschreibung der Schwachstelle. |
| Konfigurationselement | Das der Schwachstelle zugeordnete Asset. |
| Risikobewertung | Quantifizierte Risikopunktzahl, die Datensätze in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. |
| Status | Status des Datensatzes. |
| Korrekturstatus | Status der Fehlerkorrektur für einen Datensatz. |
| Zuweisungsgruppe | Zuweisungsgruppen, die für die Fehlerkorrektur verantwortlich sind. Die Zuweisung von Datensätzen zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln. |
| Korrekturmaßnahme | Wenn er einer Korrekturmaßnahme zugewiesen ist, wird in jedem Datensatz die zugewiesene Korrekturmaßnahme aufgelistet. Nachdem ein Datensatz einer Korrekturmaßnahme hinzugefügt wurde, wird er keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt. |
| Zuweisungsgruppe | Zuweisungsgruppen, die für die Fehlerkorrektur verantwortlich sind. Die Zuweisung von Datensätzen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Spalte | Beschreibung |
| --- | --- |
| | zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln. |
| Korrekturmaßnahme | Wenn er einer Korrekturmaßnahme zugewiesen ist, wird in jedem Datensatz die zugewiesene Korrekturmaßnahme aufgelistet. Nachdem ein Datensatz einer Korrekturmaßnahme hinzugefügt wurde, wird er keinen anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt. |
| In Korrekturaufgabe | Bei „true“ gibt dieser Wert an, dass sich ein Datensatz bereits in einer Korrekturaufgabe befindet. Datensätze können in mehreren Korrekturaufgaben enthalten sein, aber ein Datensatz kann nur einer Korrekturmaßnahme hinzugefügt werden. |
| Exploit vorhanden | Gibt an, ob für einen Datensatz ein bekannter Exploit vorhanden ist. |
| Zuletzt geöffnet | Datum, an dem der Datensatz zuletzt in Ihrem Now Platformgeöffnet wurde. Wenn der Datensatz geschlossen und dann erneut geöffnet wurde, ist dies der Zeitpunkt, zu dem der Datensatz zuletzt erneut geöffnet wurde. |

4. Um eine Korrekturmaßnahme zu erstellen, klicken Sie auf **Korrekturmaßnahme erstellen**.

   Wenn Sie eine Korrekturmaßnahme erstellen, werden Datensätze, die sich bereits in vorhandenen Korrekturmaßnahmen befinden, keinen neuen Korrekturmaßnahmen hinzugefügt, die Sie aus diesem Überwachungsthema erstellen.

   Wenn Datensätze aktualisiert oder neue Datensätze in Überwachungsthemen erstellt werden, können Sie Korrekturmaßnahmen erstellen.

5. Alternativ können Sie Erstellen Sie in Vulnerability Response Workspaces eine wiederkehrende Korrekturmaßnahme.

   Die Schaltfläche **Bearbeiten** ist im Menü für vorhandene Korrekturmaßnahmen verfügbar. Sie haben die Möglichkeit, die Felder und Bedingungen in einem angezeigten modalen Fenster zu ändern. Alle Änderungen, die Sie vornehmen und im Datensatz der Korrekturmaßnahme speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. Füllen Sie in Schritt 1 des Dialogfelds „Korrekturmaßnahme erstellen“ die Felder aus.

   Geben Sie im Feld Kurzbeschreibung Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt und Ihnen hilft, sie in der Aufgabenliste zu finden und nachzuverfolgen.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können.

   Ab Version 17.1 können Sie beim Erstellen einer Korrekturmaßnahme für Überwachungsthemen, die Hostschwachstellenenthalten, doppelte angreifbare Elemente in den erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbaren Elemente automatisch zu aktualisieren, müssen Sie das Kontrollkästchen **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren** aktivieren.

**Hinweis:**
Ab Version 18.0 wird dieses Kontrollkästchen in Schritt 2 angezeigt.

7. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme nach der Erstellung generieren.

**Hinweis:**
Für Version 18.0 ist die Option **Keine** nicht verfügbar.

8. Überprüfen Sie in Schritt 3, Übertragung, wie viele Datensätze Sie der Korrekturmaßnahme hinzufügen möchten, und prüfen Sie, wie viele Datensätze aus anderen aktiven Korrekturmaßnahmen für die Übertragung verfügbar sind.

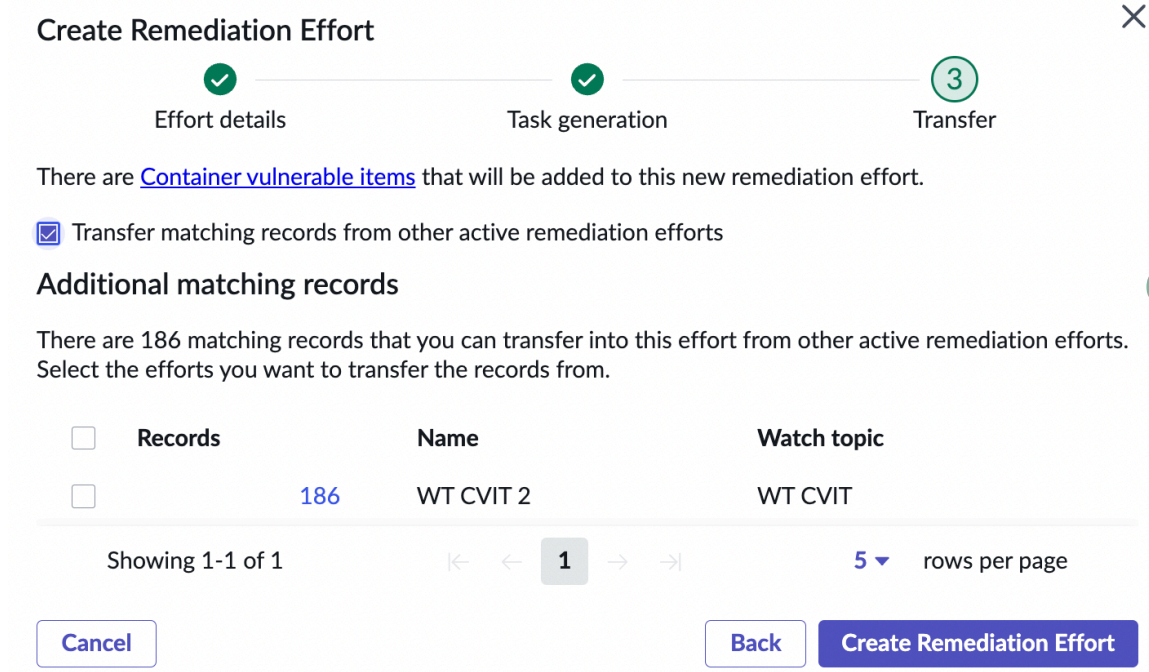
   Wenn keine neuen, aktiven Datensätze zum Hinzufügen vorhanden sind, wird der folgende Text angezeigt:

   Es sind keine aktiven Datensätze verfügbar, die Sie dieser neuen Korrekturmaßnahme hinzufügen können.

   Alle zusätzlichen Datensätze, die für die Übertragung an diese Maßnahme verfügbar sind, werden unter Zusätzliche übereinstimmende Datensätze aufgelistet.

   Aktivieren Sie ab Version 18.0 das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen übertragen**, und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie von anderen aktiven Korrekturmaßnahmen übertragen möchten.

**Version 18.0 Korrekturmaßnahme erstellen**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie auf Korrekturmaßnahme **erstellen geklickt**haben, wird in wenigen Minuten die neue Korrekturmaßnahme angezeigt. Abhängig von der Anzahl der Datensätze kann es einige Zeit dauern, bis der neue Datensatz ausgefüllt ist. Eine Nachricht zeigt an, ob der Datensatz noch ausgefüllt wird.

Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem Überwachungsthema verfügbar sind, das zu ihrer Erstellung verwendet wurde, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

Wenn Sie Datensätze auswählen, die aus einer vorhandenen Maßnahme übertragen werden sollen, und die vorhandene Maßnahme alle Datensätze in Ihre neue Maßnahme überträgt, wird die Korrekturmaßnahme geschlossen, aus der Sie die Datensätze verschoben haben. Weitere Informationen dazu, wie sich die Datensatzübertragung auf die mit den Korrekturmaßnahmen verknüpften Korrekturaufgaben auswirkt, finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in Vulnerability Response Workspaces.

**Hinweis:**
Wenn keine Datensätze aus dem Überwachungsthema verfügbar sind oder Datensätze zur Übertragung ausgewählt wurden, ist die Schaltfläche **Korrekturmaßnahme erstellen** deaktiviert.

Die geplante Aufgabe `Populate Efforts` wird alle 10 Minuten ausgeführt, um die Daten in den Widgets basierend auf der ausgewählten Bedingung auszufüllen.

Klicken Sie auf die Registerkarte Korrekturfortschritt, um den Fortschritt der Fehlerkorrektur anzuzeigen. Klicken Sie auf ein beliebiges Element, um Details anzuzeigen, einschließlich Datensatztyp, Risikopunktzahl, Risikobewertung, Prozentsatz der korrigierten Datensätze, Datensätze im Status „Zurückgestellt“ und „Nicht zurückgestellt“ und Gesamtzahl der Datensätze, die im Überwachungsthema verwendeten Bedingungen und der Status der Korrektur. Die Informationen zum Korrekturstatus, z. B. Korrekturziel und Korrekturstatus, werden aus der Tabelle „Angreifbare Elemente“ zusammengefasst. Für die höchste Datensatz-Risikopunktzahl wird ein Rollup aus der Tabelle „Schwachstellenrechner“ durchgeführt, während für die Risikopunktzahl ein Rollup aus dem durchgeführt wird **Rechner für Schwachstellen-Rollup** > **Rollup von Korrekturmaßnahme** .

Auf der Registerkarte Korrekturaufgaben werden die Aufgaben für alle Arten von Problemen angezeigt. Die Felder werden ausgefüllt, wenn die folgenden geplanten Aufgaben ausgeführt werden. Sie werden alle 15 Minuten automatisch ausgeführt:

- Rollup der Werte für angreifbare Anwendungselemente zu Schwachstelle und Gruppe.
- Rollup der Werte des angreifbaren Containerelements für Schwachstelle und Gruppe.
- Rollup der Testergebniswerte zum Testen der Ergebnisgruppe und des Konfigurationstests.
- Rollup der Werte für angreifbare Elemente zu Schwachstelle und Gruppe.

In der Listenansicht können Sie Korrekturbemühungen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe oder ein angreifbares Element öffnen und die Detailseite anzeigen. Klicken Sie auf die Auslassungspunkte Weitere Aktionen und dann auf **Untersuchung starten**, um eine Korrekturaufgabe zu lösen.

9. **Wahlweise:** Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, ist Wiederkehrende Maßnahme **bearbeiten** im Menü oben rechts in einem Überwachungsthema verfügbar. Wählen Sie diese Option aus, um den wiederkehrenden Aufwand zu bearbeiten.

Alle Änderungen, die Sie vornehmen und im Datensatz der Korrekturmaßnahme speichern, wirken sich nicht auf andere Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

### Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe

Erstellen Sie bei Bedarf eine Korrekturaufgabe aus einer Korrekturmaßnahme. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Datensätze aus, die Sie manuell hinzufügen möchten.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Für Version 18.0 von Vulnerability Responsekönnen Sie keine Korrekturaufgabe aus der Datensatzansicht einer Korrekturmaßnahme erstellen.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Klicken Sie oben links im Arbeitsbereich bei angezeigter Homepage auf das Symbol für die Listenansicht, um die Zielseite der **Liste** anzuzeigen.
3. Klicken Sie unter Korrekturmaßnahmen auf **Aktiv** oder **Alle**.
4. Klicken Sie in der angezeigten Liste auf einen Datensatz, um ihn zu öffnen.
   Die Übersichtsregisterkarte des Datensatzes wird angezeigt.
5. Klicken Sie auf die Registerkarte **Angreifbare** Elemente.
   Die Liste der Datensätze wird angezeigt.
6. Um eine neue Korrekturaufgabe zu erstellen, wählen Sie in der Spalte Nummer die Datensätze aus, die Sie hinzufügen möchten.
7. Klicken **Sie auf Korrekturaufgabe erstellen**.
8. Füllen Sie im angezeigten Modal die Felder aus.
9. Klicken Sie auf **Erstellen**.
10. Die neue Korrekturaufgabe wird mit den von Ihnen ausgewählten aktiven Datensätzen angezeigt.

### Erstellen Sie in Vulnerability Response Workspaces eine wiederkehrende Korrekturmaßnahme

Sie können wiederkehrende Korrekturmaßnahmen erstellen und planen, die automatisch zu den von Ihnen festgelegten Zeitpunkten generiert werden.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können automatisch wiederkehrende Korrekturmaßnahmen nach einem Zeitplan erstellen, um Schwachstellen nachzuverfolgen, die möglicherweise auftreten und sofortige und laufende Maßnahmen erfordern.

Ab Version 18.0 ist die Option **Wiederkehrende Maßnahme erstellen** inaktiv, da Sie keine wiederkehrende Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen können. Wenn Sie ein Überwachungsthema deaktivieren, für das bereits eine wiederkehrende Maßnahme geplant ist, wird erst dann eine neue Korrekturmaßnahme erstellt, wenn das Überwachungsthema aktiviert ist. Außerdem werden die Details zu **Aufwandsserie** und **Datum der nächsten Wiederholung** oben rechts ausgeblendet. Nachdem Sie das Überwachungsthema aktiviert haben, wird beim bevorstehenden Zeitplan eine Korrekturmaßnahme erstellt.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Zielseite (Homepage) ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.

   Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen.

   **Hinweis:**
   Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen zum Übertragen von Datensätzen finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen in den Vulnerability Response Arbeitsbereichen.

3. Wählen Sie in einem Überwachungsthema oben rechts in der Liste Korrekturmaßnahme **erstellen die Option Wiederkehrende Maßnahme erstellen**aus.

   Das Dialogfeld „Wiederkehrende Maßnahme erstellen“ wird angezeigt.

4. Füllen Sie in Schritt 1, Aufwandsdetails, die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung den Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, die Ihnen hilft, sie zu finden und in der Aufgabenliste nachzuverfolgen.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können. Beispiel: Schwachstellen in nach außen gerichteten Assets.

   Ab Version 17.1 können Sie beim Erstellen einer Korrekturmaßnahme für Überwachungsthemen, die Hostschwachstellenenthalten, doppelte angreifbare Elemente in den erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren aktivieren**.

   **Hinweis:**
   Ab Version 18.0 wird dieses Kontrollkästchen in Schritt 2 angezeigt.

5. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die angreifbaren Elemente in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme nach der Erstellung generieren.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine (es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie Datensätze manuell zu einer Korrekturaufgabe für diese Maßnahme hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe.

   **Hinweis:**
   Für Version 18.0 von Vulnerability Responseist die Option **Keine** nicht verfügbar.

7. Klicken Sie auf **Weiter**, um fortzufahren.
8. Wählen Sie in Schritt 3, Wiederholung, die Häufigkeit aus.

   a. Definieren Sie den Wiederholungszeitplan.

   Verwenden Sie die Listen, um den Monat/Tag/Stunde/Minute auszuwählen, für die die Korrekturmaßnahme erstellt werden soll. Die Zeitzone für die Planung ist standardmäßig Ihre Zeitzone.

   **Hinweis:**
   Wenn viele Schwachstellen vorhanden sind, sollten Sie die Erstellung außerhalb der Geschäftszeiten festlegen.

   Wenn die Aufgabe am letzten Tag des Monats erstellt werden soll, erstellt die regelmäßige Aufgabe die wiederkehrende Korrekturmaßnahme am letzten Tag des Monats. Wenn der Monat keine 31 Tage hat, wird eine Nachricht angezeigt.

   b. **Wahlweise:** Wählen **Sie Schwachstellen** auf aktive Schwachstellen in dieser Korrekturmaßnahme übertragen aus, um sie in jede nachfolgende erstellte Korrekturmaßnahme zu übernehmen.

9. Klicken Sie auf **Zeitplanserie**.
   Eine Meldung wird angezeigt, dass der wiederkehrende Korrekturdatensatz erstellt wurde. Die neue Korrekturmaßnahme wird nicht sofort angezeigt, sondern erstellt, wenn Sie sie geplant haben. Sie wird in Ihren Listen angezeigt, nachdem sie von der geplanten Aufgabe erstellt wurde.

   Das Datum, an dem die Korrekturmaßnahme erstellt wird, wird im entsprechenden Überwachungsthema angezeigt. Weitere Informationen dazu, wie sich die Datensatzübertragung auf die mit den Korrekturmaßnahmen verknüpften Korrekturaufgaben auswirkt, finden Sie unter Lebenszyklen von Korrekturbemühungen, Korrekturaufgaben und Datensätzen in Vulnerability Response Workspaces.

### Übertragen Sie Datensätze an Korrekturmaßnahmen in den Vulnerability Response Arbeitsbereichen

Sie können Datensätze aus vorhandenen Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Wenn Sie mit einer Zero-Day-Bedrohung oder einer sehr kritischen Schwachstelle konfrontiert werden, die Sie schnell beheben möchten, möchten Sie möglicherweise alle aktiven Datensätze, die Sie für diese Schwachstelle bereits haben, in einer einzigen Korrekturmaßnahme zusammenfassen. Jeder Datensatz kann jedoch nur in einer Anstrengung enthalten sein, und Datensätze können sich zwischen Überwachungsthemen überschneiden. Um sie alle zu erfassen, müssen Sie diese Datensätze aus mehreren vorhandenen Maßnahmen in eine einzige Korrekturmaßnahme übertragen.

Angenommen, Sie haben eine Korrekturmaßnahme erstellt, die eine Schwachstelle mit hoher Priorität enthält. Da diese Schwachstelle weit verbreitet ist und sich möglicherweise auf andere Bereiche in Ihrer Umgebung auswirkt, verfügen Sie möglicherweise über Datensätze, die dieser Schwachstelle bereits in vorhandenen Korrekturmaßnahmen zugeordnet sind. Um diese Datensätze so zu kombinieren, dass sie sich alle in einer Korrekturmaßnahme befinden, können Sie Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme übertragen.

**Hinweis:**
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen finden Sie unter Erstellen Sie in Vulnerability Response Workspaces eine wiederkehrende Korrekturmaßnahme.

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Zielseite (Homepage) ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.
3. Klicken **Sie auf Korrekturmaßnahme erstellen**.
   Das Dialogfeld „Korrekturmaßnahme erstellen“ wird angezeigt.
4. Füllen Sie in Schritt 1, Aufwandsdetails, die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, die Ihnen hilft, sie zu finden und in der Aufgabenliste nachzuverfolgen.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie in der Liste der Korrekturmaßnahmen leicht finden können. Beispiel: `Aktive Log4J-Schwachstellen`.

   a. Geben Sie im Feld Name einen Namen für Ihre neue Korrekturmaßnahme ein.
      Standardmäßig wird der Name des Überwachungsthemas angezeigt.

   b. Geben Sie im Feld Beschreibung Text ein, mit dem Sie diese Korrekturmaßnahme in der Liste der Korrekturmaßnahmen leicht finden können.

   Ab Version 17.1 können Sie beim Erstellen einer Korrekturmaßnahme für Überwachungsthemen, die Hostschwachstellenenthalten, doppelte angreifbare Elemente in den erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren aktivieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 18.0 wird dieses Kontrollkästchen in Schritt 2 angezeigt.

5. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.
6. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme nach der Erstellung generieren.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine (es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie Datensätze manuell zu einer Korrekturaufgabe für diese Maßnahme hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie in Vulnerability Manager Workspace bei Bedarf eine Korrekturaufgabe.

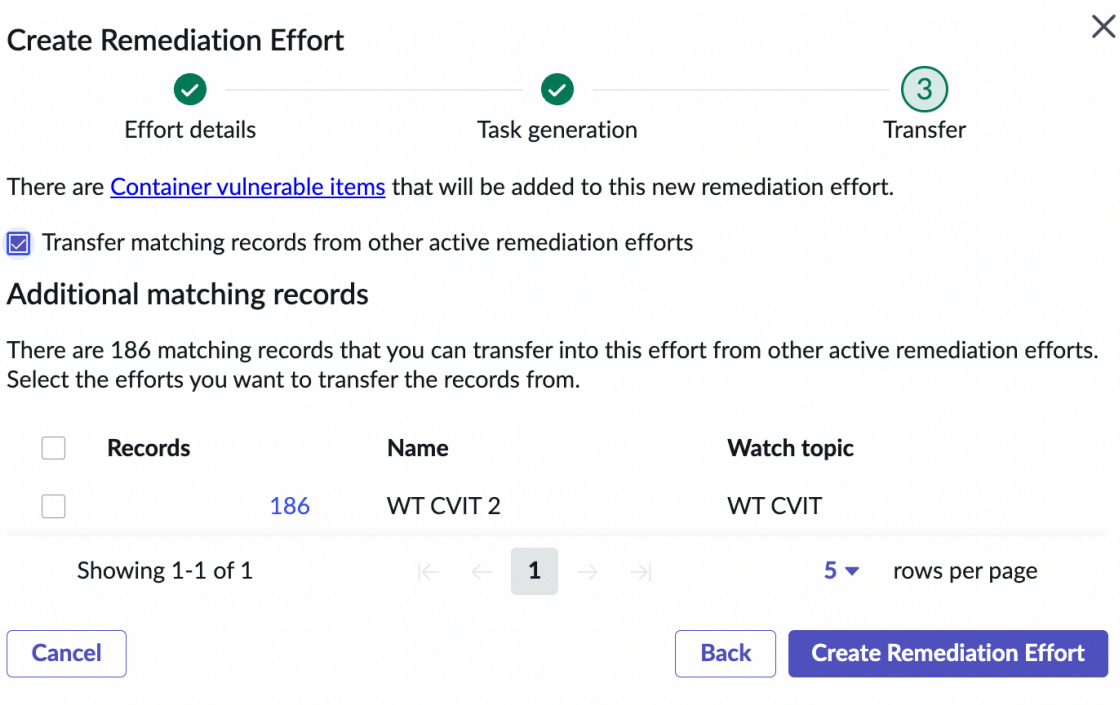
   **Hinweis:**
   Für Version 18.0 ist die Option **Keine** nicht verfügbar.
7. Klicken Sie auf **Next (Weiter)**.
8. Überprüfen Sie in Schritt 3, Übertragung, wie viele Datensätze der Korrekturmaßnahme hinzugefügt werden, und prüfen Sie, wie viele Datensätze von anderen aktiven Korrekturmaßnahmen für die Übertragung verfügbar sind.
9. Um Datensätze aus anderen Maßnahmen zu übertragen, aktivieren Sie in der Liste die Kontrollkästchen für die gewünschten Datensätze.

   Aktivieren Sie ab Version 18.0 das Kontrollkästchen **Übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen übertragen**, und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie von anderen aktiven Korrekturmaßnahmen übertragen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Version 18.0 Korrekturmaßnahme erstellen**




**10.** Klicken **Sie auf Korrekturmaßnahme erstellen**.

Nach einigen Minuten wird die neue Korrekturmaßnahme angezeigt. Abhängig von der Anzahl der Datensätze kann dies einige Zeit dauern. Eine Nachricht zeigt an, dass der Datensatz ausgefüllt wird.

Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem Überwachungsthema verfügbar sind, das zu ihrer Erstellung verwendet wurde, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

Wenn Sie Datensätze auswählen, die aus einer vorhandenen Maßnahme übertragen werden sollen, und die vorhandene Maßnahme alle Datensätze in Ihre neue Maßnahme überträgt, wird die Korrekturmaßnahme geschlossen, aus der Sie die Datensätze verschoben haben.

**Hinweis:**
Wenn weder Datensätze aus dem Überwachungsthema verfügbar sind noch Datensätze für die Übertragung ausgewählt wurden, ist die Schaltfläche **Korrekturmaßnahme erstellen** deaktiviert.

Weitere Informationen dazu, wie sich die Datensatzübertragung auf die mit den Korrekturbemühungen verknüpften Korrekturaufgaben auswirkt, finden Sie unter Datensätze übertragen oder Datensatz übertragen.

### Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Fügen Sie als Schwachstellenmanager oder Analyst eine Liste von Ausgleichskontrollen hinzu, die für die Risikominderung von angreifbaren Elementen und Korrekturaufgaben angewendet werden können.

**Vorbereitungen**
Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Einige häufig verwendete Ausgleichskontrollen sind im Lieferumfang des Basissystems enthalten. Sie können diese Ausgleichskontrollen anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Lists** > **Bibliotheken** > **Ausgleichskontrollen**. Sie können diese Ausgleichskontrollen nach Ihren Anforderungen aktivieren oder deaktivieren.

**Hinweis:**
Die Funktion „Ausgleichskontrollen“ ist nur für Host-Schwachstellen verfügbar.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Seite „Liste“ unter „Bibliotheken“ die Option **Ausgleichskontrollen**aus.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder im Formular „Ausgleichskontrollen erstellen“ aus.

**Felder im Formular „Ausgleichskontrollen erstellen“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Ausgleichskontrolle, die als Option in der Dropdown-Liste „ **Ausgleichskontrollen** “ des Dialogfelds „Ausnahme anfordern“ angezeigt wird. |
| Beschreibung | Kurze Informationen mit Details zur Ausgleichskontrolle. |
| Aktiv | Status der Ausgleichskontrolle. In der Dropdown-Liste „ **Ausgleichskontrollen** “ des Dialogfelds „Ausnahme anfordern“ werden nur aktive Kontrollen angezeigt. |

5. Wählen Sie **Speichern**.
6. Wählen Sie in der Liste „Ausgleichskontrollen“ unter „Bibliotheken“ die gewünschte Ausgleichskontrolle aus, und wählen Sie **Bearbeiten**, aktivieren oder deaktivieren Sie eine Ausgleichskontrolle, und klicken Sie auf **Speichern**, um die Ausgleichskontrollen zu ändern.
   Alle aktiven Ausgleichskontrollen werden als Option in der Dropdown-Liste „ **Ausgleichskontrollen** “ des Dialogfelds „Ausnahme anfordern“ für Risikominderungsanforderungen angezeigt.

### Nächste Maßnahme

Ab v21.0 von Vulnerability Responsekönnen Sie Ausgleichskontrollen CVEs oder TPEs zuordnen, nachdem Sie der Bibliothek Ausgleichskontrollen hinzugefügt haben. Weitere Informationen zum Zuordnen von Ausgleichskontrollen finden Sie unter Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu.

**Zugehörige Informationen**

Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu

Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu

Als Schwachstellenmanager oder Analyst können Sie relevante Ausgleichskontrollen einem CVE oder TPE zuordnen, die für Risikominderungsanforderungen angewendet werden können.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

- Wenn Sie Ausgleichskontrollen keinem CVE oder TPE zuordnen, werden alle aktiven Kontrollen im Feld Ausgleichskontrollen auswählen des Formulars „Ausnahme anfordern“ angezeigt.
- Wenn Sie eine Ausgleichskontrolle einem CVE zuordnen, wird diese Ausgleichskontrolle automatisch der TPE zugeordnet, die dem CVE zugeordnet ist.

**Hinweis:**
Die Funktion „Ausgleichskontrollen“ ist nur für Host-Schwachstellen verfügbar.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Öffnen Sie auf der Seite „Listen“ unter „Bibliotheken“ eine der folgenden Optionen, für die Sie die Steuerelemente zuordnen möchten:
   - **CVE** aus der CVEs-Liste.
   - **TPE** aus der TPE-Liste.
3. Wählen Sie **Steuerungen zuordnen aus**.

   **Hinweis:**
   Die Schaltfläche **Steuerungen** zuordnen wird nur angezeigt, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Mit anderen Worten: Sie können Ausgleichskontrollen nur dann zuordnen, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Wenn die Schaltfläche **Steuerungen** zuordnen nicht sichtbar ist, wählen Sie **Risikominderung**aktivieren aus.

4. Wählen Sie im Dialogfeld „Kontrollen zuordnen“ die Ausgleichskontrollen aus, die auf mit dem CVE oder TPE verbundene Schwachstellen zur Risikominderung angewendet werden können.
5. Wählen Sie **Absenden**.
   - Die zugehörigen Ausgleichskontrollen werden auf der Registerkarte Anwendbare Ausgleichskontrollen in der Datensatzansicht von CVE und TPE angezeigt.
   - Während ein Korrekturbesitzer eine Risikominderung anfordert, werden diese zugehörigen Ausgleichskontrollen im Feld Ausgleichskontrollen auswählen im Dialogfeld „Ausnahme anfordern“ angezeigt.

#### Zugehörige Informationen

Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Als Schwachstellenmanager und Analyst können Sie die Risikominderungsanforderungen für die Host-Schwachstellen aus einem Common Vulnerability Entry (CVE) oder Drittparteieintrag (TPE) deaktivieren oder aktivieren.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Die Risikominderung für ein CVE und einen TPE ist standardmäßig aktiviert.

**Hinweis:**
Die Funktion „Ausgleichskontrollen“ ist nur für Host-Schwachstellen verfügbar.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
   Öffnen Sie auf der Seite „Listen“ unter „Bibliotheken“ eine der folgenden Optionen, für die Sie die Risikominderungsanforderungen deaktivieren möchten:
   - **CVE** aus der CVEs-Liste.
   - **TPEs** aus der TPEs-Liste.
2. Wählen Sie **Risikominderung deaktivieren aus**.
   Der Korrekturbesitzer kann keine Risikominderung für die angreifbaren Hostelemente im Zusammenhang mit diesem CVE oder TPE anfordern. Mit anderen Worten, das Kontrollkästchen Risikominderung anfordern wird nicht angezeigt, wenn als **Grund** im Dialogfeld „Ausnahme anfordern“ die Option Mitigierende Kontrolle vorhanden ausgewählt ist.
3. Um die Risikominderungsanforderungen für angreifbare **Hostelemente zu aktivieren, wählen Sie Risikominderung**aktivieren aus.

#### Zugehörige Informationen

Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu

Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum

### Bearbeiten Sie angreifbare Hostelemente im Massenvorgang Vulnerability Manager Workspace

Ab v21.0 von Vulnerability Responsekönnen Sie den Status, die bevorzugte Lösung, den bevorzugten Patch und die Zuweisungsgruppe für mehrere Host- angreifbare Elemente (VITs) in Vulnerability Manager Workspaceaktualisieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin und jede Rolle mit der granularen Rolle sn_vul.bulk_edit.

#### Warum und wann dieser Vorgang ausgeführt wird
In Vulnerability Manager Workspacewird die Massenbearbeitungsfunktion nur für angreifbare Hostelemente unterstützt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie auf der Seite „Liste“ unter Host-Schwachstellen die angreifbaren Elemente aus, indem Sie eine der folgenden Aktionen ausführen:
   - Aktivieren Sie die Checkbox neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld Datensatzauswahl verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente,** die der Filteroption entsprechen im Feld Datensatzauswahl verwenden möchten.
3. Wählen Sie **Massenbearbeitung aus**.
4. Füllen Sie im Dialogfeld „Massenbearbeitung“ die Felder aus.

**Massenbearbeiten von modalen Feldern**

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Nur ausgewählte Elemente<br>○ Alle angreifbaren Elemente, die dem Filter entsprechen<br>○ Korrekturaufgabe<br>○ Schwachstelleneintrag<br>**Hinweis:**<br>Datensätze mit ungültigem oder außer Betrieb genommenem CI werden nicht aktualisiert. |
| Status | Change für den **Status** im angreifbaren Element. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Nicht aktualisieren<br>○ Offen<br>○ Wird untersucht<br>○ Warten auf Implementierung<br>○ Zurückgestellt<br>**Hinweis:**<br>▪ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Wenn Sie Datensätze zurückstellen, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet.<br>○ Abgeschlossen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>▪ Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu markieren, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Wenn Sie die Datensätze als falsch positiv markieren, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet.<br>○ Gelöst |
| Bevorzugte Lösung | Lösung, die auf die Korrektur aller für die Massenbearbeitung ausgewählten angreifbaren Elemente abzielt. Wählen Sie die Änderung für das Feld **Bevorzugte Lösung** im angreifbaren Element aus. Auswahlmöglichkeiten stammen aus einer Nachschlageliste der verfügbaren bevorzugten Lösungen für die ausgewählten VITs.<br>**Hinweis:**<br>○ Der Satz der verfügbaren bevorzugten Lösungen ist eine Schnittmenge aller potenziellen Lösungen der Schwachstellen in allen ausgewählten VITs.<br>○ Bei Auswahl von **Datensatzauswahl** > **Schwachstelleneintrag** Bei einer Massenbearbeitung werden alle VITs für die Schwachstelle auf die ausgewählte bevorzugte Lösung festgelegt.<br>**Hinweis:**<br>Dieser Vorgang legt die **bevorzugte Lösung** nicht auf der Schwachstelleneintragsebene fest. Durch Festlegen der **bevorzugten Lösung** auf der Schwachstelleneintragsebene wird die **bevorzugte Lösung** für alle neuen VITs festgelegt. Durch die Massenbearbeitung wird nur der aktuelle Satz von VITs geändert.<br>○ Eindeutige Schwachstellen über die Auswahlkriterien hinweg sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit anderen Kriterien für die Festlegung der **bevorzugten Lösung**auszuwählen.<br>○ Die Gesamtzahl der Lösungen, die in der Nachschlageliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt.<br>Der aktualisierte Wert wird in der Listenansicht des angreifbaren Elements angezeigt. |
| Bevorzugter Patch . | Patch, der auf die Behebung aller für die Massenbearbeitung ausgewählten angreifbaren Elemente ausgerichtet ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen.<br>◦ Der Satz der verfügbaren bevorzugten Patches ist eine Schnittmenge aller potenziellen Patches für alle ausgewählten VITs.<br>◦ Eindeutige Schwachstellen über die Auswahlkriterien hinweg sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit anderen Kriterien für die Festlegung des **bevorzugten Patch**auszuwählen.<br>◦ Die Gesamtzahl der Patches, die in der Nachschlageliste angezeigt werden kann, ist auf 170 beschränkt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt. |
| Grund | Grund für das Zurückstellen von Datensätzen:<br>◦ Warten auf Wartungsfenster<br>◦ Behebung nicht verfügbar<br>◦ Risiko akzeptiert<br>◦ Ausgleichende Steuerung vorhanden<br>◦ Sonstige<br>Grund für das Schließen von Datensätzen:<br>◦ Falsch positiv<br>**Hinweis:**<br>▪ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als Falsch positiv markieren und diese Aufgabe zur Genehmigung gesendet wird.<br>◦ Abgebrochen<br>◦ Repariert<br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status als Zurückgestellt oder Geschlossen auswählen. |
| Kurzbeschreibung | Kurzer Hinweis, in dem die Gründe für Zurückstellungs- und Falsch positiv geschlossene -Anforderungenbeschrieben werden. Diese Informationen werden im Feld Beschreibung der Korrekturaufgabe angezeigt, die für Zurückstellungs- und Geschlossen-Falsch-positive Anforderungen erstellt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status auf „Zurückgestellt“ und „Geschlossen – Falsch positiv“ setzen. |
| Bis | Datum, bis zu dem der Datensatz zurückgestellt bleibt.<br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status als Zurückgestellt auswählen. |
| Zusätzliche Informationen | Alle anderen erforderlichen Informationen. Diese Informationen werden im Feld Zusätzliche Informationen auf der Registerkarte Übersicht der Korrekturaufgabe angezeigt, die für Zurückstellungsanforderungen und geschlossene falsch positive Anforderungen erstellt wird. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungsnotizen für VIT und Korrekturaufgabe angezeigt.<br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status auf „Zurückgestellt“ und „Geschlossen – Falsch positiv“ setzen. |
| Zuweisung aufheben | Die Zuweisung aller ausgewählten Elemente für die Zuweisungsgruppe und den Korrekturbesitzer wird aufgehoben.<br>**Hinweis:**<br>○ Dieses Feld wird angezeigt, wenn Sie als Status Nicht aktualisieren auswählen.<br>○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet. |
| Zuweisungsgruppe | Zuweisungsgruppe für die Datensätze. Alle aktiven Zuweisungsgruppen werden in diesem Feld angezeigt.<br>**Hinweis:**<br>Dieses Feld wird deaktiviert, wenn Sie das Kontrollkästchen Zuweisung aufheben aktivieren. |
| Arbeitsnotizen | Text, den Sie eingeben, um die Änderungen zu beschreiben. |

5. Wählen Sie **Bearbeiten** aus.
   Eine asynchrone Massenbearbeitungsaufgabe aktualisiert die ausgewählten Datensätze. Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt, wenn Sie angreifbare Elemente in großen Mengen zurückstellen, ihre Zuweisung aufheben oder sie schließen (falsch positiv). Und diese Aufgabe wird zur Genehmigung gesendet. Sie können die Korrekturaufgabe in der Liste Korrekturaufgabe auf der Listenseite anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fordern Sie Ausnahmen für Korrekturaufgaben und Datensätze aus Vulnerability Manager Workspace an

Über den Arbeitsbereich des Schwachstellenmanagers können Schwachstellenmanager und Analysten Ausnahmen und falsch positive Meldungen für Korrekturaufgaben und -datensätze anfordern. Sie können auch Korrekturaufgaben aufteilen und Change-Anforderungen erstellen.

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin oder sn_vulc.admin.

Als Schwachstellenmanager oder Analyst können Sie diese Aufgaben über die Korrekturaufgabe und Datensätze ausführen, die Sie im Arbeitsbereich des Schwachstellenmanagers anzeigen.

Ab Version 19.0 von Vulnerability Responsekönnen Sie:

- Eine Korrekturaufgabe aufteilen, Ausnahmen anfordern und Richtlinienausnahmen für Testergebnisgruppen (TRGs) im Arbeitsbereich des Schwachstellenmanagers festlegen.
- Richtlinienausnahmen für Container-Schwachstellen (CVITs) im Vulnerability Manager Workspace anfordern.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

Ab Version 18.0 von Vulnerability Responsekönnen Sie:

- Fordern Sie Ausnahmen für Anwendungsschwachstellen (AVITs) und Container-Schwachstellen (CVITs) und deren Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers an.
- Fordern Sie eine Richtlinienausnahme für Host-Schwachstellenelemente, AVITs, CVITs und deren Korrekturaufgaben aus Vulnerability Manager Workspace an.

Sie initiieren diese UI-Aktionen aus Datensätzen im Arbeitsbereich des Schwachstellenmanagers auf die gleiche Weise, wie Korrekturbesitzer diese Aufgaben im IT-Korrekturarbeitsbereich ausführen.

Weitere Informationen finden Sie in den folgenden Themen:

- Fordern Sie ein falsch positives Ergebnis in an IT Remediation Workspace
- Fordern Sie eine Ausnahme in an IT Remediation Workspace
- Fordern Sie eine Risikominderung in an IT Remediation Workspace
- Teilen Sie eine Korrekturaufgabe in auf IT Remediation Workspace
- Erstellen Sie eine Change-Anforderung in IT Remediation Workspace
- Ausnahme mit GRC: Policy and Compliance Management in IT Remediation Workspaceanfordern



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor das Fälligkeitsdatum erreicht ist. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Erweiterung auch über die klassische Umgebung anfordern.

Verwenden Sie dasselbe Verfahren, um eine Verlängerung für ein angreifbares Anwendungselement, ein angreifbares Containerelement, eine Testergebnisgruppe und eine Korrekturaufgabe anzufordern.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereiche des Schwachstellenmanagers**.
2. Wählen Sie Listen aus.
3. Wählen Sie unter Angreifbare Host-Elemente die Option **Alle**aus.
4. Filtern Sie die Liste, indem Sie in der Spalte Status die Option „Zurückgestellt“ auswählen.
5. Wählen Sie ein zurückgestelltes angreifbares Element aus.

   **Hinweis:**
   Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Elements „Zurückgestellt“ lautet.

6. Klicken Sie auf die Schaltfläche **Verlängerung anfordern**.
7. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Elements verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Verlängerung anfordern aus**.
   Nach der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   **Hinweis:**

   - Die Anforderung durchläuft zwei Genehmigungsstufen.
   - Wenn ein zurückgestelltes angreifbares Element erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

9. Nachdem die Anforderung genehmigt wurde, werden die Notizen für Bis, Grund und Zurückstellung aktualisiert.

### Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut

Um sicherzustellen, dass Ihre Korrekturaufgaben und Datensätze zwischen geplanten Scan-Zyklen gelöst wurden, initiieren Sie bei Bedarf erneute Scans von Ihrem Now Platform.

Erforderliche Rolle: sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin.

Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Die Scanner Rapid7 und Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

So aktivieren Sie diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle der Datensätze für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Erneutes Scannen wird für Datensätze und Korrekturaufgaben mit den folgenden Integrationen in Vulnerability Manager Workspace unterstützt. Weitere Informationen finden Sie in den folgenden Themen:

- Scannen Sie Rapid7 angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut
- Scannen Sie Qualys angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut
- Scannen Sie Tenable.io und Tenable.sc angreifbare Elemente aus den Vulnerability Response -Arbeitsbereichen erneut

Um im Arbeitsbereich von Vulnerability Manager erneute Scans aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, benötigen die Datensätze einen unterstützten Scanner als Quelle.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglicherweise möchten Sie eine gefilterte Liste erstellen, in der Datensätze nach ihrer Quelle angezeigt werden. Unter Erstellen Sie eine benutzerdefinierte Liste von Datensätzen finden Sie ein Beispiel für die Erstellung einer Liste.

### Verwenden Sie die Listenansicht im Arbeitsbereich von Vulnerability Manager

Die Listenansicht im Arbeitsbereich von Vulnerability Manager ermöglicht es Schwachstellen- und Sicherheitsmanagern und Analysten, den Korrekturfortschritt für Datensätze anzuzeigen, Detailinformationen zu Vulnerability Response-Datensätzen anzuzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzuzeigen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin oder sn_vulc.admin

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Klicken Sie oben links im Arbeitsbereich bei angezeigter Homepage auf das **Listensymbol**.
3. **Wahlweise:** Klicken Sie auf **Meine Listen**, um eine Liste zu erstellen.
   Weitere Informationen zum Erstellen einer Liste finden Sie unter Erstellen Sie eine benutzerdefinierte Liste von Datensätzen.
4. In der folgenden Tabelle finden Sie die Aktionen, die Sie auf der Listenseite ausführen können.

| UI-Aktion | Beschreibung |
|---|---|
| Öffnen Sie eine Korrekturmaßnahme | |
| Bewegen Sie den Mauszeiger links neben der Spalte Nummer, während eine Liste angezeigt wird, über eine Zeile, und klicken Sie auf das kleine Informationssymbol **(i)** für einen Datensatz. | Details zu den Datensätzen werden im rechten Seitenbereich der Seite angezeigt. Zu den Details gehören:<br>○ Zuweisungsgruppe<br>○ Schwachstelle<br>○ Zugewiesen an<br>○ Kurzbeschreibung<br>○ Beschreibung<br>Sie können die Felder bearbeiten. Wenn das Kontrollkästchen Aktiv angezeigt wird, können Sie den Datensatz aktivieren oder deaktivieren. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern. |
| Liste aktualisieren | Wenn das Aktualisierungssymbol oben rechts auf der Seite angezeigt wird, laden Sie die aktuelle Seite neu. |
| Breiten zurücksetzen | Klicken Sie auf das Zahnradsymbol, um die Spaltenbreiten in Ihren Listen anzupassen. Eine Kopie der ursprünglichen Liste wird unter **Ihre Listen**gespeichert. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| UI-Aktion | Beschreibung |
|---|---|
| Kopieren Sie die URL für die angezeigte Seite | Kopieren Sie die URL, um sie an anderer Stelle zu verwenden. |
| Exportieren Sie die Seite | Geben Sie im modalen Fenster die Datei- und Bereitstellungstypen ein, und klicken Sie auf **Exportieren**. |
| Verfeinern Sie die Filter für die Daten auf der Seite. | Wählen Sie eine Spalte aus, und erweitern Sie das Menü mit den drei vertikalen Punkten, um Optionen anzuzeigen, mit denen die Daten in der Spalte weiter gefiltert werden.<br>Beispielsweise könnten Sie die Spalte Zuweisungsgruppe aus der Liste der aktiven Korrekturaufgaben nach einer bestimmten Zuweisungsgruppe filtern. |
| Filtern Sie Elemente heraus, oder gleichen Sie Elemente aus einer Zeile in einer Spalte ab | Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine der folgenden Optionen auswählen:<br>○ Übereinstimmungen anzeigen: Zeigt nur Elemente an, die der ausgewählten Zelle in der Spalte entsprechen.<br>○ Herausfiltern: Filtert die Elemente aus der Spalte heraus, die der ausgewählten Zelle in der Spalte entsprechen. |

5. Ab Version 18.0 können Sie ein angreifbares Anwendungselement aus der Liste „ **Aktiv** “ oder „ **Alle** “ unter *`Application Vulnerable items`* erstellen, indem Sie oben rechts auf die Schaltfläche **Neu** klicken.

### Erstellen Sie eine benutzerdefinierte Liste von Datensätzen

Sie können eine benutzerdefinierte Liste im Arbeitsbereich von Vulnerability Manager erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin oder sn_vulc.admin

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**.
2. Wählen Sie das **Listensymbol** aus, und klicken Sie auf **Meine Listen**.
3. Wählen Sie **Neue Liste**aus.
4. Klicken Sie im modalen Fenster „Neue Liste“ auf Mit **vorhandener beginnen**, und suchen Sie in der Auswahlliste Liste nach einer vorhandenen Liste, die als Vorlage verwendet werden soll.
5. Bearbeiten Sie den Listennamen.
6. Fügen Sie Filter hinzu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise möchten Sie möglicherweise eine Liste aktiver Datensätze für einen bestimmten Scanner erstellen, den Sie auf erneute Scans überwachen möchten. Sie können die folgenden Filter verwenden: Aktiv ist true, und Quelle enthält (Name Ihres Scanners).

7. Bearbeiten Sie die Spalten, die in Ihrer Liste angezeigt werden sollen.
8. Klicken Sie auf **Erstellen**.
   Ihre neue Liste wird angezeigt.
9. Klicken Sie alternativ auf **Eigene erstellen**, geben Sie einen Namen ein, gefolgt von **Quelle auswählen**.
10. Beginnen Sie mit der Eingabe in das Feld, und wählen Sie aus den Quellen aus, die für Ihre neue Liste angezeigt werden.
11. Klicken Sie auf **Erstellen**.
    Ihre neue Liste wird angezeigt.

**Hinweis:**
Wenn Sie das Listenmodul verlassen, ist die Liste, die beim Beenden angezeigt wird, die Liste, die Sie bei der Rückkehr sehen.

12. Um eine Liste zu löschen, klicken Sie bei angezeigter Liste oben rechts auf der Seite auf das Zahnradsymbol.

### Genehmigen Sie Anforderungen in Vulnerability Manager Workspace

Genehmigen Sie Anforderungen, die aus dem IT Remediation Workspace von Korrekturbesitzern übermittelt werden.

**Vorbereitungen**
Erforderliche Rollen:

**Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind**

| Genehmigungstyp | Genehmigungsebenen erforderlich | Genehmigerrollen | Zusätzliche Informationen |
|---|---|---|---|
| Falsch positive Genehmigungen | Eins | • Granulare Rolle sn_vul.false_positive_approver für angreifbare Elemente (VITs).<br>• sn_vul.app_false_positive_approver für angreifbare Anwendungselemente (AVITs)<br>• sn_vul_container.false_positive_approver für angreifbare Container-Elemente (CVITs)<br><br>Oder<br><br>Genehmiger müssen der Benutzergruppe „Falsch positive Genehmiger“ angehören. | - |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)**

| Genehmigungstyp | Genehmigungsebenen erforderlich | Genehmigerrollen | Zusätzliche Informationen |
|---|---|---|---|
| Ausnahmegenehmigungen (Zurückstellungen) | Zwei | • In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich<br>• In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich | Eine Ausnahmeanforderung für einen Datensatz oder eine Korrekturaufgabe wird mithilfe eines standardmäßigen zweistufigen Genehmigungsworkflows genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet und ist dann in der Warteschlange des Genehmigers 2 sichtbar. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)**

| Genehmigungstyp | Genehmigungsebenen erforderlich | Genehmigerrollen | Zusätzliche Informationen |
|---|---|---|---|
| Heben Sie die Zuweisung von Genehmigungen auf | In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich | • sn_vul.unassign_appr für AVITs und VITs<br>• sn_vul_container.unas für CVITs<br>• sn_vulc.unassign_app für Konfigurationsproble (CIs) | **Hinweis:** Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt und eine Genehmigungsgruppe zum Aufheben der Zuweisung erstellt. Benutzer (Zuweisung von Genehmiger aufheben – Ebene 1) dieser Gruppe können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Rolle „Zuweisung aufheben“ eines Genehmigers, sn_vul.unassign_approver. Sie können eine neue Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren. Um Genehmigungsregeln zu konfigurieren, navigieren Sie zum entsprechenden Modul „Genehmigungsregeln“, wählen Sie eine der folgenden Genehmigungsregeln aus, und navigieren Sie auf der Registerkarte „Genehmigungskonfigurationen“ zur **Genehmigungskonfiguration** :<br>• *Vulnerable item field change request* für ein angreifbares Element.<br>• *Vulnerability* |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)**

| Genehmigungstyp | Genehmigungsebenen erforderlich | Genehmigerrollen | Zusätzliche Informationen |
|---|---|---|---|
| Risikominderungsgenehmigungen | Zwei | • In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich<br>• In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich | Der Genehmigungs-Flow für die Risikominderung ist derselbe wie für Ausnahmegenehmigungen (Zurückstellungen). |

Weitere Informationen zum Zuweisen von Persona-Rollen zu Benutzern und Benutzern zu Gruppen finden Sie unter Vulnerability Response Personas und granulare Rollen und Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

**Hinweis:**
Fügen Sie den Genehmigungsgruppen Benutzer hinzu, bevor Sie Genehmigungsanforderungen übermitteln. Wenn Sie Anforderungen erstellen, bevor Sie Benutzer zu den Genehmigungsgruppen hinzufügen, sind die Anforderungen für die Benutzer mit der Genehmigungsberechtigung möglicherweise nicht sichtbar.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**.
   Wenn ein Genehmiger keinen Zugriff auf den Arbeitsbereich hat, können Genehmigungen um verarbeitet werden **Vulnerability Response** > **Meine Freigaben** in der klassischen Umgebung.
2. Wählen Sie das Listenansicht-Symbol ( ) aus.
   Die Listenseite wird angezeigt.
3. Wählen Sie in der gefilterten Liste „Genehmigungen“ die **Option Mir zugewiesen aus**.
4. Suchen Sie eine Anforderung, die Sie verarbeiten möchten, und wählen Sie dann den Link in der Spalte Status aus.
   Der Datensatz „Genehmigung der Änderung des Schwachstellenstatus“ (VCA#) wird angezeigt.
5. Wählen Sie eine der folgenden Optionen aus, um die Anforderung zu genehmigen oder abzulehnen.

## Richten Sie E-Mail-Benachrichtigungen in den Vulnerability Response Arbeitsbereichen ein

Identifizieren Sie Benutzer für automatische E-Mail-Erinnerungen, die an Benutzer in der Benutzergruppe „Korrekturbesitzer“ gesendet werden.

### Vorbereitungen
Erforderliche Rolle: admin

Diese Funktion generiert automatisch eine E-Mail-Zusammenfassung für Benutzer in der Benutzergruppe „Korrekturbesitzer“. Fügen Sie alle Benutzer hinzu, die E-Mail-Benachrichtigungen erhalten sollen, wie in Verwenden Sie die E-Mail-Zusammenfassung in Vulnerability Response Workspacesbeschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass Benutzer über eine aktive E-Mail-Adresse in ihrem Benutzerdatensatz verfügen und dass Sie sie der Benutzergruppe „Korrekturbesitzer“ hinzugefügt haben.

Wenn Sie die Zustellhäufigkeit, den Tag oder die Uhrzeit der E-Mails ändern oder die Funktion deaktivieren möchten, führen Sie die folgenden Schritte aus.

### Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgaben**.
2. Suchen Sie den Korrektur- **Digest generieren**, und klicken Sie darauf, um den Datensatz zu öffnen.

   Möglicherweise möchten Sie die Felder in ihren Standardeinstellungen belassen, bis Sie überprüfen, ob Benachrichtigungen gesendet werden. Standardmäßig werden E-Mails wöchentlich am Montagmorgen um 9:00 Uhr in der Zeitzone der Instanz gesendet, in der die Aufgabe ausgeführt wird.
3. Ändern Sie die Felder im Formular.
   Weitere Informationen zu den Formularfeldern finden Sie unterGenerieren von Korrektur-Digest-Formularfeldern.
4. Klicken Sie auf **Aktualisieren**.

### Nächste Maßnahme

Wenn Sie überprüft haben, dass alle zuvor aufgeführten Informationen korrekt sind und Sie Benutzer in der Benutzergruppe „Korrekturbesitzer“ haben, die E-Mails jedoch nicht wie erwartet gesendet werden, überprüfen Sie, ob Kanäle für den Empfang von E-Mail-Benachrichtigungen aktiviert sind. Weitere Informationen finden Sie unter Create notification channels .

## Referenzinformationen für Vulnerability Manager Workspace

Die folgenden Themen enthalten Links, Referenzinformationen sowie Felddaten in den Formularen und Datensätzen im Arbeitsbereich von Vulnerability Manager.

## Felder im Formular „Überwachungsthema erstellen“

In der folgenden Tabelle werden die Felder im Formular „Überwachungsthema erstellen“ in Vulnerability Manager Workspace beschrieben.

| Feld | Beschreibung |
|---|---|
| Name | Name für Ihr Überwachungsthema, z. B. Kritische AEs. |
| Eigentum von | Der Name des Benutzers, der das Überwachungsthema besitzt. |
| Anzeigereihenfolge | Geben Sie einen Wert zwischen 100 und 1000 ein. 100 ist der Standardwert. Niedrigere Werte, beginnend mit 100, werden in aufsteigender Reihenfolge in Listen angezeigt. |
| Verantwortliche Gruppe | Der Name der Gruppe, die das Überwachungsthema besitzt. |
| Aktiv | Aktivieren oder deaktivieren Sie das Überwachungsthema. Der Standardwert ist (Aktiv). |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beobachtungsliste | Fügen Sie Namen von Benutzern hinzu, die Benachrichtigungen erhalten und das Überwachungsthema anzeigen können. |
| Beschreibung | Text, der Ihr Überwachungsthema beschreibt. Dieser Text wird im Feld Beschreibung angezeigt, wenn Sie eine Korrekturmaßnahme aus diesem Überwachungsthema erstellen. |
| Kategorie | Typ des Datensatzes, für den das Überwachungsthema erstellt wird.<br>**Hinweis:**<br>Das Feld **Kategorie** wird ab Version 18.0 angezeigt. |
| Vorschau | Klicken Sie auf **Vorschau**, um eine Liste mit der Anzahl der Datensätze anzuzeigen, die Ihre Filterbedingungen zurückgeben.<br>**Hinweis:**<br>Ab Version 18.0 ist die Schaltfläche **Vorschau** nicht verfügbar. |

**Zugehörige Informationen**

Erstellen Sie in Vulnerability Manager Workspace ein Überwachungsthema

### Generieren von Korrektur-Digest-Formularfeldern

Die folgende Tabelle zeigt die Felder im Formular „Korrektur-Digest generieren“.

#### Generieren von Korrektur-Digest-Feldern

| Feld | Beschreibung |
|---|---|
| Aktives Kontrollkästchen | Diese Checkbox ist standardmäßig aktiviert. Wenn Sie keine E-Mail-Benachrichtigungen senden möchten, deaktivieren Sie dieses Feld. |
| Run-Kosten | Wöchentlich ist die Standardeinstellung. Wählen Sie eine Option aus der Liste aus. |
| Tag | Montag ist der Standardwert. Wählen Sie eine Option aus der Liste aus. |
| Zeit | Legen Sie eine Zeit für die Zustellung der E-Mails fest. Wählen Sie eine Zeitzone aus, wenn Sie eine andere Zeitzone wünschen als die, die von der Instanz verwendet wird, die den Job ausführt. |

### Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum

Ab v20.0 von Vulnerability Response können Sie als Korrekturbesitzer eine Risikominderung für ein angreifbares Host-Element oder eine Korrekturaufgabe anfordern, und Genehmiger können die Risikominderungsanforderungen genehmigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Anfordern der Risikominderung und zum Genehmigen der Risikominderungsgenehmigung finden Sie unter Fordern Sie eine Risikominderung in an IT Remediation Workspace bzw. Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

Wenn Sie eine Risikominderungsanforderung genehmigen, wird die Risikopunktzahl entsprechend dem **gewünschten Wert** (Risikobewertung) in der Status-Change-Genehmigung (VCA#) reduziert. Die höchste Risikopunktzahl der gewünschten Risikobewertung wird dem Datensatz zugewiesen, wenn Ihre Risikominderungsanforderung genehmigt wird. Das folgende Beispiel zeigt, wie die Risikopunktzahl und die ursprüngliche Risikopunktzahl aktualisiert werden, wenn Ausgleichskontrollen angewendet werden. Im folgenden Beispiel werden die standardmäßigen höchsten Risikowerte der Risikobewertungen verwendet.

**Auswirkung von Ausgleichskontrollen auf die Risikopunktzahl und die ursprüngliche Risikopunktzahl**

| Szenario | Risikobewertung | Risikopunktzahl | Ursprüngliche Risikopunktzahl (Berechnete Risikopunktzahl) |
|---|---|---|---|
| Daten vor v20.0 | 2 – Hoch | 80 | Das Feld ist vor v20.0 nicht verfügbar. |
| Nach dem Upgrade auf v20.0 | 2 – Hoch | 80 | NULL |
| Die berechnete Risikopunktzahl ändert sich während der Erfassung in 90 | 1 – Kritisch | 90.0 | NULL |
| Wenn Sie Ausgleichskontrollen anwenden | 3 – Mittel | 69 | 90.0 |
| Die berechnete Risikopunktzahl ändert sich während der Erfassung in 70 | 3 – Mittel | 69 | 70 |
| Die berechnete Risikopunktzahl ändert sich während der Erfassung in 50 | 3 – Mittel | 50 | 50 |
| Die berechnete Risikopunktzahl ändert sich während der Erfassung in 80 | 3 – Mittel | 50 | 80 |
| Wenn die Ausgleichskontrollen am **Bis-Datum für Risikominderung**ablaufen | 2 – Hoch | 80 | NULL |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Auswirkung von Ausgleichskontrollen auf eine Korrekturaufgabe

Wenn Ihre Anforderung zur Risikominderung für eine Korrekturaufgabe genehmigt wird, wirken sich Ausgleichskontrollen auf die angreifbaren Elemente wie folgt aus:

- Die auf die Korrekturaufgabe angewendeten Ausgleichskontrollen werden auf die angreifbaren Elemente angewendet (außer denen im Status „Geschlossen“), deren Risikopunktzahl höher ist als die Risikopunktzahl, die dem **Wert Gewünscht** in der Statusänderungsgenehmigung einer Korrekturaufgabe entspricht. Und die Risikopunktzahl dieser angreifbaren Elemente wird entsprechend dem **gewünschten Wert**reduziert.
- Das **Bis-Datum für die Risikominderung** bleibt für die angreifbaren Elemente, auf die bereits eine Ausgleichskontrolle angewendet wird, unverändert. Sie wird nicht mit dem **Bis-Datum für die Risikominderung** der Korrekturaufgabe aktualisiert.
- Das **Bis-Datum für die Risikominderung** wird nur dann auf die angreifbaren Elemente heruntergerollt, wenn zuvor keine Ausgleichskontrolle auf ein angreifbares Element angewendet wurde. Wenn Sie die Ausgleichskontrollen erneut auf die Korrekturaufgabe anwenden, wird das **Bis-Datum für die Risikominderung** nicht auf die angreifbaren Elemente übertragen, da das vorhandene **Bis-Datum für die Risikominderung** der angreifbaren Elemente Priorität erhält.
- Wenn einer Korrekturaufgabe, auf die bereits Ausgleichskontrollen angewendet werden, ein neues angreifbares Element hinzugefügt wird, wird das Risiko nicht auf die angreifbaren Elemente reduziert.

## Auswirkung einer Ausgleichskontrolle auf ein angreifbares Element

Wenn Ihre Anforderung zur Risikominderung für ein angreifbares Element genehmigt wird:

- Its neue Risikopunktzahl wird im Feld **Risikopunktzahl** angezeigt, und die alte Risikopunktzahl (berechnete Risikopunktzahl) wird in das Feld **Ursprüngliche Risikopunktzahl verschoben**. Diese Änderung gilt bis zu dem im Feld **Bis Datum für Risikominderung** angegebenen Datum.
- Wenn für ein angreifbares Elementwährend der Erfassung bereits Ausgleichskontrollen angewendet wurden:
  - Wenn die berechnete Risikopunktzahl größer als die Risikopunktzahl ist, bleibt die Risikopunktzahl gleich und die ursprüngliche Risikopunktzahl wird mit der berechneten Risikopunktzahl aktualisiert.
  - Wenn die berechnete Risikopunktzahl kleiner als die Risikopunktzahl ist, werden sowohl die Risikopunktzahl als auch die ursprüngliche Risikopunktzahl mit der berechneten Risikopunktzahl aktualisiert.
- Wenn ein Konfigurationselement (CI) für einangreifbares Element mit bereits angewendeter Ausgleichskontrolle geändert wird:
  - wird das CI für ein angreifbares Element standardmäßig aktualisiert, da die Systemeigenschaft `sn_sec_cmn.update_on_ci_change` auf „true“ festgelegt ist.

    Die Ausgleichskontrollen gelten weiterhin für das angreifbare Element.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das angreifbare Element wird geschlossen, und eine neue VIT wird erstellt, wenn die Systemeigenschaft *sn_sec_cmn.update_on_ci_change* auf „false“ festgelegt ist.

  Die Ausgleichskontrollen gelten weiterhin für das neue angreifbare Element, und das **Bis-Datumfür Risikominderung**, die **ursprüngliche Risikopunktzahl** und die **Risikopunktzahl** bleiben gleich.

- Wenn ein angreifbares Element vom Scanner erneut geöffnet wird und bereits Ausgleichskontrollen darauf angewendet werden, wird nach dem erneuten Öffnen dieselbe Ausgleichskontrolle angewendet.

**Zugehörige Informationen**

Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Ordnen Sie Ausgleichskontrollen CVEs oder TPEs für Risikominderungsanforderungen zu

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

#unique_1317_Connect_42_li-risk-reduction-vmws

## IT Remediation Workspace

IT-Teams zeigen IT-orientierte Aufgaben und Informationen an, z. B. Lösungen und betroffene Konfigurationselemente. IT-Teams können Zeit bei der Behebung von Schwachstellen sparen, indem sie einfach Change-Anforderungen erstellen, angreifbare Elemente erneut scannen und Ausnahmeanforderungen über den Arbeitsbereich „IT-Fehlerkorrektur“ senden.

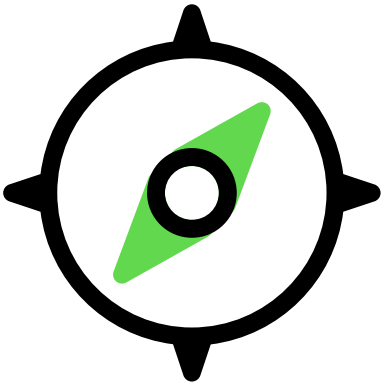
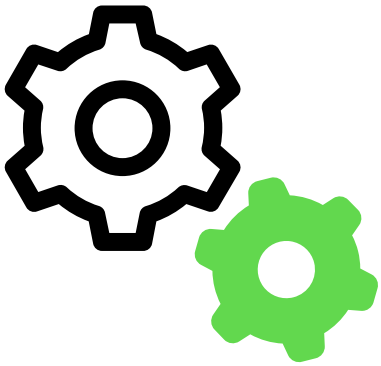
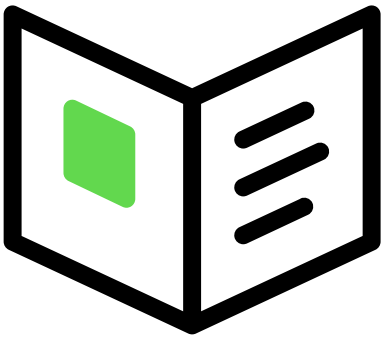
## Übersicht

v18.0 IT Remediation Workspace-Demo

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erste Schritte

| Erkunden | Beheben | Referenz |
| --- | --- | --- |
|  |  |  |
| Erfahren Sie mehr über den IT Remediation Workspace | Erfahren Sie, wie Sie Schwachstellen und Fehlkonfigurationen im IT-Korrekturarbeitsbereich beheben können | Erfahren Sie mehr über zusätzliche Informationen, die für die Verwendung von IT Remediation Workspace erforderlich sind |

## Problembehandlung und Hilfe

- Security Operations in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### IT Remediation Workspace erkunden

IT Remediation Workspace ist für IT-Korrekturbesitzer und IT-Gruppen gedacht. Sie besteht aus Homepage- und Listenansichten sowie Datenvisualisierungen, auf die Sie klicken können, um die Ihnen zugewiesenen Korrekturaufgaben und die Anzahl der Ihnen zugewiesenen Datensätze mit Lösungen anzuzeigen.

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
| --- | --- |
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

IT Remediation Workspace besteht aus den folgenden Zielseiten, Listen und Formularen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zielseite (Homepage).**

Die Zielseite der Homepage besteht aus einer Liste der Ihnen zugewiesenen Korrekturaufgaben und der Ihnen zugewiesenen Datensätze mit Lösungen.

Sie können auf eine Korrekturaufgabe klicken, um die Details anzuzeigen und eine Untersuchung zu starten. In der Listenansicht können Sie Korrekturbemühungen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe öffnen und **auf Mir** zuweisen klicken, um die Aufgabe sich selbst zuzuweisen und die Untersuchung zu starten.

**Hinweis:**
Wenn Sie sich die Aufgabe in der Korrekturaufgabe nicht selbst zuweisen, können Sie keine UI-Aktionen auf der Ebene des angreifbaren Elements anzeigen.

Klicken Sie auf die Auslassungspunkte Weitere Aktionen und dann auf **Untersuchung starten**, um eine Korrekturaufgabe zu lösen.

Eine zusätzliche Bewertungsliste, **Angreifbare CIs**, wird in der Ansicht „Home“ angezeigt. Die Datenvisualisierung der angreifbaren CIs zeigt Konfigurationselemente mit AEs, die Ihnen oder Ihren Gruppen zugewiesen sind. Weitere Informationen finden Sie unter Zeigen Sie Konfigurationselemente mit Schwachstellen in an IT Remediation Workspace.

Die angezeigte Seite enthält die folgenden Informationen:

- Ihnen zugewiesene aktive Korrekturaufgaben
- Ihnen zugewiesene Datensätze mit bevorzugten Lösungen.
- Die Liste der Ihnen zugewiesenen Korrekturaufgaben.

Weitere Informationen dazu, was Sie auf dieser Seite tun können, finden Sie unter Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace.

**Seite „Dashboards“**

Die Seite „Dashboards“ besteht aus dem Dashboard „Schwachstellenkorrektur“. Weitere Informationen zur Seite „Dashboards“ finden Sie unter Dashboardübersicht.

**Listen-Seite**

Diese Ansicht besteht aus standardmäßigen und benutzerdefinierten Listenseiten für Korrekturaufgaben, angreifbare Elemente, Lösungen und Ausnahmeanforderungen, die Ihnen zugewiesen sind.

- Listen: Standardlisten für Korrekturaufgaben, angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationstestergebnisse, die Ihnen und Ihrer Gruppe zugewiesen sind, Lösungen und Ausnahmeanforderungen.
- Meine Listen: In dieser Ansicht werden alle Listen angezeigt, die Sie auf der Zielseite der Liste umbenannt haben, sowie alle von Ihnen erstellten Listen.

Die Listenansicht wird mit Links zu Arbeiten, die Ihnen und Ihren Gruppen zugewiesen sind, zu angreifbaren Elementen, die Ihnen und Ihren Gruppen zugewiesen sind, Lösungen und Ihren Ausnahmeanforderungen angezeigt.

Sie können auch eigene Listen erstellen, um den Fortschritt der Fehlerkorrektur zu überwachen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Listen für **angreifbare CIs** werden in der Listenansicht angezeigt. Die Lösungsliste wird angezeigt, wenn die Anwendung Vulnerability Solution Management installiert ist. Diese Karte zeigt Lösungsdaten, potenzielle und bevorzugte Lösungen von Drittanbietern zu Ihren angreifbaren Elementen.

Weitere Informationen dazu, was Sie auf dieser Seite tun können, finden Sie unter Verwenden Sie die Listenansicht im IT Remediation Workspace.

### Sehen Sie sich ein Workflow-Beispiel in an IT Remediation Workspace

Sehen Sie sich ein Beispiel für einen End-to-End-Workflow im IT Remediation Workspacean. Erfahren Sie, wie IT-Spezialisten den Arbeitsbereich verwenden können, um kritische angreifbare Elemente zu überwachen und die ihnen zugewiesenen Schwachstellen zu beheben.

**Vorbereitungen**
Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

**Prozedur**

Klicken Sie auf die folgende Abbildung, um die Schritte des Workflows anzuzeigen.
IT Remediation Workspace-Demo

Das Image enthält die folgenden Aufgaben:

- Zeigen Sie auf der Homepage (Zielseite des IT-Korrekturbesitzers) die Korrekturaufgaben an, die Ihnen zugewiesen sind. Wechseln Sie zwischen Arbeit, die Ihnen und Ihrer Gruppe zugewiesen ist. Sehen Sie sich die Korrekturaufgaben mit Lösungen an.
- Klicken Sie auf die Listenansicht, um die **Listen** der Ihnen zugewiesenen Arbeit anzuzeigen.
- Identifizieren Sie in der Listenansicht mit der ausgewählten Liste **Meiner Gruppe zugewiesen** die Arbeit und weisen Sie sich selbst zu.
- In einem offenen Korrekturaufgaben-Datensatz:
  - Klicken Sie auf die Registerkarte **Übersicht**, um die angreifbaren Elemente (AEs) und betroffenen Konfigurationselemente (CIs) anzuzeigen, die dem Datensatz zugeordnet sind.
  - Klicken Sie auf die Registerkarte **Lösungen**, um bevorzugte und potenzielle Lösungen anzuzeigen.
  - Klicken Sie auf die Registerkarte **Details**, um bearbeitbare Felder zu ändern.
  - Klicken Sie auf die folgenden UI-Aktionen: **Als falsch positiv**markieren, **Change erstellen**, **Aufgabeaufteilen, Ausnahme anfordern**. Befolgen Sie die Anweisungen in den Dialogfeldern, um bei der Korrektur zu helfen.

### Dashboardübersicht

Die Seite „Dashboards“ in Next ExperienceIT Remediation Workspace stellt das Dashboard „Schwachstellenkorrektur“ in der Benutzeroberfläche von [] bereit, das verwendet werden kann, um sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können das Dashboard „Schwachstellenkorrektur“ anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** und wählen Sie das Symbol Dashboards. Weitere Informationen zum

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Schwachstellenkorrektur“ finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.

Sie können ein benutzerdefiniertes Dashboard erstellen, indem Sie das Symbol „Weitere Optionen“ und **dann Neues Dashboard erstellen**auswählen.

### IT Remediation Workspace verwenden

Der IT-Korrekturarbeitsbereich bietet eine konsolidierte Liste von Hostschwachstellen, Anwendungsschwachstellen, Containerschwachstellen und Fehlkonfigurationen, die Ihnen und Ihrer Gruppe zugewiesen sind. Sie können diesen Arbeitsbereich verwenden, um Fehler zu beheben und Ausnahmen für Schwachstellen und Fehlkonfigurationen anzufordern.

### Verwenden Sie die E-Mail-Zusammenfassung in Vulnerability Response Workspaces

Verwenden Sie E-Mail-Benachrichtigungen, um Ihren Fortschritt bei der Korrektur anzuzeigen, und erinnern Sie sich daran, wenn Aufgaben sich dem SLA nähern oder dieses überschritten haben.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

#### Warum und wann dieser Vorgang ausgeführt wird

Kommen Sie als Korrekturbesitzer in Ihren Arbeitsbereich, und sehen Sie sich Ihre E-Mail-Benachrichtigung als Zusammenfassung Ihrer Arbeit an. Sehen Sie, was Sie erreicht haben, was bevorsteht und was überfällig ist. Verwenden Sie die Benachrichtigung, um Ihre kritischen Korrekturaktionen zu organisieren und zu priorisieren. Klicken Sie auf einen Link in der E-Mail, um direkt zu Ihrem Arbeitsbereich zu gelangen. Benachrichtigungen können IT-Spezialisten dabei unterstützen, den Status ihrer Arbeit auf einen Blick zu behalten. Helfen Sie als Schwachstellenmanager Ihren IT-Spezialisten, für Korrekturaufgaben direkt über ihren E-Mail-Service auf die Plattform zuzugreifen.

Weitere Informationen zur Konfiguration dieser Funktion finden Sie unter Richten Sie E-Mail-Benachrichtigungen in den Vulnerability Response Arbeitsbereichen ein.

Die E-Mail enthält standardmäßig die Aufgaben, die Sie geschlossen haben, die Gesamtzahl der Ihnen und Ihren Gruppen zugewiesenen aktiven Aufgaben, neu zugewiesene Aufgaben, geschlossene VITs und andere Informationen.

#### Prozedur

1. Navigieren Sie zu Ihrer E-Mail, suchen Sie eine Benachrichtigung, und klicken Sie darauf, um sie zu öffnen. Die Benachrichtigung wird mit Informationen zu Ihrem Arbeitsstatus angezeigt.
2. Klicken Sie auf Zum Arbeitsbereich wechseln, um zu Ihrem **Arbeitsbereich** zu navigieren.

### Verwenden Sie Datensätze in IT Remediation Workspace

Verwenden Sie Datensätze, um Ihren Fortschritt bei der Korrektur und die Auswirkungen angreifbarer Elemente auf Ihre Assets anzuzeigen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren Sie in Ihrer Instanz Now Platform zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Navigieren Sie zu einem Datensatz für ein angreifbares Element, und öffnen Sie ihn entweder über die Zielseite der Homepage oder über die Listenansicht.

   Die Registerkarte „Details“ enthält oben im Formular-Header Informationen, die sich auf die Art der Schwachstelle beziehen, z. B. CVE-2013-5014, erkannt auf LINUX-DAL-4331. Unter der Formularkopfzeile werden Werte für Status, Risikobewertung und Korrekturzieldatum angezeigt.
3. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie für den Datensatz der Korrekturaufgabe ausführen können.



## Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace

Korrekturaufgaben werden automatisch aus Korrekturmaßnahmen erstellt und zugewiesen. IT-Teams und Korrekturverantwortliche zeigen Korrekturaufgaben im IT Remediation Workspacean.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen erstellen, um die Korrektur voranzutreiben, werden Korrekturaufgaben automatisch erstellt und den IT-Teams basierend auf der Gruppe zugewiesen, die den Datensätzen in einer Korrekturmaßnahme zugeordnet ist.

Zeigen Sie die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs mit Schwachstellen auf der Registerkarte Angreifbare **CIs** oder in der Liste Ihnen und Ihrer Gruppe zugewiesene angreifbare CIs in der Listenansicht an.

### Prozedur

1. Navigieren Sie in Ihrer Instanz Now Platform zu **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Klicken Sie im Abschnitt „Korrekturaufgaben“ auf einen Korrekturaufgabendatensatz (VUL), um ihn zu öffnen.
3. **Wahlweise:** Alternativ können Sie auf der Homepage oben links auf das Listensymbol klicken, um alle Ihnen und Ihren Gruppen zugewiesenen Korrekturaufgaben und Datensätze (Arbeit) anzuzeigen.
   Weitere Informationen zur Verwendung der Listenansicht finden Sie unter Verwenden Sie die Listenansicht im IT Remediation Workspace.
4. Klicken Sie auf der Homepage oder in der Listenansicht auf einen Korrekturaufgabendatensatz (VUL), um ihn zu öffnen.

   Die folgende Abbildung zeigt die Abschnitte eines Korrekturaufgabendatensatzes und die verfügbaren Daten.

   Zwischen den Registerkarten **Lösungen** und **Change** -Anforderungen auf den Registerkarten der zugehörigen Liste, die in der folgenden Abbildung dargestellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind, können Sie auf die Registerkarte **Details** klicken, um einige der Informationen im Datensatz zu aktualisieren, z. B. die Zuweisungsgruppe. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.

Die Registerkarte „Details“ enthält oben im Formular-Header Informationen, die sich auf die Art der Aufgabe beziehen, z. B. Schwachstellen auf XYZ-Servern (San Diego). Unter der Formularkopfzeile werden Werte für Status, Risikobewertung, Zuweisungsgruppe, Korrekturstatus und der Prozentsatz der aktiven Datensätze angezeigt, die Sie korrigiert haben.

5. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie über den Datensatz der Korrekturaufgabe ausführen können.

   Auf der Registerkarte Lösungen werden Informationen zu bevorzugten und potenziellen Lösungen angezeigt, die der mit dem Aufgabendatensatz verknüpften Schwachstelle am besten entsprechen. Lösungen sind Patches, die Ihre IT-Teams anwenden, um Schwachstellen zu beheben.

   Wenn die Anwendung Vulnerability Solution Management installiert ist, sind *bevorzugte Lösungen* die Lösungen mit den höchsten Ersatzwerten, die auf Datensätzeangewendet werden. Die Liste der Lösungen basiert auf den Datensätzen in der Korrekturaufgabe.

   Um die Lösungen anzuzeigen, navigieren Sie im Datensatz der Korrekturaufgabe zu **Lösungen** > **Bevorzugte Lösungen**.

   Potenzielle Lösungen. Alle Lösungen, die für VIs in dieser Aufgabe verfügbar sind. Navigieren zu **Lösungen** > **Potenzielle Lösungen**.

   Sie können die CIs (Assets), die von dieser Schwachstelle betroffen sind, im Datensatz der Korrekturaufgabe anzeigen, indem Sie zu navigieren **Übersicht** > **Betroffene CIs**.

### Verwenden Sie die Listenansicht im IT Remediation Workspace

Mit der Listenansicht in IT Remediation Workspacekönnen Sie Korrekturaufgaben und Datensätze anzeigen, die Ihnen und Ihren Gruppen zugewiesen sind. Sie können auch Ihre Ausnahme- und falsch positiven Anforderungen für Korrekturaufgaben und angreifbare Elemente nachverfolgen und Lösungen anzeigen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Klicken Sie auf das Listensymbol.
   Die Listenansicht wird angezeigt.
   - Klicken Sie auf eine gefilterte Liste, um die Gesamtzahl der aktiven Korrekturaufgaben oder Datensätze anzuzeigen, die Ihnen oder Ihrer Gruppe zugewiesen sind. Unter Verwenden Sie Datensätze für Korrekturaufgaben in IT Remediation Workspace finden Sie weitere Informationen dazu, was Sie mit diesen Datensätzen tun können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die Gesamtzahl der Ihnen oder Ihren Gruppen zugewiesenen AEs mit Lösungen an. Klicken Sie auf die Karte **Bevorzugte Lösungen für VIs**, um die Liste anzuzeigen.
- Zeigen Sie die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs mit Schwachstellen auf der Registerkarte Angreifbare **CIs** oder in der Liste Ihnen und Ihrer Gruppe zugewiesene angreifbare CIs in der Listenansicht an.

3. **Wahlweise:** Klicken Sie auf **Meine Listen**.

   (Optional) Führen Sie die folgenden Schritte aus, um eine neue Liste zu erstellen:

   a. Klicken Sie links unten auf der Seite auf **Neue Liste**.

   b. Klicken Sie im modalen Fenster „Neue Liste“ auf Mit **vorhandener beginnen**, und suchen Sie in der Auswahlliste Liste nach einer vorhandenen Liste, die als Vorlage verwendet werden soll.

   c. Bearbeiten Sie den Listennamen.

   d. Fügen Sie Filter hinzu.
   Beispielsweise möchten Sie möglicherweise eine Liste aktiver angreifbarer Elemente für einen bestimmten Scanner erstellen, den Sie überwachen möchten. Sie können beispielsweise die folgenden Filter verwenden: Aktiv ist true, und Quelle enthält (Name Ihres Scanners).

   e. Bearbeiten Sie die Spalten, die in Ihrer Liste angezeigt werden sollen.

   f. Klicken Sie auf **Erstellen**.
   Ihre neue Liste wird angezeigt.

   g. Klicken Sie alternativ auf **Eigene erstellen**, geben Sie einen Namen ein, gefolgt von **Quelle auswählen**.

   h. Beginnen Sie mit der Eingabe in das Feld, und wählen Sie aus den Quellen aus, die für Ihre neue Liste angezeigt werden.

   i. Klicken Sie auf **Erstellen**.
   Ihre neue Liste wird angezeigt.

   **Hinweis:**
   Wenn Sie das Listenmodul verlassen, ist die Liste, die beim Beenden angezeigt wird, die Liste, die Sie bei der Rückkehr sehen. Um die von Ihnen erstellten benutzerdefinierten Listen zu löschen, klicken Sie in der angezeigten Liste rechts im Bereich auf das Zahnradsymbol.

4. In der folgenden Tabelle erfahren Sie, was Sie in der Listenansicht tun können.

### Weisen Sie sich in eine Korrekturaufgabe zu IT Remediation Workspace

Weisen Sie den Datensatz aus einem Korrekturaufgabendatensatz im Arbeitsbereich Vulnerability Response sich selbst zu.

**Vorbereitungen**
Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Option ist nur für Datensätze von Korrekturaufgaben verfügbar, die Ihnen noch nicht zugewiesen sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen** > **Listenansicht** > **Arbeit meiner Gruppe**.
2. Klicken Sie auf eine Korrekturaufgabe (VUL#), um sie zu öffnen.
3. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite **auf Mir zuweisen**.

   Die Korrekturaufgabe wird in der Liste „Meine Arbeit“ unter Korrekturaufgaben in der Listenansicht angezeigt.
4. Sie können Datensätze auch sich selbst zuweisen, indem Sie dieselben Schritte aus offenen Datensätzen ausführen.
   Die Schaltfläche **Mir** zuweisen ist nur verfügbar, wenn Ihnen der Datensatz noch nicht zugewiesen ist.

## Zeigen Sie Konfigurationselemente mit Schwachstellen in an IT Remediation Workspace

Die folgenden Erweiterungen wurden den Korrekturaufgaben mit Version 16.1 der Anwendung Vulnerability Response hinzugefügt.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_changion, sn_vul_container.remediation_owner oder sn_vulc.remediation_owner. Die Rolle „itil“ oder „cmdb_read“ ist auch erforderlich, wenn Sie CI-Daten in den Arbeitsbereichen anzeigen möchten.

### Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die Konfigurationselemente (CIs) an, die Ihnen zugewiesen sind und Schwachstellen aufweisen. Klicken Sie auf Bewertungsliste für angreifbare **CIs**. Klicken Sie oben links auf die Filterliste, um zwischen **Mirzugewiesen und Meinen Gruppen zugewiesen zu wechseln**. Klicken Sie in der Listenansicht auf die Links.

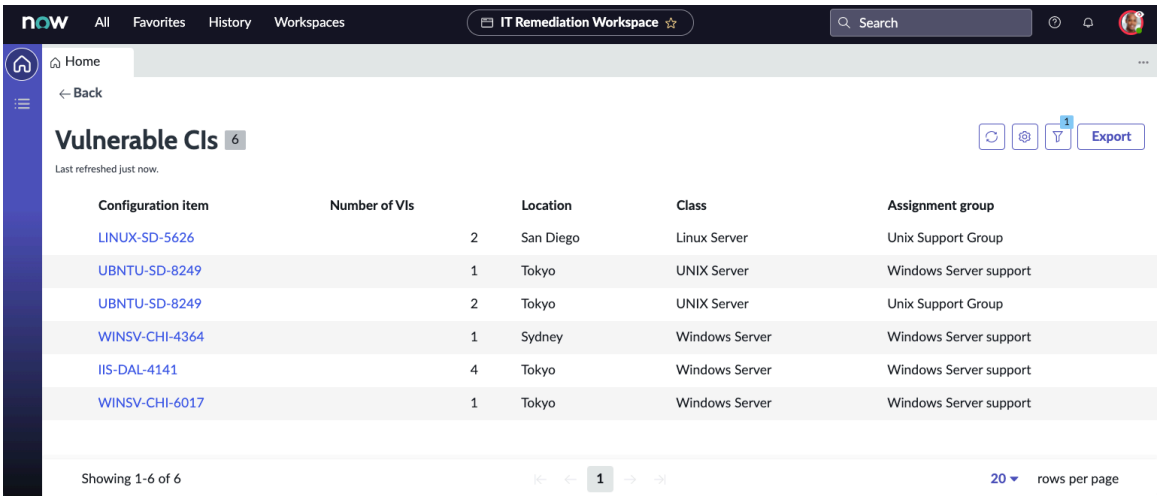
### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
   Die Zielseite der Homepage wird angezeigt.
2. Alternativ können Sie diese Listen über die Links in der Listenansicht anzeigen oder zu den entsprechenden Modulen navigieren, z. B. **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
3. Wählen Sie eine, um fortzufahren.
   Je nachdem, was im Filterumschalter ausgewählt ist, können Sie die Listen der folgenden Datensätze anzeigen, die Ihnen oder Ihnen und Ihren Gruppen zugewiesen sind.
4. Klicken Sie auf die Bewertungsliste Angreifbare **CIs**.

   Die Liste der CI-Datensätze wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf ein Konfigurationselement, um den zugehörigen Datensatz zu öffnen.
   Der Datensatz wird angezeigt.

   Mit den zugehörigen Listen können Sie Details und verschiedene zugehörige Datensätze anzeigen. Zu den neuen verfügbaren Daten in diesem Datensatz mit diesem Release gehören:

   - Eine Zeitleiste, die die aktuelle Aktivität für diesen Datensatz anzeigt.
   - Alle Change-Anforderungen, die diesem CI zugeordnet sind.
   - Navigieren Sie einfach zu Bewertungslisten, und zeigen Sie die Korrekturaufgaben, angreifbaren Elemente und bevorzugten Lösungen an, die diesem CI zugeordnet sind.
   - Ab 18.0 können Sie zu den Bewertungslisten navigieren und die diesem CI zugeordneten bevorzugten Patches anzeigen. Bevorzugte Patches sind die Patches, die den angreifbaren Elementen zugeordnet sind. Auf der Registerkarte Patches in der zugehörigen Liste werden die installierten und fehlenden Patches für die CIs angezeigt.
   - Informationen über das CI, einschließlich Klasse, Standort, Internetverbindung, Umgebung und Wartungsplan.

### Fordern Sie ein falsch positives Ergebnis in an IT Remediation Workspace

Markieren Sie aus einem Korrekturaufgabendatensatz im Arbeitsbereich Vulnerability Response ein falsch positives Ergebnis.

## Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change oder sn_vul_container.remediation_owner

Ein falsch positives Ergebnis ist eine Bedingung, bei der der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist. Es kann mehrere Gründe geben, z. B. falsche Klassifizierung, falsche Logik oder falscher Algorithmus im Scanner. Ein Korrekturbesitzer kann eine Genehmigungsanforderung für Falschmeldungen aus Datensätzen für angreifbare Elemente (VIs) oder Korrekturaufgaben (RTs) senden.

Ab Version 18.0 können Sie Ausnahmen für angreifbare Anwendungselemente und angreifbare Containerelemente anfordern.

Weitere Informationen zu falsch positiven Meldungen in der klassischen Umgebung in der Anwendung Vulnerability Response finden Sie unter Falsch positive Ergebnisse – Übersicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Suchen Sie eine Korrekturaufgabe oder angreifbare Elemente, die Sie als falsch positiv markieren möchten.
3. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Als falsch positiv markieren**.
4. Geben Sie im angezeigten Dialogfeld Informationen zur Anforderung ein, und klicken Sie auf **Anforderungsgenehmigung**.
5. Beantworten Sie im modalen Fenster „Fragebogen ausfüllen“ die Fragen, und klicken Sie auf **Absenden**.

**Hinweis:**
Ab Version 18.0 können Sie den Fragebogen beantworten, um zusätzliche Informationen zu Ihrer Anforderung für den Genehmiger bereitzustellen. Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn das Kontrollkästchen **Fragebogen zum Markieren von Falschmeldungen** aktivieren im Formular „Ausnahmeverwaltungskonfiguration“ aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren Sie Exception Management für Vulnerability Response.

Ihre Anforderung wird zur Genehmigung übermittelt. Eine Nachricht zeigt an, dass die Anforderung erfolgreich übermittelt wurde. Eine falsch positive Anforderung für ein angreifbares Element oder eine Korrekturaufgabe erfordert nur einen einzigen Genehmiger.

Um den Status Ihrer Genehmigungsanforderungen im Arbeitsbereich für IT-Korrekturen anzuzeigen, klicken Sie auf der Listenseite unter Ausnahmeanforderungen auf **Meine Anforderungen**. Die Nummer für die Anforderung (VCA#) wird angezeigt, wenn Sie den VI- oder Korrekturaufgaben-Datensatz aus der Liste öffnen.

Nachdem die Anforderung genehmigt wurde, geht der Status des AE- oder Aufgabendatensatzes in „Geschlossen“ über. Aktive AEs in Aufgabendatensätzen, die als falsch positiv markiert sind, werden ebenfalls geschlossen.

Wenn die Anforderung abgelehnt wird:

- Der Status ändert sich im VI- oder Aufgabendatensatz nicht. Aktive AEs bleiben offen.
- Der Anforderungsdatensatz (VCA#) wird in der Spalte Genehmigungsstatus in Ihrer Listenansicht unter Meine Anforderungen als **Abgelehnt** angezeigt.

## Erstellen Sie eine Change-Anforderung in IT Remediation Workspace

Erstellen Sie aus einem Korrekturaufgabendatensatz eine Change-Anforderung. Alternativ können Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owneroder sn_vulc.admin

**Hinweis:**
Die itli-Rolle ist erforderlich, wenn Sie Change-Anforderungen aus IT Remediation Workspaceübermitteln möchten.

### Warum und wann dieser Vorgang ausgeführt wird

Es kann verschiedene Gründe geben, warum Sie eine Change-Anforderung für eine Korrekturaufgabe erstellen möchten. Normalerweise liegt dies daran, dass Ihre Untersuchung ein manuelles Eingreifen erfordert, um die Schwachstellen zu beheben.

Weitere Informationen zu Change-Anforderungen und zum Erstellen von Change-Anforderungen aus der klassischen Umgebung finden Sie unter Change Management für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 19.0 von Vulnerability Responsekönnen Sie Change-Anforderungen für Testergebnisgruppen (TRGs) in IT Remediation Workspaceerstellen.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Suchen Sie eine Korrekturaufgabe, für die Sie eine Change-Anforderung erstellen möchten.
3. Erweitern Sie in den UI-Aktionsschaltflächen auf der rechten Seite die Liste, und wählen Sie eine der folgenden aus:
   - Klicken **Sie auf Change erstellen**
   - **Zu vorhandenem Change hinzufügen**
4. Um eine neue Change-Anforderung zu erstellen, füllen Sie im angezeigten Dialogfeld die Felder aus. Weitere Informationen zu den Formularfeldern finden Sie unter Erstellen Sie Change Request-Formularfelder.
5. Wählen **Sie Change-Anforderung erstellen aus**.
   Der Datensatz der Korrekturaufgabe wird angezeigt, und eine Meldung weist darauf hin, dass die Change-Anforderung erfolgreich erstellt wurde.

   Klicken Sie in einem Datensatz auf den zugehörigen Link Change-Anforderungen, um alle mit dem Datensatz verknüpften Change-Anforderungen anzuzeigen.
6. Alternativ führen Sie die folgenden Schritte aus, um diese Korrekturaufgabe einer vorhandenen Change-Anforderung hinzuzufügen.
   a. Klicken Sie auf den Abwärtspfeil, um die Liste auf der Schaltfläche **Change erstellen** zu erweitern.
   b. Wählen **Sie Zu vorhandenem Change hinzufügen aus**.
   c. Klicken Sie im angezeigten Modal auf das Suchsymbol, um die Liste der vorhandenen Change-Anforderungen anzuzeigen.
   d. Um der Liste Bedingungen hinzuzufügen, um die Liste der Change-Anforderungen zu fokussieren, klicken Sie oben rechts im modalen Fenster auf das Filtersymbol (Trichter).
   e. Klicken Sie im neuen Fenster, das angezeigt wird, auf **Erweiterte Ansicht**.
   f. Verwenden Sie den Bedingungsgenerator, um Bedingungen zu erstellen.
   g. Wählen Sie **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**h.** Klicken Sie in der Liste auf eine Change-Anforderung, um sie auszuwählen.
Ein aktualisiertes Modal wird mit Ihrer Auswahl angezeigt.

**i.** **Wahlweise:** Aktivieren Sie im modalen Fenster das Kontrollkästchen CIs zu CR hinzufügen, um Konfigurationselemente aus allen aktiven angreifbaren Elementen zum Change Request hinzuzufügen.

**j.** Wählen **Sie Change hinzufügen aus**.
Der Korrekturdatensatz wird angezeigt, und eine Meldung weist darauf hin, dass die Change-Anforderung erfolgreich erstellt und zur Genehmigung übermittelt wurde.

- Klicken Sie in der Nachricht auf den Link **Change** anzeigen, um den Change Request (CHG)-Datensatz zu öffnen.
- Wählen Sie im Korrekturaufgaben-Datensatz den Menülink **Change** -Anforderungen aus, um alle mit dem Datensatz verknüpften Change-Anforderungen anzuzeigen.

Navigieren Sie alternativ in der klassischen Umgebung zu **Selfservice** > **Meine Anforderungen**. Nachdem Sie den Change gesendet und implementiert haben, wird die Korrekturaufgabe automatisch in den Status Gelöst verschoben, wenn die Statussynchronisierung aktiviert ist. Weitere Informationen zu Status und Statussynchronisierung in Change-Anforderungen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe.

### Teilen Sie eine Korrekturaufgabe in auf IT Remediation Workspace

Identifizieren Sie aus einem Korrekturaufgabendatensatz eine Teilmenge angreifbarer Elemente, und erstellen Sie eine neue Korrekturaufgabe für sie.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_changion, sn_vul_container.remediation_owner, oder sn_vulc.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können einzelne angreifbare Elemente aus der Liste auf der Registerkarte „Angreifbare Elemente“ auswählen und in eine neue Korrekturaufgabe verschieben.

Anwendungsfälle für die Aufteilung von AEs aus vorhandenen Korrekturaufgaben in neue Aufgaben können die folgenden Beispiele umfassen:

- Sie möchten eine oder mehrere Change-Anforderungen für eine Split-Gruppe erstellen.
- Sie möchten eine Split-Gruppe einem anderen Benutzer in Ihrer Zuweisungsgruppe neu zuweisen.
- Sie fordern eine Zurückstellung oder Ausnahme für eine Split-Gruppe an, da Sie wissen, dass einige Schwachstellen in bestimmten Konfigurationselementen (CIs) nicht bis zum Zieldatum behoben werden können.

Weitere Informationen zu Change-Anforderungen und zur Aufteilung einer Korrekturaufgabe in der klassischen Umgebung und für Versionen von Vulnerability Response vor v15.0 finden Sie unter Teilen Sie eine Korrekturaufgabe auf.

Ab v19.0 von Vulnerability Responsekönnen Sie Aufgaben für Testergebnisgruppen aufteilen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

Ab Version 18.0können Sie Aufgaben für angreifbare Anwendungselemente und angreifbare Containerelemente aufteilen.

### Prozedur

1. Klicken Sie bei angezeigter Korrekturaufgabe auf die Registerkarte **Angreifbare Elemente**, falls diese nicht bereits ausgewählt ist.
2. Wählen Sie in der Liste die AEs aus, die Sie in eine neue Korrekturaufgabe verschieben möchten.
3. Klicken Sie **auf Aufgabe teilen**.
4. Im angezeigten Dialogfeld wird die Anzahl der VIs angezeigt, die Sie aus der Liste ausgewählt haben.
5. Klicken Sie erneut auf **Aufgabe** teilen.
   Die folgende Bestätigungsmeldung wird mit einem Link zur neuen Korrekturaufgabe angezeigt.

   Alternativ können Sie den Bedingungsgenerator zum Filtern von AEs verwenden.
6. Suchen Sie eine Korrekturaufgabe, die Sie aufteilen möchten.
7. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Aufgabe teilen**.
   Nach einigen Minuten wird der Bedingungsgenerator angezeigt.
8. Verwenden Sie im angezeigten Modal den Bedingungsgenerator, um die Teilmenge der angreifbaren Elemente zu identifizieren, die einer neuen Korrekturaufgabe hinzufügen soll.
9. Klicken Sie **auf Aufgabe teilen**.
   Wenn eine Meldung angezeigt wird, dass keine angreifbaren Elemente Ihren Bedingungen entsprechen, müssen Sie Ihre Kriterien anpassen und erneut auf **Aufgabe** aufteilen klicken. Bearbeiten Sie das Feld „Kurzbeschreibung“ nach Bedarf. Dieses Feld kann Ihnen helfen, Ihre neue Korrekturaufgabe zu finden, nachdem sie erstellt wurde.

   Wenn AEs mit Ihren Bedingungen übereinstimmen, wird die Anzahl der übereinstimmenden AEs in einer Meldung angezeigt, wie in der vorherigen Abbildung dargestellt.
10. **Wahlweise:** Klicken Sie auf den Link **Vorschau auf Elemente** anzeigen, um die AEs anzuzeigen, die Ihren Filterbedingungen entsprechen.
    Die neue Korrekturaufgabe wird als neue Registerkarte oben im Datensatz angezeigt.

### Fordern Sie eine Ausnahme in an IT Remediation Workspace

Fordern Sie aus einem Korrekturaufgabendatensatz eine Ausnahme für eine Korrekturaufgabe an.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_changion, sn_vul_container.remediation_owner, oder sn_vulc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Oder Sie stellen fest, dass eine Korrekturaufgabe nicht bis zu ihrem Zieldatum gelöst werden kann. Wenn Ihre Korrektur nicht mit einer veröffentlichten Sicherheitsrichtlinie, einem Standard oder einer Leitlinie für Schwachstellenmanagement oder Sicherheit übereinstimmt, können Sie eine Ausnahme anfordern.

Sie können Ausnahmen für Korrekturaufgaben und angreifbare Elemente aus dem IT-Korrekturarbeitsbereich anfordern, die Ihnen zugewiesen sind.

Ab Version 19.0 von Vulnerability Responsekönnen Sie Ausnahmen für Testergebnisse von ] anfordern.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

Ab Version 18.0können Sie Ausnahmen für angreifbare Anwendungselemente und angreifbare Containerelemente anfordern.

Weitere Informationen zum Anfordern von Ausnahmen in der klassischen Umgebung finden Sie unter Fordern Sie eine Ausnahme für eine Korrekturaufgabe an.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Suchen Sie eine Korrekturaufgabe, für die Sie eine Ausnahme anfordern möchten.
3. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Ausnahme anfordern**.
4. Geben Sie im angezeigten Dialogfeld das Enddatum für die Ausnahme ein, wählen Sie einen Grund aus der Liste aus, und fügen Sie weitere erforderliche Informationen hinzu.
5. Klicken Sie **auf Ausnahme anfordern**.
6. Beantworten Sie im modalen Fenster „ **Fragebogen** ausfüllen“ die Fragen, und klicken Sie auf **Absenden**.

**Hinweis:**
Ab Version 18.0 können Sie den Fragebogen beantworten, um zusätzliche Informationen zu Ihrer Anforderung für den Genehmiger bereitzustellen. Das Modal „ **Fragebogen** ausfüllen“ wird nur angezeigt, wenn das Kontrollkästchen **Fragebogen zum Anfordern einer Ausnahme** aktivieren im Formular „ **Ausnahmeverwaltungskonfiguration“ aktiviert** ist.

Eine Nachricht zeigt an, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit einem standardmäßigen zweistufigen Genehmigungsworkflow genehmigt. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der Ebene 2 gesendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Datensatz der Korrekturaufgabe oder VI wechselt zu „Wird überprüft“, während die Ausnahmeanforderung geöffnet ist.
- Der Datensatz der Korrekturaufgabe oder VI wechselt zu „Zurückgestellt“, wenn die Anforderung genehmigt wird.
- Der Ausnahmeanforderungsdatensatz wird geschlossen, nachdem Ihre Ausnahmeanforderung genehmigt wurde.

Um den Status Ihrer Genehmigungsanforderungen anzuzeigen, klicken Sie auf der Listenseite unter Ausnahmeanforderungen auf **Meine Anforderungen**. Die Nummer für die Anforderung (VCA#) wird angezeigt, wenn Sie den VI- oder Korrekturaufgaben-Datensatz aus der Liste öffnen.

- Wenn die Anforderung abgelehnt wird, zeigt der Anforderungsdatensatz (VCA#) in der Spalte Genehmigungsstatus in Ihrer Listenansicht unter Meine Anforderungen **Abgelehnt** an.
- Sie müssen eine neue Ausnahmeanforderung senden, wenn Sie dieses Element dennoch zurückstellen möchten.

### Ausnahme mit GRC: Policy and Compliance Management in IT Remediation Workspaceanfordern

Ab Version 18.0 können Sie die Richtlinienausnahmen für angreifbare Hostelemente (AEs), Anwendungsschwachstellenelemente (AVITs), Korrekturaufgaben (VULs) und Anwendungskorrekturaufgaben (AVULs) über IT Remediation Workspaceanfordern.

## Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner, sn_vul.app_security_change, sn_vul_container.remediation_owner oder sn_vulc.admin

## Warum und wann dieser Vorgang ausgeführt wird

Ab Version 19.0 von Vulnerability Responsekönnen Sie Richtlinienausnahmen für Testergebnisgruppen (TRGs), Container-Schwachstellenelemente (CVITs) und deren Korrekturaufgaben anfordern.

**Hinweis:**
Ab v19.0 von Vulnerability Responsewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v19.0 | Terminologie v19.0 und höher |
|---|---|
| Testergebnisgruppen | Korrekturaufgaben |
| Konfigurationsprobleme | Konfigurationstestergebnisse |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**.
2. Wählen Sie im Anwendungsnavigator das Listensymbol ( ) aus.
3. Wählen Sie auf der Seite „Liste“ unter „Angreifbare Host-Elemente“, „Angreifbare Anwendungselemente“ oder „Korrekturaufgaben“ den Datensatz aus, für den Sie eine Ausnahme anfordern möchten.
   Der von Ihnen ausgewählte Datensatz muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Schaltfläche **Ausnahme anfordern**.
5. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Felder des Formulars „Ausnahme anfordern“ für Richtlinienausnahmen.
6. Wählen Sie **Ausnahme anfordern aus**.
7. Beantworten Sie im Dialogfeld „Fragebogen ausfüllen“ die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie **Absenden**aus.

**Hinweis:**
Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn die Fragebogendetails der jeweiligen Integrationsregistrierung hinzugefügt werden.

Eine Nachricht wird angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management .

### Fordern Sie eine Risikominderung in an IT Remediation Workspace

Ab v20.0 von Vulnerability Responsekönnen Sie die Reduzierung des Risikos für ein angreifbares Host-Element oder eine Korrekturaufgabe anfordern.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

### Warum und wann dieser Vorgang ausgeführt wird

Ab v21.0 von Vulnerability Response:

- Sie können eine Risikominderung für eine Korrekturaufgabe anfordern, wenn ihre angreifbaren Elemente demselben gemeinsamen Schwachstelleneintrag (CVE) oder Drittanbietereintrag (TPE) zugeordnet sind, für den die Risikominderung aktiviert ist.
- Sie können keine Risikominderung für eine Korrekturaufgabe mit angreifbaren Elementen anfordern, die verschiedenen CVEs zugeordnet sind, obwohl die Risikominderung für CVEs aktiviert ist.

**Hinweis:**
Die Funktion „Ausgleichskontrollen“ ist nur für Host-Schwachstellen verfügbar.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**.
2. Öffnen Sie auf der Seite „Liste“ ein angreifbares Host-Element oder eine Korrekturaufgabe.
3. Wählen Sie das Menü mit den drei Punkten und **dann Ausnahme anfordern**aus.
4. Füllen Sie im Popup „Ausnahme anfordern“ die Felder aus.

#### Modales Fenster „Ausnahme anfordern“.

| Feld | Beschreibung |
|---|---|
| Grund | Grund für Ihre Ausnahmeanforderung. Wählen Sie für die Risikominderungsanforderung die Option *„Mitigierende Kontrolle vorhanden“ aus*. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Informationen zum Hinzufügen neuer Grundoptionen finden Sie unter Definieren Sie die Ursachenzuordnung für Richtlinien. |
| Zurückstellungsanforderung | Differenzieren Sie den Datensatz. Dieses Feld ist standardmäßig ausgewählt.<br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn im Feld **Grund** die Option *Mitigating Control in Place* (Mitigierende Kontrolle vorhanden) ausgewählt ist. |
| Risikominderungsanforderung | Ermöglicht die Anforderung einer Reduzierung der Risikopunktzahl.<br>**Hinweis:**<br>Diese Checkbox wird nur angezeigt, wenn im Feld **Grund** die Option *Mitigating Control in Place* (Mitigierende Kontrolle vorhanden) ausgewählt ist. |
| Aktuelle Risikobewertung | Aktueller Schweregrad des Risikos.<br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Request for Risk Reduction** (Risikominderung anfordern) aktiviert ist. |
| Gewünschte Risikobewertung | Neue Risikobewertung, die Sie dem Datensatz zuweisen möchten.<br>Die höchste Risikopunktzahl in diesem Risikobewertungsbereich wird auf den Datensatz angewendet, wenn Ihre Anforderung genehmigt wird.<br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Request for Risk Reduction** (Risikominderung anfordern) aktiviert ist. |
| Wählen Sie Ausgleichskontrollen aus | Grund für Ihre Anforderung zur Reduzierung der Risikobewertung. |
| Bis | Datum, an dem die Zurückstellungs- oder Risikominderungsanforderung abläuft.<br>Wenn die Ausnahmeanforderung abläuft: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Der Datensatz wird in den Status „Offen“ zurückgesetzt.<br>○ Die Ausgleichskontrollen laufen ab.<br>○ Die berechnete Punktzahl ersetzt eine reduzierte Punktzahl. |
| Hinweise zur Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. |

5. Wählen Sie **Ausnahme anfordern aus**.
6. Beantworten Sie im Dialogfeld „Fragebogen ausfüllen“ die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie **Absenden**aus.

**Hinweis:**
Das Modal „Fragebogen beantworten“ wird nur angezeigt, wenn der Fragebogen für die Ausnahmeverwaltung aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren Sie Exception Management für Vulnerability Response.

Eine Nachricht wird angezeigt, die besagt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde. Eine Benachrichtigung über Ihre Anforderung wird an den Genehmiger gesendet.

- Wenn Sie eine Zurückstellung und Risikominderung anfordern:
  - Zwei Status-Change-Genehmigungen (VCA#) werden für Zurückstellung und Risikominderung erstellt.
  - Der Status des Datensatzes ändert sich in Wird überprüft.
- Wenn Sie nur eine Risikominderung anfordern:
  - Eine Statusänderungsgenehmigung (VCA#) wird erstellt.
  - Der Status ändert sich nicht.

Bei Genehmigung oder Ablehnung Ihrer Anforderung erhalten Sie eine Benachrichtigung.

Weitere Informationen dazu, wie das **Bis-Datum für die Risikominderung** für eine Korrekturaufgabe und ein angreifbares Element aktualisiert wird, wenn eine Risikominderungsanforderung genehmigt wird, finden Sie unter Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum.

## Nächste Maßnahme

Sie erhalten eine Benachrichtigung, wenn Ihre Anforderung vom Genehmiger genehmigt oder abgelehnt wird. Weitere Informationen zum Genehmigungsprozess finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

### Zugehörige Informationen

Grundlegendes zu Ausgleichskontrollen zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Fügen Sie der Bibliothek eine Ausgleichskontrolle hinzu

Auswirkung der Ausgleichskontrollen auf Risikopunktzahl und Ablaufdatum

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace

Vergewissern Sie sich, dass die angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie bei Bedarf erneute Scans aus IT Remediation Workspace in Ihrem Now Platform.

Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Erneutes Scannen wird für die folgenden Integrationen in IT Remediation Workspaceunterstützt. Weitere Informationen finden Sie in den folgenden Themen:

- Scannen Sie Qualys angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut
- Scannen Sie Rapid7 angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut
- Scannen Sie Tenable.io und Tenable.sc angreifbare Elemente aus den Vulnerability Response -Arbeitsbereichen erneut

Erforderliche Rollen: sn_vul.remediation_owner für IT Remediation Workspace.

### Scannen Sie Qualys angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut

Vergewissern Sie sich, dass die angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie erneute Scans im Produkt Qualys bei Bedarf aus IT Remediation Workspace in Ihrer Instanz von Now Platform.

#### Vorbereitungen

Informationen zum Initiieren eines erneuten Scans für das Produkt Qualys aus der klassischen Umgebung finden Sie unter Initiieren Sie einen erneuten Scan für Qualys Vulnerability Integration.

Die Scanner Qualys sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

So aktivieren Sie diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

Weitere Informationen zum Einrichten des Scanners Qualys finden Sie unter Richten Sie Scannergeräte ein und Erweiterte Qualys-Konfigurationen und -Änderungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die das Produkt Qualys als Quelle aus IT Remediation Workspace in Ihrem Now Platformhaben.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Qualys stammen.
- Um im IT-Korrekturarbeitsbereich erneute Scans aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen sein.

Erforderliche Rollen:

- sn_vul.remediation_owner für IT Remediation Workspace.
- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus Vulnerability Manager Workspace.

### Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   **Hinweis:**
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle mit diesem Datensatz verknüpften AEs gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
3. Wählen Sie im modalen Fenster Erneut scannen ein Optionsprofil aus.
   Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys -Scan von Ihrem Now Platform®aus initiieren. Optionsprofile enthalten Qualys Scan-Einstellungen.
4. Klicken Sie im modalen Fenster Erneut scannen auf **Erneutes Scannen anfordern**.
   Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
5. Klicken Sie in der Meldung auf den Link **Status** anzeigen, um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCAN#) wird angezeigt. Unterhalb der Datensatzkopfzeile mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:

   - In der Detailliste werden die Scan-Nummer des übergeordneten Scans, die Scanner-Quelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
   - In der Liste „Scans“ werden alle untergeordneten Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in Abgeschlossen.
   - Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens.

Alle AEs, die in den Status „Geschlossen/Korrigiert“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Qualys -Integrationen importiert.

### Scannen Sie Rapid7 angreifbare Elemente aus den Vulnerability Response Arbeitsbereichen erneut

Vergewissern Sie sich, dass die angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie erneute Scans im Produkt Rapid7 bei Bedarf aus dem IT-Fehlerkorrektur-Arbeitsbereich in Ihrer Now Platform -Instanz.

**Vorbereitungen**
Informationen zum Initiieren eines erneuten Scans für das Produkt aus der klassischen Umgebung finden Sie unter Initiieren Sie einen erneuten Scan für die Rapid7 Schwachstellenintegration. Dieses Thema enthält auch Informationen zum Planen von Scans mit den Integrationsparametern in der Integrationsinstanz Rapid7.

Die Scanner Rapid7 sind in der Anwendung Vulnerability Response standardmäßig deaktiviert. Wenn Sie versuchen, einen erneuten Scan aus den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die die Anwendung Rapid7 als Quelle haben, ist die **Schaltfläche Erneut scannen** nicht verfügbar.

So aktivieren Sie diese Scanner als Benutzer mit der Rolle sn_vul.vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt, und **Erneut scannen** ist als UI-Aktion verfügbar.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die das Produkt Rapid7 InsightVM als Quelle aus dem IT-Korrekturarbeitsbereich in Ihrem Now Platformhaben.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Rapid7 stammen.
- Um im IT-Korrekturarbeitsbereich erneute Scans aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rolle: sn_vul.remediation_owner für den Arbeitsbereich „IT-Korrektur“.

sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus Vulnerability Manager Workspace



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   **Hinweis:**
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle mit diesem Datensatz verknüpften AEs gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
3. Klicken Sie im Dialogfeld „Erneutes Scannen bestätigen“ auf Erneutes **Scannen anfordern**.
   Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
4. Klicken Sie in der Meldung auf den Link **Status** anzeigen, um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCAN#) wird angezeigt. Unterhalb der Datensatzkopfzeile mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:

   - In der Detailliste werden die Scan-Nummer des übergeordneten Scans, die Scanner-Quelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
   - In der Liste „Scans“ werden alle untergeordneten Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in Abgeschlossen.
   - Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt.

   Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens.

   Alle AEs, die in den Status „Geschlossen/Korrigiert“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Rapid7 -Integrationen importiert.

### Scannen Sie Tenable.io und Tenable.sc angreifbare Elemente aus den Vulnerability Response -Arbeitsbereichen erneut

Vergewissern Sie sich, dass die angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden. Initiieren Sie erneute Scans in den Produkten Tenable.io und Tenable.sc bei Bedarf aus dem IT-Fehlerkorrektur-Arbeitsbereich in Ihrer Now Platform -Instanz.

### Vorbereitungen

Informationen zum Initiieren eines erneuten Scans für die Produkte Tenable.io und Tenable.sc aus der klassischen Umgebung von Vulnerability Responsefinden Sie unter Initiieren Sie einen erneuten Scan für die Tenable.sc -Integration und Initiieren Sie einen erneuten Scan für die Tenable.io -Integration.

Um erneute Scans von Now Platformdurchzuführen, benötigen Sie Ihre Tenable-Anmeldeinformationen. Weitere Informationen zum Einrichten der Scanner Tenable.io und Tenable.sc und zum Importieren Ihrer Anmeldeinformationen aus Tenable finden Sie unter Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die das Produkt Tenable.io oder Tenable.sc als Quelle aus dem IT-Korrekturarbeitsbereich in Ihrem Now Platformhaben.
- In einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als **Geschlossen**befinden, und alle zugeordneten AEs müssen aus dem Produkt Tenable.io oder Tenable.sc stammen.
- Um erneute Scans in IT Remediation Workspace aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

- sn_vul.remediation_owner für IT Remediation Workspace
- sn_vul.vulnerability_analyst oder sn_vul.vulnerability_admin aus Vulnerability Manager Workspace

### Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   **Hinweis:**
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle mit diesem Datensatz verknüpften AEs gescannt.

2. Klicken Sie oben rechts in einem Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind diejenigen, die von den Scan-Anmeldeinformationsintegrationen Tenable.io und Tenable.sc importiert wurden.
3. Klicken Sie im modalen Fenster auf das Suchsymbol.

   Verwenden Sie im angezeigten modalen Fenster Scan-Anmeldeinformationen auswählen die Filter in den Spaltenüberschriften, um den Namen, die Instanz und/oder Instanzen und die Anmeldeinformationstypen auszuwählen, die Sie verwenden möchten.

   Weitere Informationen finden Sie in der folgenden Tabelle.

4. Klicken Sie im aktualisierten Dialogfeld „Erneut scannen“ auf **Erneutes Scannen anfordern**.
   Die Meldung Die Scan-Anforderung wird verarbeitet wird angezeigt.
5. Klicken Sie in der Meldung auf den Link **Status** anzeigen, um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCAN#) wird angezeigt. Unterhalb der Datensatzkopfzeile mit der Scan-Nummer zeigen die zugehörigen Elementlisten die folgenden Informationen an:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Detailliste werden die Scan-Nummer des übergeordneten Scans, die Scanner-Quelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
- In der Liste „Scans“ werden alle untergeordneten Scans und deren Status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in Abgeschlossen.
- Die Liste „Quelle“ zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt.

Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens.

Alle AEs, die in den Status „Geschlossen/Korrigiert“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.io - oder Tenable.sc -Integrationen importiert.

### IT Remediation Workspace Referenzinformationen

Die folgenden Themen enthalten Links, Referenzinformationen sowie Felddaten in den Formularen und Datensätzen in IT Remediation Workspace.

### Erstellen Sie Change Request-Formularfelder

Die folgende Tabelle zeigt die Felder und ihre Beschreibung im Formular „Change Request erstellen“.

| Feld | Beschreibung |
|---|---|
| Änderungstyp | Normal: Normal ist die Standardeinstellung.<br><br>Standard: Es werden zwei zusätzliche Felder angezeigt:<br><br>Standard-Change-Kategorie: Wählen Sie eine Kategorie aus der Liste aus<br><br>Standard-Change-Vorlage: Wählen Sie eine Vorlage aus der Auswahlliste aus, die für diese Change-Anforderung verwendet werden soll<br><br>Notfall – Priorität „Kritisch“. |
| CIs zu Change-Anforderung hinzufügen | Standardmäßig aktiviert. Wenn diese Option aktiviert ist, fügt die Change-Anforderung alle Konfigurationselemente (CIs) hinzu, die zu aktiven angreifbaren Elementen in dieser Korrekturmaßnahme gehören. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Priorität | Hoch ist die Standardeinstellung. Wählen Sie eine Priorität aus der Liste aus. |
| Zuweisungsgruppe | Die Zuweisungsgruppe wird standardmäßig aus dem Überwachungsthema übernommen. Klicken Sie auf das Suchsymbol, und wählen Sie im modalen Fenster eine andere Zuweisungsgruppe aus. |
| Geplantes Enddatum | Klicken Sie auf das Kalendersymbol, um ein geplantes Enddatum auszuwählen. |
| Zugewiesen an | Der aktuelle Benutzer ist standardmäßig der Korrekturaufgabe zugewiesen. Klicken Sie auf das Suchsymbol, und wählen Sie im modalen Fenster einen anderen Benutzer aus. |
| Kurzbeschreibung | Die Kurzbeschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten. |
| Beschreibung | Die Beschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten. |
| Begründung | Begründung aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten. |
| Implementierungsplan | Vorausgefüllt mit Informationen zur bevorzugten Lösung, falls verfügbar. Zeigen Sie die Lösung an, oder geben Sie einen Begründungsplan ein. |

**Zugehörige Informationen**

Erstellen Sie eine Change-Anforderung in IT Remediation Workspace

### Felder des Formulars „Ausnahme anfordern“ für Richtlinienausnahmen

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Richtlinienausnahmen ausfüllen müssen.

#### Formular „Ausnahme anfordern“.

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |
| Kontrollziel | Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und sich der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ ändert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Ausnahme anfordern“. (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in Policy and Compliance festgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen. |
| Grund | Grund für die Anforderung einer Ausnahme. |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden. |

**Zugehörige Informationen**

Ausnahme mit GRC: Policy and Compliance Management in IT Remediation Workspaceanfordern

### Felder des Ausnahmeformulars für Risikominderung anfordern

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Risikominderungsanforderungen ausfüllen müssen.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Grund | Grund für Ihre Ausnahmeanforderung. Wählen Sie für die Risikominderungsanforderung die Option *„Mitigierende Kontrolle vorhanden“ aus*.<br><br>Informationen zum Hinzufügen neuer Grundoptionen finden Sie unter Definieren Sie die Ursachenzuordnung für Richtlinien. |
| Zurückstellungsanforderung | Differenzieren Sie den Datensatz. Dieses Feld ist standardmäßig ausgewählt.<br><br>**Hinweis:** Dieses Feld wird nur angezeigt, wenn im Feld **Grund** die Option *Mitigating Control in Place* (Mitigierende Kontrolle vorhanden) ausgewählt ist. |
| Risikominderungsanforderung | Ermöglicht die Anforderung einer Reduzierung der Risikopunktzahl. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Ausnahme anfordern“. (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Diese Checkbox wird nur angezeigt, wenn im Feld **Grund** die Option *Mitigating Control in Place* (Mitigierende Kontrolle vorhanden) ausgewählt ist. |
| Aktuelle Risikobewertung | Aktueller Schweregrad des Risikos.<br>**Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Request for Risk Reduction** (Risikominderung anfordern) aktiviert ist. |
| Gewünschte Risikobewertung | Neue Risikobewertung, die Sie dem Datensatz zuweisen möchten.<br>Die höchste Risikopunktzahl in diesem Risikobewertungsbereich wird auf den Datensatz angewendet, wenn Ihre Anforderung genehmigt wird.<br>**Hinweis:** Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Request for Risk Reduction** (Risikominderung anfordern) aktiviert ist. |
| Wählen Sie Ausgleichskontrollen aus | Grund für Ihre Anforderung zur Reduzierung der Risikobewertung. |
| Bis | Datum, an dem die Zurückstellungs- oder Risikominderungsanforderung abläuft.<br>Wenn die Ausnahmeanforderung abläuft:<br>• Der Datensatz wird in den Status „Offen“ zurückgesetzt.<br>• Die Ausgleichskontrollen laufen ab.<br>• Die berechnete Punktzahl ersetzt eine reduzierte Punktzahl. |
| Hinweise zur Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. |

## Erkunden Sie den Arbeitsbereich „Schwachstellenbewertung“.

Der Arbeitsbereich für Schwachstellenbewertungen wurde für den Manager von Schwachstellenereignissen entwickelt, um eine Gefährdungsbewertung durchzuführen und kritische Schwachstellen-Ereignisse proaktiv zu verwalten, insbesondere während der kritischen Schwachstellen-Ereignisse wie Zero-Day-Ereignisse.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem eine kritische Schwachstelle identifiziert wurde, können Schwachstellen-Event-Manager die potenziellen Auswirkungen und Risiken im Zusammenhang mit der Schwachstelle bewerten. Die Analysten können die betroffenen Systeme, Anwendungen oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

Der Arbeitsbereich „Schwachstellenbewertung“ enthält:

**Seite „Risikobewertung“**

Bietet detaillierten Einblick in die Assets, die Schwachstellen ausgesetzt sind, und angreifbare Software. Die Risikobewertungsfunktion bietet Folgendes:

- Transparenz in Bezug auf betroffene Assets für Schwachstelle und betroffene Software
- Möglichkeit, eigenständige Bewertungen für ein einzelnes CVE oder angreifbare Software durchzuführen
- Transparenz in Bezug auf betroffene Assets für CVEs mit bekannter Ausnutzung von CISA-Schwachstellen
- Transparenz des Risikos durch zusätzliches Discovery-Modell und zusätzliche Assets.
- Möglichkeit zum Erstellen angreifbarer Elemente

**Seite „Schwachstellenbewertung“**

Die Seite „Schwachstellenbewertung“, auf der Sie Schwachstellen-Krisen-Ereignisse von der Bewertung bis zur Lösung mithilfe des Schwachstellen-Krisenmanagement-Workflows behandeln können. Mit dem Workflow können Sie relevante Schwachstellen-Ereignisse nachverfolgen, das damit verbundene Risiko analysieren, eine Gefährdungsbewertung für mehrere Bestände durchführen (z. B. Softwareinstallationsbestand) und sie als Krise für ein erhöhtes Reaktionsengagement deklarieren. Anschließend können Sie den Schwachstellenbewertungsdatensatz einem schwerwiegenden Security Incident zuordnen und das Security Incident Response Team in die Lage versetzen, auf die Krise zu reagieren.

- Erstellen und ändern Sie Schwachstellenbewertungen für kritische Schwachstellenereignisse
- Erfassen Sie Schlüsselattribute der Schwachstelle, um das Risiko zu berechnen
- Führen Sie eine Schwachstellenbewertung durch, um das Risikoniveau und die Priorität zu bestimmen
- Deklarieren Sie die Schwachstellenbewertung als kritisches Ereignis
- Ordnen Sie die Schwachstellenbewertung einem schwerwiegenden Security Incident zu, indem Sie die Schwachstellenbewertung mit einem schwerwiegenden Security Incident verknüpfen, vorschlagen oder heraufstufen.

**Listen-Seite**

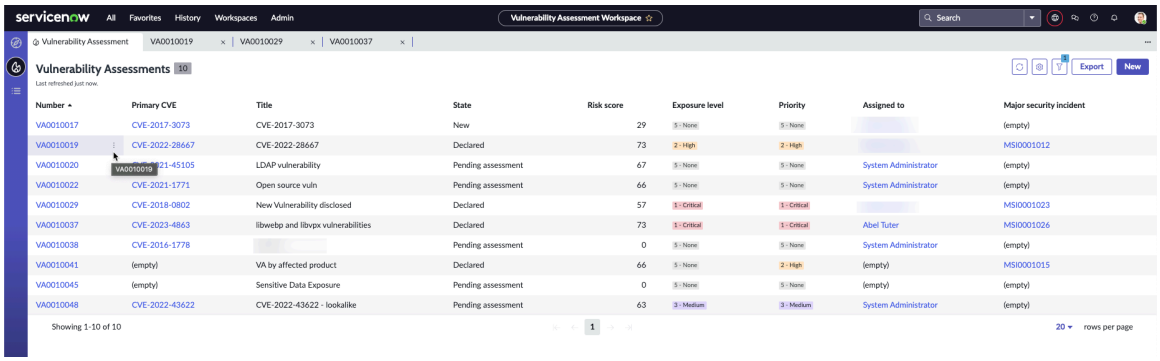
Die Listenseite umfasst eine Bibliothek mit:

- CVEs
- TPEs
- CWEs

Die folgende Abbildung zeigt die Homepage des Schwachstellenbewertungs-Arbeitsbereichs.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Risikobewertung erkunden

Die Risikobewertung verwendet das CPE-Framework (Common Platform Enumeration), das Teil des CVEs-Systems (Common Vulnerabilities and Exposures) ist, um das Schwachstellenrisiko Ihrer Assets durch Schwachstellensoftware zu bewerten. Diese Bewertung wird mithilfe eines Software-Discovery-Modells durchgeführt.

Durch die Verwendung eines Übereinstimmungsalgorithmus werden die relevanten CPEs zugeordnet und dem Software-Discovery-Modell zugeordnet, wodurch potenzielle Gefährdungen identifiziert werden können.

Sie können die Risikobewertung nach CVE oder Software verwenden, um das Risiko potenzieller Schwachstellen für die folgenden Szenarien zu identifizieren:

- Schwachstellen, die von herkömmlichen Scannern möglicherweise nicht erkannt werden
- Zero-Day-Schwachstellen, bevor der Scanner die Signatur für die Schwachstellenerkennung bereitstellt

Die Risikobewertung bietet eine Frühwarnung, um diese Schwachstellen zu beheben und die Reife des Schwachstellenmanagementprogramms zu verbessern.

Voraussetzungen für Risikobewertung

### Verfügbare Versionen

| Anwendung | Version |
|---|---|
| Plugin „Vulnerability Emergency Response“ (sn_vul_analyst). | 2.0 |
| Vulnerability Response | 20.0 |
| Vulnerability Response mit NVD | 1.3 |
| Vulnerability Response integration with CISA | 1,2 |
| Vulnerability Response Integration with NVD<br>**Hinweis:**<br>Weitere Informationen finden Sie unter Grundlegendes zu den NVD-Integrationen. | 1.3 |
| Software Asset Management | Software Asset Management Foundation-Plugin - oder Software Asset Management Professional -Plugin |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Kompatibilität und Systemanforderungen

Die Anwendung Vulnerability Response ist auf der ServiceNow Storeverfügbar. Die Anwendung ITSM Software Asset Management (com.snc.asset_management) ist für das Risikobewertungsmodul erforderlich. Diese Anwendung verwaltet alle Ihre Assets und Softwarelizenzen, und die Version SAM Foundation dieser Anwendung ist Teil der Anwendung Vulnerability Response, die Sie aus dem ServiceNow Storeherunterladen.

**Wichtig:**
Die Anwendung „Risikobewertung“ funktioniert mit den folgenden Plugins:

- Software Asset Management Foundation-Plugin (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Software Asset Management-Plugin (com.snc.software_asset_management)

Um sicherzustellen, dass die Anwendung SAM Foundation in Ihrer Instanz installiert ist, navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach com.snc.asset_management. Wenn die Anwendung nicht installiert ist, wählen **Sie Installieren**aus. Da die Anwendung „Risikobewertung“ Zugriff auf die Asset-Daten in Ihrer Instanz Now Platform® erfordert, müssen die Asset-Management-Anwendungen über Daten verfügen, auf die verwiesen werden kann. Die Tabelle „Software-Discovery-Modelle“ (cmdb_sam_sw_discovery_model) und die Softwareinstallationen (cmdb_sam_sw_install) erfordern Daten.

## Übereinstimmende Algorithmusfelder für Software-Discovery-Modelle

Mit der Anwendung Software Asset Management Professional können Sie ein Software-Discovery-Modell bearbeiten, um erkannte Software, die nicht vollständig normalisiert wurde (teilweise normalisiert, Herausgeber normalisiert oder Übereinstimmung nicht gefunden), manuell im Formular „Software-Discovery-Modelle“ zu normalisieren, damit sie abgeglichen werden kann. Ab Version 20.0 von Vulnerability Response wird das normalisierte Discovery-Modell unterstützt, das von Software Asset Management Professionalstammt. Die folgenden Felder werden für den Übereinstimmungsalgorithmus für Software-Discovery-Modelle verwendet.

| CPE (Softwaremodell) | SAM-Grundlagen | SAM Professional |
|---|---|---|
| Lieferant | Primärer Schlüssel | Primärer Schlüssel |
| Produkt | Anzeigename | Anzeigename |
| Version | Erkannter Herausgeber | Erkannter Herausgeber |
| Edition | Erkanntes Produkt | Erkanntes Produkt |
| | Erkannte Version | Erkannte Version |
| | | Normalisierter Herausgeber |
| | | Normalisiertes Produkt |
| | | Normalisierte Version |

**Hinweis:**
Die Anwendung SAM Professional ist nicht Teil des Kernprodukts Vulnerability Response von ServiceNow Store und erfordert ein separates Abonnement.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Systemeigenschaft

Um die von CISA ausgenutzten Schwachstellen automatisch für die Gefährdungsbewertung zu verarbeiten, legen Sie die Systemeigenschaft *sn_vul_analyst.enable_exposure_for_cisa* auf *true*fest. Der Standardwert ist *false*.

## Geplante Aufgaben

Im Folgenden finden Sie die geplanten Aufgaben.

| Name der geplanten Aufgabe | Beschreibung |
|---|---|
| Überprüfen Sie das potenzielle Schwachstellenrisiko | Verarbeitet die Delta-CVEs, -Software und -Installationen, um das Risiko zu erhalten.<br>**Hinweis:** Diese regelmäßige Aufgabe wird alle 12 Stunden ausgeführt. Sie wird über einen längeren Zeitraum ausgeführt als die anderen regelmäßigen Aufgaben. |
| Fügen Sie das von CISA ausgenutzte CVE in die Konfiguration für das Risiko ein | Bei Bedarf. Fügt die CISA-CVEs in die Tabelle „Risikokonfiguration“ ein, um das Risiko zu berechnen. |
| Führen Sie eine Gefährdungsbewertung für konfigurierte CVEs aus | Bei Bedarf. Berechnet das Risiko für alle CVE-Datensätze in der Tabelle „Risikokonfiguration“. |
| Führen Sie Software-Gefahrenpotenzial aus | Bei Bedarf. Berechnet das Risiko für alle Softwaredatensätze in der Tabelle „Risikokonfiguration“. |

## Wichtige Begriffe

- **Konfidenzpunktzahl:** Eine Konfidenzpunktzahl ist ein Maß für die Zuverlässigkeit bei der Bereitstellung einer Empfehlung für ein Feld. Je höher die Punktzahl, desto zuverlässiger die Empfehlung. Beispielberechnungen finden Sie unter Beispiel für die Berechnung der Vertrauenspunktzahl.
- **Softwareinstallationsanzahl:** Anzahl der von der Schwachstelle betroffenen Software-Assets.
- **Softwaremodell:** Softwaremodell, das dem Produkt zugeordnet ist. Zeigen Sie Detailinformationen für das Softwaremodell an, um das Ergebnis des Softwaremodells anzuzeigen. Weitere Informationen finden Sie unter Software Asset Management Foundation plugin discovery models and software installations .

### Risikobewertung nach CVE

Bei der Risikobewertung werden häufige Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVEs) verwendet, um das Risiko Ihrer Assets mithilfe des Software-Discovery-Modells zu bewerten. Sie können die Gefährdungsbewertung nach CVE verwenden, um das Risiko potenzieller Schwachstellen zu identifizieren.

Informationen zur Bewertung des Risikos nach CVE finden Sie unter:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie CVEs hinzu, um das Risiko zu bewerten
- Erstellen Sie VIs für CVEs für die Risikobewertung
- Aktivieren oder deaktivieren Sie CVEs für die Risikobewertung
- Exportieren Sie betroffene CIs für die Risikobewertung
- Beispiel für die Berechnung der Vertrauenspunktzahl


### Fügen Sie CVEs hinzu, um das Risiko zu bewerten

Fügen Sie der Gefährdungskonfigurationsliste von CVEs in der Risikobewertung gängige Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVEs) hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie **Hinzufügen**.
3. Wählen Sie im Dialogfeld „CVE hinzufügen“ die CVEs aus, die Sie der Liste hinzufügen möchten, und klicken Sie auf die Option **Hinzufügen**.
   CVEs, die sich bereits in der Liste befinden, werden nicht erneut hinzugefügt. Die restlichen werden der Liste der CVEs hinzugefügt.

**Hinweis:**
Klicken Sie auf das Filtersymbol, um zur **erweiterten Ansicht** zu navigieren, und geben Sie die CVEs an, die Sie anzeigen möchten.

### Erstellen Sie VIs für CVEs für die Risikobewertung

Erstellen Sie angreifbare Elemente (AEs) auf der Seite „Risikobewertung“. Schwachstellen-Event-Manager analysieren dann diese Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu beheben.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Warum und wann dieser Vorgang ausgeführt wird

Nachdem das Risiko bewertet wurde, wird die Liste für die potenzielle Bewertung im Datensatz der Risikobewertung mit der Anzahl der Konfigurationselemente (CIs) angezeigt. Sie können die Datensätze auswählen und in der **Listenaktion** Angreifbare Elemente erstellen auswählen, um angreifbare Elemente (AEs) für die CIs zu erstellen, in denen die angreifbare Software vorhanden ist, und für die allgemeinen Schwachstellen und Gefährdungen (CVEs). AEs werden im Hintergrund erstellt. Dieser Prozess kann einige Zeit dauern. Nachdem die Elemente erstellt wurden, können Sie zur VI-Tabelle navigieren, um die erstellten Datensätze anzuzeigen.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie die erforderlichen CVEs aus, und wählen Sie die Option Angreifbare Elemente **erstellen** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Dialogfeld „ **Angreifbare Elemente erstellen“ die Option Angreifbare Elemente erstellen** aus.
4. Klicken Sie auf den Link **Status** anzeigen, um den Status des Hintergrundauftrags anzuzeigen, der zum Erstellen der AEs verwendet wird.

### Aktivieren oder deaktivieren Sie CVEs für die Risikobewertung

Für die Delta-Verarbeitung eines CVE können Sie es aktivieren und es so der aktiven Liste der CVEs hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie die erforderlichen aktiven CVEs aus, und wählen Sie die Option **Deaktivieren** aus.
   Die CVEs sind deaktiviert.

   **Hinweis:**
   Um Software zu aktivieren, führen Sie denselben Vorgang durch und wählen die Option **Aktivieren** aus.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte Aktiv anzuzeigen.

### Exportieren Sie betroffene CIs für die Risikobewertung

Sie können die Liste der betroffenen Assets für ein neues CVE nachverfolgen, indem Sie die Konfigurationselemente (CIs), die sich auf einen Risikobewertungsdatensatz beziehen, in eine Excel-Tabelle exportieren. Dieses Blatt kann verwendet werden, um die Asset-Details und -Besitzer freizugeben, um Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte Softwareinstallationen enthält die aktiven CIs, die sich auf den Softwaredatensatz beziehen. Diese CIs werden in der Spalte **Installiert auf** gespeichert.
3. Wählen Sie die Option **Exportieren** aus.
4. Wählen Sie im Dialogfeld „Exportieren“ den Dateityp und den Bereitstellungstyp aus, um die zugehörigen CIs zu exportieren.
5. Wählen Sie die Option **Exportieren** aus.

### Beispiel für die Berechnung der Vertrauenspunktzahl

Beispiel für die Berechnung der Konfidenz für eine Zero-Day-Schwachstelle basierend auf den Informationen zu Common Vulnerabilities and Exposures (CVE).

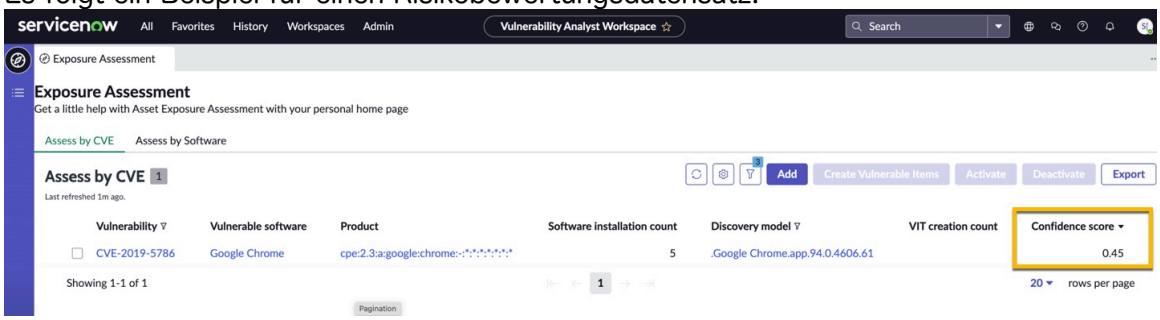


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

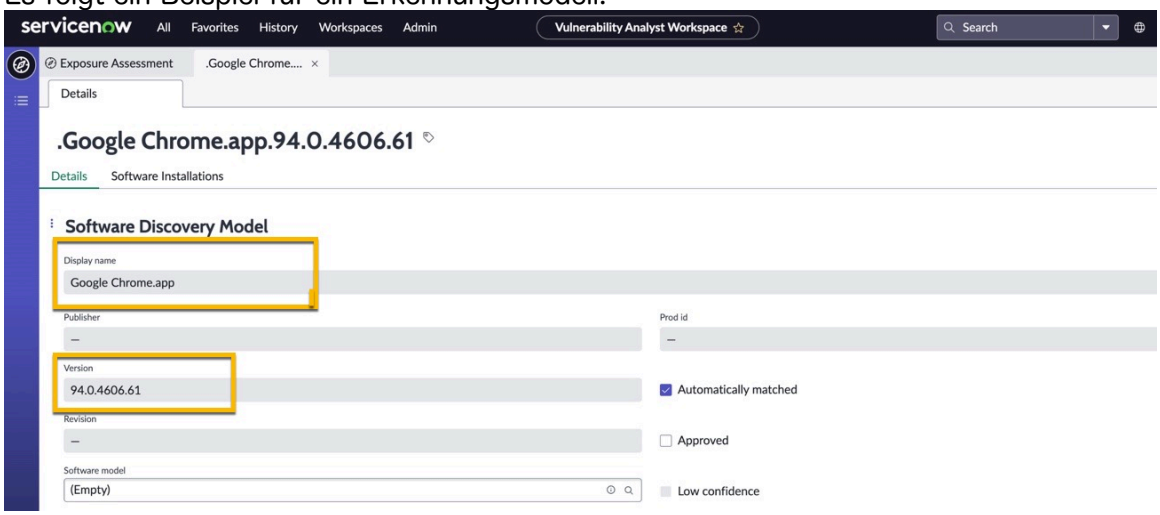
Im Folgenden finden Sie ein Beispiel für die Berechnung der Konfidenzpunktzahl aus den Informationen der Common Platform Enumeration (CPE) von **CVE-2019-5786**.

**Hinweis:**
Um die CPEs anzuzeigen, können Sie die Spalte Schwachstelle nach Schwachstelle gruppieren. Weitere Informationen zum Anzeigen der Details zu angreifbarer Software finden Sie unter Zeigen Sie Details zu angreifbarer Software an.

Es folgt ein Beispiel für einen Risikobewertungsdatensatz:




Es folgt ein Beispiel für ein Erkennungsmodell:




### So berechnen Sie die Konfidenzpunktzahl

Der Konfidenzpunktzahlbereich liegt zwischen 0 und 1. Basierend auf den CPE-Informationen wird die Konfidenzpunktzahl anhand der folgenden Formel berechnet:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) +
 (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

```
.45
```

**Hinweis:**
Informationen zu den zur Berechnung der Konfidenzpunktzahl verwendeten Werten finden Sie unter Referenztabellen der Vertrauensbewertung für die Risikobewertung.

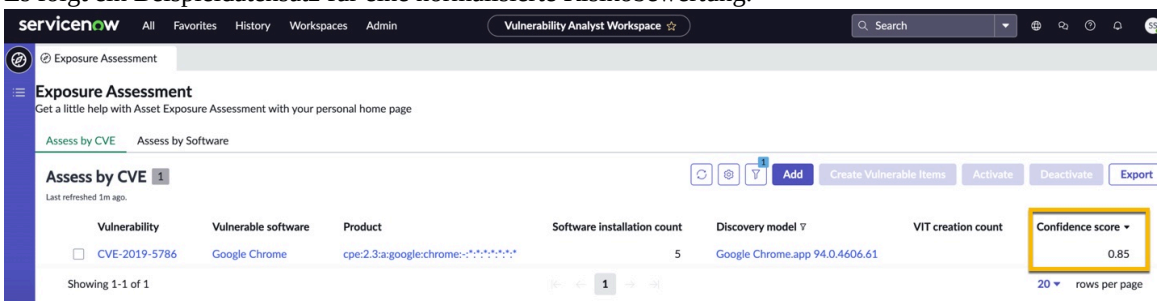
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

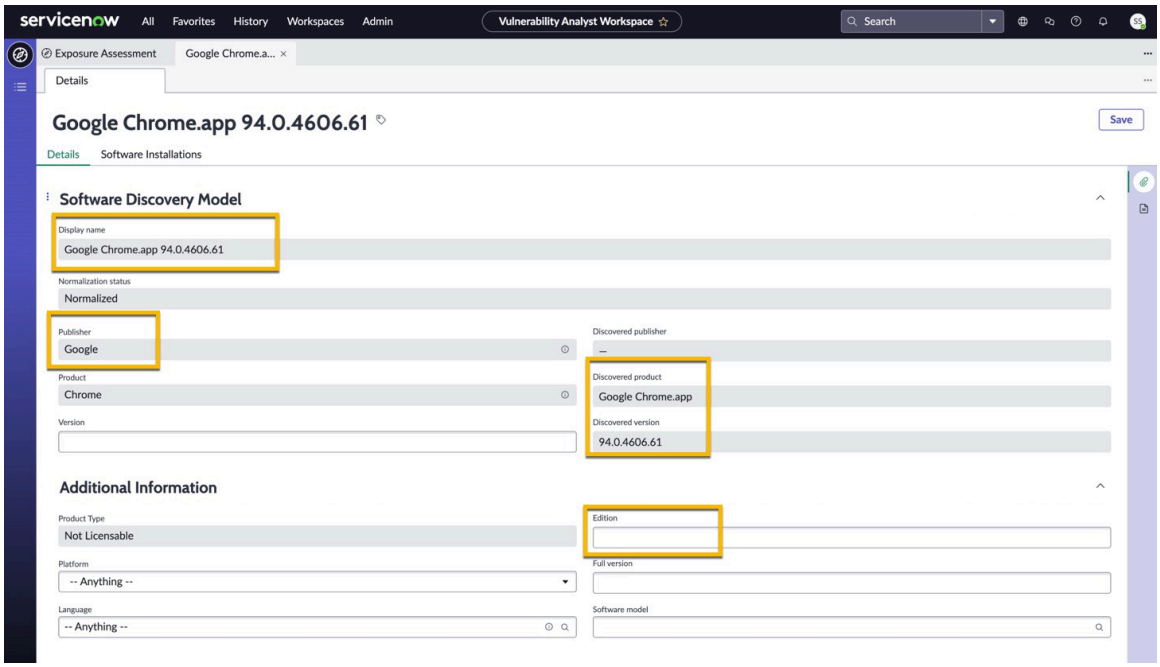
### Berechnung der Konfidenzpunktzahl, wenn das Softwaremodell mit dem normalisierten Discovery-Modell abgeglichen wird

Wenn Sie das normalisierte Discovery-Modell verwenden, bieten die zusätzlichen Informationen, die für das Software-Discovery-Modell verfügbar sind, eine verbesserte Konfidenzpunktzahl. Im Folgenden finden Sie die Beispielberechnung:

Es folgt ein Beispieldatensatz für eine normalisierte Risikobewertung.




Es folgt ein Beispiel für ein normalisiertes Erkennungsmodell.




((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100

=

((25) + (15) + (15) + (15) + (15) + (10)) / 100

=

85 / 100

=

.85

**Hinweis:**
Informationen zu den zur Berechnung der Konfidenzpunktzahl verwendeten Werten finden Sie unter Referenztabellen der Vertrauensbewertung für die Risikobewertung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie Details zu angreifbarer Software an

Zeigen Sie die Details der angreifbaren Software an, in diesem Fall Google Chrome. Sie wird mit dem Discovery-Modell und der Common Platform Enumeration (CPE) abgeglichen. Diese CPE-Version wirkt sich auf alle Google Chrome-Versionen aus.

#### Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren Sie zu **Alle**, und geben Sie *sn_vul_software.LIST*ein.
2. Suchen Sie in der Liste der angreifbaren Software nach **cpe:2.3:a:google:Chrome:-:*:*:*:*:*:*:***, um die Informationen anzuzeigen.

### Referenztabellen der Vertrauensbewertung für die Risikobewertung

Referenzwerte, die zur Berechnung der Konfidenzpunktzahl verwendet werden.

## Referenztabellen

### Referenztabelle für die Berechnung der Vertrauensbewertung

| Segment der angreifbaren Software | Discovery-Modellsegment | Punktzahl | Discovery-Modell – Segment „Genaue Übereinstimmung“. | Punktzahl für exakte Übereinstimmung |
|---|---|---|---|---|
| Herausgeber | Anzeigename | 15 | Herausgeber | 5 |
| Modell | Anzeigename | 15 | Modell | 5 |
| Version | Anzeigename | 10 | Version | 5 |
| Anzeigename | Anzeigename | 10 | Anzeigename | 5 |

### Zusammenfassungstabelle der Vertrauensbewertung

| Punktzahl | Wert |
|---|---|
| Summe aller Punktzahlen | 75 |
| Basispunktzahl<br>**Hinweis:**<br>Mindestpunktzahl für alle übereinstimmenden Discovery-Modelle. | 25 |
| Gesamtpunktzahl | 100 |

### Risikobewertung durch Software

Risikobewertung für Zero-Day-Schwachstellen, wenn Common Vulnerabilities and Exposures (CVEs) für das Asset oder Konfigurationselement nicht verfügbar ist. Sie verwendet die Softwareinformationen, um das Risiko mithilfe des Software-Discovery-Modells zu bewerten.

Informationen zur Bewertung des Gefahrenpotenzials nach Software finden Sie unter:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie Software für die Risikobewertung hinzu
- Erstellen Sie AEs für Software zur Risikobewertung
- Aktivieren oder deaktivieren Sie Software für die Risikobewertung
- Exportieren Sie betroffene CIs für Software im Arbeitsbereich „Schwachstellenbewertung“.

### Fügen Sie Software für die Risikobewertung hinzu

Fügen Sie dem Modul „Risikobewertung“ neue Software hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten** > **Hinzufügen**.
2. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Herausgeber | Herausgeber der Software. |
| Produkt | Produktname der Software. |
| Version | Version des Softwareprodukts. |
| Edition | Edition der Software. |

**Hinweis:**
Wenn Sie versuchen, ein Risiko für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

3. Wählen Sie die Option **Hinzufügen** aus.

### Erstellen Sie AEs für Software zur Risikobewertung

Erstellen Sie angreifbare Elemente (AEs) auf der Seite „Risikobewertung“. Schwachstellen-Event-Manager analysieren dann diese Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu beheben.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Wählen Sie die Datensätze aus, für die Sie VIs erstellen möchten.
3. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.
4. Wählen Sie im Dialogfeld „Angreifbare Elemente erstellen“ aus:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vorhandene Schwachstelle
- Neue Schwachstelle

5. Wählen Sie die Option **Angreifbare Elemente erstellen aus**.

### Aktivieren oder deaktivieren Sie Software für die Risikobewertung

Um die weitere Delta-Verarbeitung von Software zu stoppen, können Sie sie deaktivieren und sie so aus der aktiven Liste der Software entfernen.

**Vorbereitungen**
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Zum Deaktivieren wählen Sie die erforderliche aktive Software und dann die Option **Deaktivieren** aus.
   Die Software ist deaktiviert.

   **Hinweis:**
   Um Software zu aktivieren, führen Sie denselben Vorgang durch und wählen die Option **Aktivieren** aus.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte Aktiv anzuzeigen.

### Exportieren Sie betroffene CIs für Software im Arbeitsbereich „Schwachstellenbewertung“.

Sie können die Liste der betroffenen Assets für neue Software nachverfolgen, indem Sie die Konfigurationselemente (CIs), die sich auf einen Risikobewertungsdatensatz beziehen, in eine Excel-Tabelle exportieren. Dieses Blatt kann verwendet werden, um die Asset-Details und -Besitzer freizugeben, um Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

**Vorbereitungen**
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

**Prozedur**

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte Softwareinstallationen enthält die aktiven CIs, die sich auf den Softwaredatensatz beziehen. Diese CIs werden in der Spalte **Installiert auf** gespeichert.
3. Wählen Sie die Option **Exportieren** aus.
4. Wählen Sie im Dialogfeld „Exportieren“ den Dateityp und den **Bereitstellungstyp** aus, um die zugehörigen **CIs** zu exportieren.
5. Wählen Sie die Option **Exportieren** aus.

### Erkunden der Schwachstellenbewertung

Der Arbeitsbereich für Schwachstellenbewertungen wurde für den Manager von Schwachstellenereignissen entwickelt, um ein Schwachstellenereignis zu erstellen und eine Schwachstellenbewertung durchzuführen, insbesondere während der Zero-Day-Schwachstellenanalyse.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können den Arbeitsbereich für Schwachstellenbewertungen verwenden, um kritische Schwachstellen zu verwalten, z. B.:

- Zero-Day-Schwachstellen mit Schweregrad „Kritisch“ oder „Hoch“.
- Neue Bedrohungsinformationen für eine Schwachstelle identifiziert
- Schnelle Ausnutzung einer Schwachstelle mit Schweregrad „Kritisch“ oder „Hoch“.

## Arbeitsbereich für Schwachstellenbewertung und Vulnerability Crisis Management

Identifizieren und erstellen Sie als Schwachstellen-Event-Manager einen Schwachstellen-Event-Datensatz für relevante Schwachstellen. Sobald Sie das angreifbare Ereignis erstellt haben, können Sie eine Risikobewertung durchführen, die Risikoattribute manuell aktualisieren und die Risikopunktzahl automatisch berechnen. Mit dem Schwachstellenbewertungs-Arbeitsbereich können Sie die folgenden Aktionen ausführen, um Schwachstellen-Krisenereignisse von der Einführung bis zur Lösung zu behandeln.

- Erstellen Sie einen Schwachstellenbewertungsdatensatz
- Ändern Sie den Datensatz der Schwachstellenbewertung
- Führen Sie eine Schwachstellenbewertung durch
- Überprüfen Sie die Bewertungsdetails
- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

## Voraussetzungen für die Schwachstellenbewertung

### Verfügbare Versionen

| Anwendung | Version |
|---|---|
| Plugin „Vulnerability Emergency Response“ (sn_vul_analyst). | 2.0 |
| Vulnerability Response | 20.0 |
| Vulnerability Response mit NVD<br>**Hinweis:**<br>Weitere Informationen finden Sie unter Grundlegendes zu den NVD-Integrationen. | 1.4.2 |
| Vulnerability Response integration with CISA | 1,2 |
| Datenmodell für SBOM | 1.1.2 |
| Software Bill of Materials Zentral | 2.0.2 |
| Software Asset Management | Software Asset Management Foundation-Plugin - oder Software Asset Management Professional -Plugin |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Verfügbare Versionen (Fortsetzung)

| Anwendung | Version |
|---|---|
| Management schwerwiegender Sicherheits-Incidents | 2.2.5 |

## Geplante Aufgaben

Im Folgenden sind die geplanten Aufgaben aufgeführt.

| Name der geplanten Aufgabe | Beschreibung |
|---|---|
| Schwachstellenbewertung | Aktualisiert die Tabelle der betroffenen Konfigurationselemente und die Quelle des CI, wenn angreifbare Elemente (VITs oder AVITs) nach der Bewertung erstellt werden.<br>**Hinweis:**<br>Diese planmäßige Aufgabe wird täglich ausgeführt. Sie wird über einen längeren Zeitraum ausgeführt als die anderen regelmäßigen Aufgaben. |

**Zugehörige Informationen**

Schwachstellen-Krisenmanagement

### Erstellen Sie einen Schwachstellenbewertungsdatensatz

Erstellen Sie Bewertungsdatensätze für relevante Schwachstellen. Nachdem Sie die Bewertung erstellt haben, können Sie die erste Risikobewertung initiieren, den Datensatz manuell aktualisieren und die Risikopunktzahl automatisch berechnen.

#### Vorbereitungen

Sie müssen Teil der Zuweisungsgruppe „Ereignismanager für Schwachstellenbewertung“ im Basissystem sein, um die mit der Schwachstellenbewertung verbundenen Aufgaben ausführen zu können. Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Schwachstellenbewertungsdatensatz für relevante Schwachstellen erstellen, indem Sie den Event-Datensatz entweder einem primären CVE oder einem betroffenen Produkt zuordnen.

#### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Klicken Sie auf das Symbol **Schwachstellenbewertung**.
3. Wählen Sie **Neu**.
4. Geben Sie einen geeigneten Titel in das Feld **Titel** ein.
5. **Wahlweise:** Wählen Sie im Feld **Primäres** CVE ein primäres CVE aus, das dem neuen Bewertungsdatensatz zugeordnet werden soll.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Alle vorläufigen Details im Bewertungsdatensatz werden basierend auf dem von Ihnen ausgewählten oder erstellten Produkt oder dem primären CVE, das Sie dem Datensatz zuordnen, ausgefüllt.

6. Wählen Sie **Absenden**.
Der Schwachstellenbewertungsdatensatz mit dem von Ihnen eingegebenen Titel wird erstellt und auf einer neuen Registerkarte „Schwachstellenbewertung“ angezeigt. Standardmäßig wird der Schwachstellenbewertungsdatensatz auf der Registerkarte **Details** angezeigt.

**Hinweis:**
Standardmäßig werden die Details des zugeordneten/zugeordneten primären CVE angezeigt.

- Wenn während der Erstellung des Schwachstellenbewertungs-Ereignisdatensatzes kein primäres CVE ausgewählt wird, wird ein Standarddatensatz erstellt.
- Wenn dem primären CVE CVEs zugeordnet sind, werden die zugehörigen CVEs auf der Registerkarte „ **Schwachstelleneinträge** “ ausgefüllt. Sie können weitere zugeordnete CVEs über die Registerkarte „ **Schwachstelleneinträge** “ hinzufügen.

7. Navigieren Sie zur Registerkarte **Betroffene Produkte**.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Herausgeber | Herausgeber der Software.<br>Das ist ein Pflichtfeld. |
| Produkt | Produktname der Software.<br>Das ist ein Pflichtfeld. |
| Version | Version des Softwareprodukts. |
| Edition | Edition der Software. |

**Hinweis:**
Wenn Sie versuchen, eine Schwachstelle für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

c. Wählen Sie **OK**.

8. Wählen Sie **Speichern**.

### Aktualisieren Sie den Auto-Flush-Datensatz der Schwachstellenbewertung

Aktualisieren Sie den Auto-Flush-Datensatz der Schwachstellenbewertung.

**Vorbereitungen**
Erforderliche Rolle: sn_vul_analyst.vul_event_manager



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem ist die Aufbewahrungsdauer für Schwachstellenbewertungsdatensätze auf 6 Monate festgelegt. Wenn der Status eines Schwachstellenbewertungsdatensatzes geschlossen ist, werden die Schwachstellenbewertungsdatensätze nur bis zum festgelegten Aufbewahrungszeitraum gespeichert. Die zugehörigen Datensätze dieser Bewertung werden nach 6 Monaten aus allen zugehörigen Tabellen entfernt.

### Prozedur

1. Navigieren zu **Alle** > **Automatisch entleeren**.
2. Öffnen Sie den Datensatz mit der Tabelle sn_vul_analyst_vulnerability_assessment.
3. Aktivieren Sie die Checkbox **Aktiv**, um die Option zum automatischen Leeren für den Schwachstellenbewertungsdatensatz zu aktivieren.
4. Klicken Sie auf **Aktualisieren**.

## Ändern Sie den Datensatz der Schwachstellenbewertung

Aktualisieren Sie den Schwachstellenbewertungsdatensatz nach seiner Erstellung. Basierend auf den Werten des Felds können Sie die Risikopunktzahlberechnen.

### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

### Warum und wann dieser Vorgang ausgeführt wird

Nachdem das primäre CVE der Schwachstellenbewertung hinzugefügt wurde, wird der Datensatz in den Status Bewertung ausstehend verschoben. Sie können weitere zugehörige CVEs auf der Registerkarte „ **Schwachstelleneinträge**“ hinzufügen oder die von dieser Schwachstelle betroffenen Produkte über die Registerkarte „ **Betroffene Produkte** “ hinzufügen. Sie können weitere Änderungen an den **Risikobewertungsfeldern** vornehmen, und die **Risikopunktzahl** für den Bewertungsdatensatz wird automatisch entsprechend aktualisiert.

### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**.
2. Aktualisieren Sie die Felder auf der Registerkarte **Details**.

| Feld | Beschreibung |
|---|---|
| Titel | Titel, der den Datensatz des Schwachstellenereignisses beschreibt. |
| Primäres CVE | Primäres CVE, das Sie dem Event-Datensatz zugeordnet haben. |
| Status | Aktueller Status des Event-Datensatzes. |
| Priorität | Priorität des Event-Datensatzes auf einer Skala von 1 bis 5. |
| Warnungsquelle | Quelle des potenziellen Schwachstellenereignisses. |
| Risikopunktzahl | Automatisch berechnete Risikopunktzahl.<br><br>Standardmäßig nicht bearbeitbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Risikoniveau | Die Gefährdungsstufe des Schwachstellenereignisses auf einer Skala von 1 bis 5. |
| Zuweisungsgruppe | Die Zuweisungsgruppe, der der Event-Datensatz zugewiesen ist. |
| Zugewiesen an | Der Benutzer, dem der Event-Datensatz zugewiesen ist. |
| Beschreibung | Detaillierte Beschreibung des Event-Datensatzes. |

3. Navigieren Sie zur Registerkarte **Schwachstelleneinträge**, um zugeordnete oder zugehörige CVEs hinzuzufügen.
   a. Wählen Sie **Neu**.
   b. Suchen Sie im **Eingabefeld Schwachstelle** nach dem Datensatz.
   c. Wählen Sie den Schwachstellendatensatz aus, den Sie dem Bewertungsdatensatz zuordnen möchten.
   d. **Wahlweise:** Wählen Sie **Durchsuchen** aus, um eine Datei zu suchen und anzuhängen.
   e. Wählen Sie **Speichern**.
   Die von Ihnen ausgewählten Schwachstellendatensätze werden dem Bewertungsdatensatz hinzugefügt und auf der Registerkarte **Schwachstelleneinträge** angezeigt.
4. **Wahlweise:** Fügen Sie betroffene Produkte hinzu.
5. Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzuan.
6. Ändern Sie die **Risikoattribute** für das primäre CVE, das dem Datensatz des Schwachstellenbewertungsereignisses zugeordnet ist.

| Feld | Beschreibung |
|---|---|
| Speicherbeschädigung | Gibt an, ob dieser Event-Datensatz den Arbeitsspeicher beschädigen kann. |
| Ausführbarer Remotecode | Gibt an, ob die Remoteausführung von Code möglich ist. |
| Lokale Berechtigungsausweitung | Gibt an, ob eine lokale Schwachstelle bezüglich der Berechtigungseskalation vorhanden ist. |
| Nicht autorisierter Zugriff | Gibt an, ob eine Schwachstelle für nicht autorisierten Zugriff vorhanden ist. |
| DDoS | Gibt an, ob das potenzielle Event Distributed Denial of Service beinhalten könnte. |
| Angriffskomplexität | Gibt die Komplexität des Anhangs an.<br>Optionen sind Niedrig, Mittel oder Hoch. |
| Angriffsvektor | Gibt den potenziellen Pfad oder die Methode des Angriffs an.<br>Optionen sind: Netzwerk, Angrenzendes Netzwerk, Lokal, Physisch, Keine. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Erforderliche Berechtigungen | Gibt die Berechtigungsebene an, die ein Angreifer zum Ausnutzen der Schwachstelle benötigt.<br><br>Optionen sind Keine, Niedrig oder Hoch. |
| Anwenderinteraktion | Gibt an, ob Benutzerinteraktion erforderlich ist, um die Schwachstelle auszunutzen. |
| Auswirkung auf die Vertraulichkeit | Gibt das Maß der potenziellen Auswirkung auf die Vertraulichkeit der Schwachstelle an.<br><br>Optionen sind Keine, Niedrig oder Hoch |
| Umfangsänderung | Gibt an, ob sich der Umfang der Bewertung geändert hat. |
| Auswirkung auf die Verfügbarkeit | Gibt die potenziellen Auswirkungen einer erfolgreich ausgenutzten Missbrauchschwachstelle auf die Verfügbarkeit an. Verfügbarkeit bezieht sich auf die Zugänglichkeit von Informationsressourcen.<br><br>Optionen sind Keine, Niedrig oder Hoch |
| Auswirkung auf die Integrität | Gibt die potenziellen Auswirkungen einer erfolgreich ausgenutzten Missbrauchschwachstelle auf die Integrität an. Integrität bezieht sich auf die Vertrauenswürdigkeit und die garantierten Richtigkeit von Informationen.<br><br>Optionen sind Keine, Niedrig oder Hoch |
| Korrekturstufe | Gibt den Status oder die Verfügbarkeit der Korrektur für die Schwachstelle an.<br><br>Optionen sind Offizielle Korrektur, Temporäre Korrektur, Problemumgehung, Nicht verfügbar, Nicht definiert. |
| Reife des Exploit-Codes | Gibt die Wahrscheinlichkeit an, dass die Schwachstelle basierend auf dem vorhandenen Status der Exploit-Techniken und der Codeverfügbarkeit ausgenutzt wird.<br><br>Optionen sind Nicht nachgewiesen, Proof-of-Concept, Funktional, Hoch und Nicht definiert. |
| Berichtskonfidenz | Gibt an, wie sicher Sie sind, dass die Schwachstelle vorhanden ist. |

7. Geben Sie relevante Kommentare in das Feld **Verfassen** ein.
   - Geben Sie Ihre Arbeitsnotizen in das Feld **Arbeitsnotizen (privat)** ein.
   - Geben Sie Ihre Kommentare (für alle sichtbar) in das Feld **Kommentare** ein.
8. **Speichern Sie** den Bewertungsdatensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basierend auf den Aktualisierungen, die Sie an den **Risikoattributfeldern** für das primäre CVE oder das betroffene Produkt vorgenommen haben, das dem **Bewertungsdatensatz** zugeordnet ist, wird das Feld Risikopunktzahl automatisch aktualisiert.

**Hinweis:**
Um die Regeln oder Kriterien des Basissystem-Risikopunktzahlrechners zu ändern, navigieren Sie zu **Alle** > **Rechner für Schwachstellenbewertung** > **Risikorechner für Schwachstellenbewertung** > **Schwachstellenbewertung – Risikoregel**. Sie können Kriterien hinzufügen und die Gewichtung vorhandener Kriterien auf Feldebene nach Bedarf ändern.

### Nächste Maßnahme
Führen Sie eine erste Bewertung des Event-Datensatzes durch.

## Löschen Sie zugeordnete CVEs oder betroffene Produkte aus dem Datensatz der Schwachstellenbewertung

Löschen Sie einen Schwachstellen-Ereignisdatensatz, wenn er nicht mehr benötigt wird.

### Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

### Warum und wann dieser Vorgang ausgeführt wird
Sie können CVEs oder betroffene Produkte, die dem Schwachstellenbewertungsdatensatz zugeordnet sind, löschen. Sie können Schwachstelleneinträge/zugehörige CVEs oder betroffene Produkte nur löschen, wenn sie sich im Status „ **Neu** “ oder „ **Ausstehend** “ befinden.

### Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Schwachstellenbewertung**.
2. Wählen Sie den Schwachstellenbewertungsdatensatz aus.
3. Wählen Sie die Registerkarte **Schwachstelleneinträge** oder **Betroffene Produkte** aus.
4. Wählen Sie das zugeordnete CVE oder den betroffenen Produktdatensatz aus.
5. Wählen Sie **Löschen**.

**Hinweis:**
Die Schaltfläche **Löschen** wird nur für einen Bewertungsdatensatz angezeigt, wenn er sich im Status „ **Neu** “ oder „ **Ausstehende Bewertung** “ befindet.

## Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

Fügen Sie zusätzliche Links und Informationen zum Bewertungsdatensatz hinzu.

### Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den Bewertungsdatensatzeintrag aus.
3. Wechseln Sie zur Registerkarte **Zugehörige Links**.
4. Geben Sie eine relevante Beschreibung in das Feld **Beschreibung** ein.
5. Geben Sie die URL in das Feld **Link** ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **OK**.
   Der zugehörige Link wird hinzugefügt und auf der Registerkarte Zugehörige Links aufgelistet.

### Führen Sie eine Bewertung durch

Nachdem Sie den Schwachstellenbewertungsdatensatz erstellt und die Risikoattributfelder aktualisiert haben, führen Sie eine Bewertung des Event-Datensatzes aus.

#### Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager

#### Warum und wann dieser Vorgang ausgeführt wird
Führen Sie eine erste Bewertung durch, nachdem ein Ereignis für eine relevante Schwachstelle erstellt wurde und festgestellt wurde, dass es ein Risiko für Systeme und Daten darstellt. Der Zweck dieser Aktivität besteht darin, die Bedrohung weiter zu analysieren, indem die Risikobewertung mit einer eingehenden Risikobewertung aktualisiert wird.

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**.
2. Wählen Sie den relevanten Datensatz aus der Liste der Schwachstellenbewertungs-Ereignisdatensätze aus.
3. Wählen **Sie Bewerten** aus, um die Schwachstellenbewertung auszuführen.
   Der Hintergrundauftrag „ Vulnerability Response – Schwachstellenbewertungsevent verarbeiten“ wird initiiert, und eine entsprechende Benachrichtigung wird angezeigt.
4. Wählen Sie in der Benachrichtigung **Status** anzeigen aus, um den Status des ausgeführten Auftrags anzuzeigen.
5. Wählen Sie **Speichern**.

   Auf der Registerkarte **Bewertungen** werden Bewertungsdetails angezeigt. Wenn die Bewertung verarbeitet wird, werden die **VITs** oder **AVITs**, die den angreifbaren Einträgen oder CVEs zugeordnet sind, auf der Registerkarte „Angreifbare Elemente“ oder „Angreifbare Anwendungselemente“ angezeigt.

#### Ergebnisse

- Angreifbare Elemente oder TPEs im Zusammenhang mit den zugeordneten CVEs werden während der Bewertung abgerufen. Die mit den angreifbaren Elementen verbundenen CIs werden ebenfalls identifiziert und in der Tabelle „Betroffene Konfigurationselemente“ angezeigt.
- Wenn die zugeordneten CIs in der betroffenen CI-Tabelle nicht vorhanden sind, werden die identifizierten CIs der Tabelle hinzugefügt und der **Feldwert Hat angreifbares Element** wird auf **True**und der Wert des Felds **Quelle** wird auf Scanner festgelegt.
- Wenn das CI bereits in der betroffenen CI-Tabelle vorhanden ist, wird nur der **Feldwert Hat angreifbares Element** auf **True** festgelegt, und der Wert **Quellfelder** für das CI bleibt derselbe wie beim Erstellen des Bewertungsdatensatzes.
- Wenn nach der Bewertung angreifbare Elemente erstellt werden, wird eine geplante Aufgabe zur Schwachstellenbewertung ausgeführt, um die Tabelle der betroffenen CIs und die Quelle des CI zu aktualisieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

#### Zugehörige Informationen

Registerkarte „Bewertung“

Registerkarte „Übersicht“

### Registerkarte „Bewertung“

Überprüfen Sie die Bewertungsergebnisse auf der Registerkarte „Bewertung“. Nachdem Sie eine Bewertung des Schwachstellenereignisses durchgeführt haben, wird der Datensatz mit den Daten aus Software Bill of Materials und Software Asset Management korreliert und mit Visualisierungen angezeigt.

Die Registerkarte „Bewertung“ füllt Daten (falls verfügbar) basierend auf dem von Ihnen erstellten Bewertungsdatensatz und korreliert die Details mit Bewertungen aus Software Asset Management - und Software Bill of Materials -Komponentendaten in der CMDB.

## Funktionsweise der Bewertung

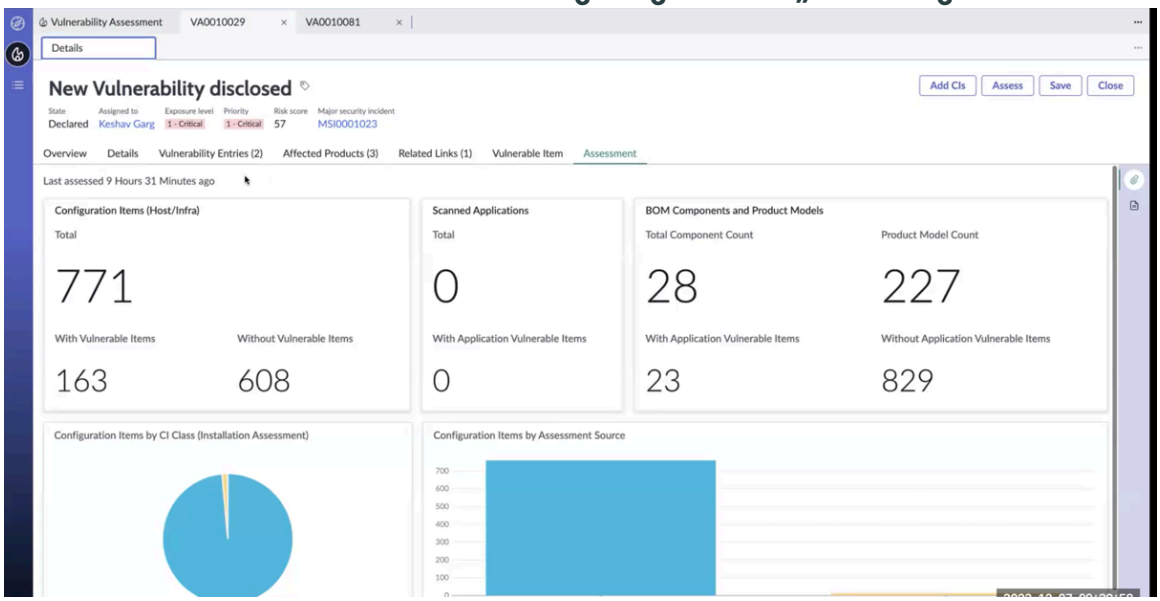
Wenn Sie auf die Schaltfläche Bewerten klicken, wird eine Bewertung für alle zugehörigen **CVEs** und betroffenen Produkte unter Verwendung der Daten Software Asset Management und SBOM initiiert. Ein Hintergrundauftrag wird ausgelöst, und wenn die Bewertung verarbeitet wird, werden die **VITs** oder **AVITs**, die den angreifbaren Einträgen oder CVEs zugeordnet sind, auf den Registerkarten „Angreifbare Elemente“ und „Angreifbare Anwendungselemente“ angezeigt.

- Alle angreifbaren Elemente oder TPEs im Zusammenhang mit dem CVE werden identifiziert.
- Die Konfigurationselemente (Configuration Items, CIs), die sich auf die angreifbaren Elemente beziehen, werden ebenfalls identifiziert und in der Tabelle der betroffenen Konfigurationselemente angezeigt.
- Wenn die CIs in der betroffenen CI-Tabelle nicht vorhanden sind, werden die identifizierten CIs der Tabelle hinzugefügt und die Kennzeichnung **Hat angreifbares Element** wird auf „wahr“ gesetzt, und der Wert des Felds **Quelle** wird auf Scanner festgelegt.
- Wenn das CI bereits in der Tabelle der betroffenen Konfigurationselemente vorhanden ist, wird nur die Kennzeichnung **Hat angreifbares Element** auf „true“ gesetzt, und die **Quelle** bleibt gegenüber dem Zeitpunkt der Erstellung des Bewertungsdatensatzes unverändert.
- Wenn nach der Bewertung angreifbare Elemente erstellt werden, wird eine geplante Aufgabe zur Schwachstellenbewertung ausgeführt, um die Tabelle der betroffenen CIs und die Quelle des CI zu aktualisieren.
- Im Bewertungsarbeitsbereich können Sie Zeitstempel anzeigen, um die letzte Bewertung der Events anzuzeigen. Die Registerkarte **Bewertung** ist nur sichtbar, wenn die neuen Bewertungen erstellt werden. Wenn die Bewertung den Status „In Bearbeitung“ aufweist, wird der letzte Bewertungsstatus angezeigt, da die Bewertung ausgeführt wird. Um den aktualisierten Bewertungsstatus anzuzeigen, müssen Sie die Seite aktualisieren. Sobald die Bewertung abgeschlossen ist, kann der Benutzer alle zugehörigen Registerkarten für diese Bewertung anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Arbeitsbereich für Schwachstellenbewertung – Registerkarte „Bewertung“




Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

- Konfigurationselemente (Host/Infra)
- Gescannte Anwendungen
- Stücklistenkomponenten und Produktmodelle
- Konfigurationselemente nach CI-Klasse (Installationsbewertung)
- Konfigurationselemente nach Bewertungsquelle: Zeigt die Liste der betroffenen Konfigurationselemente an.

## Datenvisualisierungen

| Name | Typ | Beschreibung |
|---|---|---|
| Konfigurationselemente (Host/Infra) | Einzelne Punktzahl | Zeigt die Anzahl der CIs mit und ohne VIs an.<br><br>Das Widget „Configuration Items“ zeigt die Gesamtanzahl der CIs an, die dem Bewertungsdatensatz zugeordnet wurden. Das Widget zeigt außerdem die Konfigurationselemente mit angreifbaren Elementen und ohne angreifbare Elemente an. |
| Gescannte Anwendungen | Anzahl | Gesamtanzahl der mit AVITs gescannten Anwendungen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
|---|---|---|
| | | **Hinweis:** Sie können die Anzahl der gescannten Anwendungen für primäre und sekundäre CVEs anzeigen. |
| Stücklistenkomponenten und Produktmodelle | Einzelne Punktzahl | Gesamtanzahl der Komponenten, Anzahl der Produktmodelle, Anzahl mit angreifbaren Anwendungselementen, Anzahl ohne angreifbare Anwendungselemente. |
| Konfigurationselemente nach Bewertungsquelle | Gestapelter Balken | Betroffene Konfigurationselemente, gestapelt nach der Bewertungsquelle. |
| Konfigurationselemente nach CI-Klasse (Installationsbewertung) | Kreisdiagramm | Konfigurationselemente nach CI-Klasse gestapelt. |

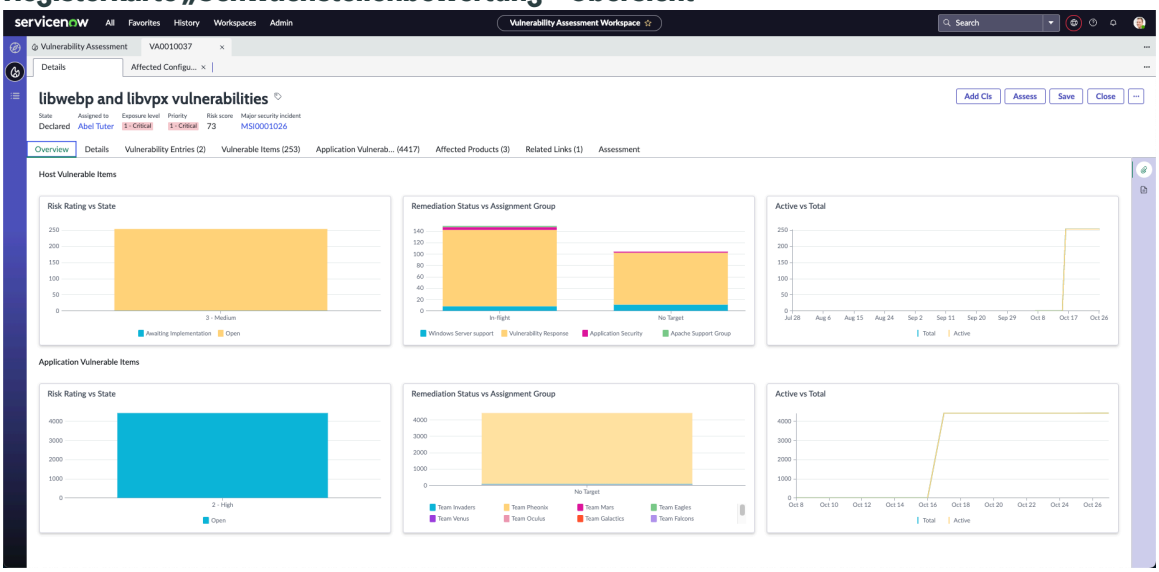
### Registerkarte „Übersicht“

Übersicht über die Bewertungsdetails, die auf der Registerkarte Übersicht angezeigt werden. Nachdem Sie die erste Bewertung durchgeführt haben, wird der Datensatz mit den Daten aus Software Bill of Materials und Software Asset Management korreliert und mit Visualisierungen angezeigt.

## Registerkarte „Übersicht“

Die Registerkarte Übersicht füllt Daten (falls verfügbar) basierend auf dem von Ihnen erstellten Bewertungsdatensatz und korreliert die Details mit Bewertungen aus Software Asset Management - und Software Bill of Materials -Daten in der CMDB. Die zugehörigen Listen namens

### Registerkarte „Schwachstellenbewertung – Übersicht“




Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbare Host-Elemente (Host/Infra)
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt
- Angreifbare Anwendungselemente
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt

## Datenvisualisierungen

### Angreifbare Host-Elemente

| Name | Typ | Beschreibung |
|---|---|---|
| Risikobewertung vs. Status | Gestapelter Balken | Status der angreifbaren Elemente, gestapelt nach Risikobewertung. |
| Korrekturstatus vs. Zuweisungsgruppe | Gestapelter Balken | Korrekturstatus des angreifbaren Elements, gestapelt nach seiner Zuweisungsgruppe. |
| Aktiv vs. Gesamt | Liste und Linie | Gesamtzahl der mit diesem Eintrag verknüpften angreifbaren Elemente im Vergleich zu aktiven angreifbaren Elementen. |

### Angreifbare Anwendungselemente

| Name | Typ | Beschreibung |
|---|---|---|
| Risikobewertung vs. Status | Gestapelter Balken | Status der angreifbaren Anwendungselemente, gestapelt nach Risikobewertung. |
| Korrekturstatus vs. Zuweisungsgruppe | Gestapelter Balken | Korrekturstatus des angreifbaren Anwendungselements, gestapelt nach Zuweisungsgruppe. |
| Aktiv vs. Gesamt | Liste und Linie | Gesamtzahl der mit diesem Eintrag verknüpften angreifbaren Anwendungselemente im Vergleich zu aktiven angreifbaren Elementen. |

### Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und eine Gefährdungsstufe zu

Weisen Sie dem Schwachstellenbewertungsdatensatz Priorität und Gefährdungsstufe manuell zu.

**Vorbereitungen**
Erforderliche Rolle: sn_vul_analyst.vul_event_manager



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich „Schwachstellenbewertung“.**.
2. Wählen Sie einen Schwachstellenbewertungsdatensatz aus.
3. Navigieren Sie auf der Registerkarte **Details** zu **Risiko Attribute**.
4. Wählen Sie eine **Priorität** aus der Liste der Optionen aus.
5. Wählen Sie eine **Risikostufe** aus der Liste der Optionen aus.
6. Wählen Sie **Speichern**.

## Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu

Fügen Sie manuell die CIs in Ihrer Organisation hinzu, die Ihrer Meinung nach dem Schwachstellenbewertungsdatensatz zugeordnet werden sollen, aber nach der ersten Bewertung nicht in den betroffenen CIs angezeigt werden sollen.

### Vorbereitungen

Erforderliche Rolle: sn_vul_analyst.vul_event_manager

### Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie CIs hinzu, von denen Sie wissen, dass sie möglicherweise betroffen sind, aber nach Abschluss der Bewertung nicht angezeigt werden. Sie können CIs nur hinzufügen, wenn sich der Bewertungsdatensatz im Status „ **Erklärt“** oder **„Ausstehende Bewertung“** befindet.

### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den erforderlichen Bewertungsdatensatz aus der Liste aus.
3. Wählen **Sie CIs hinzufügen aus**.
4. Wählen Sie die Konfigurationselemente im Dialogfeld „Konfigurationselemente“ aus.
5. Wählen **Sie CIs hinzufügen aus**.
   Der Hintergrundauftrag Vulnerability Response – Konfigurationselemente zu Event hinzufügen wird initiiert, und eine entsprechende Benachrichtigung wird angezeigt.
6. Wählen Sie in der Benachrichtigung **Status** anzeigen aus, um den Status des ausgeführten Auftrags anzuzeigen.

### Ergebnisse

Datensätze werden der Tabelle „Betroffene Konfigurationselemente“ mit der **Quelle***Manuell*hinzugefügt.

### Nächste Maßnahme

Navigieren Sie zur Registerkarte **Bewertung**, und aktualisieren Sie das Widget **„Konfigurationselemente (Host/Infra)** “, um die hinzugefügten CIs anzuzeigen.

## Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente

Erstellen Sie angreifbare Elemente (VIs) oder angreifbare Anwendungselemente (AVITs) im Arbeitsbereich für Schwachstellenbewertungen. Schwachstellenanalysten analysieren die Liste der VIs und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu beheben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Manager für Schwachstellenereignisse sollte in der Lage sein, eines, viele oder alle Suchergebnisse für Gefährdung auszuwählen, um angreifbare Elemente zu erstellen.

- Angreifbares Anwendungselement für SBOM-Bewertungsergebnisse, denen keine AVITs zugeordnet sind
- Angreifbare Elemente für Konfigurationselemente, denen keine VITs zugeordnet sind
- Ordnen Sie den angreifbaren Elementen ein primäres CVE zu.

### Erstellen Sie VIs für Konfigurationselemente ohne zugeordnete angreifbare Elemente

Erstellen Sie VITs für angreifbare Elemente für Konfigurationselemente, die durch die Schwachstellenbewertung identifiziert wurden, aber dem Datensatz sind keine VITs zugeordnet.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wechseln Sie zur Registerkarte **Bewertung**.
4. Wählen Sie im Widget **„Configuration Items (Host Infra)“** die Option **Ohne Konfigurationselemente** aus.
5. Wählen Sie aus der Liste „ **Betroffene Konfigurationselemente** “ die Konfigurationselemente aus, für die Sie VITs erstellen möchten.
6. Wählen **Sie Angreifbares Element erstellen aus**.
   Der Hintergrundauftrag Vulnerability Response – Manuelle VITs erstellen Schwachstellenbewertung wird initiiert, und eine entsprechende Benachrichtigung wird angezeigt.
7. Wählen Sie in der Benachrichtigung **Status** anzeigen aus, um den Status des ausgeführten Auftrags anzuzeigen.
   Angreifbare Elemente für die von Ihnen ausgewählten betroffenen Konfigurationselemente werden erstellt.

   Das Widget „ **Configuration Items (Host Infra)** “ zeigt jetzt dasselbe CI in der Anzahl **mit angreifbaren Elementen** an.

### Erstellen Sie angreifbare Anwendungselemente (AVITs) für betroffene Produktmodelle oder Komponenten ohne zugeordnete angreifbare Anwendungselemente

Erstellen Sie angreifbare Anwendungselemente (AVITs) für betroffene Produkte oder Komponenten, die durch die Schwachstellenbewertung identifiziert wurden, aber dem Datensatz sind keine AVITs zugeordnet.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wechseln Sie zur Registerkarte **Bewertung**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie im Widget **„Stücklistenkomponenten und Produktmodelle** “ die Option **Ohne Anzahl angreifbarer Anwendungselemente** aus.
5. Wählen Sie die betroffenen Produktmodelle, für die Sie AVITs erstellen möchten, aus der Liste „ **Betroffene Produktmodelle** “ aus.
6. Wählen **Sie Angreifbares Anwendungselement erstellen**.
   Der Hintergrundauftrag Vulnerability Response – Manuelle VITs erstellen Schwachstellenbewertung wird initiiert, und eine entsprechende Benachrichtigung wird angezeigt.
7. Wählen Sie in der Benachrichtigung **Status** anzeigen aus, um den Status des ausgeführten Auftrags anzuzeigen.
   Angreifbare Anwendungselemente für die von Ihnen ausgewählten betroffenen Produktmodellelemente werden erstellt. für das primäre CVE, das dem Datensatz zugeordnet ist.

   Das Widget „ **Stücklistenkomponenten und Produktmodelle** “ zeigt jetzt dasselbe Produktmodell oder dieselbe Komponente in der Anzahl **mit angreifbaren Anwendungselementen** an.

### Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

Sie können den Bewertungsdatensatz mit einem Major Security Incident verknüpfen, vorschlagen oder heraufstufen, sofern Sie Zugriff auf die Anwendung Management schwerwiegender Sicherheits-Incidents haben.

#### Vorbereitungen
Erforderliche Rolle: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können den Bewertungsdatensatz so verschieben, dass er einem vorhandenen schwerwiegenden Security Incident zugeordnet wird, eine neue MSI aus dem Bewertungsdatensatz erstellen oder den Schwachstellenbewertungsdatensatz zu einem schwerwiegenden Security Incident heraufstufen. Nutzen Sie die Funktionen von Management schwerwiegender Sicherheits-Incidents, z. B. die Integrationen mit Microsoft Teams und Microsoft SharePoint.

Sie können den Link zu schwerwiegenden Security Incidents auch im Arbeitsbereich von Vulnerability Manager für angreifbare Elemente anzeigen. Der Link MSIM wird der Schwachstellenbewertung zugeordnet, die für die angreifbaren Elemente und sowie in den anderen Arbeitsbereichen von Vulnerability Responseangezeigt wird.

#### Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**.
2. Wählen Sie den Bewertungsdatensatz aus, den Sie mit einem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie auf der Registerkarte **Details** das Symbol „ **Weitere Aktionen** “ aus.
4. Wählen Sie eine der folgenden Antworten aus.

| Option | Bezeichnung |
|---|---|
| **Mit schwerwiegendem Security Incident verknüpfen** | Wählen Sie den vorhandenen MSI-Datensatz aus der Liste der schwerwiegenden Security Incidents aus. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | Der Schwachstellenbewertungsdatensatz ist mit dem vorhandenen schwerwiegenden Security Incident verknüpft. |
| **Als schwerwiegenden Security Incident vorschlagen** | Geben Sie die folgenden Details ein, und wählen **Sie Vorschlagen aus**.<br>○ Erkennungsdatum<br>○ Begründung<br>○ Potenzieller Impact |
| **Als schwerwiegendem Security Incident heraufstufen** | Geben Sie die folgenden Details ein, und wählen Sie **Heraufstufen**aus.<br>○ Erkennungsdatum<br>○ Geschätztes Lösungsdatum<br>○ Begründung<br>○ Potenzieller Impact |

5. Wählen Sie **Speichern**.

### Nächste Maßnahme

Wählen Sie den MSI-Datensatz aus, um den Datensatz in der Ansicht Management schwerwiegender Sicherheits-Incidents zu öffnen.

**Zugehörige Informationen**

Link zu Major Security Incident

Vorschlagen als Major Security Incident

Hochstufen zu Major Security Incident

## Vulnerability Response Übersicht über die -Korrektur

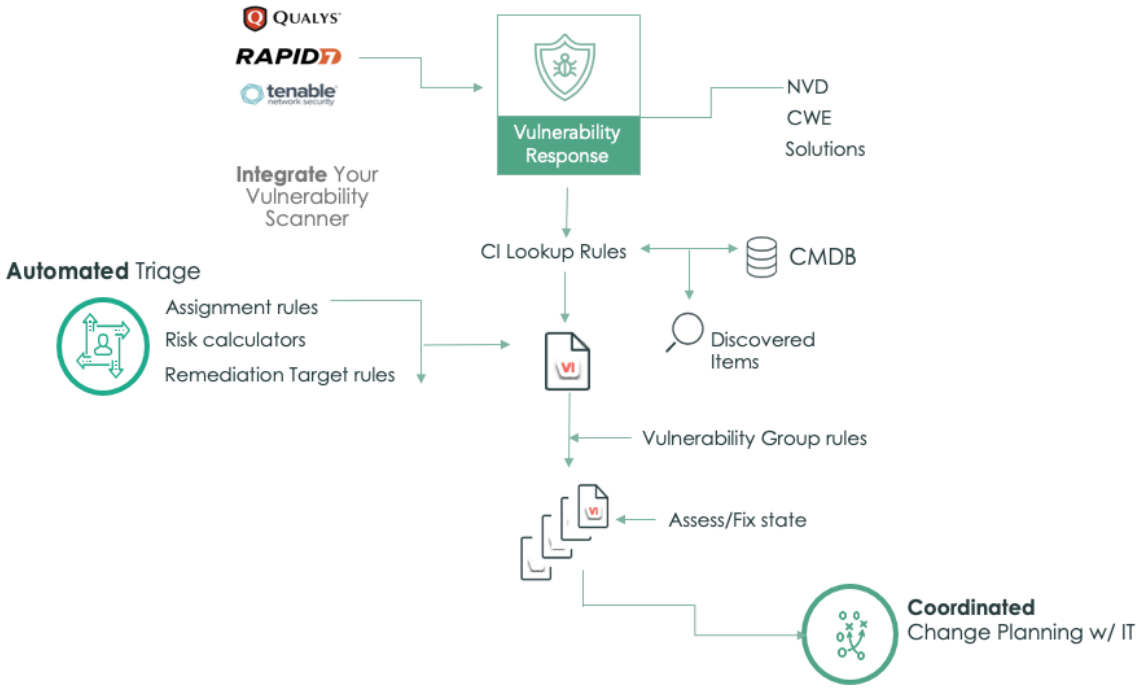
Vulnerability Response Die -Korrektur ist ein schrittweiser Prozess, der aus der Überprüfung des Importabschlusses, der Selektierung neuer Schwachstellen und der Überwachung des Fortschritts bis zum Abschluss besteht. Auf diese Weise wird die Fehlerkorrektur überschaubar, zeitnah und in vielerlei Hinsicht automatisiert.

Wenn Sie die Sicherheitslage für alle Unternehmens-Assets verstehen, können Sie die kritischsten Schwachstellen für die Korrektur identifizieren. Dieser Korrekturprozess erfordert, dass Vulnerability Response und eine Drittanbieterintegration wie Qualys Vulnerability Integration installiert und konfiguriert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vulnerability Response-Integrations-Flow**




## Überprüft den erfolgreichen Abschluss von Drittpartei-Integrationsimporten

Die erste Phase in diesem Prozess besteht darin, sicherzustellen, dass alles ordnungsgemäß funktioniert. Vulnerability Response ist voreingestellt, um Schwachstellen der National Vulnerability Database (NVD) und Common Enumeration Weakness (CWE) herunterzuladen. Durch Importe von Drittparteien erhalten Sie die Daten, die Sie zum Erstellen von angreifbaren Elementen und Korrekturaufgaben benötigen. Eine erfolgreiche Korrektur hängt vom konsistenten und erfolgreichen Import von Schwachstellen und angreifbaren Elementen ab.

Während des Imports stimmen CI-Suchregeln Drittpartei-Assets mit Assets in Configuration Management Database (CMDB)ab. Alle Assets werden im Modul „Erkannte Elemente“ gespeichert. CI-Informationen sind für die Lösungsimplementierung von entscheidender Bedeutung.

**Hinweis:**
Nachdem eine Drittanbieterintegration installiert und konfiguriert wurde, kann ein Import in einigen Fällen fehlschlagen, z. B. wenn der Drittanbieter seine API-Aufrufe einschränkt. Wenn Importe fehlschlagen, müssen sie umgehend behandelt werden.

Integrationsstatus-Ausführungsberichte für die unterstützten Drittanbieterintegrationen werden mit den -Anwendungen geliefert, um Ihnen eine grafische Übersicht über Ihre Importe zu geben. Verwenden Sie diesen Bericht, oder erstellen Sie einen eigenen, um leicht festzustellen, ob Ihr letzter Import erfolgreich war. Weitere Informationen zu unterstützten Integrationen finden Sie unter Vulnerability Response-Integrationen.

## Überprüfen und selektieren Sie Schwachstellen und angreifbare Elemente

Die nächste Phase der Korrektur erfordert die Überprüfung neuer Schwachstellen und angreifbarer Elemente. Ein angreifbares Element (VI) ist eine erkannte Kombination aus Schwachstelle und Konfigurationselement (CI). Während angreifbare Elemente gebildet werden, werden verschiedene Regeln ausgeführt, die AEs zuweisen, das von ihnen ausgehende Risiko bestimmen und Korrekturziele festlegen. Passen Sie die Regeln nach



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedarf an, um sicherzustellen, dass die angreifbaren Elemente erfolgreich selektiert wurden.

### Überwachen Sie den Fortschritt der Korrektur vorhandener Schwachstellen

Die letzte Phase der Korrektur besteht in der Überwachung Ihres Fortschritts.

- Überprüfen Sie den Status der Importe für Patch-Implementierungen, die nicht angezeigt wurden, und nehmen Sie Kontakt mit IT auf.
- Verfolgen Sie den Fortschritt bei der Erfüllung gesetzlicher Compliance-Verpflichtungen und stellen Sie deren Abschluss sicher.
- Überprüfen Sie den Status zurückgestellter Elemente, und überarbeiten oder implementieren Sie Korrekturen.
- Überwachen Sie Schwachstellenmanagement-Dashboards. Um Trends zu überprüfen, Berichte in Echtzeit anzuzeigen und Metriken zu verwenden, die die Erreichungsraten Ihrer Korrekturziele nachverfolgen, sollten Sie Ihre Prozesse möglicherweise mit der Anwendung Performance Analytics for Vulnerability Response überwachen.
- Veraltete Erkennungen in werden geschlossen Vulnerability Responsean.

### Überprüft den erfolgreichen Abschluss von Vulnerability Response Integrationsimporten

Die einfachste Möglichkeit, um festzustellen, ob Ihre Importe erfolgreich waren, ist die Verwendung eines Dashboards für den Integrationsausführungsstatus. Das Dashboard „Integrationsausführungsstatus“ bietet ein Beispiel für eine grafische Ansicht des Status von Integrationsausführungen von Drittanbietern.

Die Schwachstellenintegrationen Qualys und Rapid7 verfügen über ein Dashboard für den Integrationsausführungsstatus. Ausführliche Informationen zum Diagramminhalt finden Sie unter Qualys Statusdiagramm der Integrationsausführung oder Rapid7 Vulnerability Integration Ausführungsstatusdiagramm.

**Hinweis:**
Diagramme für Integrationen, die nicht von ServiceNow® bereitgestellt werden, können aus Berichten in einem Dashboard erstellt werden, erfordern jedoch möglicherweise ServiceNow. Weitere Informationen zum Erstellen von Berichten und Dashboards finden Sie unter Erste Schritte mit Berichten und Dashboards.

### Zeigen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente an

Die vollständigen Daten, die von Ihren Drittanbieter-Scanner-Integrationen mit Vulnerability Response erfasst wurden, werden auf den Registerkarten Erkennungen und Anfängliche Erkennungen in den Datensätzen für angreifbare Elemente (VIT) angezeigt. Sie wird auch in Erkennungsdatensätzen in der Liste „Erkennung angreifbarer Elemente“ in Ihrer Instanz Now Platform® angezeigt.

**Vorbereitungen**
Drittanbieter-Integrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden. Erkennungsdaten werden mit angreifbaren Elementen kombiniert, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn keine VI gefunden wird, wird eine neue erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_vuln.admin initiiert Integrationsausführungen und zeigt Erkennungsdaten für angreifbare Elemente an

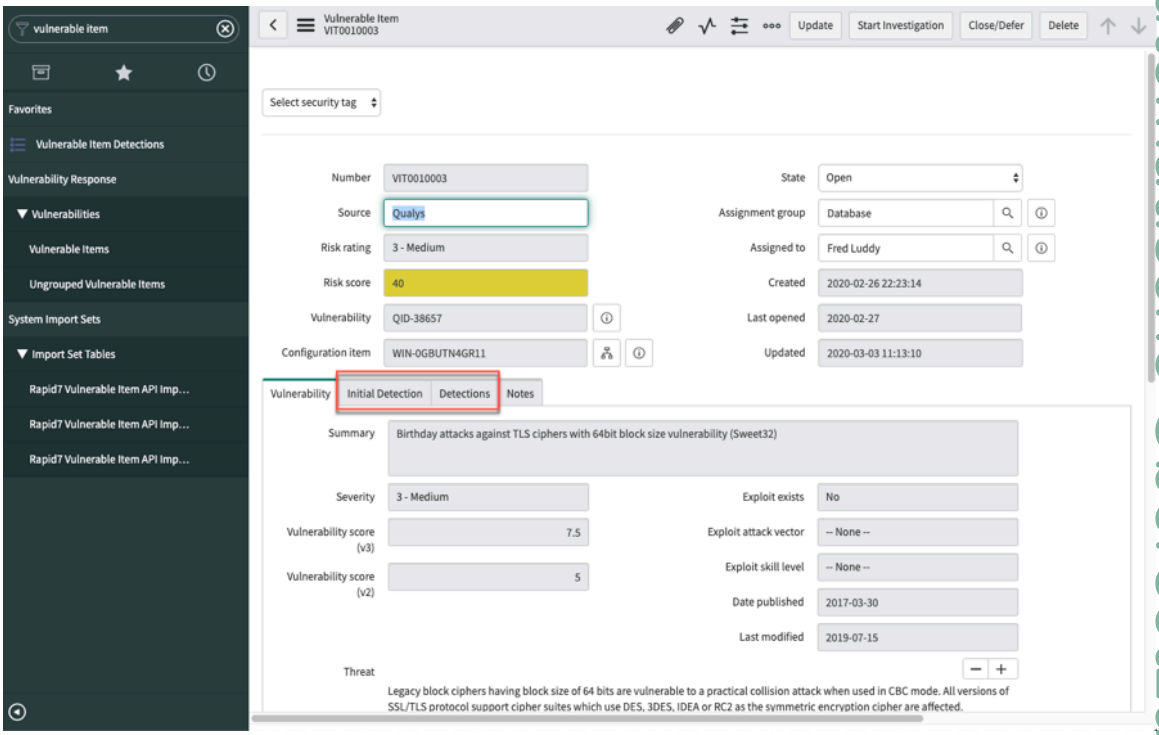
sn_vul.remediation_owner werden angreifbaren Elementen zugewiesen, die aus Erkennungen angreifbarer Elemente erstellt werden, und zeigt Daten in VI-Datensätzen an

### Prozedur

1. Um die Erkennungsdaten für angreifbare Elemente anzuzeigen, navigieren Sie zu einem Datensatz für angreifbare Elemente, und öffnen Sie ihn.

   Der Datensatz wird mit den Registerkarten Anfängliche Erkennungen und Erkennungen angezeigt.

   **Hinweis:**
   Daten, die zuvor auf der Registerkarte Konfigurationsdetails angezeigt wurden, werden zusammen mit anderen Erkennungsdaten auf den Registerkarten Anfängliche Erkennung und Erkennungen angezeigt.

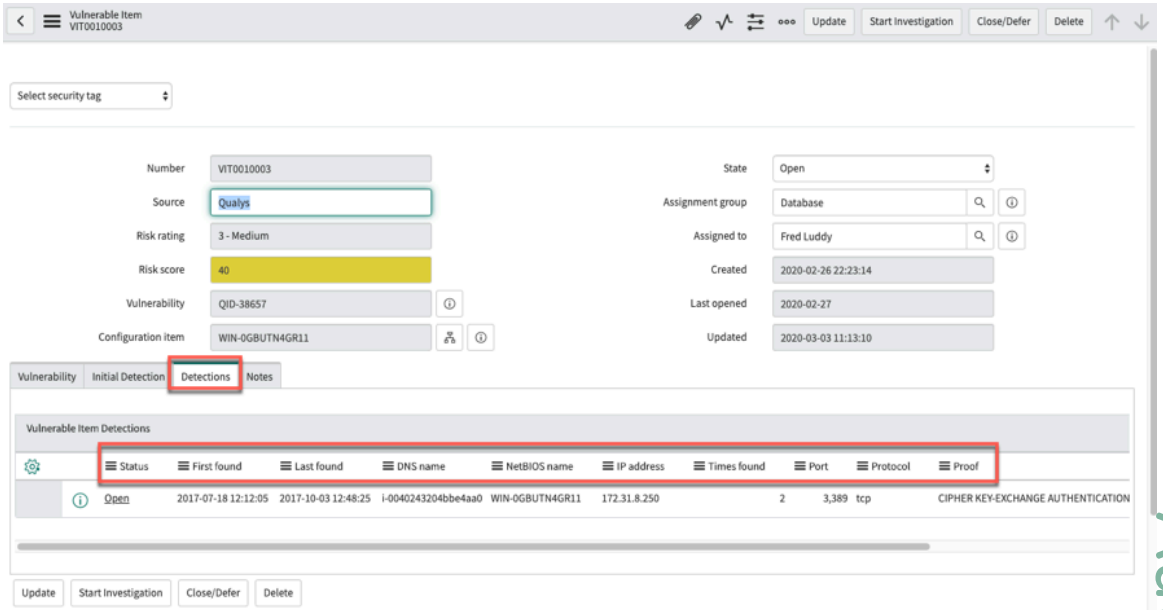



2. Klicken Sie auf die Registerkarte **Erkennungen**.

   Wenn ein angreifbares Element aus den Ergebnissen eines Drittanbieter-Scans erstellt wird, werden die Daten aus dem Scan im Erkennungsdatensatz angezeigt (siehe folgende Abbildung).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Jede Zeile im Abschnitt „Erkennungen angreifbarer Elemente“ stellt Daten aus einer bestimmten Erkennung dar. In der Spalte Zuerst gefunden wird das Datum angezeigt, an dem das angreifbare Element zuerst vom Scanner erkannt wurde. In der Spalte Zuletzt gefunden wird das Datum der aktuellen Erkennung angezeigt. Im Feld Quelle wird der Scanner angezeigt, der die Daten abgerufen hat.

**Hinweis:**
Für Qualyssind mit Erkennung angreifbarer Elemente die folgenden Felder im VI-Datensatz veraltet und werden nicht mehr ausgefüllt:

- Qualys Schweregrad
- Zuletzt aktualisiert von Quelle

Auch für Qualyswird, wie in der vorherigen Abbildung gezeigt, der Wert aus dem Scan nach Ergebnissen in der Spalte Nachweis im Erkennungsdatensatz angezeigt, wenn ein VI aus einem Scan erstellt wird. Dieser Wert wird jedoch nicht im oberen Teil des VI-Datensatzes angezeigt.

Wenn für Rapid7 ein VI aus einem Scan erstellt wird, kann der Wert für „Nachweis aus dem Scan“ sowohl in der Spalte „Nachweis“ im Erkennungsdatensatz als auch im oberen Teil des VI-Datensatzes angezeigt werden, aber nicht standardmäßig. Um diesen Wert im oberen Teil des VI-Datensatzes anzuzeigen, wählen Sie im Formularlayout das Feld Nachweis aus.

3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um das Layout der Registerkarte „Erkennungen“ im Datensatz zu konfigurieren.

   a. Die folgenden Spalten werden standardmäßig auf der Registerkarte „Erkennungen“ angezeigt.

   - Status
   - Zuerst gefunden (Daten)
   - Zuletzt gefunden (Datum)
   - DNS-Name
   - NET-BIOS-Name

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP-Adresse
- Anzahl Ermittlungen
- Port
- Protokoll
- Nachweis
- SSL

**Hinweis:**

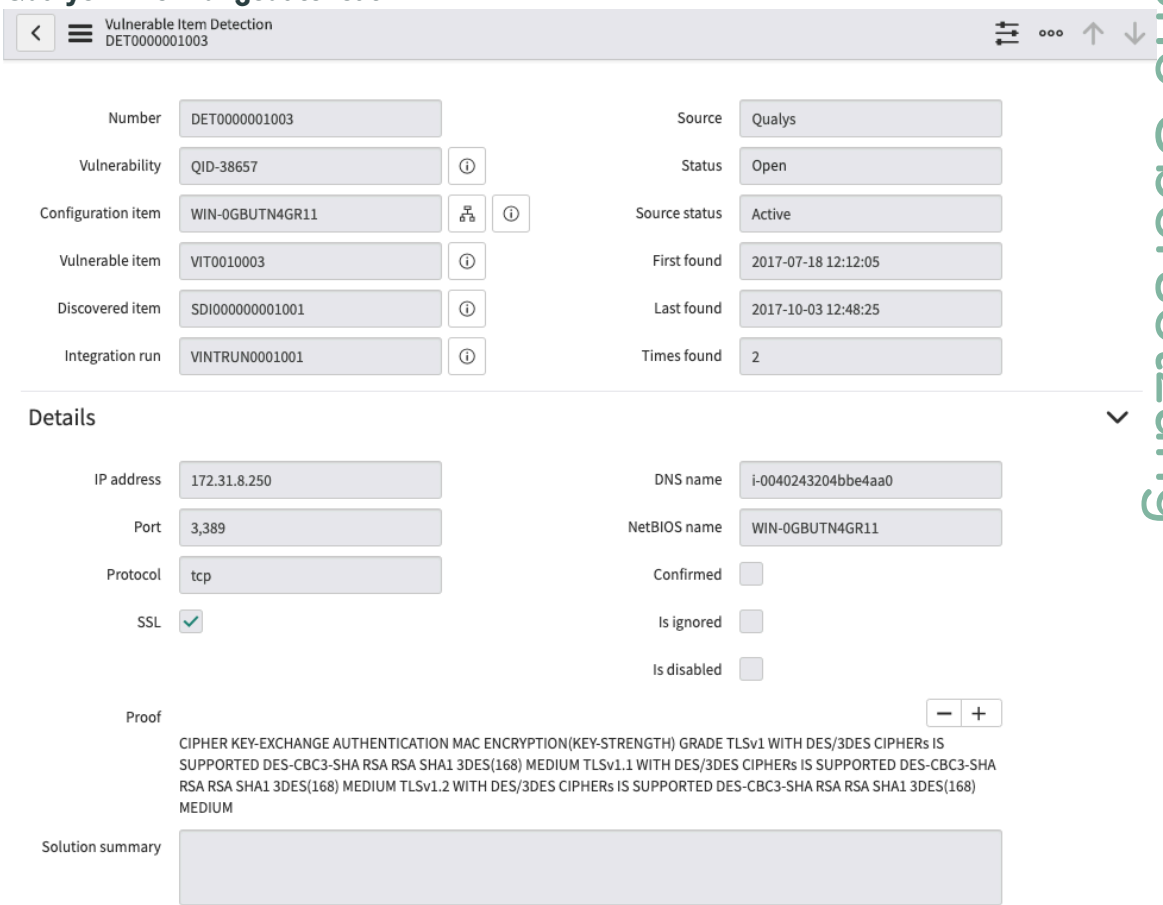
(Optional) Hinweis: Wenn in einer Spalte kein Wert vorhanden ist, wurden die Daten für dieses Feld vom Scanner nicht erkannt.

**b.** Klicken Sie auf das Zahnradsymbol ( ), um Ihre Ansicht zu personalisieren.

**c.** Wählen Sie die Spalten aus dem Slushbucket aus, um bestimmte Daten anzuzeigen, und klicken Sie auf **OK**.

**4.** Klicken Sie bei ausgewählter Registerkarte Erkennungen in der Spalte Status auf ein Element, um den Erkennungsdatensatz zu öffnen und die Details anzuzeigen, die diesem angreifbaren Element zugeordnet sind, einschließlich einer Lösungszusammenfassung (nur Rapid7 InsightVM-Integration).

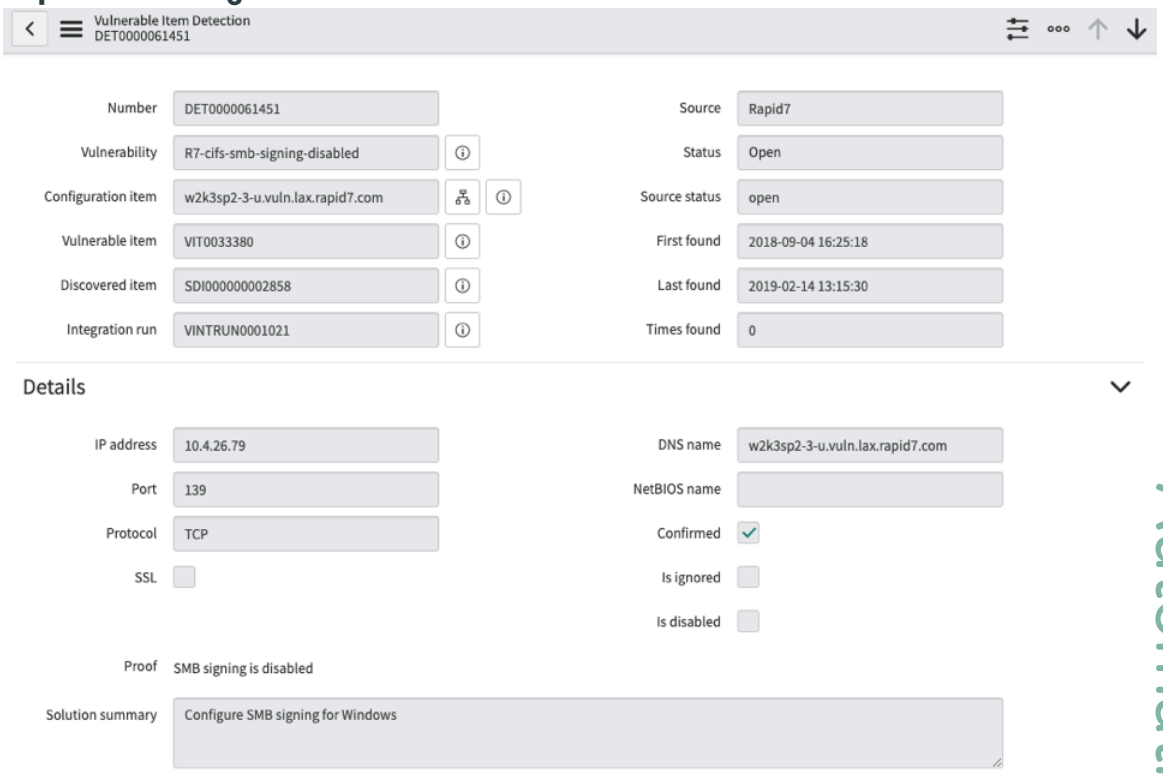
**Qualys -Erkennungsdatensatz**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Rapid7-Erkennungsdatensatz**

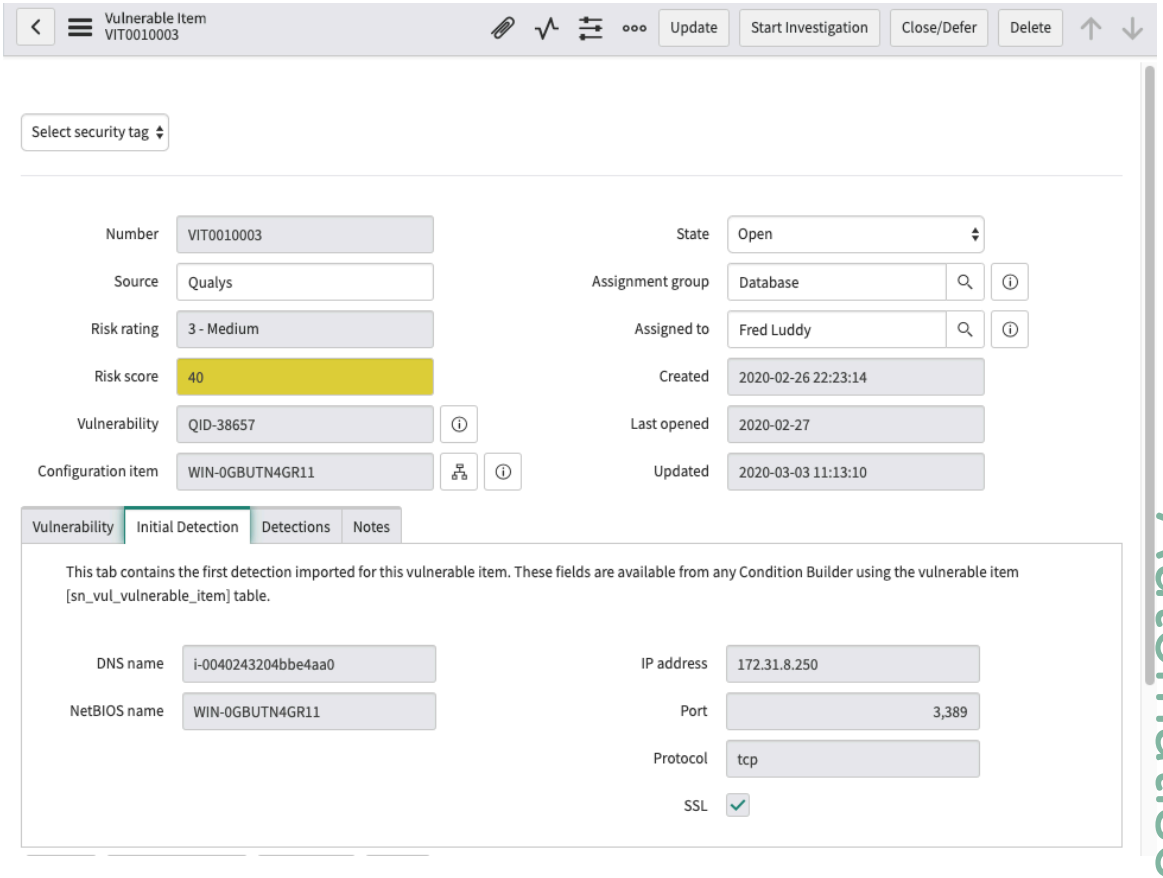



**5.** Kehren Sie zum Datensatz zurück, und wählen Sie die Registerkarte Anfängliche Erkennung aus.

Auf der Registerkarte Anfängliche Erkennungen werden die Daten angezeigt, die beim ersten Vorkommen der Erkennung vom Scanner einer Drittpartei importiert wurden. Diese Informationen auf der Registerkarte „Anfängliche Erkennung“ ändern sich nicht, wenn Erkennungsdaten aktualisiert werden.

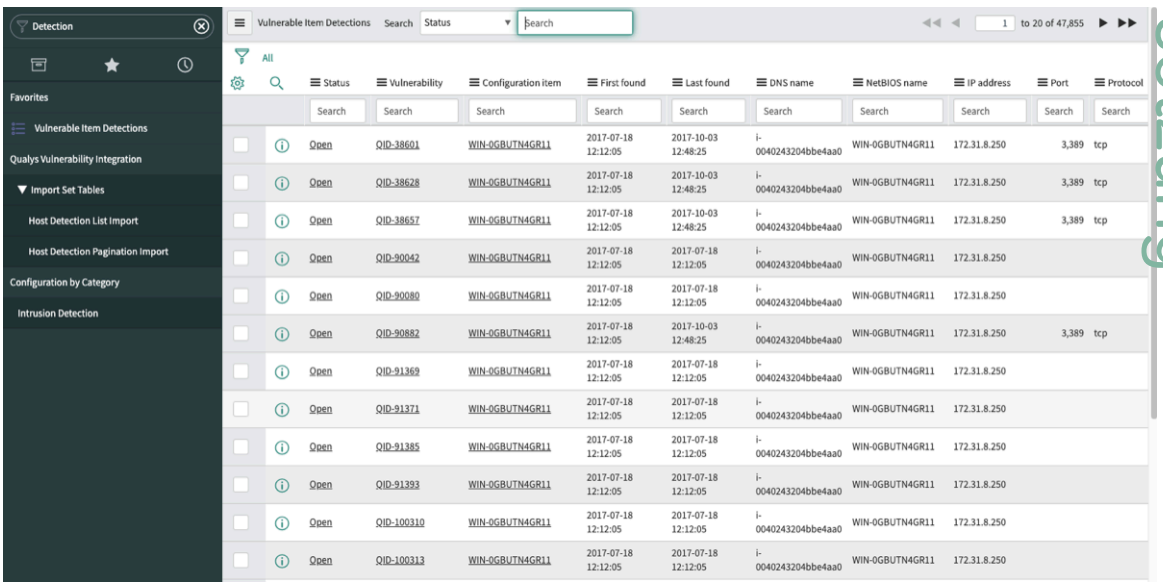
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. **Wahlweise:** Navigieren Sie zu Angreifbares Element Erkennungen, um die Liste der Erkennungen angreifbarer Elemente anzuzeigen.

   (Optional) Die Liste „Erkennung angreifbarer Elemente“ wird angezeigt. Jede Zeile in der Liste „Erkennungen angreifbarer Elemente“ stellt eine eindeutige Erkennung dar. Die Spalten zeigen dieselben Daten wie der VI-Datensatz an.




   Erkennungen werden nur durch Daten geöffnet oder geschlossen, die von einem Scanner gefunden werden. Sie führen kein Rolldown von VIs durch. Beim Importieren von Erkennungen werden diese zum Erstellen von VIs und zum Aktualisieren der Status von VIs verwendet. Wenn alle Erkennungen für ein angreifbares Element geschlossen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz lautet der Status „ geschlossen“ und der Substatus ist „ fixiert“.

**Hinweis:**
Fehler werden protokolliert, während:

- Vom Scanner abgerufene Anhänge werden verarbeitet.
- Erkennungen oder angreifbare Elemente erstellen oder aktualisieren

Weitere Informationen zur Behandlung von Erkennungsfehlern finden Sie unter Fehlerbehandlung für Erkennungen.

Wenn alle AEs für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen.

Geschlossene **AEs** mit dem **Substatus** „Korrigiert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die AEs mit der neuen Schwachstelle abgeglichen werden können.

Angreifbare Elemente, die in Ihrer Instanz auf **Gelöst** gesetzt wurden, aber nicht durch die nachfolgenden Integrationsläufe auf **Geschlossen/** Behoben gesetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Wenn alle AEs für eine Korrekturaufgabe geschlossen sind, wird der Datensatz geschlossen.

Angreifbare Elemente, die in Ihrer Instanz auf „Gelöst“ festgelegt, aber durch die nachfolgenden Integrationsausführungen nicht in „Geschlossen/Korrigiert“ geändert wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Erkennungen von Rapid7 ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um aufgelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden AEs, die auf **„Gelöst** “ gesetzt sind, aber dann nicht durch nachfolgende Scans in „ **Geschlossen/Korrigiert** “ geändert wurden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder in „ **Offen** “ zurückgesetzt.

Wenn der Scanner bei Erkennungen von Qualys weiterhin AEs findet, die auf „Gelöst“ festgelegt wurden, dann aber durch nachfolgende Scans nicht in „ **Geschlossen“/** „Korrigiert“ geändert wurden, werden diese AEs zurück in den Status „ **Offen** “ verschoben, wenn das Datum des letzten Funds nach dem Datum „Gelöst“ liegt.

### Nächste Maßnahme

Um weitere Daten anzuzeigen, einschließlich Element- und Erkennungsanzahlen, können Sie Überprüfen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente in Datensätzen der Integrationsausführung (VINTRUN)..

### Überprüfen Sie Vulnerability Response Daten zur Erkennung angreifbarer Elemente in Datensätzen der Integrationsausführung (VINTRUN).

In den Datensätzen der Integrationsausführung in Ihrer Instanz Now Platform® können Sie Erkennungsdaten für angreifbare Elemente von Drittparteien basierend auf dem Datum und der Uhrzeit der Scans suchen. Überprüfen Sie, ob der Scan erfolgreich abgeschlossen wurde, und zeigen Sie die Anzahl (Anzahl) der einzelnen Erkennungen sowie aller angreifbaren Elemente (VIs) an, die direkt als Ergebnis der Scans erstellt oder aktualisiert wurden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vuln.admin (veraltet)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Möglicherweise möchten Sie die Informationen zur Integrationsausführung, entweder Datum und Uhrzeit des Scans, oder die Datensatznummer der Integrationsausführung (VINTRUN#) aus den angreifbaren Elementen oder Erkennungsdatensätzen erhalten, um bestimmte Datensätze aus den folgenden Listen zu finden.

### Prozedur

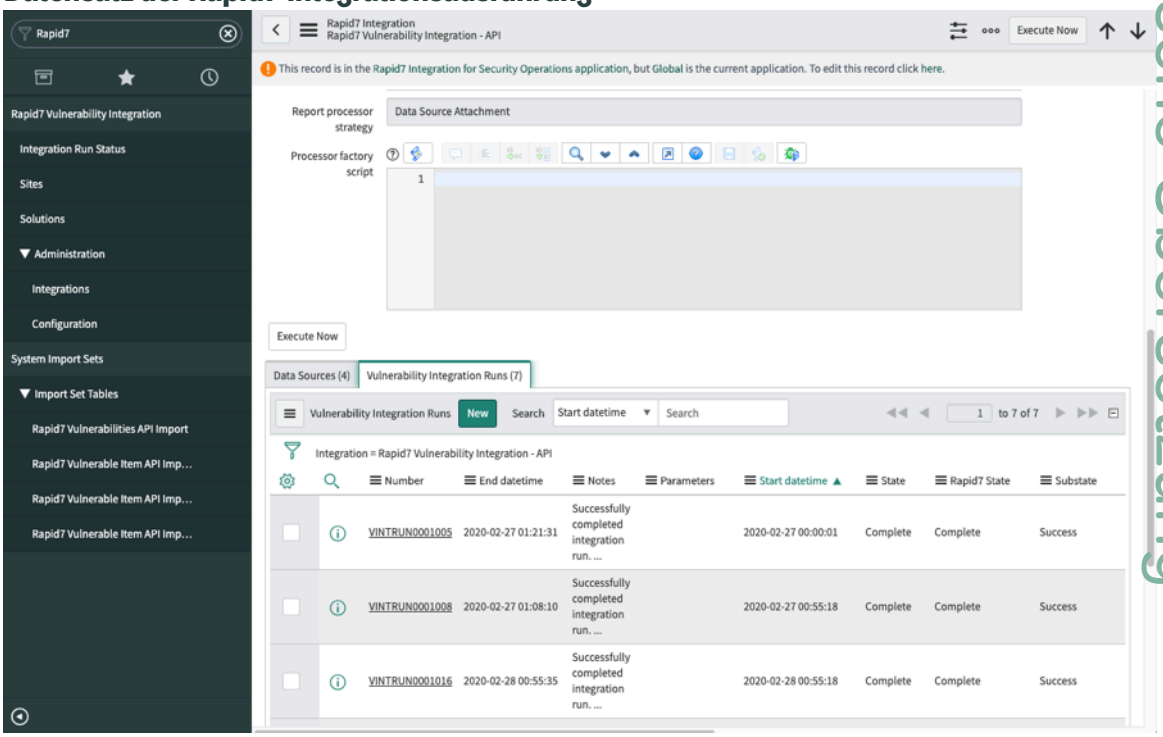
1. Wählen Sie eine, um fortzufahren.

2. Klicken Sie unten auf der angezeigten Seite auf die Registerkarte „**Schwachstellenintegrationsausführungen**“ .

3. Klicken Sie auf ein Element in der Spalte Nummer oder Importquelle, um einen Datensatz zu öffnen.

   Der Integrationsausführungsdatensatz wird angezeigt.

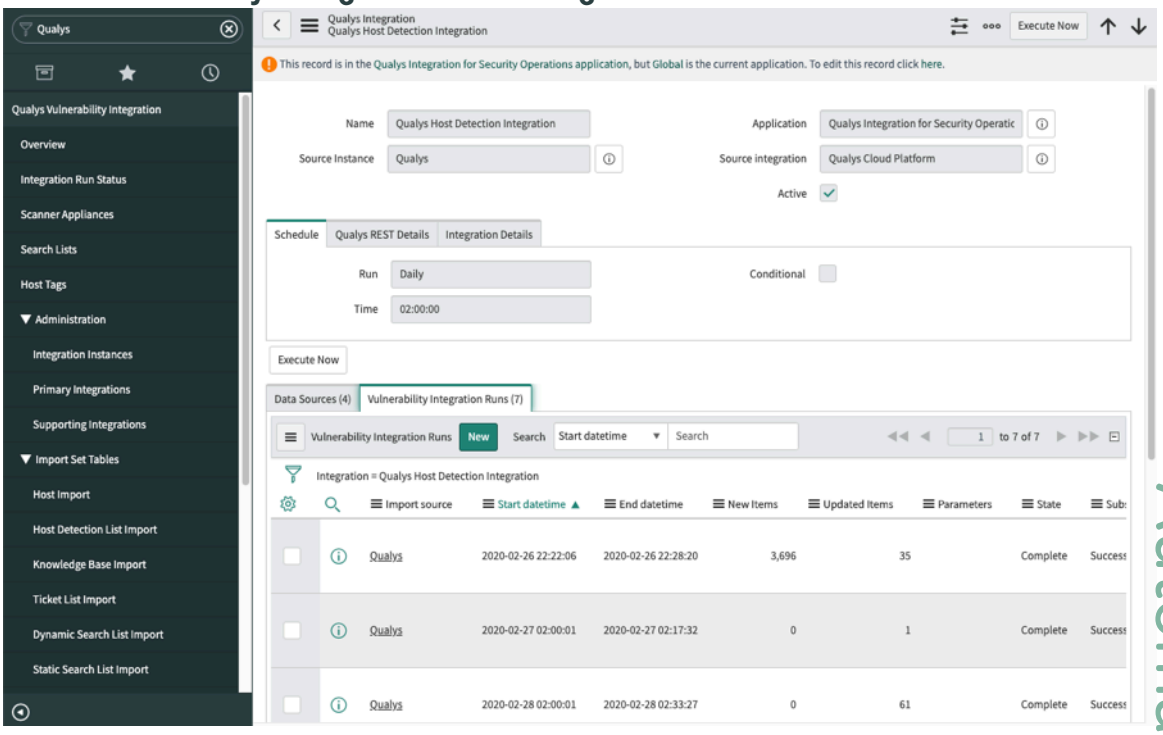
**Datensatz der Rapid7-Integrationsausführung**



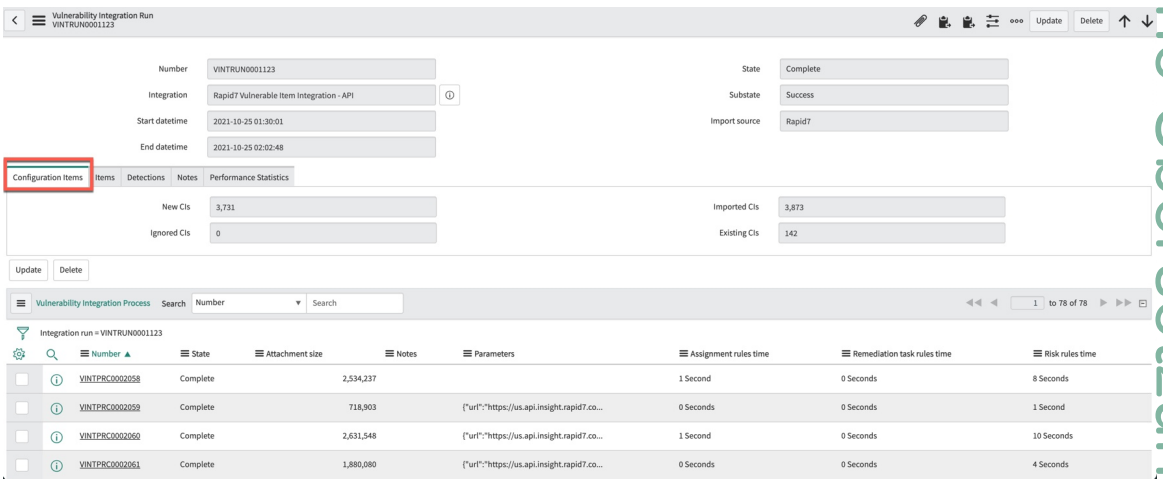

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Datensatz der Qualys-Integrationsausführung




Der Integrationsausführungsdatensatz wird angezeigt. Sie können im Feld Status überprüfen, ob die Integration erfolgreich ausgeführt wurde. Wählen Sie die Registerkarte **Konfigurationselemente aus**.



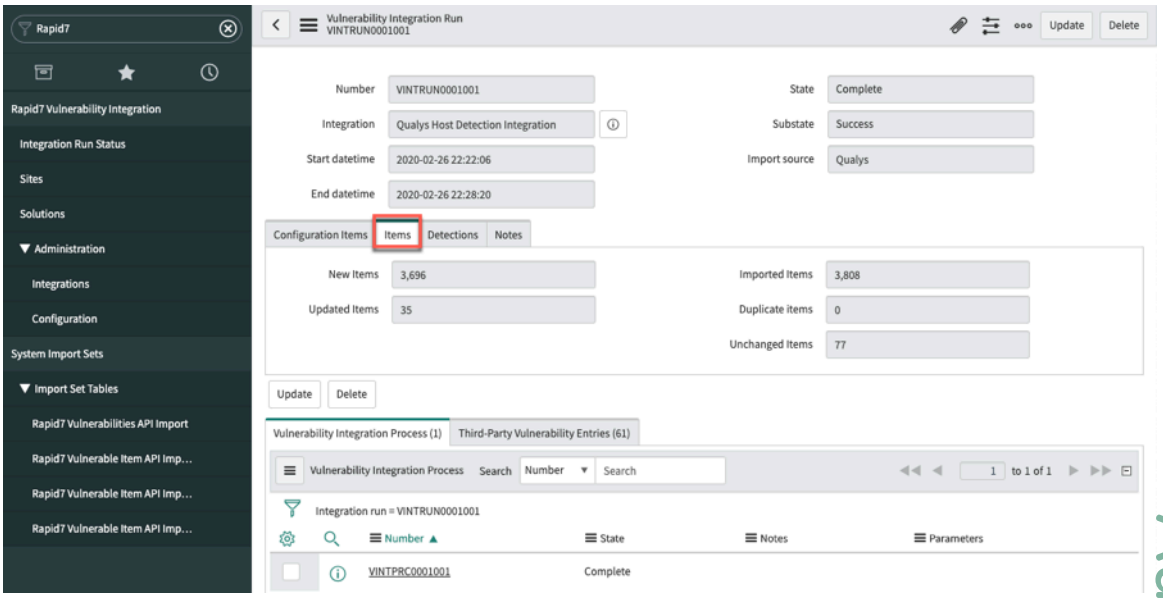

Auf der Registerkarte Konfigurationselemente werden die folgenden Informationen angezeigt:

- Auf der Registerkarte Konfigurationselemente wird die Gesamtzahl der importierten Konfigurationselemente angezeigt.
- Das Feld Neue CIs zeigt die Anzahl der im Rahmen dieser Integrationsausführung erstellten CIs an.
- Das Feld Importierte CIs zeigt die Summe aller CIs in diesem Abschnitt an.
- Der Wert des Felds Ignorierte CIs ist für die Vulnerability Response Integrationen immer 0.
- Das Feld Vorhandene CIs zeigt die Gesamtzahl der bereits vorhandenen CIs an.

**Klicken** Sie auf die Registerkarte Elemente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Auf der Registerkarte Elemente werden die folgenden Informationen angezeigt:

- Die Registerkarte Elemente zeigt die Gesamtzahl der importierten VIs an. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte „Erkennungen“ aufgeführten Zahlen hinzufügen.
- Das Feld Neue Elemente zeigt die Anzahl der angreifbaren Elemente an, die aus dieser Integrationsausführung erstellt werden.
- Das Feld Importierte Elemente zeigt die Summe aller Felder in diesem Abschnitt an.
- Das Feld „Doppelte Elemente“ ist nicht mehr ausgefüllt.
- Das Feld Aktualisierte Elemente zeigt an, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- Im Feld Unveränderte Elemente werden während der Integrationsausführung gefundene angreifbare Elemente angezeigt, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

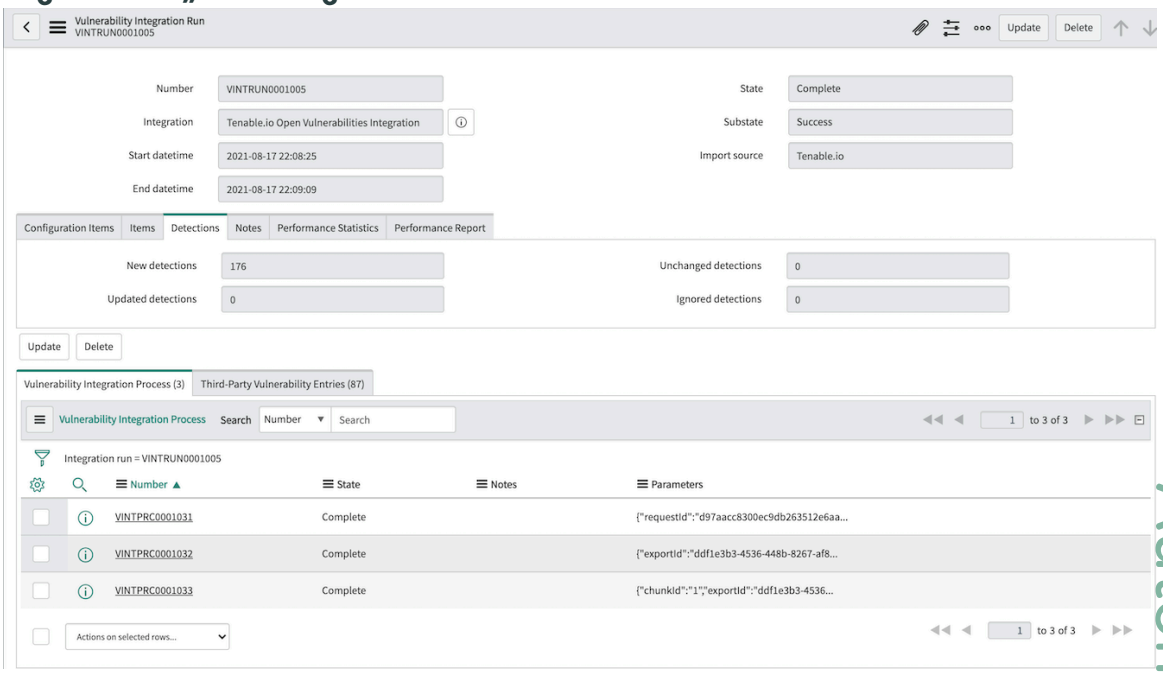
4. Klicken Sie auf die Registerkarte **Erkennungen**.

   Diese Registerkarte wird nur angezeigt, wenn die Integrationsausführung Erkennungen aufweist. Sie können die Gesamtzahl der importierten Erkennungen überprüfen, indem Sie die aufgeführten Zahlen hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Erkennungen “ aus VR v15.0**




**Hinweis:**
Vor v15.0 gab es kein Feld für ignorierte Erkennungen.

Auf der Registerkarte „Erkennungen“ werden die folgenden Informationen angezeigt:

- Ab v15 wurde ein neues Feld Ignorierte Erkennungen hinzugefügt, um die Erkennungen nachzuverfolgen, die zuvor ignoriert wurden. Mit dieser Implementierung werden die Anzahl der importierten Erkennungen und die Anzahl, die in den Datensätzen der Integrationsausführung nachverfolgt wird, konsistent. Diese Funktionalität wurde für alle Scanner implementiert, d. h. Qualys Vulnerability Integration, Rapid7 Vulnerability Integration, Tenable Vulnerability Integration und Microsoft TVM.
- Im Feld Neue Erkennungen werden neue Erkennungen angezeigt, die während dieser Integrationsausführung erstellt werden.
- Das Feld Unveränderte Erkennungen zeigt während der Integrationsausführung gefundene Erkennungen an, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.
- Das Feld Aktualisierte Erkennungen zeigt an, wie oft Erkennungen während dieser Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der aktualisierten eindeutigen Erkennungen. Wenn beispielsweise eine Erkennung im Rahmen der Integrationsausführung zweimal aktualisiert wird, wird sie zweimal gezählt und als 2 aktualisierte Erkennungen angezeigt.

**Hinweis:**
Erkennungen, die in diesen Anzahlen nicht angezeigt werden, sind Erkennungen, die sich in einem geschlossenen Status (Korrigiert) befinden, da feste Datensätze zum Aktualisieren vorhandener AEs verwendet werden. Wenn Sie mehr Transparenz in Bezug auf diese Erkennungsdatensätze wünschen, können Sie die geschlossenen VIs anzeigen, die erstellt werden, wenn keine übereinstimmende VI in einem offenen Status vorhanden ist. Weitere Informationen zu Schwachstellen im festen Status, die Sie im Setup-Assistenten für die Qualys-Integration aktivieren können, finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

**5.** Klicken Sie auf ein Element in der Spalte Nummer oder Importquelle, um einen Datensatz zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Anzeigen von Patch-Daten und Planen von Patches in Vulnerability Response

Ab v16.1 von Vulnerability Responsekönnen Sie Patches planen und Patch-Daten zusammen mit Lösungen und anderen Schwachstelleninformationen zu Datensätzen sowohl in der klassischen -Umgebung als auch in den Vulnerability Response -Arbeitsbereichen in Ihrer Now Platform -Instanz anzeigen.

### Erforderliche Rollen

Benutzer benötigen Rollen, die für die Patch-Orchestration-Integration spezifisch sind, die Sie zum Importieren Ihrer Patches verwenden, um Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie unter den unterstützten Integrationen.

- Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Responseund Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM.
- Patch-Orchestration-Daten werden in den Vulnerability Response -Dashboards angezeigt in der klassischen Umgebung.
- Zeigen Sie Daten in Bewertungslisten im Vulnerability Response Arbeitsbereichean.

### Planen von Patches

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

### Patchen Sie Daten in der klassischen Umgebung

In der klassischen Umgebung in der Anwendung Vulnerability Response :

- Um Patch-Update-Datensätze anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches**.
- Um Lösungen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Lösungen**.
- Um Ihnen zugewiesene AEs mit Patches anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**.
- Um Korrekturaufgaben anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**
- Um Datensätze erkannter Elemente anzuzeigen, navigieren Sie zu **Alle** > **Security Operations** > **Erkannte Elemente**.

#### Rollup für Patch-Daten und -Status für Patch-Orchestration in Vulnerability Response

Ab Version 16.1 von Vulnerability Response wird für Patch-Daten und -Status ein Rollup zum Patch-Update und anderen Datensätzen in der Anwendung Vulnerability Response durchgeführt.

### Patch Aktualisieren Sie Datensätze in den Arbeitsbereichen in der klassischen Umgebung in Vulnerability Response

Informationen zu Patches, Schwachstellenlösungen und Schwachstellen sind alle in der Anwendung Vulnerability Response verbunden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit Vulnerability Responseenthalten. Zeigen Sie Patch-Datensätze (VPU) in Vulnerability Response Workspaces aus der Listenansicht im IT-Korrekturarbeitsbereich an. Patch-Update-Datensätze in der klassischen Ansicht und in Vulnerability Response Workspaces enthalten die folgenden Daten:

- Daten und Informationen zur Schwachstellenlösung von Patch-Anbietern, die von der Anwendung Vulnerability Solution Management importiert werden.
- Quell-Korrekturstatus, der die Gesamtzahl der Geräte mit einer Schwachstelle enthält, die durch einen Patch behoben werden kann, sowie alle Geräte, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIs und die Gesamtzahl der VIs umfasst, für die ein Patch als bevorzugter Patch gilt.
- Zugehörige Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links für Datensätze in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in Vulnerability Response Workspaces angezeigt.
- Patch-Anforderungen, die die Korrekturbesitzer zur Genehmigung übermittelt haben.

## Erforderliche Rollen

Benutzer benötigen Rollen, die für die von Ihnen verwendete Patch Orchestration-Integration spezifisch sind, um Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie unter den unterstützten Integrationen.

- Informationen zur Integration von HCL BigFix Patch Orchestration mit Vulnerability Responseund Informationen zur Integration von Vulnerability Response Patch Orchestration mit Microsoft SCCM.
- Patch-Orchestration-Daten werden in den Vulnerability Response -Dashboards angezeigt in der klassischen Umgebung.
- Zeigen Sie Daten in Bewertungslisten im Vulnerability Response Arbeitsbereichean.

## Rollup für Patch-Daten und -Status

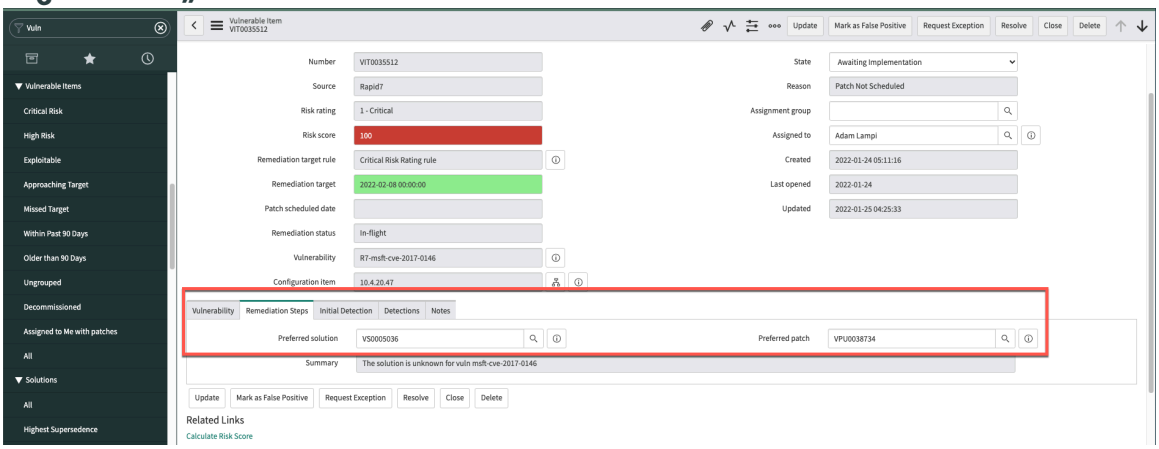
Um die angreifbaren Elemente anzuzeigen, für die Patches vorhanden sind und die Ihnen in der klassischen Umgebung zugewiesen sind, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir mit Patches zugewiesen**.

Wenn ein Datensatz für ein angreifbares Element mit einem bevorzugten Patch ausgefüllt ist, wird er nur dann automatisch in **„Warten auf Implementierung“ geändert**, wenn der Status des VI nicht **„Geschlossen**“, **„Gelöst“**, **„Zurückgestellt“** oder „ **In Überprüfung**“ ist. Um einen Drilldown in die Daten durchzuführen, um die bevorzugte Lösung und andere Daten anzuzeigen, klicken Sie im VI-Datensatz auf die Registerkarte **Remediation**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Registerkarte „Korrekturschritte“.**




Eine VI mit einem bevorzugten Patch wechselt in den folgenden Fällen zu **„Warten auf Implementierung“** :

- Wenn ein Patch für die Bereitstellung auf einem CI geplant ist, das Teil eines Sammlungsimports ist, und dem CI eine AE zugeordnet ist, lautet der Grund für das **AE Warten auf ImplementierungPatch geplant**.
- Wenn ein Patch für die Bereitstellung auf einem CI geplant ist, das Teil eines Sammlungsimports ist, und dem CI eine VI zugeordnet ist und das Korrekturzieldatum (Frist) nach dem Datum der Korrektur (Time to Remediation, TTR) liegt, wird der Status von Der VI ist **„Warten auf Implementierung** “ mit dem Grund **„Patch geplant (fehlendes Zieldatum)“**.
- Wenn ein Patch nicht für die Bereitstellung auf einem CI geplant ist, das Teil eines Sammlungsimports ist, lautet der Status des VI **„Warten auf Implementierung“**mit dem Grund **„Patch nicht geplant“**.

Klicken Sie auf das Symbol für Informationen zu **bevorzugten Patches**, um die Patch-Updates zu öffnen und die folgenden Informationen zu den zugehörigen Links anzuzeigen:

**Angreifbare Elemente**

Angreifbare Elemente, die diesem Patch zugeordnet sind.

**Zugeordnete Geräte**

Geräte mit Updates und Geräte ohne Updates.

**Patch-Bereitstellungen**

Für diesen Patch geplante Bereitstellungen auf einzelnen Computern (Assets) oder in Gruppen von Assets.

**Patch-Anforderungen**

Eine Liste der Patch-Anforderungen, die zur Genehmigung gesendet wurden, bevor sie für die Bereitstellung geplant sind.

**Potenzielle Patches**

Patches, die eine Schwachstelle beheben könnten.

Klicken Sie auf das Symbol für **Informationen zum bevorzugten Patch**, um den Datensatz zu öffnen und die zuvor aufgeführten Informationen sowie die folgenden Patch-Update-Daten anzuzeigen:

**Quellenkorrekturstatus**

Die Gesamtzahl der Geräte, für die dieser Patch erforderlich ist, und aller Geräte, auf denen der Patch fehlt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Nachbesserungsstatus**

Der Status (VIs insgesamt, % behoben, VIs zurückgestellt) für die VIs, die diesen bevorzugten Patch aufweisen.

## Bevorzugte Patches und Lösungen

Wenn eine importierte Schwachstelle mit einem Asset in [] übereinstimmt, wird in Vulnerability ResponseConfiguration Management Database (CMDB)ein angreifbares Element (AE) erstellt. Wenn das Konfigurationselement (Configuration Item, CI), das dieser VI zugeordnet ist, auch von einem Drittanbieter für Patches importiert wird und für dieselbe Schwachstelle als fehlender Patch angezeigt wird, wird ein bevorzugter Patch aufgelistet und für Ihre Lösungen zusammengefasst. Anhand dieser Informationen wissen Sie, dass für ein Asset (CI) eine Korrektur aus einem verfügbaren Patch verfügbar ist, der am besten zu seiner Schwachstelle passt.

## Anzeigen von Patches ohne Lösungen

Wenn nach einem Import keine Daten zur **Schwachstellenlösung** verfügbar sind, bleibt das Feld Schwachstellenlösung im Patch-Update-Datensatz leer. Weitere Informationen zum Anzeigen von Informationen für diese Arten von Patches finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

### Zeigen Sie Patches ohne Lösungen in an Vulnerability Response

Ab v16.0 von Vulnerability Responsesucht das System für Patches, für die es nach einem Import keine Lösungen gibt, in den Schwachstellenreferenzdaten nach Patch-IDs, damit Sie diese Patches in Schwachstellendatensätzen anzeigen können.

## Patches ohne Lösungen

Erforderliche Rolle: sn_vul.vulnerability_admin.

Die aus den Anwendungen für Patch-Orchestration und Schwachstellenlösungen sowie aus Patch-Scanner-Integrationen importierten Daten werden in der Anwendung Vulnerability Response in Patch-Update-Datensätzen verarbeitet, verbunden und angezeigt.

Wenn eine Lösung für eine Schwachstelle vorhanden ist, werden zugehörige Informationen in Ihrer Instanz korreliert und ein Rollup von den Patches zu Schwachstellenlösungen und zu den Schwachstellen durchgeführt. Um diese Informationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**.

Wenn nach einem Import keine Daten zur **Schwachstellenlösung** verfügbar sind, bleibt das Feld Schwachstellenlösung im Patch-Update-Datensatz leer. Damit Sie die zugehörigen Lösungsinformationen für diese Patches anzeigen können, ist in Ihrer Instanz standardmäßig die Systemeigenschaft [**sn_vul_patch_orch.no_solution_patch_rollup**] aktiviert. Diese Eigenschaft sucht nach Bulletin-IDs und Artikel-IDs in den Schwachstellen-Referenzdaten aus Scanner-Importen. Wenn eine Übereinstimmung gefunden wird, werden die zugehörigen Daten in die Tabelle „Potenzielle Patches“ eingetragen, und diese Informationen werden in den zugehörigen Listen der Schwachstellendatensätze angezeigt.

Wenn Sie eine große Anzahl von Schwachstellen haben oder die geplante Rollup-Aufgabe lange dauert, sollten Sie diese Systemeigenschaft deaktivieren, um mögliche Leistungsprobleme zu vermeiden. Beachten Sie jedoch, dass beim Deaktivieren dieser Systemeigenschaft importierte Lösungsdaten weder gesucht noch ein Rollup zu Ihren Schwachstellen ohne Lösungen durchgeführt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie als Benutzer mit der Rolle sn_vul.vulnerability_admin die folgenden Schritte aus, um die Systemeigenschaft zu deaktivieren:

1. Navigieren zu **sys.properties.list**.
2. Suchen Sie **sn_vul_patch_orch.no_solution_patch_rollup**, und klicken Sie darauf, um den Datensatz zu öffnen.
3. Geben Sie im Feld Wert `false`ein.
4. Klicken Sie auf **Aktualisieren**.

### Patch-Orchestration-Daten werden in den Vulnerability Response -Dashboards angezeigt

Ab v16.1 können Sie Patch-Update-Daten in der klassischen Umgebung in den Dashboards anzeigen, die in der Anwendung Vulnerability Response enthalten sind.

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen finden Sie unter Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

Sie können diese Daten auch in den Dashboards für CISO und Schwachstellenmanagement (PA) anzeigen, wenn Sie ein Abonnement für Performance Analyticshaben.

Sie können Patch-Daten auch in der klassischen Umgebung anzeigen. Weitere Informationen zu den erforderlichen Rollen und zum Anzeigen von Daten in den Dashboards Vulnerability Response in der klassischen Umgebung, die in der Anwendung Vulnerability Response enthalten sind, und in Dashboards, für die ein separates Abonnement erforderlich ist, finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.

## Zeigen Sie eine Lösung an

Zeigen Sie alle Lösungen, Lösungen mit der höchsten Ersetzung und Lösungen an, die angreifbaren Elementen zugeordnet sind, um Informationen zu Ihren Korrekturaktivitäten zu erhalten.

### Vorbereitungen

Erforderliche Rolle:
sn_vul.read, sn_vul.vulnerability_admin oder sn_vul.remediation_owner

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenanalyst oder Korrekturbesitzer können Sie verschiedene Lösungssätze im Zusammenhang mit angreifbaren Elementen anzeigen.

**Hinweis:**
Lösungsdatensätze sind schreibgeschützt, außer unter **Notizen** im Abschnitt **Interne Notizen** oder von Benutzern erstellte Lösungen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**.
2. Wählen Sie eine Lösungsliste aus.

   **Hinweis:**
   Sie können eine Lösungsliste mit Platzhaltern für den Produktnamen filtern.

3. Klicken Sie zur Überprüfung auf jedes Element.
4. **Wahlweise:** Geben Sie Notizen auf der Registerkarte **Notizen** ein, und klicken Sie mit der rechten Maustaste auf **Speichern**, um auf der Seite zu bleiben, oder klicken Sie auf **Aktualisieren**, um zu speichern und zur Liste der **Lösungen für Schwachstellen** zurückzukehren.

   **Hinweis:**
   Wenn Sie nur über die Rolle „sn_vul.read“ verfügen, können Sie diesen Schritt nicht ausführen.

## Erstellen Sie eine Schwachstellenlösung

Erstellen Sie eine Schwachstellenlösung, damit Sie Schwachstellenlösungen nachverfolgen können, die nicht durch Lösungsinhalte von Drittanbietern abgedeckt werden.

### Vorbereitungen

Erforderliche Rolle: admin, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder vulnerability.write Vulnerability Solution Management ist eine Funktion, die in der Anwendung Vulnerability Response verfügbar ist. Vulnerability Solution Management erfordert ein separates Abonnement.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Lösung aus einer der Lösungslisten erstellen. Sie müssen die Anwendung Vulnerability Solution Management installieren, bevor Sie eine Lösung erstellen können.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**.
2. Wählen Sie eine Lösungsliste aus: **Alle**, **Höchste Ersatzlösung** oder **Mit angreifbaren Elementen**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die bearbeitbaren Felder im Formular entsprechend aus.
   Sie können nicht verwendete Felder leer lassen. Weitere Informationen zu einzelnen Feldern finden Sie unter Felder des Lösungsformulars.
5. Klicken Sie im Header mit der rechten Maustaste auf **Speichern**.
   Der Lösungsdatensatz wird hinzugefügt und standardmäßig in den Listen **Alle** und **Höchste Ersetzung** angezeigt.
6. Die zugehörigen Listen werden angezeigt.

   Sie können diese Lösung den folgenden zugehörigen Listen zuordnen: Angreifbare Elemente,**Schwachstellen**von **Drittparteien, CVEs,**Ersetzungslösungen und **Vorhergehende**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Lösungen.** Wählen Sie eine Schwachstelle oder Lösung aus, und klicken Sie auf **Absenden**.

### Hinweis:

Vulnerability Solution Management ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellendatensätze manuell Lösungen zugeordnet werden.

Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf der Schwachstellenebene aktualisiert.

Wenn Sie die Beziehung zwischen einer Schwachstelle einer Drittpartei und einer Lösung ausschließen möchten, da sie für das CI, das Sie beheben, nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt, finden Sie weitere Informationen unter Schließen Sie Lösungen manuell aus Datensätzen von Drittparteien aus oder umgekehrt.

#### Schließen Sie Lösungen manuell aus Datensätzen von Drittparteien aus oder umgekehrt

Schließen Sie die Beziehung zwischen einer Schwachstelle einer Drittpartei und einer Lösung aus, da sie für das CI, das Sie korrigieren, nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt. Schließen Sie Lösungen manuell aus, indem Sie entweder eine Drittpartei-Schwachstelle oder einen Lösungsdatensatz verwenden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.write
sn_vul.remediation_owner

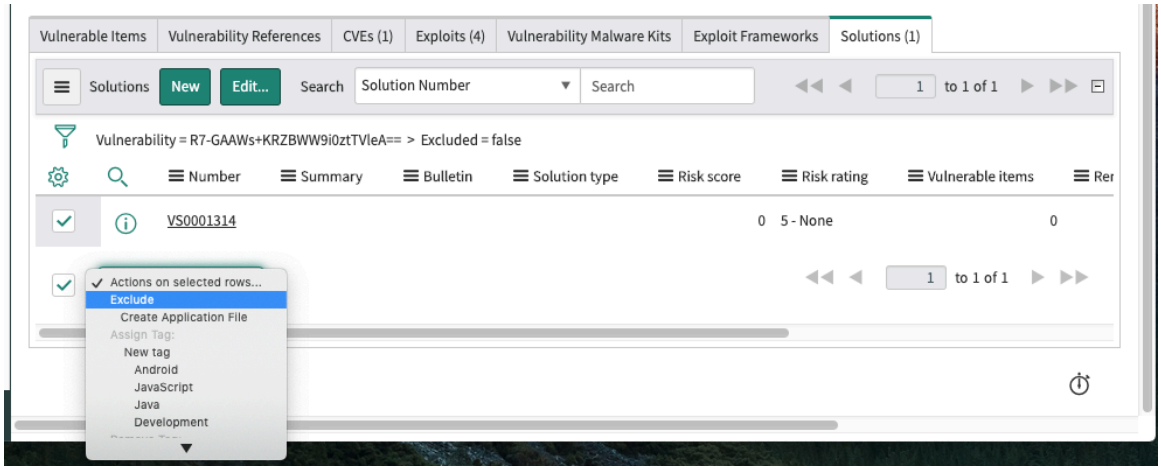
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei** oder **Vulnerability Response** > **Alle Lösungen**
2. Öffnen Sie einen Schwachstellen- oder Lösungsdatensatz einer Drittpartei.
   a. Für einen Drittpartei-Datensatz: Wählen Sie die zugehörige Registerkarte **Lösungen** aus.
   b. Für einen Lösungsdatensatz: Wählen Sie die zugehörige Registerkarte „ **Drittpartei-Schwachstellen** “ aus.
3. Aktivieren Sie das Kontrollkästchen neben jeder Schwachstelle oder jedem Lösungsdatensatz, den Sie ausschließen möchten.
4. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen** die **Option Ausschließen**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Der Drittpartei- oder Lösungsdatensatz wird nicht mehr auf der zugehörigen Registerkarte angezeigt.

Beziehungen von Drittpartei-Schwachstellen in Lösungen werden ebenfalls ausgeschlossen, wenn Lösungen aktualisiert werden oder wenn die nächtliche Aufgabe aktiviert ist.

Beziehungen von Drittpartei-Schwachstellen zu Lösungen werden während der nächtlichen geplanten Aufgabeausgeschlossen.

Der Ausschluss von Schwachstellen von Drittparteien bedeutet, dass die Lösung kein Faktor mehr für die Bewertung einer bevorzugten Lösung ist. Ausschlussauswirkungen:

- Alle Zählungen für Lösungen seit der Drittpartei-Schwachstelle, angreifbare Elemente (VIs) und Konfigurationselemente (CIs), die an die Drittpartei-Schwachstelle angehängt sind, werden nicht mehr für die Lösung gezählt.
- Bestimmen der bevorzugten Lösung für die Schwachstelle einer Drittpartei und damit der bevorzugten Lösung aller angehängten VIs und Korrekturaufgaben, die die VI enthalten.

## Selektieren Sie Schwachstellen automatisch

Die Überprüfung und Selektierung neuer Schwachstellen ist erforderlich, um eine erfolgreiche Korrektur sicherzustellen. Transformieren Sie Schwachstellenimporte in Korrekturaufgaben mit automatisierter Zuweisung angreifbarer Elemente (AE), Risikoberechnung, Korrekturzielen und AE-Gruppierung.

Beginnen Sie mit importierten Schwachstellen, stimmen Sie die nicht in der CMDB gefundenen Assets ab, priorisieren Sie die Ergebnisse, übersetzen Sie sie in automatisch zugewiesene Korrekturaktivitäten, orchestrieren Sie den Korrekturprozess und bestätigen Sie den Abschluss mit einem Validierungs-Scan.

Neue angreifbare Elemente werden beim Import normalerweise basierend auf den Regeln für Korrekturaufgaben in Korrekturaufgaben sortiert. Manchmal können angreifbare Elemente nicht gruppiert werden oder enthalten kein erkanntes Konfigurationselement.

Überblick über den Schwachstellen-Selektierungsprozess:

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Validiert, dass Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Elemente wie erwartet funktionieren. Weitere Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Aufgrund des großen Datenimportvolumens ist bei der automatisierten Zuweisung angreifbarer Elemente Vorsicht geboten.

- Validieren Sie, ob Ihre Korrekturziele korrekt sind. Unter Vulnerability Response Korrekturzielregeln finden Sie Informationen dazu, wie Korrekturzielregeln funktionieren und wie sie überarbeitet werden können.
- Nicht gruppierte angreifbare Elemente anzeigen.
  - Wenn Sie sich die nicht gruppierten angreifbaren Elemente ansehen, sollten Sie Ihre Gruppenregeln überarbeiten und einen erneuten Scan durchführen. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben.
  - Gruppieren Sie die angreifbaren Elemente manuell. Erstellen Sie eine Korrekturaufgabe manuell in Vulnerability Response für weitere Informationen.
  - Überarbeiten Sie die Risikopunktzahlen für die angreifbaren Elemente in Ihren Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.
  - Schließen Sie ältere angreifbare Elemente, die kürzlich von Ihren Drittanbieterintegrationen nicht erkannt wurden. Weitere Informationen finden Sie unter Automatisches Schließen angreifbarer Elemente und Erkennungen.
- Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizierenan.
- Recherchieren Sie, was für die Remediation getan werden muss.

  Dieser Schritt kann Folgendes umfassen:

  - Legen Sie fest, worum es jetzt geht und was Sie zurückstellen können. Diese Bestimmung basiert häufig auf der Risikopunktzahl, den betroffenen Systemen und Patches mit Change-Zeitfenstern.

    **Hinweis:**
    Korrekturzielregeln gehören zu angreifbaren Elementen. Diese Regeln werden ausgeführt, wenn das angreifbare Element importiert wird. Diese Regeln wurden zuvor im Setup-Assistenten erstellt.

  - Aktualisieren Sie angreifbare Elemente, falls erforderlich, und Zeigen Sie den Status des Korrekturziels eines Vulnerability Response angreifbaren Elements an.
  - Erstellen Sie eine **Change-Anforderung**, und weisen Sie die Korrekturaufgabe einer Zuweisungsgruppe (IT-Betrieb) zur Korrektur zu.

    **Hinweis:**
    Wenn die Schwachstelle einen Security Incident darstellt und das Plugin Security Incident Response (com.snc.security_incident) aktiviert ist, können Sie Security Incident-Datensätze stattdessen aus den Korrekturaufgaben erstellen.

  - Nachdem Sie eine oder mehrere Change-Anforderungen übermittelt haben, verschieben Sie den Gruppenstatus in „Wird untersucht“.

### Bearbeiten Sie angreifbare Elemente im Massenvorgang in Vulnerability Response

Bearbeiten Sie angreifbare Elemente im Stapel , um Zeit zu sparen, indem Sie Felder auswählen und einen asynchronen Massenbearbeitungsauftrag im Hintergrund ausführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Ab Vulnerability Response v21.0 können Sie die Zuweisung angreifbarer Hostelemente im Stapel auf der Listenseite in Vulnerability Manager Workspace] aufheben. Weitere Informationen finden Sie unter Bearbeiten Sie angreifbare Hostelemente im Massenvorgang Vulnerability Manager Workspace.

### Prozedur
1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**.
2. Wählen Sie die angreifbaren Elemente aus, indem Sie eine der folgenden Aktionen ausführen:
   - Aktivieren Sie die Checkbox neben jedem Element, wenn Sie die Option **Nur ausgewählte Elemente** im Feld Datensatzauswahl verwenden möchten.
   - Wenden Sie Filter an, wenn Sie die Option **Alle angreifbaren Elemente,** die der Filteroption entsprechen im Feld Datensatzauswahl verwenden möchten.
3. Klicken Sie auf die Schaltfläche **Massenbearbeitung**.
4. Füllen Sie im Dialogfeld „Massenbearbeitung“ die Felder aus.

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Nur ausgewählte angreifbare Elemente<br>○ Alle angreifbaren Elemente, die dem Filter entsprechen<br>○ Korrekturaufgabe<br>○ Verwundbarkeitseintrag |
| Status | Change für den **Status** im angreifbaren Element. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Nicht aktualisieren<br>○ Offen<br>○ Wird untersucht<br>○ Warten auf Implementierung<br>○ Zurückgestellt |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>▪ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Wenn Sie VITs zurückstellen, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet.<br>○ Abgeschlossen<br>**Hinweis:**<br>▪ Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu markieren, werden die Felder Grund, Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Wenn Sie die Datensätze als falsch positiv markieren, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet.<br>○ Gelöst |
| Bevorzugte Lösung | Lösung, die auf die Korrektur aller angreifbaren Elemente abzielt, die für die Massenbearbeitung ausgewählt sind. Wählen Sie die Änderung für das Feld **Bevorzugte Lösung** im angreifbaren Element (VITs) aus. Auswahlmöglichkeiten stammen aus einer Nachschlageliste der verfügbaren bevorzugten Lösungen für die ausgewählten VITs. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>◦ Der Satz der verfügbaren bevorzugten Lösungen ist eine Schnittmenge aller potenziellen Lösungen der Schwachstellen in allen ausgewählten VITs.<br>◦ Bei Auswahl von **Datensatzauswahl** > **Schwachstelleneintrag** Bei einer Massenbearbeitung werden alle VITs für die Schwachstelle auf die ausgewählte bevorzugte Lösung festgelegt.<br>**Hinweis:**<br>Dieser Vorgang legt die **bevorzugte Lösung** nicht auf der Schwachstelleneintragsebene fest. Durch Festlegen der **bevorzugten Lösung** auf der Schwachstelleneintragsebene wird die **bevorzugte Lösung** für alle neuen VITs festgelegt. Durch die Massenbearbeitung wird nur der aktuelle Satz von VITs geändert.<br>◦ Eindeutige Schwachstellen über die Auswahlkriterien hinweg sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit anderen Kriterien für die Festlegung der **bevorzugten Lösung**auszuwählen.<br>◦ Die Gesamtzahl der Lösungen, die in der Nachschlageliste angezeigt werden können, ist auf 170 beschränkt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt.<br>Der aktualisierte Wert wird in der Listenansicht des angreifbaren Elements angezeigt. |
| Bevorzugter Patch . | Patch, der auf die Behebung aller für die Massenbearbeitung ausgewählten angreifbaren Elemente ausgerichtet ist.<br>**Hinweis:**<br>◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen.<br>◦ Der Satz der verfügbaren bevorzugten Patches ist eine Schnittmenge aller potenziellen Patches für alle ausgewählten VITs.<br>◦ Eindeutige Schwachstellen über die Auswahlkriterien hinweg sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, werden Sie in einer Warnmeldung aufgefordert, VITs mit anderen Kriterien für die Festlegung des **bevorzugten Patch**auszuwählen.<br>◦ Die Gesamtzahl der Patches, die in der Nachschlageliste angezeigt werden kann, ist auf 170 beschränkt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt. |
| Grund | Grund für das Zurückstellen von Datensätzen: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Warten auf Wartungsfenster<br>○ Behebung nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Steuerung vorhanden<br>○ Sonstige<br><br>Grund für das Schließen von Datensätzen:<br>○ Falsch positiv<br><br>**Hinweis:**<br>▪ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung, Bis und Zusätzliche Informationen angezeigt.<br>▪ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als Falsch positiv markieren und diese Aufgabe zur Genehmigung gesendet wird.<br><br>○ Abgebrochen<br>○ Repariert<br><br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status als Zurückgestellt oder Geschlossen auswählen. |
| Kurzbeschreibung | Kurze Notiz, in der der Grund für Zurückstellungs- und „Falsch positiv geschlossen“-Anforderungen beschrieben wird. Diese Informationen werden im Feld Beschreibung der Korrekturaufgabe angezeigt, die für Zurückstellungs- und Geschlossen-Falsch-positive Anforderungen erstellt wird.<br><br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status auf „Zurückgestellt“ und „Geschlossen – Falsch positiv“ setzen. |
| Bis | Datum, bis zu dem der Datensatz zurückgestellt bleibt.<br><br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status als Zurückgestellt auswählen. |
| Zusätzliche Informationen | Alle anderen erforderlichen Informationen. Diese Informationen werden im Feld Zusätzliche Informationen auf der Registerkarte Übersicht angezeigt. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungsnotizen sowohl in VIT als auch in der Korrekturaufgabe angezeigt.<br><br>**Hinweis:**<br>Dieses Feld wird angezeigt, wenn Sie den Status auf „Zurückgestellt“ und „Geschlossen – Falsch positiv“ setzen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zuweisung aufheben | Die Zuweisung aller ausgewählten Elemente für die Zuweisungsgruppe und den Korrekturbesitzer wird aufgehoben. Weitere Informationen dazu, wie ein Korrekturbesitzer die Zuweisungen von angreifbaren Elementen entfernen kann, finden Sie unter Zuweisungen von angreifbaren Elementen für sich oder Ihre Gruppen entfernen.<br>**Hinweis:**<br>○ Dieses Feld wird angezeigt, wenn Sie als Status Nicht aktualisieren auswählen.<br>○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt und zur Genehmigung gesendet. |
| Zuweisungsgruppe | Zuweisungsgruppe für die VIT. Wählen Sie manuell aus, oder verwenden Sie Zuweisungsempfehlungen, wenn diese Option aktiviert ist.<br>**Hinweis:**<br>Dieses Feld ist deaktiviert, wenn Sie das Kontrollkästchen **Zuweisung aufheben** aktivieren. |
| Arbeitsnotizen | Text, den Sie eingeben, um die Änderungen zu beschreiben. |

5. Wählen Sie **OK**.
   Eine asynchrone Massenbearbeitungsaufgabe aktualisiert die ausgewählten Datensätze. Die Auftragsnummer mit einem Link wird auf der Seite „Angreifbare Elemente“ angezeigt, auf der Sie den Status anzeigen können. Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt, wenn Sie angreifbare Elemente in großen Mengen zurückstellen, ihre Zuweisung aufheben oder sie schließen (falsch positiv). Und diese Aufgabe wird zur Genehmigung gesendet.

### Nicht gruppierte Vulnerability Response angreifbare Elemente

Angreifbare Elemente werden beim Import automatisch einer Korrekturaufgabe zugewiesen. Manchmal jedoch, wenn ein angreifbares Element (VI) beispielsweise manuell erstellt wird, kann das VI verwaist werden. Das Modul **„Nicht gruppiertes** angreifbares Element“ listet die angreifbaren Elemente ohne Gruppe auf.

**Hinweis:**
Automatisierte Integrationsprozesse erstellen keine verwaisten Elemente, daher ist zu erwarten, dass dieser Anwendungsfall klein ist.

Das Aufheben der Gruppierung tritt auf, wenn ein angreifbares Element ohne Schwachstelle erstellt wurde oder keine Regel für Korrekturaufgaben vorhanden ist, die den VI einer Gruppe zuweist.

Überprüfen Sie in diesem Fall die Liste der nicht gruppierten angreifbaren Elemente, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Nicht gruppiert**.

Nach der Überprüfung haben Sie folgende Auswahlmöglichkeiten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben, um alle Elemente zu erfassen, die in dieser Liste angezeigt werden.
- Sie können Erstellen Sie eine Korrekturaufgabe manuell in Vulnerability Response und der Gruppe manuell Elemente aus dieser Liste hinzufügen oder eine Bedingung definieren, die diesen Elementen entspricht.
- Sie können eine vorhandene Korrekturaufgabe öffnen und der Gruppe alle relevanten angreifbaren Elemente hinzufügen, solange sie sich im Status „Offen“ oder „Wird untersucht“ befindet.

**Hinweis:**
Manuell hinzugefügte angreifbare Elemente werden nicht automatisch durch Regeln für Korrekturaufgaben oder Gruppenbedingungen aus Korrekturaufgaben entfernt.

Weitere Informationen zum Verhalten von Korrekturaufgaben und Aufgabenregeln finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.

### Zeigen Sie nicht gruppierte Vulnerability Response angreifbare Elemente an

Angreifbare Elemente, die keiner Gruppe zugewiesen sind, werden in einer anzeigbaren Liste platziert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Nicht gruppierte angreifbare Elemente**.
2. Überprüfen Sie die angreifbaren Elemente in der Liste.
3. Klicken Sie auf jedes angreifbare Element, um es anzuzeigen und zu bestimmen, wie es in eine Gruppe aufgenommen werden soll.

### Fügen Sie ein angreifbares Element manuell einer Korrekturaufgabe hinzu

Wenn ein angreifbares Element nicht gruppiert ist, können Sie es einer Korrekturaufgabe hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Notieren Sie die Nummer der Schwachstelle.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
3. Wählen Sie eine Korrekturaufgabe (VUL) für Ihr angreifbares Element aus.
4. Wählen Sie rechts unten **Bearbeiten** aus.
5. Geben Sie die Nummer des **angreifbaren Elements** in das Suchfeld für Sammlung ein.
6. Wählen Sie das angreifbare Element aus der Sammlung aus, und fügen Sie es der Liste hinzu.
7. Klicken Sie auf **Speichern**.

## Entfernen Sie Zuweisungen von angreifbaren Elementen für sich oder Ihre Gruppen

Weisen Sie Datensätze angreifbarer Elemente in den Anwendungen Vulnerability Response und Application Vulnerability Response neu zu.

### Vorbereitungen

Erforderliche Rolle: sn_vul.remediation_owner

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie feststellen, dass sich angreifbare Elemente (VITs) nicht in Ihrem Umfang für die Korrektur befinden, oder wenn Sie der Meinung sind, dass Ihnen oder Ihren Gruppen Datensätze fälschlicherweise zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernen für Datensätze von angreifbaren Elementen und Korrekturaufgaben.

Die **Schaltfläche Zuweisung** aufheben wird in den folgenden Datensätzen mit einem anderen Status als „Geschlossen“ oder „Gelöst“ angezeigt:

- Korrekturaufgaben (VULs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response Arbeitsbereichen. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, werden die Felder **Zugewiesen an** und**Zuweisungsgruppe** in allen zugehörigen VITs ebenfalls gelöscht.
- Angreifbare Elemente (VITs) sowohl in der klassischen Umgebung als auch in den Vulnerability Response Arbeitsbereichen.
- Angreifbare Anwendungselemente (AVITs).
- Angreifbare Containerelemente (CVITs).

### Prozedur

1. Navigieren Sie in der klassischen Umgebung oder im Arbeitsbereich des IT-Korrekturverantwortlichen zu einem Ihnen zugewiesenen Datensatz für angreifbare Elemente (VIT), der sich in einem anderen Status als Geschlossen oder Gelöst befindet.
2. Um die Felder **Zugewiesen an** und **Zuweisungsgruppe** zu löschen, wählen Sie oben im Datensatz die Option Zuweisung **aufheben**aus.
3. **Wahlweise:** Navigieren Sie alternativ zu einer **AVIT**, die Ihnen oder Ihren Gruppen zugewiesen ist, und klicken Sie auf Zuweisung aufheben, um die Zuweisungsfelder zu löschen.
4. Geben Sie im Dialogfeld „Zuweisung aufheben“ Arbeitsnotizen an, und wählen Sie **Absenden**.
5. **Wahlweise:** Wenn Sie die Zuweisungsfelder für mehrere VITs in einer Liste löschen möchten, wählen Sie die gewünschten **VITs**und dann Massenbearbeitung aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wählen Sie im Dialogfeld „Massenbearbeitung von angreifbaren Elementen“ im Feld **Datensatzauswahl** die Option **Nur ausgewählte angreifbare Elemente** aus, aktivieren Sie das Kontrollkästchen **Zuweisung** aufheben, und wählen Sie **OK**.
Weitere Informationen zu Massenbearbeitungen finden Sie unter Massenbearbeitung von angreifbaren Elementen in Vulner Response.

**b.** Wählen Sie die ID der Korrekturaufgabe aus, die in der Benachrichtigung angezeigt wird.

**6.** Zeigen Sie die folgenden Informationen an:

- Die von Ihnen bereitgestellten Arbeitsnotizen werden im Abschnitt „Notizen“ angezeigt.
- Auf der Registerkarte **Statusänderungsgenehmigung** wird der Statusänderungsgenehmigungsdatensatz mit dem Status Wird überprüft angezeigt, was bei der Nachverfolgung des Genehmigungs-Workflows hilft.
- Auf der Registerkarte „ **Angeforderte Genehmigungen** “ wird Ihre Anforderung zur Entfernung von Ihnen oder Ihrer Zuweisungsgruppe im Status „Angefordert“ angezeigt.

### Ergebnisse

Die Anforderung wird mithilfe eines standardmäßigen einstufigen Genehmigungsworkflows genehmigt. Weitere Informationen finden Sie unter Anforderungen in Vulnerability Manager Workspaces genehmigen.

- Wenn Ihre Anforderung genehmigt wird, gehen der Statusänderungsgenehmigungsdatensatz und der angeforderte Genehmigungsdatensatz in den Status Genehmigt über. Sie und Ihre Gruppen werden aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernt. Nicht zugewiesen wird im Feld **Zuweisungstyp** angezeigt, und die Korrekturaufgabe und dieVITs werden in der Liste des nicht zugewiesenen Moduls für Configuration Complianceangezeigt.

  Benachrichtigungen, dass Datensätze nicht zugewiesen sind, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Informationen zum Konfigurieren der Genehmigungskennzeichnung, der Benachrichtigungen und der Standardzuweisungsgruppe finden Sie unter Zuweisungen von angreifbaren Elementen und Korrekturaufgaben entfernen.

- Wenn Ihre Anforderung abgelehnt wird, wird der Status des Change-Genehmigungsdatensatzes und des angeforderten Genehmigungsdatensatzes in den Status „Abgelehnt“ geändert.

**Hinweis:**
Als Schwachstellenadministrator können Sie die Systemeigenschaft `sn_vul.unassign_vr.approval_required` auf „ **false** “ setzen, um den Genehmigungsprozess zu deaktivieren.

### Nächste Maßnahme

Navigieren Sie zu den Nicht zugewiesenen Modulen für die Anwendungen Vulnerability Response und Application Vulnerability Response Container Vulnerability Response, überwachen Sie alle nicht zugewiesenen Datensätze auf Elemente, die in Ihren Bereich fallen könnten, und weisen Sie sie sich selbst neu zu.

## Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Vulnerability Response

Genehmigen Sie Anforderungen zum Entfernen angreifbarer Elemente aus einer Zuweisungsgruppe oder einem einzelnen Benutzer in der Anwendung Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: Zum Aufheben der Zuweisung von Genehmigungen ist ein Genehmiger in der Gruppe „Genehmiger – Ebene 1“ erforderlich.

- sn_vul.unassign_approver für AVITs und VITs
- sn_vul_container.unassign_approver für CVITs

### Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt und eine Genehmigungsgruppe zum Aufheben der Zuweisung erstellt. Benutzer der Gruppe „Genehmigerzuweisung aufheben – Ebene 1“ können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Rolle „Zuweisung aufheben“ eines Genehmigers, sn_vul.unassign_approver. Sie können eine neue Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren. Um eine Genehmigungsregel zu konfigurieren, wählen Sie im Modul „Genehmigungsregeln“ eine der folgenden Genehmigungsregeln aus, und navigieren Sie auf der Registerkarte „Genehmigungskonfigurationen“ zur **Genehmigungskonfiguration** :

- *`Vulnerable item field change request`* für ein angreifbares Element.
- *`Vulnerability field change request`* für eine Korrekturaufgabe.
- *`Application vulnerability field change request`* für ein angreifbares Anwendungselement (AVIT).
- *`Approval for container management`* für ein angreifbares Containerelement (CVIT).

Weitere Informationen zu Genehmigungsregeln und -konfigurationen finden Sie unter Genehmigungsworkflow-Konfigurationen für Anforderung zum Aufheben der Zuweisung.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Freigaben** für VITs und AVITs. Navigieren Sie alternativ zu **Alle** > **Container Vulnerability Response** > **Meine Freigaben** für CVITs.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung ab, indem Sie die entsprechenden Kommentare hinzufügen.

#### Automatisches Schließen angreifbarer Elemente und Erkennungen

Sie können veraltete Erkennungen und angreifbare Elemente (AEs), die stillgelegten CIs zugeordnet sind, mithilfe des Moduls „Konfiguration automatisch schließen“ automatisch schließen.

Um die Option zum automatischen Schließen zu konfigurieren, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Konfiguration für automatisches Schließen**. In den folgenden Szenarien können Sie veraltete Erkennungen und VIs automatisch schließen:

- Veraltete Erkennungen in automatisch schließen Vulnerability Response
- Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Weitere Informationen zum Arbeiten mit deaktivierten Konfigurationselementen finden Sie unter Arbeiten mit deaktivierten Konfigurationselementen.

#### Arbeiten mit deaktivierten Konfigurationselementen

Außer Betrieb genommene Konfigurationselemente (CIs) werden in den Status „Stillgelegt“, „Archiviert“ oder „Gelöscht“ in Configuration Management Database (CMDB)verschoben. Vulnerability Response enthält angreifbare Elemente (AEs), die aus CIs bestehen. Wenn der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status eines CI auf „Deaktiviert“ aktualisiert wird, werden die zugehörigen AEs mit dem Substatus „CI außer Betrieb genommen“ geschlossen.

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „Deaktiviert“ ändert, können Sie die zugehörigen AEs automatisch schließen. Weitere Informationen zum automatischen Schließen der zugeordneten AEs finden Sie unter Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Das stillgelegte CI wird schließlich archiviert oder dauerhaft aus dem CMDBgelöscht.

Auswirkung der Außerkraftsetzung der CIs:

- **Auswirkung auf erkannte Elemente:** Wenn das CI stillgelegt wird, wird das zugehörige erkannte Element (DI) als „CI außer Betrieb genommen“ markiert.
- **Auswirkung auf angreifbare Elemente:** Wenn der Status eines DI auf „CI außer Betrieb genommen“ aktualisiert wird, wird der zugehörige VI geschlossen, und der Abschnitt „Notizen“ wird automatisch aktualisiert.

**Hinweis:**
Der Status eines DI wird automatisch auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Dagegen wird der Status einer VI nur dann auf Geschlossen aktualisiert, wenn die Option **VIs in Verbindung mit stillgelegten CIs automatisch schließen** aktiviert ist. Weitere Informationen zum automatischen Schließen der zugeordneten AEs finden Sie unter Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Die regelmäßige Aufgabe `Close detections/VIs for decommissioned CIs` wird täglich für die aktualisierten DIs ausgeführt. Wenn die Konfigurationsoption für das automatische Schließen für stillgelegte CIs aktiviert ist, wird der DI identifiziert, der ein stillgelegtes CI enthält, und der zugehörige VI wird mit dem Substatus „CI stillgelegt“ geschlossen. Wenn alle VIs in einer Korrekturaufgabe geschlossen sind und ihr Substatus „CI außer Betrieb genommen“ ist, wird die Korrekturaufgabe ebenfalls mit dem Substatus „Abgebrochen“ geschlossen. Um die außer Betrieb genommenen VIs anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Angreifbare Elemente** > **Außer Betrieb genommen**.

**Hinweis:**
Wenn ein CI aus dem Status „Deaktiviert“ in den ursprünglichen Status zurückversetzt wird, wird auch der Eintrag „Erkannte Elemente“ aktualisiert. VIs werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

### Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Wenn Configuration Management Database (CMDB) den Status der Lebenszyklusphase eines Konfigurationselements (CI) in „Deaktiviert“ ändert, können Sie die zugehörigen angreifbaren Elemente (AEs) und Erkennungen automatisch schließen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Um die zugeordneten VIs und Erkennungen automatisch zu schließen, müssen Sie die Option zum automatischen Schließen von VIs aktivieren, die stillgelegten CIs zugeordnet sind. Wenn diese Option aktiviert ist, werden neue und vorhandene VIs und Erkennungen, die für dasselbe CI gemeldet werden, automatisch erstellt oder im Status „Geschlossen“ aktualisiert. Diese basieren auf der Asset-ID in der Scanner-Nutzlast und dem Eintragsstatus „Erkannte Elemente“. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit deaktivierten Konfigurationselementen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Der Status eines DI wird auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Dagegen wird der Status einer VI nur dann auf Geschlossen aktualisiert, wenn die Option **VIs in Verbindung mit stillgelegten CIs automatisch schließen** aktiviert ist.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Konfiguration für automatisches Schließen** > **Konfigurationselement-Lebenszyklus**.
2. Um angreifbare Elemente, die den stillgelegten CIs zugeordnet sind, automatisch zu schließen, aktivieren Sie das Kontrollkästchen **VIs, die mit stillgelegten CIs verknüpft sind,** automatisch schließen.
3. Wählen Sie **Aktualisieren**.

**Hinweis:**
Wenn ein CI bereits stillgelegt wurde, bevor die Option **VIs in Verbindung mit stillgelegten CIs automatisch schließen** aktiviert ist, werden VIs nur für neue Erkennungen von Scannern erstellt. Der Status dieser VIs ist „Geschlossen“ und der Substatus ist „CI außer Betrieb genommen“.

Sie können VIs mit dem Status „CI außer Betrieb genommen“ nicht manuell erneut öffnen, indem Sie die Optionen **Erneut öffnen** oder **Massenbearbeitung** verwenden.

Geschlossene AEs mit dem Substatus „Korrigiert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die AEs mit der neuen Schwachstelle abgeglichen werden können. Weitere Informationen finden Sie unter Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente.

#### Veraltete Erkennungen in werden geschlossen Vulnerability Response

Das Modul „Veraltete Erkennungen automatisch schließen“ hilft Ihnen, ältere, veraltete angreifbare Erkennungen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden, automatisch zu bereinigen. Wenn Sie diese Erkennungen in den Status „Geschlossen“ verschieben, wird die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben in Ihrer Instanz Now Platform reduziert, und Sie können Assets in Ihrer CMDB abgleichen.

## Übersicht und wichtige Begriffe

Um ein genaueres Rollup für Erkennungsdaten zu Ihren angreifbaren Elementen durchzuführen, hilft Ihnen das Modul „Veraltete Erkennungen automatisch schließen“ bei der Bereinigung älterer, veralteter Erkennungen von angreifbaren Elementen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden. Weitere Informationen zu dieser Funktion finden Sie im folgenden Anwendungsfall und im Artikel Veraltete Erkennungen automatisch schließen [KB 0958638] .

In früheren Versionen von Vulnerability Responsehat das Modul „Angreifbare Elemente automatisch schließen“ automatisch angreifbare Elemente, die von Ihren Drittanbieter-Scanner-Integrationen nicht gefunden oder aktualisiert wurden, automatisch in den Status „Geschlossen – Veraltet“ überführt.

Bevor Sie die Funktion „Veraltete Erkennungen automatisch schließen“ aktivieren, überprüfen Sie die folgenden Begriffe, wie Status zu angreifbaren Elementen und Korrekturaufgaben zusammengefasst werden und welche Voraussetzungen für Ihre Drittanbieterintegrationen erfüllt sind, die Erkennungsdaten importieren.

Informationen zum Aktivieren der Funktion finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Wichtige Begriffe

**Veraltete Erkennungen**

Bezieht sich auf Erkennungen, die angreifbaren Elementen in Ihrer Instanz Now Platform® zugeordnet sind, die veraltet sind und seit längerer Zeit nicht mehr gefunden, aktualisiert oder durch Integrationsscans von Drittanbietern erkannt wurden.

**Zuletzt gefundene Erkennungen**

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner einer Drittpartei bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuelle oder letzte Datum und die letzte Uhrzeit, zu der Erkennungen vom Scanner erneut gefunden wurden.

**Zuletzt gescannte Assets**

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner einer Drittpartei bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuelle Datum und die aktuelle Uhrzeit, zu der ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.

## Anwendungsfall

Manchmal werden Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Drittanbieter-Scannern gelöscht, und die zugehörigen Erkennungen werden nicht durch Erkennungen von angreifbaren Elementen aktualisiert. Daher werden die Erkennungen und die zugehörigen angreifbaren Elemente in der Anwendung Vulnerability Response nicht aktualisiert und inaktiv (veraltet).

Um diese veralteten Erkennungen zu schließen, die unveränderte Daten zu angreifbaren Elementen aufweisen, und als nächstes die Anzahl der aktiven VIs und Korrekturaufgaben (RTs) zu reduzieren, aktivieren Sie Veraltete Erkennungen automatisch schließen. Diese Funktion schließt automatisch Erkennungen angreifbarer Elemente, die kürzlich nicht gefunden oder von Ihren Scanner-Integrationen einer Drittpartei basierend auf den von Ihnen festgelegten Suchkriterien und einem Alter in Tagen aktualisiert wurden.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) verfügt über mehrere Asset-IDs, und eine dieser IDs wurde in den letzten 90 Tagen nicht in eine Erkennung von einem Drittanbieter-Scanner importiert. Diese Funktion schließt automatisch diese Erkennung, die keine neuen Schwachstellendaten enthält, sodass die zugehörige VI geschlossen werden kann.

Da einem VI mehr als eine Erkennung zugeordnet sein kann, geht diese Funktion nur für die Erkennungen über, die durch die von Ihnen festgelegten Parameter als veraltet eingestuft wurden. Wenn beispielsweise einem AE vier Erkennungen zugeordnet sind und zwei Erkennungen veraltet sind, d. h. in den letzten 90 Tagen keine neuen Schwachstellendaten importiert wurden, schließt diese Funktion nur die veralteten Erkennungen. Bevor die VI geschlossen werden kann, müssen Sie zuerst die beiden anderen offenen Erkennungen beheben.

## Rollup von Erkennungsstatus zu AEs

Um die automatisch geschlossenen Erkennungen von Erkennungen zu unterscheiden, die von Scannern von Drittanbietern geschlossen wurden, wurde für das Feld Status der neue Wert Veraltet hinzugefügt. Die möglichen Werte für dieses Feld sind Offen, Geschlossen und Veraltet. „Veraltet“ gibt an, dass eine Erkennung durch die Erkennungsfunktion für automatisches Schließen geschlossen wurde.

Statusrangfolge: Offen > Geschlossen > Veraltet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn Erkennungen Offen sind, bleibt der zugehörige VI-Status Offen.
2. Wenn keine Erkennungen Offen, einige Geschlossen und andere Veraltet sind, geht der zugehörige VI-Status in Geschlossen – Behoben über.
3. Wenn alle Erkennungen „Veraltet“ sind, geht der zugehörige VI-Status in „Geschlossen – Veraltet“ über.

   Ab Vulnerability Response 20.0 befindet sich der zugeordnete AE im Status „Geschlossen“, wenn sich eine Erkennung im Status „Geschlossen – Veraltet“ befindet. Der Status des AE wechselt nicht in „Geschlossen – Veraltet“. Dadurch wird verhindert, dass der VI erneut geöffnet wird, wenn eine neue Erkennung erkannt wird, sodass Sie nicht den gesamten Prozess durchlaufen müssen. Um dieses Verhalten umzukehren, deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren** im Formular „Konfiguration für automatisches Schließen“. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

4. Wenn die Erkennung „Veraltet“ ist und sich der zugeordnete VI im Status „Geschlossen“ befindet, wechselt der Status des VI nicht in „Geschlossen – Veraltet“. Dadurch wird verhindert, dass der VI erneut geöffnet wird, wenn eine neue Erkennung erkannt wird, sodass Sie nicht den gesamten falsch positiven Anforderungs- und Genehmigungsprozess durchlaufen müssen. Um dieses Verhalten umzukehren, deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren** im Formular „Konfiguration für automatisches Schließen“. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

### Rollup von VI-Status zu Korrekturaufgaben (VUL)

Statusrangfolge: Offen > Geschlossen – Repariert > Geschlossen – Veraltet

1. Wenn VIs in einer VUL (Korrekturaufgabe) Offen sind, wird der VUL-Status nicht geändert.
2. Wenn mindestens ein VI „Geschlossen – repariert“ und der Rest „Geschlossen – Veraltet“ ist, geht der VUL-Status in „Geschlossen – repariert“ über.
3. Wenn alle VIs in einer VUL „Geschlossen – Veraltet“ sind, geht der VUL-Status in „Geschlossen – Abgebrochen“ über.

### Erkennungen für automatisches Schließen und Anforderungen für die Integration von Drittparteien

Microsoft TVM-Benutzer und Veraltete Erkennungen automatisch schließen

| Prüflistenelement | Beschreibung |
|---|---|
| Die Microsoft TVM-Schwachstellenintegration | Wenn Sie bei der Microsoft TVM Vulnerability Integration **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Ausführung der Microsoft TVM Machine Vulnerabilities Integration (Vollständiger Import) innerhalb der letzten sieben Tage. Diese Integration wird wöchentlich ausgeführt.<br><br>Wenn Veraltete Erkennungen automatisch schließen aktiviert und für **zuletzt gefundene Erkennungen**konfiguriert sind und die Integration von Microsoft TVM-Computer- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Prüflistenelement | Beschreibung |
| --- | --- |
| | Schwachstellen deaktiviert ist oder ein Datenimport innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen wurde, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, aber einige veraltete Erkennungen werden möglicherweise nicht wie erwartet geschlossen.<br><br>Wenn Sie **Zuletzt gescannte Assets** als Grundlage für Ihre Suche auswählen, ist die Ausführung von Microsoft TVM Machine Vulnerabilities Integration nicht erforderlich.<br><br>So aktivieren Sie diese Integration:<br><br>**1.** Navigieren zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integration**.<br><br>**2.** Suchen und aktivieren Sie **Microsoft TVM Machine Vulnerabilities Integration (Vollständiger Import)**. |
| (Optional) Stellen Sie mehrere Instanzen der Microsoft TVM-Integrationen in Ihrer Umgebung bereit. | Sie können optional mehrere Instanzen der Integrationen in Ihrer Umgebung bereitstellen.<br><br>Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden bei Instanzen, deren Integrationsausführungen erfolgreich abgeschlossen wurden, automatisch auf „Veraltet“ gesetzt.<br><br>Wenn Veraltete Erkennungen automatisch schließen aktiviert ist und Sie die wöchentlich in einer Instanz ausgeführten Integrationen deaktivieren, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, aber einige Erkennungen werden möglicherweise nicht wie erwartet in den Status „Veraltet“ versetzt. |

Qualys -Benutzer und Veraltete angreifbare Elemente automatisch schließen

- Alle aktivierten Qualys Drittanbieterintegrationen, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es sind keine spezifischen Qualys Anwendungen erforderlich.
- Sie können optional mehrere Instanzen der Qualys -Integrationen in Ihrer Umgebung bereitstellen.
- Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden in allen Instanzen automatisch auf „Veraltet“ gesetzt.

Rapid7 Benutzer und Veraltete Erkennungen automatisch schließen

| Prüflistenelement | Beschreibung |
| --- | --- |
| Die Rapid7 Schwachstellenintegration | Wenn Sie **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Ausführung |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Prüflistenelement | Beschreibung |
| --- | --- |
| | einer der Rapid7 Comprehensive Vulnerable Item Integrations (Integrationen von [] Comprehensive Vulnerable Item Integrations) innerhalb der letzten sieben Tage. Diese umfassenden Integrationen werden wöchentlich ausgeführt:<br>• Für das Data Warehouse Rapid7 Nexpose ist eine erfolgreiche Ausführung der Integration von Rapid7 Comprehensive Vulnerable Item Integration erforderlich.<br>• Für Rapid7 InsightVMist eine erfolgreiche Ausführung über die Rapid7 Comprehensive Vulnerable Item Integration – API erforderlich.<br><br>Wenn Veraltete Erkennungen automatisch schließen aktiviert und für **zuletzt gefundene Erkennungen**konfiguriert ist und die Integrationen von Rapid7 Comprehensive Vulnerable Items deaktiviert sind oder ein Datenimport innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen wurde, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, aber Einige veraltete Erkennungen werden möglicherweise nicht wie erwartet geschlossen.<br><br>Wenn Sie **Zuletzt gescannte Assets** als Grundlage für Ihre Suche auswählen, ist keine umfassende Rapid7 Integrationsausführung erforderlich.<br><br>So aktivieren Sie diese Integrationen:<br>1. Navigieren zu **Rapid7 Vulnerability Integration** > **Administration** > **Integration**.<br>2. Suchen und aktivieren Sie die Rapid7 Comprehensive Vulnerable Item Integration, die Sie benötigen.<br><br>**Hinweis:**<br><br>Zusätzlich zu diesen Integrationen, die wöchentlich ausgeführt werden, verfügen Rapid7 Nexpose und Rapid7 InsightVM jeweils über täglich ausgeführte VI-Integrationen, die Rapid7-Integration für angreifbare Elemente und die Rapid7-Integration für angreifbare Elemente – API.<br><br>Wenn sowohl die tägliche als auch die wöchentliche Rapid7 Integration aktiviert sind, wird jeweils nur eine Integration ausgeführt. Wenn eine dieser Integrationsaufgaben ausgeführt wird, wird die Aufgabe für die andere Integration bis zur nächsten geplanten Aufgabe übersprungen. |
| (Optional) Stellen Sie mehrere Instanzen der Rapid7 -Integrationen in Ihrer Umgebung bereit. | Sie können optional mehrere Instanzen der umfassenden Integrationen in Ihrer Umgebung bereitstellen.<br><br>Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Prüflistenelement | Beschreibung |
| --- | --- |
| | oder deaktiviert. Veraltete Erkennungen werden bei Instanzen, deren Integrationsausführungen erfolgreich abgeschlossen wurden, automatisch auf „Veraltet“ gesetzt.<br><br>Wenn Veraltete Erkennungen automatisch schließen aktiviert ist und Sie die Integrationen deaktivieren, die wöchentlich in einer Instanz ausgeführt werden, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, aber einige Erkennungen werden möglicherweise nicht wie erwartet in den Status „Veraltet“ versetzt. |

Anwender von Tenable Vulnerability Integration und Veraltete angreifbare Elemente automatisch schließen

- Alle aktivierten Integrationen aus der Integration von Tenable Vulnerability, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es sind keine spezifischen Tenable Vulnerability-Integrationen erforderlich.
- Sie können optional mehrere Instanzen der Tenable Vulnerability-Integration in Ihrer Umgebung bereitstellen.
- Veraltete Erkennungen automatisch schließen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden in allen Instanzen automatisch auf **„Veraltet“ gesetzt**.

Nachdem Sie sich vergewissert haben, dass Ihre Integrationen ordnungsgemäß konfiguriert sind, lesen Sie Veraltete Erkennungen in automatisch schließen Vulnerability Response, um die Funktion zu aktivieren.

## Aktualisieren Sie die Informationen von „Veraltete angreifbare Elemente automatisch schließen“ auf „Veraltete Erkennungen automatisch schließen“.

Wenn Sie für das Modul „Veraltete Erkennungen automatisch schließen“ zuvor „Veraltete angreifbare Elemente automatisch schließen“ verwendet haben:

- Der Wert für die Anzahl der Tage, die Sie für die Option **Zuletzt gescannte** Assets in Veraltete angreifbare Elemente automatisch schließen eingegeben haben, wird automatisch für **Assets** beibehalten, die zuletzt in Veraltete Erkennungen automatisch schließen gescannt wurden.
- Der Wert für die Anzahl der Tage, die Sie für die Option **Zuletzt gefunden angreifbare Elemente in** Veraltete angreifbare Elemente automatisch schließen eingegeben haben, wird automatisch für **Erkennungen beibehalten, die zuletzt in Veraltete Erkennungen automatisch schließen gefunden** wurden.
- Vorhandene offene Erkennungen mit „Geschlossen – Veraltet“ für angreifbare Elemente werden gemäß den Konfigurationseinstellungen für automatisches Schließen in „Veraltet“ überführt, wenn die geplante Aufgabe `Auto-Close Stale Detections` nach dem Upgrade ausgeführt wird.

Rollup-Informationen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn ein angreifbares Element vor dem Upgrade Geschlossen – Veraltet war und alle seine Erkennungen nach dem Upgrade als Veraltet markiert werden, bleibt der VI-Status Geschlossen – Veraltet.
- Wenn ein angreifbares Element vor dem Upgrade Geschlossen – Veraltet war und nur einige seiner Erkennungen nach dem Upgrade als Veraltet markiert sind und der Rest vom Scanner geschlossen wurde, wird das angreifbare Element gemäß der Rollup-Logik in Geschlossen – Repariert geändert.

### Veraltete Erkennungen in automatisch schließen Vulnerability Response

Aktivieren Sie Veraltete Erkennungen automatisch schließen, um veraltete angreifbare Erkennungen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden, automatisch zu schließen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vuln.admin (veraltet) oder ein Schwachstellenmanager mit der granularen Rolle sn_vul.manage_auto_close_stale_vi.

Weitere Informationen zu dieser Funktion, zu wichtigen Begriffen und zu allen Setups, die möglicherweise für Ihre Drittanbieterintegrationen erforderlich sind, die Erkennungsdaten importieren, finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

#### Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Konfiguration für automatisches Schließen** > **Veraltete Erkennungen**.
   Das Formular „Veraltete Konfiguration automatisch schließen“ wird angezeigt.
2. Füllen Sie die Felder aus.
3. Wählen Sie für das Feld **Veraltete Erkennungen automatisch schließen basierend auf** eine Option für Ihre Suche aus.

   Beide Suchvorgänge entsprechen dem Alter älterer, veralteter Erkennungen in Tagen bis zu einem von Ihrem Scanner bereitgestellten Datum.

   - **Zuletzt gefundene Erkennungen**. Mit dieser Option wird nach dem aktuellen oder letzten Datum gesucht, an dem Erkennungen erneut vom Scanner gefunden wurden.

     **Hinweis:**
     Für Rapid7 - und Microsoft TVM-Benutzer wird eine Warnmeldung angezeigt, dass aktuelle Erkennungsinformationen erforderlich sind.

     Wenn Sie **Zuletzt gefundene Erkennungen** auswählen, um Ihre Suche darauf zu stützen, erfordert diese Funktion eine erfolgreiche Integrationsausführung einer der Rapid7 Comprehensive Vulnerable Item-Integrationen innerhalb der letzten sieben Tage.

     Wenn Sie **Zuletzt gefundene Erkennungen** als Grundlage für Ihre Suche auswählen, erfordert diese Funktion eine erfolgreiche Integrationsausführung der Microsoft TVM-Integration von Computerschwachstellen (Vollständiger Import) innerhalb der letzten sieben Tage.

   - **Zuletzt gescannte Assets**. Mit dieser Option wird nach dem aktuellen Datum gesucht, an dem ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.
4. Vergewissern Sie sich nur für Rapid7 - und Microsoft TVM-Benutzer, dass alle erforderlichen Integrationen aktiviert sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Rapid7 Vulnerability Integration verstehen und Informationen zur Integration von Microsoft Threat and Vulnerability Management Vulnerability.

5. Um das Modul zu aktivieren, klicken Sie auf das Kontrollkästchen Aktiv, um es auszuwählen.
6. Geben Sie im Feld **Zuletzt gefundene Erkennungen (vor Tagen)** das Alter älterer, veralteter Erkennungen in Tagen ein.

   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben. Dieser Wert wird verwendet, um ein von Ihrem Scanner bereitgestelltes Datum abzugleichen. Wenn 90 und **Zuletzt gefundene Erkennungen** angezeigt werden, werden alle in den letzten 90 Tagen nicht gefundenen Erkennungen automatisch geschlossen. Wenn 90 und **Zuletzt gescannte Assets** angezeigt werden, werden alle Erkennungen, die mit Assets verknüpft sind, die in den letzten 90 Tagen nicht gescannt wurden, automatisch geschlossen.

   **Hinweis:**

   Es besteht eine Beziehung zwischen dem Feld **Zuletzt gefundene Erkennungen/ Zuletzt gescannte Assets (vor Tagen)** für diese Funktion und dem Feld **Importieren seit** in der Rapid7 Comprehensive Vulnerable Item Integration – API und der Microsoft TVM Machine Vulnerabilities-Integration.

   Für diese Integrationen ist das Feld **Importieren seit** auf den Konfigurationsseiten standardmäßig leer.

   Wenn Sie keinen Wert eingeben oder das Feld keinen Wert hat, werden die Daten für die Anzahl der im Feld **Zuletzt gefundene Erkennungen/Zuletzt gescannte Assets (vor Tagen)** konfigurierten Anzahl von Tagen verwendet.

   Beispiel: Wenn die Anzahl der im Formular für die automatische Schließung definierten Tage 90ist und das Feld **Importieren seit** auf den Integrationskonfigurationsseiten leer ist, werden bei der ersten Integrationsausführung die Daten für die letzten 90 Tage importiert. Die Felder „ **Importieren seit** “ für die Integration von Rapid7 Comprehensive Vulnerable Item Integration – API und die Integration von Microsoft TVM Machine Vulnerabilities können bearbeitet werden, sodass Sie auch beliebige Werte angeben können. Der 90-Tage-Wert wird als Standard angegeben, wenn das Feld leer bleibt, damit die Funktion zum automatischen Schließen die Falschmeldungen nicht schließt.

   Diese Beziehung zwischen diesen Feldern gilt nur für die erste Integrationsausführung. Danach hat eine Änderung des **Felds Zuletzt gefundene Erkennungen/Zuletzt gescannte Assets (vor Tagen)** im Formular „Veraltete angreifbare Erkennungen automatisch schließen“ keine Auswirkungen auf das Feld **Importieren seit** auf den Integrationskonfigurationsseiten. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass bei nachfolgenden Integrationsausführungen nur die Delta-Informationen importiert werden.

7. **Wahlweise:** Aktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für zurückgestellte AEs** ignorieren, um veraltete Erkennungen zu ignorieren, die zurückgestellten AEs oder AEs zugeordnet sind, die derzeit auf Zurückstellung überprüft werden.

   (Optional) Wenn Sie diese Option deaktiviert lassen, werden alle Erkennungen geschlossen, die Ihren Kriterien entsprechen und zurückgestellten VIs oder VIs zugeordnet sind, die zur Zurückstellung überprüft werden. Die zurückgestellten VIs oder VIs, die überprüft werden und diesen Erkennungen entsprechen, werden basierend auf



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Rollup-Logik ebenfalls automatisch geschlossen. Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

Wenn Sie diese Option aktivieren, werden beim automatischen Schließen alle Erkennungen übersprungen, die Ihren Kriterien entsprechen und zurückgestellten VIs oder VIs zugeordnet sind, die zur Zurückstellung überprüft werden.

8. **Wahlweise:** Deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren**.
Standardmäßig ist diese Checkbox aktiviert, damit die geschlossene VI nicht erneut geöffnet wird, wenn eine neue Erkennung im Zusammenhang mit dieser geschlossenen VI erkannt wird.

   (Optional) Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response.

9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

   Die regelmäßige Aufgabe Veraltete Erkennungen automatisch schließen wird täglich ausgeführt. Die Aufgabe gibt an, ob Sie das Datum ausgewählt haben, an dem Erkennungen zuletzt gefunden wurden, oder ob das Datum, an dem Assets zuletzt gescannt wurden. Die entsprechenden Erkennungen gehen in den Status „Veraltet“ über. Die Funktion „Veraltete Erkennung automatisch schließen“ schließt veraltete Erkennungen nur für aktive Integrationsinstanzen. Die angreifbaren Elemente und Erkennungen, die aktiven Integrationsinstanzen zugeordnet sind, werden geschlossen.

   Nachdem die Erkennungen als Veraltet markiert wurden und der Scanner meldet, dass diese Erkennung erneut gefunden wurde, wird das Feld Status der Erkennungen in „Offen“ geändert. Die entsprechenden angreifbaren Elemente der Erkennung werden ebenfalls erneut geöffnet.

   Wenn die Erkennung außerdem als Veraltet markiert ist und der Scanner feststellt, dass sie behoben ist, geht die Erkennung in Geschlossen über. Für den Status wird auch ein Rollup zu den AEs durchgeführt.

## Erstellen Sie eine Korrekturaufgabe manuell in Vulnerability Response

Das manuelle Erstellen einer Korrekturaufgabe erfolgt, wenn Sie angreifbare Elemente nach etwas anderem als den Kriterien für Korrekturaufgabenregeln gruppieren möchten. Sie können beispielsweise Aufgaben für einen bestimmten Manager oder für aktive, neue Exploits wie Ransomware erstellen, die verschiedene Schwachstellen enthalten. Sie können sie auch verwenden, um nicht gruppierte angreifbare Elemente zu gruppieren.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.

   Korrekturaufgabenregeln funktionieren genauso wie zuvor Regeln für Schwachstellengruppen und stehen Ihnen weiterhin zur Verfügung. Möglicherweise möchten Sie die Regeln für Korrekturaufgaben jedoch inaktiv lassen, da Sie sich an die Funktionen vertraut gemacht haben, die Ihren Sicherheitsmanagern und IT-Teams in den Arbeitsbereichen zur Verfügung stehen.

2. Wählen Sie eine der Kategorien für Aufgaben aus, um die Liste zu öffnen.

3. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu bestimmten Feldern finden Sie unter Felder des Formulars „Korrekturaufgabe“..
5. Klicken Sie auf **Absenden**.
   Wenn die Aufgabe erstellt wird, sucht die zugehörige Liste „Angreifbares Element“ mit dem **Filtertyp** „ **Bedingung** “ oder **„Filtergruppe** “ nach allen übereinstimmenden angreifbaren Elementen und zeigt sie an.

   Sie können den zugehörigen Link **Erneut auf Schwachstellen scannen** verwenden, um einen von ServiceNow® initiierten Scan manuell auszulösen. Informationen zum Konfigurieren eines Schwachstellenscanners finden Sie unter Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und -scans.

   Für eine Qualys Vulnerability-Integration ist ein Standardscanner im Modul „ **Schwachstellenscanner“** vorinstalliert. Dieser Scanner ist standardmäßig deaktiviert. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Standard**, um den Qualys-Scanner so zu aktivieren, dass er mit dem zugehörigen Link Auf Schwachstellen scannen in den Formularen **für** Korrekturaufgaben und angreifbare Elemente funktioniert.

   Der zugehörige Link **Aktualisierungsstatus** zeigt das Datum und die Uhrzeit der letzten Aktualisierung an. Es werden Informationen aus den AEs in der Korrekturaufgabe zusammengefasst. Weitere Informationen finden Sie unter Felder des Formulars „Korrekturaufgabe“.. Wenn eine Aufgabe basierend auf einer bestimmten Schwachstelle erstellt wird, wird diese Schwachstelle im Korrekturaufgabenformular aufgelistet.

   Wenn Sie ein zugeordnetes angreifbares Element öffnen, werden alle zugeordneten Korrekturaufgabeneinträge auf der **Registerkarte** der zugehörigen Liste Korrekturaufgabe angezeigt.

### Fügen Sie der Vulnerability Response-Gruppe Benutzer hinzu

Wenn die Funktion Schließen/Zurückstellen verwendet wird, um ein angreifbares Element zurückzustellen oder zu schließen, ohne dass ein Scan erforderlich ist, wird die Gruppe Vulnerability Response benachrichtigt, um die Anforderung zu genehmigen oder abzulehnen. Sie können die entsprechenden Benutzer zuweisen.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.
2. Öffnen Sie die Gruppe Vulnerability Response.
3. Klicken Sie auf die zugehörige Liste **Gruppenmitglieder** und dann auf **Bearbeiten**.
4. Wählen Sie einen oder mehrere Namen in der Liste **Sammlung** aus.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**.

#### Zugehörige Informationen

Einen Benutzer erstellen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verwalten Sie einzelne angreifbare Elemente manuell

Angreifbare Elemente stellen ein Konfigurationselement (CI) mit einer bestimmten Schwachstelle dar. Angreifbare Elemente werden aus Quellen von Drittanbietern importiert oder verwenden die SAM-NVD-Informationen (Link), um Schwachstelleneinträge mit Softwaredatensätzen zu vergleichen, die aus dem Softwaremodul Asset-Management abgerufen wurden.

Angreifbare Elemente sind in Korrekturaufgaben enthalten, die durch Schwachstellenregeln definiert sind. Normalerweise sind Korrekturaufgaben der Ort, an dem Gruppen angreifbarer Elemente zugewiesen und bearbeitet werden.

Angreifbare Elemente können im Modul „ **Angreifbare** Elemente“ in einem Massenvorgang angezeigt und bearbeitet werden. Datensätze für angreifbare Elemente zeigen Informationen aus der Schwachstelle auf der Registerkarte **Schwachstelle** an. Auf dieser Registerkarte kann angegeben werden, ob öffentliche oder aktive Exploits dafür vorhanden sind. Außerdem wird angezeigt, ob dies durch einen Patch, eine Konfigurationsänderung oder eine Kombination aus beidem behoben werden kann. Wenn während der Deduplizierung IP-Adressen gefunden werden, werden sie in einer zugehörigen Liste angezeigt.

Wenn ein CI aus der CMDB entfernt wird, werden auch alle zugehörigen angreifbaren Elemente entfernt.

Wenn einer Korrekturaufgabe ein angreifbares Element hinzugefügt wird, wird die Gruppe in der Liste Korrekturaufgaben der **angreifbaren** Elemente angezeigt.

Wenn eine Aufgabe erstellt wird, die sich auf ein angreifbares Element auswirkt, wird die Aufgabe in der zugehörigen Liste „ **Betreffende Aufgaben** “ der angreifbaren Elemente angezeigt.

Angreifbare Elemente können manuell erstellt werden. Sie können Security Incidents oder Change-Anforderungen erstellen und manuell schließen oder zurückstellen. Regeln für Korrekturaufgaben können auf manuell erstellte angreifbare Elemente angewendet werden.

Korrekturaufgaben und Regeln für Korrekturaufgaben wurden erweitert, um die Aufgabenfunktionalität zu übernehmen. Angreifbare Elemente können nicht als übergeordnete Aufgabe verknüpft werden.

### Erstellen Sie Vulnerability Response angreifbare Elemente

Mehrere Methoden erstellen angreifbare Elemente (VI). In den meisten Fällen wird eine Integration mit einem Schwachstellenscanner installiert und so konfiguriert, dass die Ergebnisse jede Nacht importiert werden. Es gibt Fälle, z. B. bei physischen Sicherheitsschwachstellen, in denen Sie Datensätze für angreifbare Elemente manuell hinzufügen möchten.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

#### Warum und wann dieser Vorgang ausgeführt wird

Manuell erstellte VIs und automatisch erstellte VIs werden durch Korrekturaufgabenregeln und Gruppenbedingungen automatisch hinzugefügt und aus Korrekturaufgaben entfernt.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Wählen Sie eine Kategorie aus, um die Liste zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.
   Informationen zu den Feldern für angreifbare Elemente finden Sie unter, Vulnerability Response Formularfelder für angreifbare Elemente.
5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.

   Die Regeln für Korrekturaufgaben werten das angreifbare Element aus und fügen es einer vorhandenen Aufgabe hinzu oder erstellen eine neue Aufgabe. Wenn die Auswertung fehlschlägt, wird das angreifbare Element der Liste der nicht **gruppierten** angreifbaren Elemente hinzugefügt.

   Wenn Sie ein neues angreifbares Element speichern, werden alle aktivierten Rechner ausgeführt.

   **Hinweis:**
   Pro **Zielfeld** darf jeweils nur ein Rechner aktiv sein. Wenn Sie eines aktivieren, werden alle anderen mit demselben **Zielfeld** deaktiviert.

6. Sie können auf eine der zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

   Sie können den zugehörigen Link Nach Schwachstellen scannen verwenden, um einen von ServiceNow® initiierten **Scan** manuell auszulösen. Informationen zum Konfigurieren eines Schwachstellenscanners finden Sie unter Konfigurieren und verwalten Sie Qualys Schwachstellenscanner und -scans.

   Für eine Qualys Vulnerability-Integration ist ein Standardscanner im Modul „ **Schwachstellenscanner“** vorinstalliert. Dieser Scanner ist standardmäßig deaktiviert. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Standard**, um den Qualys-Scanner so zu aktivieren, dass er mit dem zugehörigen Link Auf Schwachstellen scannen in den Formularen **für** Korrekturaufgaben und angreifbare Elemente funktioniert.

   Die folgenden Bearbeitungs- und Korrekturoptionen werden in der Headerleiste verfügbar:

   - Aktualisieren: Speichert Aktualisierungen im Formular.
   - Security Incident erstellen: Erstellt einen Security Incident.
   - Schließen: Schließt das Element. Wenn alle Elemente in der Gruppe geschlossen sind, wird die Korrekturaufgabe automatisch geschlossen.
   - Ausnahme anfordern: Sendet eine Anforderung zum Zurückstellen eines Elements.
   - Auflösen: Löst das Element auf.
   - Löschen: Entfernt das angreifbare Element.

**Zugehörige Informationen**

Bearbeiten Sie angreifbare Elemente im Massenvorgang in Vulnerability Response

## Zurückstellen eines angreifbaren Elements

Wenn Sie feststellen, dass das mit einem angreifbaren Element (VIT) verbundene Problem ein geringes Risiko aufweist und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion „ **Zurückstellen** “ verwenden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

Eine regelmäßige Aufgabe wird täglich ausgeführt und überprüft, ob zurückgestellte angreifbare Elemente vorhanden sind, deren Datum der Wiedereröffnung erreicht wurde. An dem Tag, an dem die Zurückstellung des VI abläuft, wird der Datensatz erneut geöffnet.

Ab Vulnerability Responsev20.0 wird vor dem erneuten Öffnen eines zurückgestellten AE geprüft, ob eine Ausnahmeregel für einen zurückgestellten AE gilt, und die Felder **Grund** und **Bis** werden gemäß der Ausnahmeregel aktualisiert. Der Status des AEs bleibt bis zum letzten Ablaufdatum zurückgestellt.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie **auf Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Bis | Wählen Sie das Datum aus, an dem der Status „Zurückgestellt“ abläuft und die Korrekturaufgabe erneut aktiviert wird.<br><br>**Hinweis:**<br>Ab Version 18.0 von Vulnerability Response (VR) wird der Status der VIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ zurückgesetzt, wenn ein zurückgestelltes angreifbares Element geschlossen und von einem Scanner erneut geöffnet wird, bevor das Ausnahmefenster abläuft. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_vit_in_active_exception_window auf true fest. Außerdem bleibt das zurückgestellte Bis-Datum bestehen, auch nachdem das angreifbare Element geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle ist sn_vul.manage_exception_configuration für Lese- und Schreibvorgänge.<br><br>Nachdem der Datensatz übermittelt wurde und E- Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Ablaufdatum innerhalb einer Woche liegt. Nach Ablauf des Zurückstellungsdatums wird das angreifbare Element auf „Offen“ zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Falsch positiv<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Klicken Sie auf **Absenden**.
   Die Gruppe wird als Wird **überprüft**gekennzeichnet. Ein **zugehöriger** Link Erneut öffnen wird angezeigt. Das Datum und der Grund für die Wiedereröffnung werden in Arbeitsnotizen auf der Registerkarte **Status-Change-Genehmigungen** angezeigt.

### Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor das Fälligkeitsdatum erreicht ist. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Element.
3. Wählen Sie **Verlängerung anfordern aus**.

> **Hinweis:**
> Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Elements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Elements verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Nach der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   **Hinweis:**
   - Die Anforderung durchläuft zwei Genehmigungsstufen.
   - Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Notizen für Bis, Grund und Zurückstellung aktualisiert.

### Aktualisieren Sie Vulnerability Response angreifbare Elemente

Der zugehörige Link **Status** aktualisieren wird verwendet, um angreifbare Elemente zu überprüfen, um festzustellen, ob zusätzliche angreifbare Elemente vorhanden sind, die zu einer Korrekturaufgabe gehören. Verwenden Sie diese Option, wenn eine Aktualisierung außerhalb der geplanten Aufgabe gerechtfertigt ist.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write oder, sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)
Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Der zugehörige Link **Status** aktualisieren kann nur im Korrekturaufgabenformular im Status „ **Offen** “ oder „ **Wird untersucht** “ bearbeitet werden, indem eine Filtergruppe verwendet wird oder der Filtertyp



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Bedingung“ ist. Diese Inspektion wird unabhängig vom Status des Kontrollkästchens **Angreifbare Elemente automatisch aktualisieren** durchgeführt.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen beliebigen Datensatz im Status „ **Offen“** oder **„Wird untersucht** “.
3. Klicken Sie auf den Link **Status** aktualisieren.
   Neue angreifbare Elemente werden auf der Registerkarte **Angreifbare** Elemente angezeigt.

## Identifizieren und eskalieren Sie Sicherheitsprobleme in Software von Drittanbietern

Sie können Software-Schwachstellen anzeigen, die von Einträgen von Drittanbietern zurückgegeben werden, um die Behebung zu bestimmen. Verwenden Sie diese Informationen, um die Einträge angreifbarer Software mit einem Software-Discovery-Modell Asset-Management abzugleichen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **Drittpartei**.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.
3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zum Identifizieren von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie nach Bedarf Korrekturaufgaben lösen.

## Identifizieren und eskalieren Sie Sicherheitsprobleme mit NVD

Wenn CVE-ID-Datensätze (Common Vulnerability and Exposures Identifier) aus der National Vulnerability Database (NVD) heruntergeladen werden, werden sie mit der Software in Ihrem Unternehmensnetzwerk verglichen, die vom Software Asset Discovery-Modell identifiziert wird. Wenn eine CVE-ID mit angreifbarer Software oder einem Konfigurationselement in Ihrem Netzwerk übereinstimmt, wird ein angreifbares Element erstellt. Sie verwenden die Informationen im CVE-ID-Datensatz, um zu entscheiden, ob das angreifbare Element zur Korrektur eskaliert werden soll.

### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **NVD**.
   Eine Liste der CVE-IDs, die vom NVD heruntergeladen wurden, wird angezeigt. Updates aus dem NVD können bei Bedarf und durch geplante Ausführungen aus den NIST National Vulnerability Database Integration-Datensätzen unter durchgeführt werden **Alle** > **Administration** > **Integrationen**.
2. Klicken Sie auf einen CVE-Datensatz, um die folgenden Informationen anzuzeigen:
   - eine Zusammenfassung für die CVE-ID.
   - ein Verweis auf einen CWE-Eintrag (Common Weakness Enumeration), falls zutreffend.
   - Die Schwachstellenpunktzahl der CVE-ID im Common Vulnerability Scoring System (CVSS). Weitere Informationen zu CVSS finden Sie auf der Website der National Vulnerability Database .
3. Klicken Sie auf die zugehörigen Listen, um weitere Informationen zu Schwachstellen zu erhalten.

   **Verwundbarkeitsreferenzen**

   Name, Beschreibung und URL für die angegebene Schwachstelle und Verweis darauf.

   **Exploits**

   Details

   **Schwachstellen**

   Liste der CWE-Schwächen.
4. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zum Identifizieren von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie nach Bedarf Korrekturaufgaben lösen.

## Identifizieren und eskalieren Sie Sicherheitsprobleme mit CWE

Zeigen Sie die Bibliothek von CWE-Datensätzen (Common Weakness Enumeration) aus der National Vulnerability Database (NVD) an, um zu verstehen, wie sie sich auf die CVE-Datensätze (Common Weakness Enumeration) beziehen. Verwenden Sie dann diese Informationen, um die Einträge der angreifbaren Software mit einem Software-Discovery-Modell Asset-Management abzugleichen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_write

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **CWE**.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen CWE-Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.
3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zum Identifizieren von Schwachstellen zu erhalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeigen Sie den Status des Korrekturziels eines Vulnerability Response angreifbaren Elements an

Wenn ein angreifbares Element sein Korrekturzieldatum fast erreicht (oder überschritten) hat, wie durch eine Korrekturzielregel definiert, wird der Datensatz des angreifbaren Elements mit einem Status aktualisiert. Diese Informationen können dem Analysten helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

#### Vorbereitungen

Erforderliche Rolle:
sn_vul.vulnerability_admin

sn_vul.read_remediation_target_rules [schreibgeschützt]

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Eine regelmäßige Aufgabe mit der Bezeichnung **Korrekturziele evaluieren** wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl von Tagen liegt, bevor die Korrektur überfällig ist, wird dem Datensatz des angreifbaren Elements ein Korrekturstatus hinzugefügt.

Weitere Informationen zu Korrekturzielregeln finden Sie unter Vulnerability Response Korrekturzielregeln.

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Angreifbare Elemente**.
2. Klicken Sie auf das angreifbare Element, das Sie überprüfen möchten.
   Wenn das Korrekturdatum für das angreifbare Element innerhalb des Bereichs der in der Korrekturzielregel festgelegten Bedingungen liegt, ist die Registerkarte **Status** des Korrekturziels sichtbar.
3. Klicken Sie auf die Registerkarte **Status** des Korrekturziels.
4. Klicken Sie auf den Statusdatensatz des Korrekturziels, um ihn zu überprüfen.

**Hinweis:**
Informationen zum Anzeigen der Anzahl der angreifbaren Elemente mit dem Status „Ziel erreicht“, „In Ausführung“ und „Vergangenes Ziel“ finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.

#### Zugehörige Informationen

Erstellen oder bearbeiten Sie Vulnerability Response Korrekturzielregeln

## Arbeiten mit nicht abgeglichenen CIs

Als Schwachstellenmanager und Analyst können Sie nicht abgeglichene Konfigurationselemente (CIs) anzeigen und neu klassifizieren, nicht abgeglichene erkannte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente abstimmen, CI-Suchregeln auf die ausgewählten erkannten Elemente erneut anwenden und vorhandene CIs deduplizieren.

### Nicht klassifizierte Hardware neu klassifizieren

Klassifizieren Sie nicht klassifizierte Hardware neu, indem Sie die CI-Suchregeln aktualisieren.

**Vorbereitungen**
Erforderliche Rolle: sn_sec_cmn.admin

**Warum und wann dieser Vorgang ausgeführt wird**
In der Tabelle „Hostimportzuordnung“ [sn_sec_cmn_src_cmdb_map] werden die eingehenden Variablen der Nutzlast und ihre entsprechenden Zuweisungen in der Tabelle „Erkannte Elemente“ angezeigt. Gelegentlich können Diskrepanzen in den Namenskonventionen zwischen Scanner und Discovery dazu führen, dass die Hardware nicht klassifiziert wird. Stellen Sie beim Erstellen eines neuen nicht klassifizierten Hardware-CI sicher, dass der Name in der Nutzlast nur den Hostnamen enthält. Später, wenn Discovery das Asset identifiziert, kann es in die entsprechende CI-Klasse neu klassifiziert werden. Bei Bedarf kann ein Skript geschrieben werden, um einen abgeleiteten Wert zu generieren, der mit dem CI-Namen in Discovery und der Configuration Management Database (CMDB) übereinstimmt.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option zum erneuten Klassifizieren von erkannten Elementen nicht unterstützt.

**Prozedur**

1. Navigieren zu **Alle** > **Vulnerability Response** > **Hostimportzuordnungen**.
2. Wählen Sie eine Quelle aus.
3. Wählen Sie in der Liste Zielfeld die Option **Name**aus.
   Die **Checkbox Skript** verwenden wird sichtbar.

   **Hinweis:**
   - Das Skript ist nur verfügbar, wenn **Name** aus der Liste Zielfeld ausgewählt wird.
   - Um ein Skript für andere Optionen in der Zielfeldliste hinzuzufügen, müssen Sie die UI-Richtlinie wie folgt deaktivieren:
     - Deaktivierung von „Set Use script false“ (Verwendungsskript auf „falsch“ festlegen).
     - Deaktivierung von „Verwendungsskript anzeigen oder ausblenden“.
     - Entfernen der Bedingung „Zielfeld ist Name“ in „Skriptrichtlinie anzeigen oder ausblenden“.
   - Die Tabelle „Hostimportzuordnungen“ wird mit zwei neuen Spalten aktualisiert: Skript und Skript verwenden.
4. Aktivieren Sie das Kontrollkästchen **Skript** verwenden.
   Im Feld **Skript** wird das Standardskript angezeigt, Sie haben jedoch die Möglichkeit, ein benutzerdefiniertes Skript zu erstellen. In diesem Feld können Sie die Quell- und abgeleiteten Werte angeben, um sie an der Benennungskonvention der Datenbank auszurichten. Der vom Skript generierte Wert wird in sourcePayload['Derived'][rule.source_field] gespeichert. Stellen Sie sicher, dass die CI-Suchregeln so angepasst sind, dass beim Einchecken der entsprechenden Tabellen Quellnutzlast-, abgeleitete und Zielattributwerte verwendet werden.
5. Gehen Sie wie folgt vor, um das Skript auf ältere doppelte Datensätze anzuwenden:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Vulnerability Response Erkannte Elemente**

b. Wählen Sie die doppelten Datensätze aus.

c. Wählen Sie in der Liste Aktion für ausgewählte Zeilen die **Option CI-Suchregeln erneut anwenden aus**.
Zeigt eine Übereinstimmung mit einem vorhandenen Asset an.

6. Gehen Sie wie folgt vor, um das Skript für Tenable.ioanzuwenden:

a. Navigieren zu **Vulnerability Response Hostimportzuordnungen**.

b. Wählen Sie das Skript für die Zeile mit NetBIOS-, HOSTNAMES- und FQDNS-Namen als **Quellfeld** aus.

c. Aktualisieren Sie das Skript für jedes Element.

**Hinweis:**
Für Tenable.iogibt der Scanner ein Array für NetBIOS, HOSTNAMES und FQDNS-Namen zurück, für das das Skript nicht wie erwartet funktioniert.

Da die Host-Importzuordnung für Tenable.io**netBIOS_name** im Feld **Quelle** enthält, müssen Sie ein Skript schreiben. Während der Suche wird ein anderes Quellfeld, **NETBIOS**, verwendet, das ein Array von Werten enthält. Daher wird der Tabelle eine neue Zeile hinzugefügt, und dieselbe Logik muss in eine Schleife im Skript geschrieben werden. Ebenso für **FQDNS** und **HOSTNAMES**.

7. Gehen Sie wie folgt vor, um das Skript für Rapid7anzuwenden:

a. Navigieren zu **Alle** > **Vulnerability Response Hostimportzuordnungen**.

b. Aktualisieren Sie für Rapid7 Zeilen mit FQDN und Hostname die Suchmethode auf Skript.

**Hinweis:**
Für Rapid7wird die CI-Suchmethode auf Feld für FQDN und Hostname festgelegt, wodurch verhindert wird, dass das Skript verwendet wird.

### Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren

Konfigurationselemente (CIs), die nicht in Configuration Management Database (CMDB) gefunden werden, werden in eine sichtbare Liste der erkannten Elemente platziert. Diese Liste bietet eine praktische Möglichkeit, nicht abgeglichene CIs neu zu klassifizieren.

### Vorbereitungen

Erforderliche Rolle:
sn_vul.read (mindestens, um nicht abgeglichene CIs anzuzeigen)

und

itil oder Asset (zur Neuklassifizierung)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird
Als Schwachstellenanalyst können Sie nicht abgeglichene CIs anzeigen.

Die Aktion zum erneuten Klassifizieren ist nur für CIs der Klasse `sn_sec_cmn_unmatched_ci` verfügbar, wenn Sie über die Rollen „itil“ oder „asset“ verfügen. Sobald ein CI neu klassifiziert wurde, kann es nicht mehr über die Benutzeroberfläche neu klassifiziert werden. Sie können im CI-Formular oder in der CI-Listenansicht eine Neuklassifizierung durchführen, indem Sie den **Klassenwert** ändern. Weitere Informationen finden Sie unter Reclassify a CI .

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**.
2. Klicken Sie zur Überprüfung auf jedes Element.
3. Um Korrekturen an den Informationen in den Feldern des Formulars „ **Erkanntes Element** “ vorzunehmen, bearbeiten Sie sie auf dieser Seite, und klicken Sie mit der rechten Maustaste auf **Speichern**. Alle Daten, die diesen Feldern hinzugefügt oder darin belassen werden, werden bei der Neuklassifizierung in das resultierende **Konfigurationselement** übertragen.
4. Wenn alles richtig aussieht, klicken Sie auf **Neu klassifizieren**.
5. Wählen Sie in der Auswahlliste einen **Klassennamen** aus, und klicken Sie auf **Absenden**. Die **erkannte Elementklasse** wird aktualisiert, das **Feld Status** wird in Reklassifiziert geändert, und alle Daten befinden sich in der CMDB.

## Nicht übereinstimmende erkannte Elemente abstimmen

Erstellen Sie eine regelmäßige Aufgabe, um nicht abgeglichene erkannte Elemente abzugleichen.

### Vorbereitungen
Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird
Ein angreifbares Element (VI) besteht aus einer Schwachstelle und einem Konfigurationselement (CI). Wenn eine VI erstellt wird, ist das CI, das ihr zum Zeitpunkt der Erstellung hinzugefügt wird, möglicherweise veraltet. Nicht abgeglichene CI-Informationen werden nicht abgeglichen, wenn sich die Informationen in der CMDB ändern. Wenden Sie zum Abgleichen Suchregeln für Konfigurationselemente (Configuration Item, CI) auf die Elemente an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.

Sie können einen geplanten Aufgabenbedarf ausführen, um die CI-Übereinstimmungsregel für die erkannten Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach der erneuten Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Erkennungen und angreifbare Elemente werden ebenfalls aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente.

### Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge > Nicht abgeglichene erkannte Elemente abgleichen**.
2. Klicken Sie auf der Seite „Hintergrundaufträge“ auf **Abgleichsauftrag erstellen**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können nur das Feld **Parameter** bearbeiten.

**Formular „Hintergrundauftrag“.**

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Auftragsnummer. |
| Erstellt von | Benutzer, der die Aufgabe erstellt hat. |
| Parameter | Parameter zum Abgleichen der nicht abgeglichenen erkannten Elemente:<br>○ limit: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen.<br>○ firstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichprozess mit dem ersten erkannten Element. |
| Status | Aktueller Status des Hintergrundauftrags. |
| Statusbeschreibung | Beschreibung des aktuellen Status des Hintergrundauftrags. |
| Auftragstyp | Typ des Auftrags. Der Wert ist **Nicht abgeglichene erkannte Elemente abgleichen**. |
| Gestartet um | Zeit, zu der der Auftrag gestartet wurde. |
| Endete um | Zeitpunkt, zu dem der Auftrag abgeschlossen wurde. |
| Auftragsdauer | Gesamtzeit, die für den Abschluss der Aufgabe benötigt wurde. |
| Substatus | Substatus für den ausgewählten Status. |
| Notizen | Anzahl der verarbeiteten Datensätze. |

4. Klicken Sie auf **Absenden**.

**Hinweis:**
- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen**.
- Sie können nicht abgeglichene CIs nicht abgleichen oder CI-Suchregeln erneut anwenden, während Sie Hosts oder angreifbare Elemente importieren.

### Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente an

Wenden Sie die Suchregeln für Konfigurationselemente (Configuration Item, CI) erneut auf ausgewählte erkannte Elemente aus der Listenansicht der erkannten Elemente an. Wenn sich das CI ändert, nachdem Sie die Regeln erneut angewendet haben, werden die erkannten Elemente mit dem neuen CI und den betroffenen Erkennungen aktualisiert. Angreifbare Elemente werden ebenfalls aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

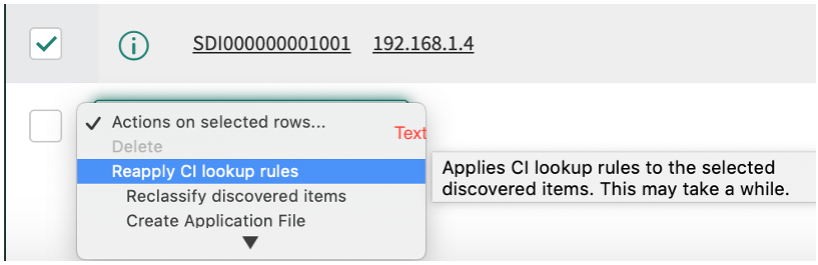
### Vorbereitungen
Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente.

Weitere Informationen zu den Konzepten des CI-Abgleichs und der CMDB, der Suche nach erkannten Elementen, der regelbasierten Identifizierung und andere detaillierte Informationen zur Funktionsweise des CI-Abgleichs finden Sie im Artikel CI-Abgleich in Vulnerability Response [KB0998706] in der HI Knowledge Base.

### Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge** > **CMDB** > **Erkannte Elemente**.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie **auf Aktion für ausgewählte Zeilen**.




3. Wählen Sie in der Liste **CI-Suchregeln erneut anwenden aus**.

   Die Regeln werden auf diese erkannten Elemente erneut angewendet.

4. Klicken Sie in der Nachricht auf **Status** anzeigen.

   Der Status wird im Hintergrundauftragsformular angezeigt.

**Hinweis:**
Im Feld **Notizen** gibt das Attribut Erkannte Elemente konnten aufgrund einer Ausnahme nicht verarbeitet werden mit einem Wert ungleich Null an, dass beim erneuten Anwenden einer CI-Suchregel ein Fehler oder eine Ausnahme aufgetreten ist. Überprüfen Sie die Systemprotokolle auf weitere Details.

### Schritte zum Verhindern doppelter oder verwaister Datensätze nach dem Ausführen von Vulnerability Response CI-Suchregeln

Ergreifen Sie Maßnahmen, um doppelte oder verwaiste Datensätze zu verhindern, die aus dem Abgleich von (Konfigurationselementen (CIs) innerhalb von CMDBresultieren).

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Durchlaufen und Abgleichen in der CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Gründliches Testen und Debuggen von Verarbeitungsskripts in den Regeln trägt dazu bei, das Risiko später im Prozess auftretender Probleme zu verringern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Doppelte oder verwaiste Datensätze werden verhindert

- Verwenden Sie kleine Teilmengen von Daten, die für die getestete CI-Suchregel spezifisch sind.
  - Setzen Sie alle CI-Suchregeln, mit Ausnahme der getesteten, auf Inaktiv.
  - Analysieren Sie die importierten CIs, um sicherzustellen, dass Sie das erwartete Verhalten beobachten und die Übereinstimmung ordnungsgemäß erfolgt.
- Überprüfen Sie die übereinstimmenden CIs
  - Untersuchen Sie die Anzahl der übereinstimmenden im Vergleich zu nicht übereinstimmenden CIs. Stellen Sie sicher, dass der Prozentsatz akzeptabel ist. Schauen Sie sich nicht nur die erste Seite an, das ist wahrscheinlich die erste eingefügte.
  - Suchen Sie manuell nach CIs.
  - Überprüfen Sie, ob Benennungs- oder Feldprobleme vorliegen (z. B. Suche nach einer bestimmten Domäne).

    Wenn es angemessen erscheint, fügen Sie zusätzliche Übereinstimmungsregeln hinzu.
- Überprüfen Sie nicht abgeglichene CIs
  - Navigieren Sie zur Tabelle Nicht abgeglichene CIs.
  - Nach Klasse des Konfigurationselements gruppieren.
  - Überprüfen Sie alle Klassen, die nicht richtig aussehen (Zertifikate, Netzwerkkarten, Images).
    - Finden Sie heraus, warum sie nicht mit dem richtigen CI übereinstimmten.
    - Soll die Klasse ausgeschlossen werden?
    - Soll die Klasse auf eine zugehörige Klasse hochgestuft werden?
- Überprüfen Sie CI-Status wie **Deaktiviert**.
- Entfernen Sie die Testdaten
  - Sobald Sie das richtige oder erwartete Verhalten bei der CI-Übereinstimmung beobachten, beginnen Sie von vorne.
  - Neu beginnen durch: Löschen der zum Testen verwendeten Daten: (siehe Abschnitt „**Daten aus Tabellen** löschen“)
    - Erkannte Elemente
    - Angreifbare Elemente
    - Korrekturaufgaben
  - Alle CI-Übereinstimmungsregeln werden manuell erneut ausgeführt.

Weitere Informationen zu CI-Suchregeln und Qualysfinden Sie im Artikel KB0750656 .

Weitere Informationen zu CI-Suchregeln und Rapid7finden Sie in KB0818096 .

## Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und feststellen, dass etwas nicht stimmt. Wenn in einer Entwicklungs- oder Leistungsumgebung etwas nicht stimmt, können Sie aus einer besseren Umgebung erneut klonen, aber das ist nicht immer eine Option.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Ausführen dieser Aktionen erfordert ServiceNow.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

- Verwenden von **„Alle Datensätze löschen“** in der **Tabellenkonfiguration**.
- Konfigurieren Sie die **Tabellenbereinigung**, indem Sie zu **Auto Flushes** (sys_auto_flush.list) navigieren und einen neuen **Auto-Flush-** Datensatz erstellen.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

  Wenn Sie `truncateTable` verwenden, müssen Sie das Kontrollkästchen Datensatz für Rollback in den Hintergrundskripts deaktivieren. Andernfalls wird eine Kopie der Tabelle und zugehöriger kaskadierender Tabellen erstellt, was zu lange dauert und höchstwahrscheinlich fehlschlägt.

**Hinweis:**
Verwenden Sie `truncateTable` niemals in einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschungen in Produktions- oder freigegebenen Umgebungen ausführen.

### Vorhandene Konfigurationselemente werden dedupliziert

Immer wenn Konfigurationselemente (CIs) durch eine Deduplizierungsaufgabe aktualisiert werden, werden auch die erkannten Elemente (DIs) aktualisiert, die sich auf diese CIs beziehen. Die angreifbaren Elemente (AEs) und Erkennungen werden ebenfalls mit dem CI aktualisiert.

Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente.

#### Zugehörige Informationen

Deduplizierungsaufgaben nachbessern

## Korrekturaufgaben lösen

Die Flexibilität von Vulnerability Response ermöglicht es Ihnen, Schwachstellen auf die für Ihre Sicherheitsorganisation geeignete Weise zu beheben.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird
Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, ändern Sie den Status der Korrekturaufgabe in Gelöst, und warten Sie auf den nächsten Scan. Erneute Scans werden automatisch durch den im Setup-Assistenten konfigurierten Drittanbieter-Importzeitplan ausgelöst.

**Hinweis:**

Wenn die Statussynchronisierung aktiviert ist, werden Korrekturaufgaben automatisch in den Status Gelöst verschoben, nachdem eine Change-Anforderung, die einer Korrekturaufgabe (VUL) zugeordnet ist, implementiert wurde und sich im Überprüfungsstatus befindet. Weitere Informationen finden Sie unter Change Management für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Mir zugewiesen**.
2. Klicken Sie auf einen Datensatz, der sich im Status „Offen“ befindet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Status „Offen“ gibt an, dass der Datensatz noch nicht bearbeitet wurde. Das Formular wird angezeigt:

- Informationen zur Korrekturaufgabe
- Gruppenkonfigurationsdetails
- Notizen
- Zugeordnete angreifbare Elemente
- Aufgaben-SLAs
- Change-Anforderungen

3. Führen Sie Ihre Analyse der Gruppe durch.
4. Wenn Sie bereit sind, mit der Arbeit an dem Datensatz zu beginnen, wählen Sie eine der folgenden Optionen aus.

| Option | Bezeichnung |
|---|---|
| **Wenn das angreifbare Element ein Risiko für Ihre IT-Umgebung darstellt, erstellen Sie einen CHG-Datensatz, und eskalieren Sie das Problem an das Change-Management- Team.** | Weisen Sie die Gruppe der entsprechenden Gruppe oder Einzelperson zu, und klicken Sie auf **Change erstellen**. |
| **Wenn das angreifbare Element ein potenzielles Sicherheitsrisiko für Ihre Organisation darstellt, erstellen Sie einen Security Incident-Datensatz, und eskalieren Sie das Problem an das Security Incident Response -Team.** | Klicken Sie auf **Security Incident erstellen**.<br><br>Diese Schaltfläche wird nur angezeigt, wenn Security Incident Response aktiviert ist. Eine Berechnung der Geschäftsauswirkung wird angewendet, der Incident wird zugewiesen und der Security Incident wird erstellt. |

Nachdem Sie eine Change-Anforderung erstellt haben, wird der entsprechende Datensatz in der zugehörigen Liste „ **Change** -Anforderungen“ im Formular „Schwachstellengruppe“ angezeigt.

5. Wenn Sie der Meinung sind, dass das Problem ein geringes Risiko darstellt und zurückgestellt werden kann, klicken Sie auf **Ausnahme anfordern**.
Anweisungen dazu finden Sie unter Korrekturaufgabe zurückstellen.
6. Wenn Sie der Meinung sind, dass das Problem sofort ohne weitere Analyse geschlossen werden kann, klicken Sie auf **Schließen**.
Anweisungen dazu finden Sie unter Schließen Sie eine Korrekturaufgabe.

Eine geplante Aufgabe für die Integration einer Drittpartei aktualisiert und scannt Datensätze automatisch in festgelegten Intervallen. Die angreifbaren Elemente werden am nächsten geplanten Datum und zur nächsten geplanten Uhrzeit gescannt. Alternativ können Sie eine Schwachstellenprüfung manuell über den zugehörigen Link **Nach** Schwachstellen scannen initiieren.

Wenn der Scan die Schwachstelle im Konfigurationselement erneut findet und sie nicht als Behoben markiert, kehrt das angreifbare Element in den Status Wird untersucht zurück. Wenden Sie sich an die IT-Abteilung, um die Change-Anforderung erneut zu öffnen.

Wenn der Scan die Schwachstelle nicht findet und zurückgibt, dass das angreifbare Element als Repariert markiert wurde, geht das angreifbare Element in den Status Geschlossen – Repariert über und wird während des Imports geschlossen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nur wenn sich alle angreifbaren Elemente in einer Aufgabe im Status Geschlossen – Repariert befinden, wird die Korrekturaufgabe automatisch geschlossen. Korrekturaufgaben mit angreifbaren Elementen in anderen geschlossenen Status als „Repariert“ müssen manuell geschlossen werden.

### Korrekturaufgabe zurückstellen

Wenn Sie feststellen, dass das mit einer Korrekturaufgabe (VUL) verbundene Problem eine niedrige Priorität hat und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion „ **Ausnahme anfordern** “ verwenden.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Korrekturaufgabe aus einem Korrekturaufgaben-Datensatz in den Vulnerability Response Arbeitsbereichen zurückstellen. Nachdem Sie die Anforderung gesendet haben, wird sie zur Genehmigung gesendet. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Eine regelmäßige Aufgabe wird täglich ausgeführt und überprüft, ob zurückgestellte Korrekturaufgaben vorhanden sind, deren Datum der Wiedereröffnung erreicht wurde. An dem Tag, an dem die Zurückstellung der Aufgabe abläuft, wird die Aufgabe erneut geöffnet.

**Hinweis:**
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen , kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-Anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „Geschlossen“ oder „Zurückgestellt“.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie **auf Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Bis | Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird.<br><br>Nachdem der Datensatz übermittelt wurde und E- Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Nach Ablauf des Zurückstellungsdatums wird die Korrekturaufgabe auf „ **Offen** “ |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Falsch positiv<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Klicken Sie auf **Absenden**.
   Die Gruppe wird als Wird überprüft gekennzeichnet. Ein **zugehöriger** Link Erneut öffnen wird angezeigt. Das Datum und der Grund für die Wiedereröffnung werden in Arbeitsnotizen auf der Registerkarte **Status-Change-Genehmigungen** angezeigt.

### Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe an

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie ihr zurückgestelltes Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Elemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Elemente sollten sich jedoch im Status „Zurückgestellt“ befinden und ihre aktuellen „Bis“-Daten vor dem „Aktualisiert bis“-Datum liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das einer Korrekturaufgabe zugeordnete Problem sofort ohne weitere Analyse geschlossen werden kann, können Sie die Funktion „ **Schließen** “ verwenden.

### Vorbereitungen

Erforderliche Rolle: admin

In den Arbeitsbereichen Vulnerability Response durchläuft eine Korrekturaufgabe dieselben Status wie eine Schwachstellengruppe in früheren Versionen von Vulnerability Response. Wenn alle AEs in einer Korrekturaufgabe geschlossen sind, geht die Korrekturaufgabe in den Status „Inaktiv“ über.

**Wichtig:**
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen , kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-Anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus den Status „ Geschlossen “ oder „Zurückgestellt “.

### Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Klicken Sie auf die Schaltfläche **Schließen/Zurückstellen**.
3. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Status | Wählen Sie einen Status aus.<br><br>Die Auswahlmöglichkeiten lauten wie folgt:<br><br>○ Zurückgestellt<br>○ Geschlossen |
| Bis | Nur im **Popup** -Fenster Zurückstellungsstatus verfügbar.<br><br>Wählen Sie das Datum aus, an dem der Status **Zurückstellen**abläuft und die Korrekturaufgabe erneut aktiviert wird.<br><br>Nachdem der Datensatz übermittelt wurde und E- Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Nach Ablauf des Zurückstellungsdatums wird das angreifbare Element auf „ **Offen** “ zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet. |
| Grund | Geben Sie den Grund für das Schließen des Problems ein. |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

4. Klicken Sie auf **Absenden**.
   Die Gruppe wird als **Geschlossen**markiert.

## Identifizieren doppelter angreifbarer Elemente von mehreren Scannern

Wenn Sie mehrere Scanner für dasselbe Asset verwenden, um Schwachstellen zu erkennen, werden möglicherweise mehrere angreifbare Elemente (VIs) erstellt. Sie können diese doppelten VIs identifizieren, um sicherzustellen, dass die doppelten Schwachstellen nicht den Korrekturbesitzern zugewiesen werden.

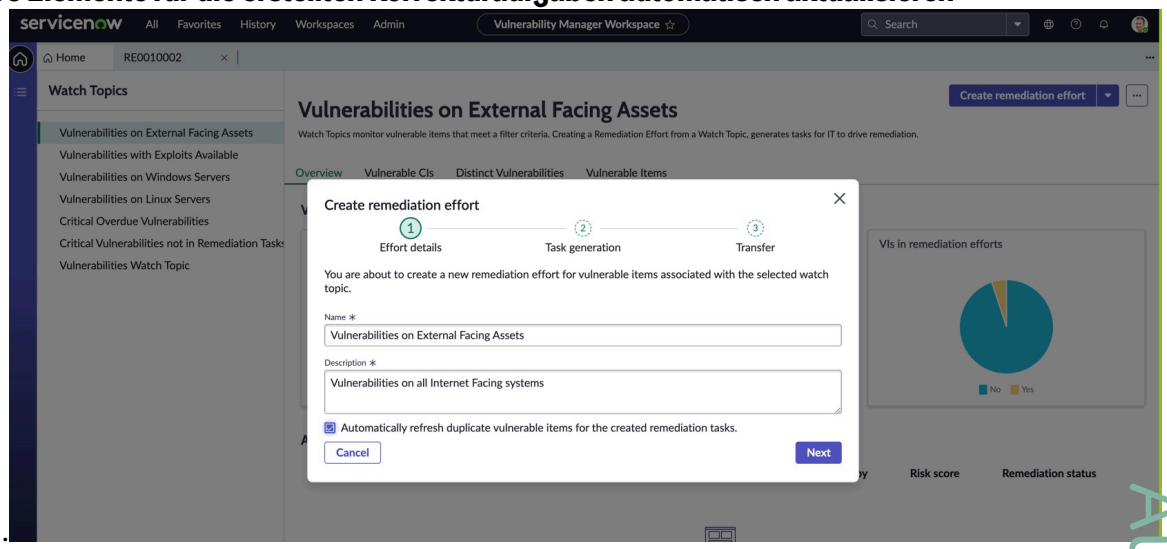
Diese Lösung ist nur möglich, wenn dieselben Schwachstellen erkannt werden, z. B. dieselben Common Vulnerabilities and Exposures (CVEs). Die Schwachstellenkombination hängt von den verwendeten Scannern ab. Zum Beispiel haben Qualys und Tenable ihren eigenen Schwachstellentyp, d. h. Einträge von Drittparteien (TPEs), und andere Scanner wie Microsoft Defender for Endpoint erkennen Schwachstellen basierend auf CVEs.

Ab Version 17.1 können Sie beim Erstellen einer Korrekturmaßnahme doppelte angreifbare Elemente in den erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie die Option **Doppelte**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren aktivieren.**




**Doppelte VIs anzeigen**: Identifizieren Sie doppelte angreifbare Elemente, die von mehreren Scannern im System gemeldet wurden. Sie können die doppelte VI als Gelöst markieren. Weitere Informationen finden Sie unter Doppelte Schwachstellen automatisch beheben. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mithilfe von CVEs erstellt wird. Weitere Informationen finden Sie unter Vulnerability Response-Korrekturaufgabe und Status angreifbarer Elemente.

Potenzielle Duplikate werden für die folgenden Schwachstellenkombinationen identifiziert:

| Scanner-Kombination | Typ der Schwachstelle |
|---|---|
| Scanner 1 und Scanner 2 | CVE |
| Scanner 1 und Scanner 2 | CVE und TPE |

### Doppelte Schwachstellen automatisch beheben

Ab Vulnerability Response (VR) v17.1 können Sie doppelte Schwachstellen in einem Asset automatisch beheben.

Wenn ein Asset mit mehreren Scannern gescannt wird, besteht die Möglichkeit, dass dieselbe Schwachstelle von den verschiedenen Scannern in Form von Duplikaten identifiziert wird. Wenn die Scanner Qualys und Microsoft beispielsweise dieselbe Schwachstelle identifizieren, können Sie festlegen, dass die doppelte Schwachstelle automatisch behoben wird.

#### Beispielszenario

VR erstellt einen Datensatz, VI1, für Schwachstelle 1 aus dem Microsoft Defender for Endpoint-Scanner. Ein zweiter Datensatz, VI2, wird vom Qualys-Scanner für dieselbe Schwachstelle erstellt. Das Korrekturteam wendet die Patches an, die die VI1- und VI2-Datensätze möglicherweise auflösen. Wenn Sie den Qualys-Scanzeitplan über einen Tag hinaus konfigurieren, gibt Microsoft Defender bis zu diesem Zeitpunkt die Informationen zur behobenen Schwachstelle zurück, und VR schließt den VI1-Datensatz als Geschlossen/Behoben.

In diesem Szenario befindet sich der VI2-Datensatz noch im Status „Offen“, und VR wartet auf die Qualys-Scan-Ergebnisse. In dieser Situation verbleiben VI-Datensätze vom zweiten Scanner im Status „Offen“, auch wenn der Patch angewendet wird und die VI vom anderen Scanner als behoben bestätigt wird.

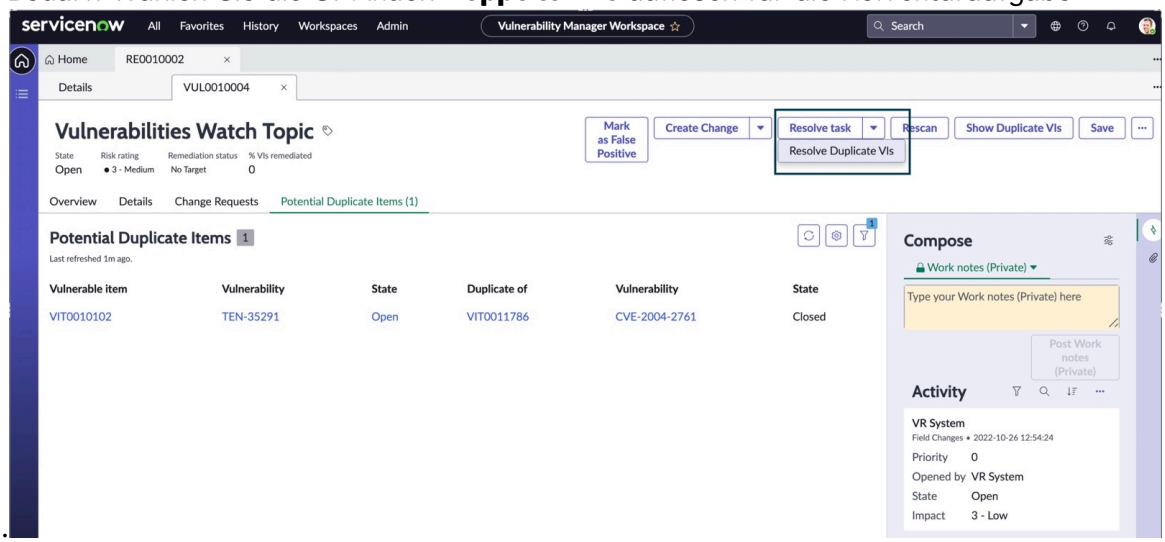
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Situation zu beheben, sollten Sie den doppelten Schwachstellendatensatz basierend auf der Bedingung auflösen, dass die Schwachstelle vom ersten Scanner geschlossen wird.

Beheben Sie Schwachstellen auf folgende Weise:

- Bei Bedarf: Wählen Sie die UI-Aktion **Doppelte AEs** auflösen für die Korrekturaufgabe aus.




- Automatisiert: Aktivieren Sie die Systemeigenschaft `sn_vul.auto_resolve_duplicate_vit`, um doppelte angreifbare Elemente automatisch aufzulösen. Die tägliche regelmäßige Aufgabe „Doppelte VITs bei Korrekturaufgabe aktualisieren und auflösen“ aktualisiert die doppelten Elemente automatisch.

Die doppelten VIs werden dann als gelöst markiert.

**Hinweis:**
Der Datensatz für aufgelöste Schwachstellenelemente wird erneut geöffnet, wenn der Scanner sie als **Nicht**behoben identifiziert.

## Erstellen und bearbeiten Sie eine Klassifizierungsgruppe

Erstellen Sie Gruppen, damit die zugrunde liegenden Regeln dieser Gruppe die Tabellendatensätze basierend auf den Bedingungen klassifizieren können. Die Regeln können verwendet werden, um ein beliebiges Feld in der entsprechenden Tabelle auszuwählen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.manage_classification_rule

### Prozedur

1. Navigieren Sie zur Tabelle „Systemeigenschaften“.
2. Fügen Sie in der Systemeigenschaft `sn_sec_cmn.classificationTables` den Namen der Tabelle hinzu, für die Sie die Klassifizierungsgruppe erstellen möchten.
3. Erstellen Sie eine neue Geschäftsregel, indem Sie der Geschäftsregel in der in der Gruppe definierten Tabelle das folgende Codefragment hinzufügen:

```
var KlassifizierungCalc = neu
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vul_classification_rule');
KlassifizierungCalc.calculate();
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Business Rules werden bereitgestellt, um die Klassifizierung während der Erfassung für die Tabellen „Erkannte Elemente“ und „Schwachstelleneintrag“ auszuführen. Für andere Tabellen müssen Sie die Geschäftsregeln hinzufügen, damit die Klassifizierungsregeln bei der Erfassung vorhanden sind.

4. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**.
5. Klicken Sie im Kontextmenü der Klassifizierungsgruppen auf **Neu**.
6. Füllen Sie die Felder des Formulars aus.

**Formular „Schwachstellenklassifizierungsgruppe“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der neuen Klassifizierungsgruppe. |
| Aktiv | Option zum Aktivieren der Gruppe. |
| Beschreibung | Beschreibung der neuen Klassifizierungsgruppe. |
| Tabelle | Tabelle, auf deren Grundlage die Regeln ausgeführt werden.<br>**Hinweis:**<br>Das Vulnerability Response-Basissystem enthält Klassifizierungsgruppen für erkannte Elemente und Schwachstellen. |

### Erstellen und bearbeiten Sie eine Klassifizierungsregel

Erstellen Sie Regeln, um eingehende Schwachstellen automatisch den richtigen Teams zur Korrektur zu klassifizieren.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

#### Warum und wann dieser Vorgang ausgeführt wird
Bei der Erstellung klassifizieren diese Regeln die Schwachstellen als zu einer Plattform oder einer Anwendung gehörend. Sie können diese Regeln so konfigurieren, dass sie den Wert eines bestimmten Felds im Schwachstelleneintrag ersetzen.
Verwenden Sie diese Regeln, um die Berechnung vorgelagert in die Tabelle „Eintrag für Drittpartei-Schwachstellen“ zu verschieben, um die Wiederverwendung von Inhalten zu ermöglichen.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**.
2. Um eine Klassifizierungsgruppe anzuzeigen, klicken Sie auf diese Gruppe.
3. Klicken Sie im Kontextmenü der Klassifizierungsregeln auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Schwachstellenklassifizierungsregel“

| Feld | Beschreibung |
|---|---|
| Name | Name der neuen Klassifizierungsregel. |
| Aktiv | Option zum Aktivieren der Regel. |
| Beschreibung | Beschreibung der neuen Klassifizierungsregel. |
| Ausführungsbefehl | Reihenfolge, in der die Regel ausgeführt werden soll. |
| Erweiterte Ansicht | Option zum Anzeigen zusätzlicher Felder in den Abschnitten mit Registerkarten. |
| Wenn diese Bedingung erfüllt ist | |
| Bedingungstyp | Typ der Bedingung für die Regel. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ **Filter**: Grundlegende Filterbedingungen, um zu bestimmen, ob die Regel verwendet werden soll oder nicht.<br>○ **Filtergruppe**: Satz von mehreren Bedingungen, die zusammen verwendet werden. Die Regel wird basierend auf den in der Filtergruppe definierten Bedingungen ausgewertet.<br>○ **Skript**: Geskriptete Bedingung, die verwendet wird, um zu bestimmen, wann diese Regel angewendet werden soll.<br>Dieses Feld wird nur angezeigt, wenn die Option **Erweiterte Ansicht** ausgewählt ist. |
| Bedingung | Bedingung für die Regel. Definieren Sie Bedingungen basierend auf der Spalte, die in der Spalte für den erforderlichen Schwachstelleneintrag ausgewählt ist. Sie können mehrere Bedingungen hinzufügen, um die Regel zu verfeinern. Dieses Feld wird nur angezeigt, wenn im Feld **Bedingungstyp** die Option **Filter** ausgewählt wird.<br>**Hinweis:**<br>Wenn Sie mehrere Bedingungen oder Vorlagen definieren, können Sie nur aus einer übergeordneten und einer untergeordneten Tabelle auswählen. Sie können nicht aus zwei oder mehr untergeordneten Tabellen auswählen. |
| Filtergruppe | Gruppe von Filtern. Die Gruppe wird definiert, wenn ein Satz von Bedingungen wiederholt an mehreren Stellen verwendet wird. Klicken Sie auf das Symbol „ “ ), um die Filtergruppe auszuwählen. Weitere Informationen finden Sie unter Filtergruppen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | in Security Operations erstellen und definieren. Dieses Feld wird nur angezeigt, wenn im Feld **Bedingungstyp** die Option **Filtergruppe** ausgewählt wird. |
| Skript | Skript, das ausgewertet wird, um zu bestimmen, wann diese Regel angewendet werden soll. Sie können Ihren Code schreiben und die Antwort auf „true“ oder „false“ festlegen. Dieses Feld wird nur angezeigt, wenn im Feld **Bedingungstyp** die Option **Skript** ausgewählt wird |
| Diese Werte festlegen | |
| Klassifizierung | Klassifizierung der Regel. Um eine Option auszuwählen, klicken Sie auf das Glühbirnensymbol ( ). In der Liste werden die Optionen für Plattform und Anwendung angezeigt. Alternativ können Sie eine eigene Klassifizierung eingeben, die nicht in der Liste enthalten ist. |
| Klassifizierungstyp | Typ der Klassifizierung. Dieses Feld zeigt die gefilterte Liste der Klassifizierungstypen basierend auf dem ausgewählten Wert für das Feld **Klassifizierung**. |
| Werttyp | Typ des Werts, der mithilfe dieser Regel zugewiesen wird. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ **Vorlage**: Wählen Sie eine Vorlage. Sie können eine erforderliche Vorlage verwenden.<br>○ **Skript**: Wählen Sie ein bereits vorhandenes Skript aus, oder schreiben Sie ein eigenes benutzerdefiniertes Skript.<br>Dieses Feld wird nur angezeigt, wenn die Option **Erweiterte Ansicht** ausgewählt ist. |
| Vorlage | Eine weitere Bedingung für die Regel neben den Feldern **Klassifizierung** und **Klassifizierungstyp**. Wählen Sie eine Kombination von Feldern und Werten aus, die Sie festlegen möchten, wenn die Regel ausgewertet wird. Dieses Feld wird nur angezeigt, wenn **Vorlage** im Feld **Werttyp** ausgewählt wird. |
| Skriptwert | Skript zum Festlegen von Werten für den aktuellen Datensatz. Dieses Feld definiert, welche Werte in den Feldern in Schwachstelleneinträgen festgelegt werden sollen. Dieses Feld wird nur angezeigt, wenn im Feld **Werttyp** die Option **Skript** ausgewählt wird. |

5. Um die neue Regel zu erstellen, klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Example:**
Verwenden Sie VR-Klassifizierungsregeln, um die Logik zu vorgelagerten Tabellen wie „Schwachstelle“ und „Erkannte Elemente“ hinzuzufügen und zu berechnen. Sie können die Ausgabe mehrmals wiederverwenden und so die Leistung von Regeln wie Zuweisungsregeln verbessern. Klassifizieren Sie beispielsweise den Drittparteieintrag (TPE) als Java, und verwenden Sie die Ausgabe in den Zuweisungsregeln mehrmals. Beispiel für eine Zuweisungsregel:

```
VI.TPE.Classfication Type
        | IS | Java
```

### Wenden Sie eine Regel auf eine vorhandene Schwachstelle an

Wenn Sie eine Klassifizierungsregel ändern, führen Sie alle aktiven Regeln für alle Schwachstelleneinträge erneut aus. Sie können die vorhandenen Schwachstellen auch nachrüsten, indem Sie die neu erstellten Klassifizierungsregeln auf die vorhandenen Schwachstellen anwenden.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellenklassifizierungsregeln**.
2. Um eine Regel auszuwählen, aktivieren Sie das Kontrollkästchen neben der Regel.
3. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
4. Klicken Sie **auf Erneut anwenden**.

### Deaktivieren oder löschen Sie eine Klassifizierungsregel

Deaktivieren oder löschen Sie eine Klassifizierungsregel, wenn sie nicht mehr benötigt wird oder relevant ist.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

#### Warum und wann dieser Vorgang ausgeführt wird
Wenn eine Klassifizierungsregel deaktiviert oder gelöscht wird, verbleiben die Daten, mit denen die Felder **Klassifizierung** und **Classification_type** von dieser gelöschten Regel ausgefüllt wurden, in ihren jeweiligen Tabellen.

Wenn Sie diese Daten löschen möchten, erstellen Sie eine Regel mit leeren Werten in den Feldern **Klassifizierung** und **Classification_type**, und wenden Sie die Gruppe erneut an. Sobald diese neue Regel erneut angewendet wird, werden die Änderungen in allen Datensätzen berücksichtigt, für die diese Regel basierend auf den Bedingungen der Regel gilt.

#### Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellenklassifizierungsregeln**.
2. Um die Regel auszuwählen, die Sie löschen möchten, klicken Sie auf das Kontrollkästchen neben der Regel.
3. Führen Sie einen der folgenden Schritte aus, um die Regel zu löschen:
   - Klicken Sie in der Liste Aktion für ausgewählte Zeilen auf **Löschen**.
   - Wählen Sie die Regel aus, und klicken Sie auf die Schaltfläche **Löschen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.

> **Hinweis:**
> Wenn Sie nicht auf diese Schaltfläche klicken, bleibt die Regel im System. Von der Regel referenzierte Schwachstellen verweisen weiterhin auf sie.

## Change-Management Aufgaben für Vulnerability Response

Erstellen Sie aus Korrekturaufgaben (RTs) Change-Anforderungen, ordnen Sie RTs vorhandenen Change-Anforderungen zu, oder teilen Sie Korrekturaufgaben in neue Aufgaben mit Teilmengen angreifbarer Elemente (VI) auf.

Erstellen und verwalten Sie Change-Anforderungen direkt aus einer Korrekturaufgabe, wenn ein manueller und kontrollierter Prozess jeglicher Art für die Änderung oder Entfernung von unterstützten Konfigurationselementen (CIs) in Ihrer CMDB erforderlich ist. Das Erstellen und Verwalten von Change-Anforderungen direkt aus einem Datensatz hilft Ihnen, Schwachstellen schnell zu untersuchen und zu beheben.

Unter Change Management für Vulnerability Response finden Sie eine Übersicht über die Funktionsweise von Change Management mit der Anwendung Vulnerability Response und die Systemanforderungen.

In den folgenden Themen erfahren Sie, wie Sie Change-Anforderungen erstellen, Korrekturaufgaben vorhandenen Change-Anforderungen zuordnen und Korrekturaufgaben aufteilen. Unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben finden Sie Informationen darüber, wie Statusfelder in Change-Anforderungen (CHG) Korrekturaufgaben automatisch lösen.

### Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Erstellen Sie als IT-Korrekturbesitzer eine Change-Anforderung (CHG) direkt aus einer Korrekturaufgabe (VUL) für alle angreifbaren Elemente in der Gruppe. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, die die bevorzugte Lösung enthalten, um Ihre Untersuchung auf Schwachstellen zu beschleunigen, die ein manuelles Eingreifen erfordern.

**Vorbereitungen**
Erforderliche Rollen: Zum Erstellen einer Change-Anforderung: jeder Benutzer mit der Rolle itil. Die Rolle „sn_vul.remediation_owner“ wird auch automatisch zugewiesen, wenn die Rolle „itil“ einem Benutzer zugewiesen wird.

Erforderliche Rolle: Für die Genehmigung von Change-Anforderungen: Benutzer mit den Rollen „itil“, „admin“, „sn_change_write“, „change_manager“.

**Warum und wann dieser Vorgang ausgeführt wird**
Informationen zum Erstellen einer Change-Anforderung aus den Vulnerability Response -Arbeitsbereichen finden Sie unter Erstellen Sie eine Change-Anforderung in IT Remediation Workspace.

Führen Sie die folgenden Schritte aus, um eine Change-Anforderung aus der klassischen Umgebung zu erstellen.

Sie können Change-Anforderungen direkt aus einer Korrekturaufgabe erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

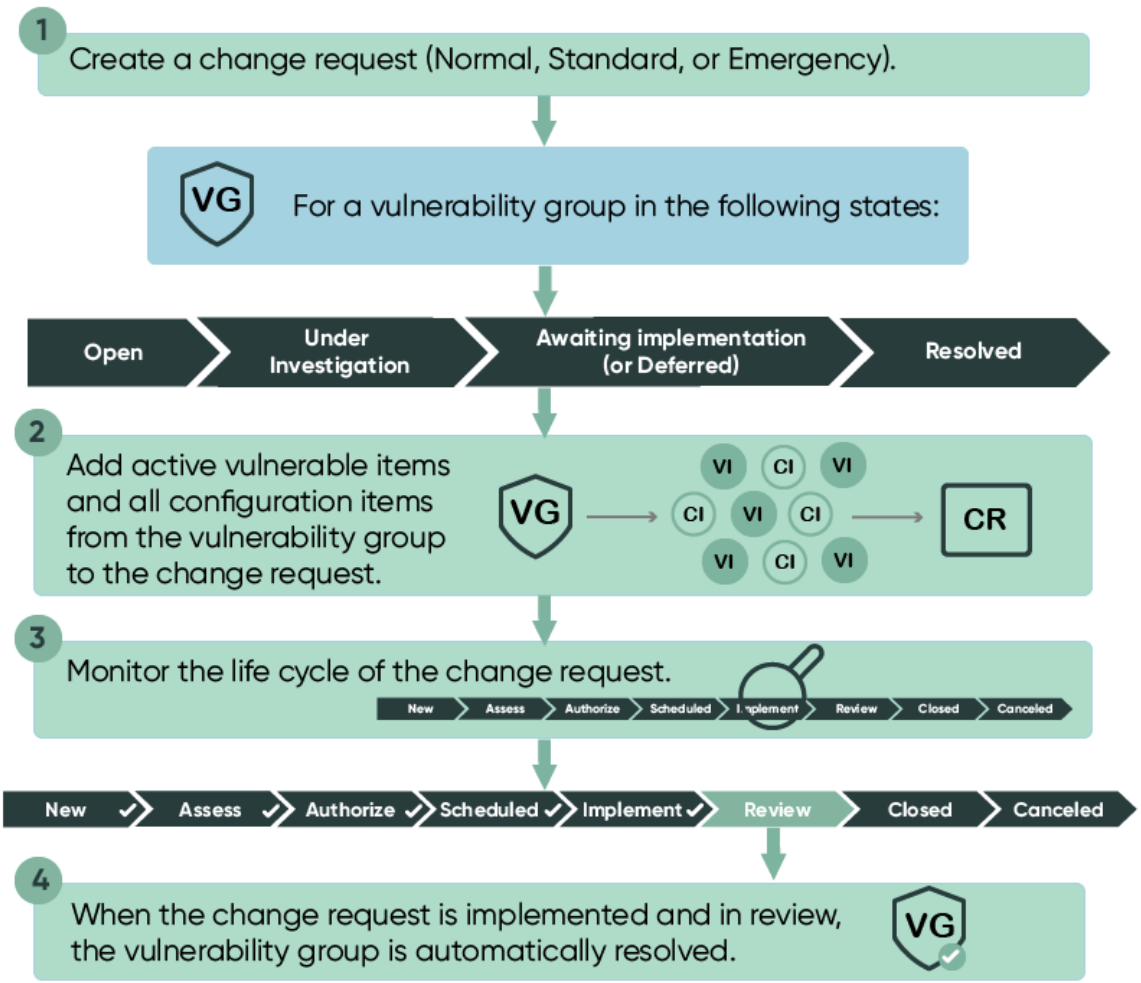


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standard Ein vorab autorisierter Change, der geringes Risiko und relativ häufig ist und einem bestimmten Verfahren oder einer Arbeitsanweisung folgt.
- Normal. Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsebenen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall. Eine Änderung zur Lösung eines schwerwiegenden Incidents.

Die folgende Abbildung zeigt den grundlegenden Ablauf für die Erstellung einer Change-Anforderung aus einer VUL (Korrekturaufgabe). Die detaillierten Schritte für diesen Flow folgen der Abbildung.

Der Datensatz der Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Bildern ist VG = Korrekturaufgabe oder ein VUL-Datensatz.




Automatische Übersetzung

**Hinweis:**

Wichtige Punkte zum Erstellen neuer Change-Anforderungen:

- Sie können neue Change-Anforderungen für jede Korrekturaufgabe (VUL) in einem anderen Status als Geschlossenerstellen.
- Stellen Sie sicher, dass Sie einen Genehmiger für andere Change-Anforderungen als Standard (vorab genehmigt) haben, die Sie erstellen oder einer VUL zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies beschleunigt das Verschieben der VUL zur Lösung. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter Fügen Sie der Vulnerability Response-Gruppe Benutzer hinzu.

- Bevor eine Korrekturaufgabe gelöst werden kann, müssen alle Aufgaben in mindestens einer CHG, die der VUL zugeordnet ist, abgeschlossen sein, damit die Change-Anforderung implementiert und in den Überprüfungsstatus verschoben werden kann.

### Prozedur

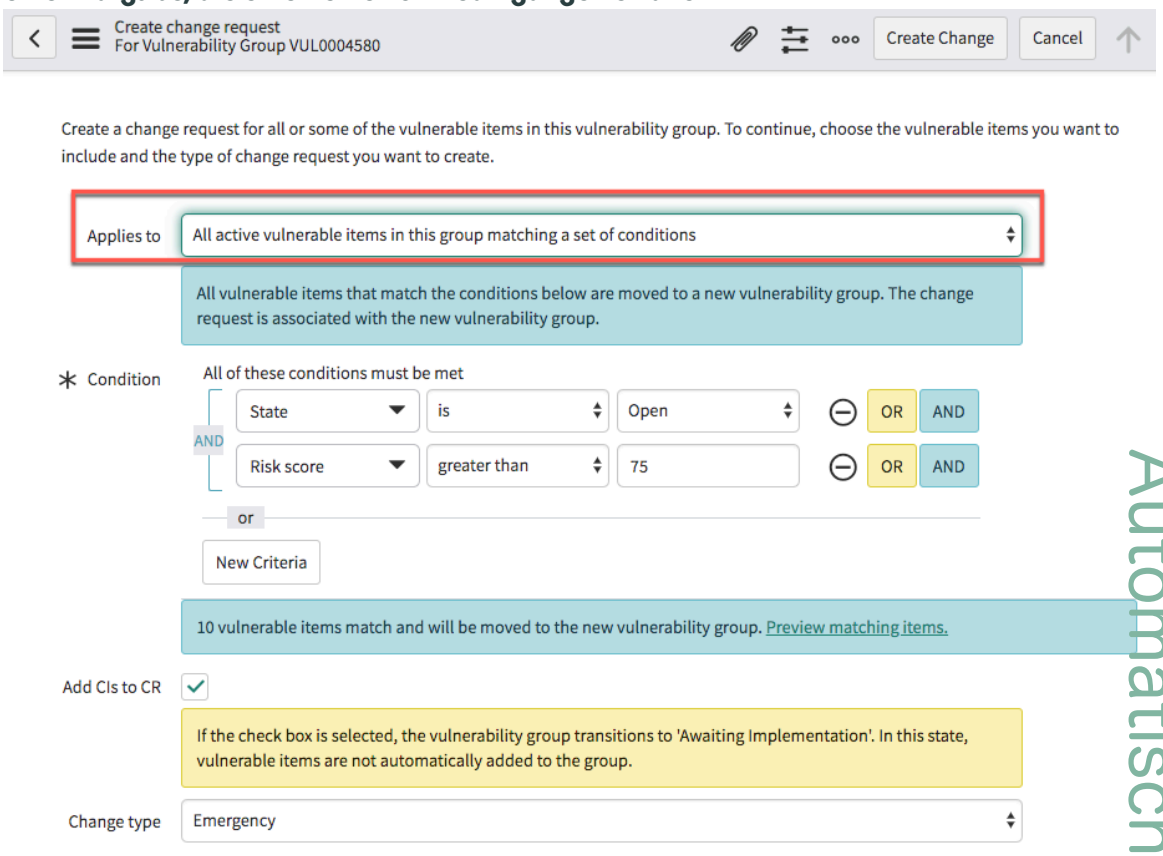
1. Um eine vollständige Change-Anforderung aus einem vorhandenen Korrekturaufgaben-Datensatz zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.
   Die Liste der Korrekturaufgaben, die Ihrer Zuweisungsgruppe zugewiesen sind, wird angezeigt.
2. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** , um das Dashboard „Korrekturübersicht“ anzuzeigen und eine VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
3. Alternativ können Sie in der Spalte Nummer auf eine Korrekturaufgabe klicken, um den Datensatz zu öffnen und die Details anzuzeigen.
   Der Datensatz wird angezeigt.
4. Wenn der VUL-Datensatz angezeigt wird, für den Sie die Change-Anforderung erstellen möchten, klicken Sie oben rechts im Datensatz auf **Change erstellen**.
   Das Formular Change Request erstellen wird angezeigt.
5. Füllen Sie die Felder aus.

   a. Wählen Sie in der Auswahlliste des Felds Betrifft eine Option aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Erstellen Sie ein Change-Anforderungsformular für angreifbare Elemente in einer Aufgabe, die eine Reihe von Bedingungen erfüllen**




**b. Wahlweise:** Wenn im Formular angezeigt, klicken Sie auf den Link **Preview matching items** (Übereinstimmende Elemente in der Vorschau anzeigen), um eine Liste der VIs anzuzeigen, die Ihren Filterkriterien entsprechen.
Die Vorschau der Korrekturaufgabenliste wird angezeigt. Sie können Elemente in dieser Vorschauliste auswählen und UI-Aktionen für sie ausführen. Diese Aktionen werden jedoch auch für die VUL ausgeführt. Wenn Sie beispielsweise einen VI aus der Vorschauliste löschen, wird dieser VI auch aus der VUL gelöscht.

**c.** Schließen Sie nach Abschluss der Vorschau das Browserfenster, um zum Change Request-Formular zurückzukehren.

**d.** Wählen Sie für das Kontrollkästchen CIs zu CA hinzufügen eine Option aus, um fortzufahren.

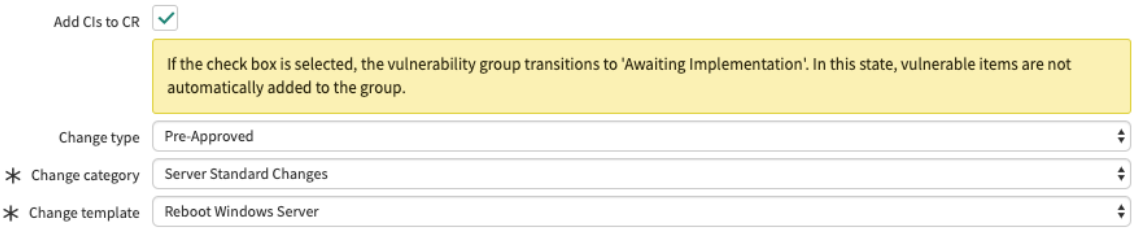
**e.** Wählen Sie in der Auswahlliste für das Feld Change-Typ einen aus, um fortzufahren.

Die Funktion liest automatisch die Typen von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von Standard in Vorab genehmigtändern, wird Ihr neuer Name automatisch in der Auswahlliste Change-Typ

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unter Change-Anforderung erstellen aus angezeigt, wie in der folgenden Abbildung dargestellt.




Die Felder im Abschnitt „Change Request-Vorschau“ des Formulars sind vorab mit Informationen aus der VUL ausgefüllt. Bei Bedarf können diese Feldwerte bearbeitet werden. Überprüfen Sie beispielsweise die Werte in den Feldern in der folgenden Abbildung:

**Geplantes Enddatum**

Dieses Datum (2019-10-10) ist derselbe Wert, der im Feld Korrekturzieldatum der VUL angezeigt wird. Dieser Wert wird aus dem frühesten Korrekturzieldatum der angreifbaren Elemente abgeleitet, die zur VUL gehören. Wenn Sie eine Change-Anforderung für ein kritisches Problem erstellen, das ein früheres Korrekturdatum erfordert, sollten Sie diesen Wert und den Wert im Feld Priorität bearbeiten.

**Begründung**

In diesem Feld wird die Anzahl der CIs angezeigt, die der CHG hinzugefügt wurden. Wenn Sie zusätzliche Informationen hinzufügen möchten, sollten Sie diesen Text bearbeiten. Beispielsweise können Sie in diesem Feld eine Notiz zu dem Filter hinzufügen, den Sie zum Erstellen der neuen VUL verwendet haben, z. B. Risikopunktzahl größer als 75. Dieser Text kann Ihnen helfen, Ihre neue Change-Anforderung und Schwachstellengruppe zu finden.

**Implementierungsplan**

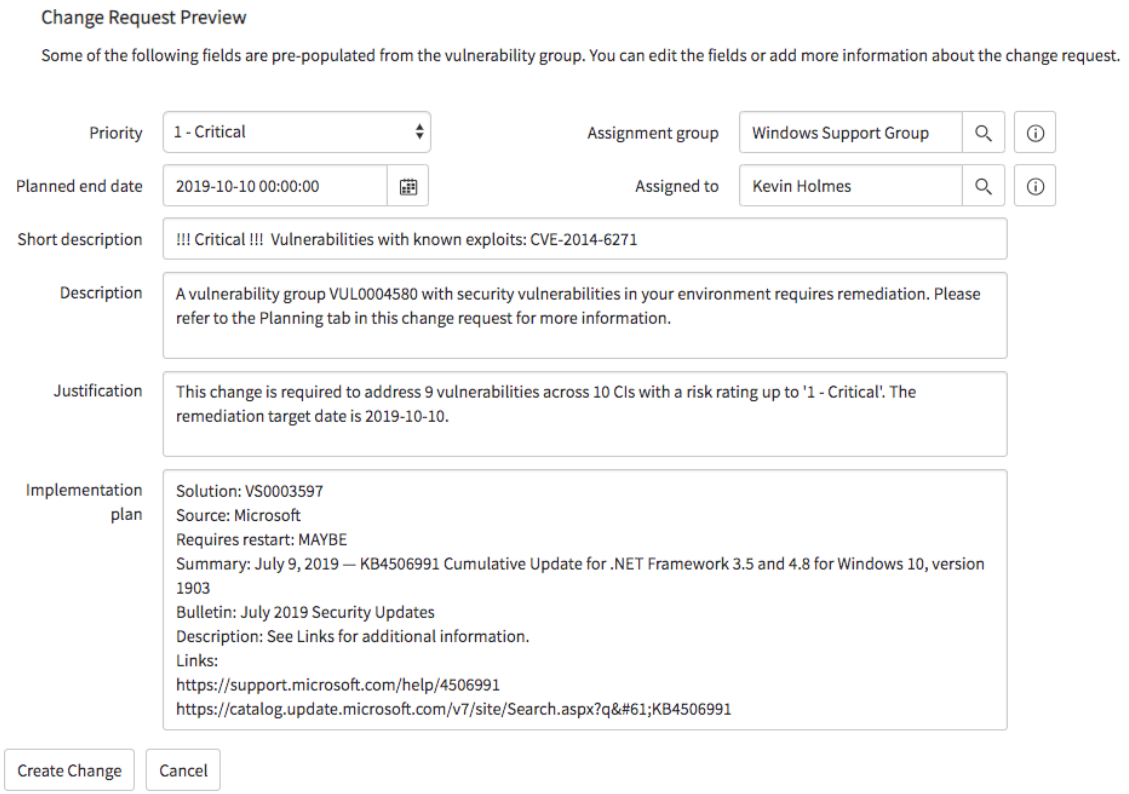
In diesem Feld wird die bevorzugte Lösung für die Schwachstelle angezeigt.

**Zuweisungsgruppe und Zugewiesen an**

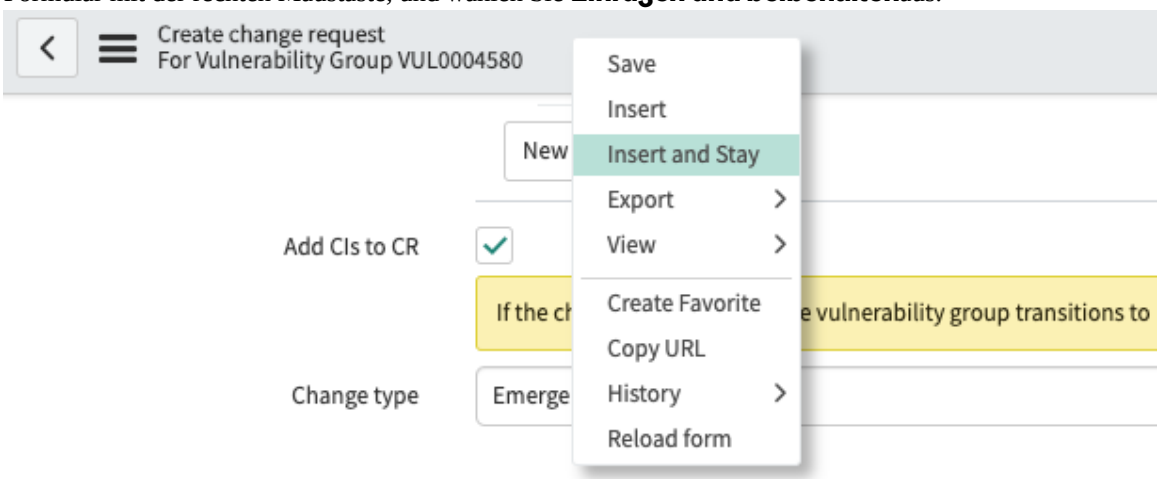
Bearbeiten Sie diese Felder, um die Zuweisungsgruppe zu ändern, oder weisen Sie diese Change-Anforderung einem Benutzer in einer Ihrer Zuweisungsgruppen neu zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



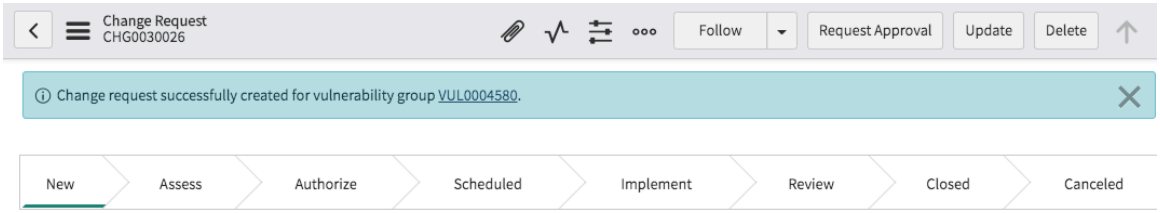

6. Setzen Sie die Vorschau fort, und bearbeiten Sie die Felder nach Bedarf.
7. Um Ihre Änderungen zu speichern und auf dieser Seite zu bleiben, klicken Sie im grauen Banner oben im Formular mit der rechten Maustaste, und wählen Sie **Einfügen und beibehalten**aus.




8. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie eine aus, um fortzufahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**

Bei einer Korrekturaufgabe im Status Offen, bei der die Felder Zuweisungsgruppe und Zugewiesen an nicht zugewiesen (leer) sind, wird der aktuell angemeldete Benutzer automatisch der Aufgabe zugewiesen, nachdem Sie auf **Change erstellen geklickt**haben. Außerdem muss das Kontrollkästchen CIs zu CA hinzufügen aktiviert sein. Oben in der VUL wird eine blaue Bestätigungsmeldung angezeigt, die auf diese Zuweisung hinweist.

### Nächste Maßnahme

Überwachen Sie die Change-Anforderung und die Change-Aufgaben, um sicherzustellen, dass sie abgeschlossen und die Change-Anforderung implementiert ist. Nachdem diese CHG implementiert und in den Status Überprüfung verschoben wurde, wird die VUL automatisch in den Status Gelöstverschoben, wenn die Statussynchronisierung aktiviert ist. Weitere Informationen zur Statussynchronisierung finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

## Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Vermeiden Sie es als IT-Korrekturbesitzer, doppelte Change-Anforderungen (CHG) zu erstellen, wenn Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie eine Korrekturaufgabe (VUL) einer Change-Anforderung zuordnen, die bereits in Ihrer Instanz verfügbar ist.

### Vorbereitungen

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: beliebiger Benutzer mit der itil-Rolle. Die Rolle „sn_vul.remediation_owner“ wird auch automatisch einem Benutzer zugewiesen, wenn die Rolle „itil“ zugewiesen wird.

### Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung in IT Remediation Workspace.

Der Datensatz der Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Bildern ist VG = Korrekturaufgabe oder ein VUL-Datensatz.

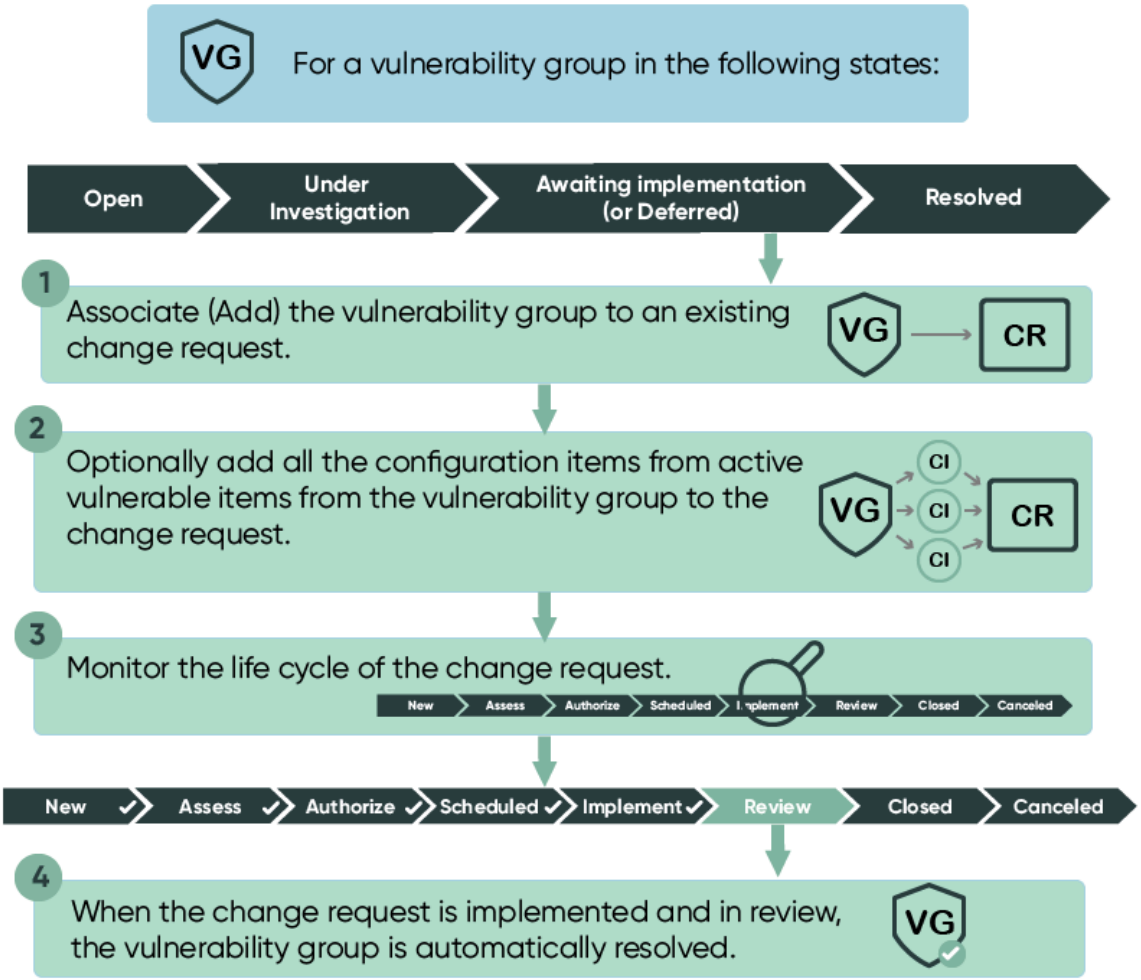
Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung in IT Remediation Workspace.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Besitzer einer Korrektur können Sie Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Datensätzen der Korrekturaufgaben zuordnen. Die folgende Abbildung zeigt den grundlegenden Flow für die Zuordnung einer Change-Anforderung zu einer vorhandenen VUL (VG). Die detaillierten Schritte für diesen Flow folgen der Abbildung.

**Workflow zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung**




**Hinweis:**

Sie können eine vorhandene Change-Anforderung einer VUL in jedem Status zuordnen („Offen“, „Wird untersucht“, „Warten auf Implementierung“, „Geschlossen“ und „Zurückgestellt“). Wenn Sie eine Change-Anforderung einer vorhandenen VUL zuordnen, werden der Change-Anforderung nur die aktiven AEs hinzugefügt.

Um zu vermeiden, dass Change-Anforderungen doppelt erstellt werden, sollten Sie vorhandene Change-Anforderungen anzeigen, die bereits einer VUL zugeordnet sind. Informationen zum einfachen Nachverfolgen der Anzahl der Change-Anforderungen, die sich auf eine bestimmte VUL beziehen, finden Sie in der Spalte „CR-Anzahl“ in der Liste „Korrekturaufgaben“. Wenn nicht angezeigt, klicken Sie oben rechts auf das Einstellungssymbol ( ). Verschieben Sie die Spalte „CR-Anzahl“ von Verfügbar zu Ausgewählt, und klicken Sie auf **OK**.

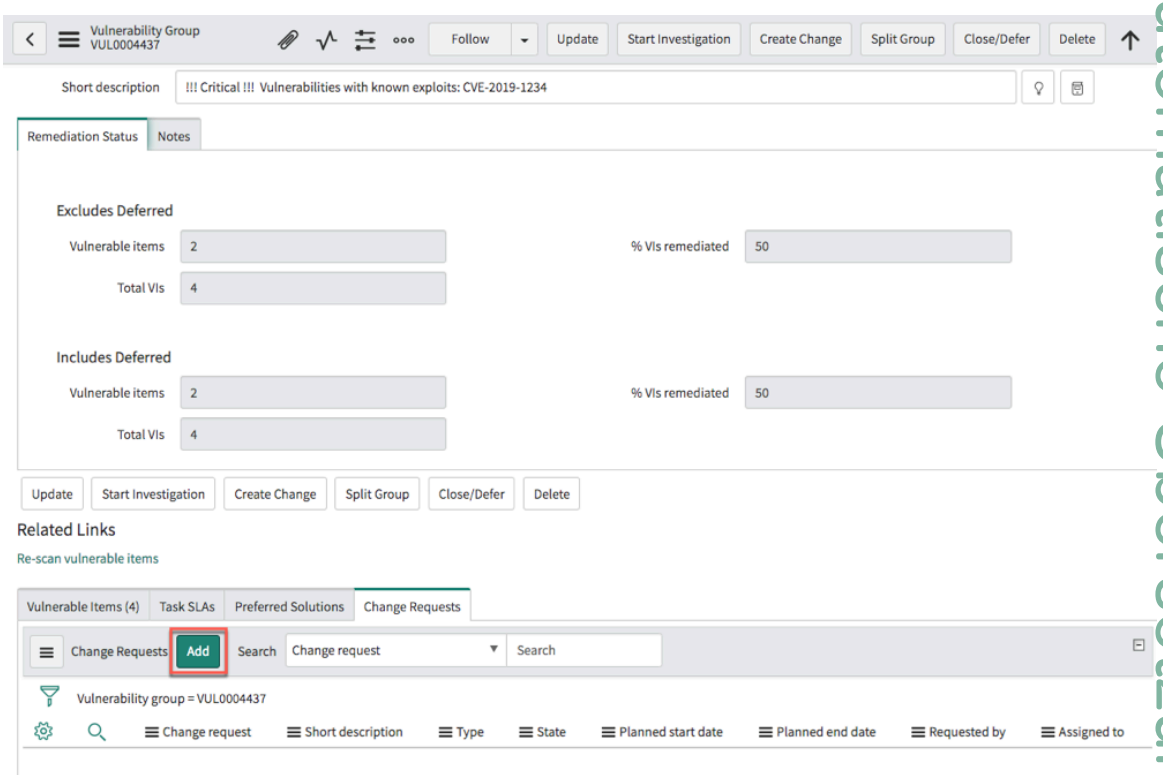
Um die neue Spalte automatisch auszufüllen, führen Sie für Kunden mit vorhandenen Daten in dieser Tabelle die folgende geplante Aufgabe aus: Neue CR-Anzahlspalte füllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

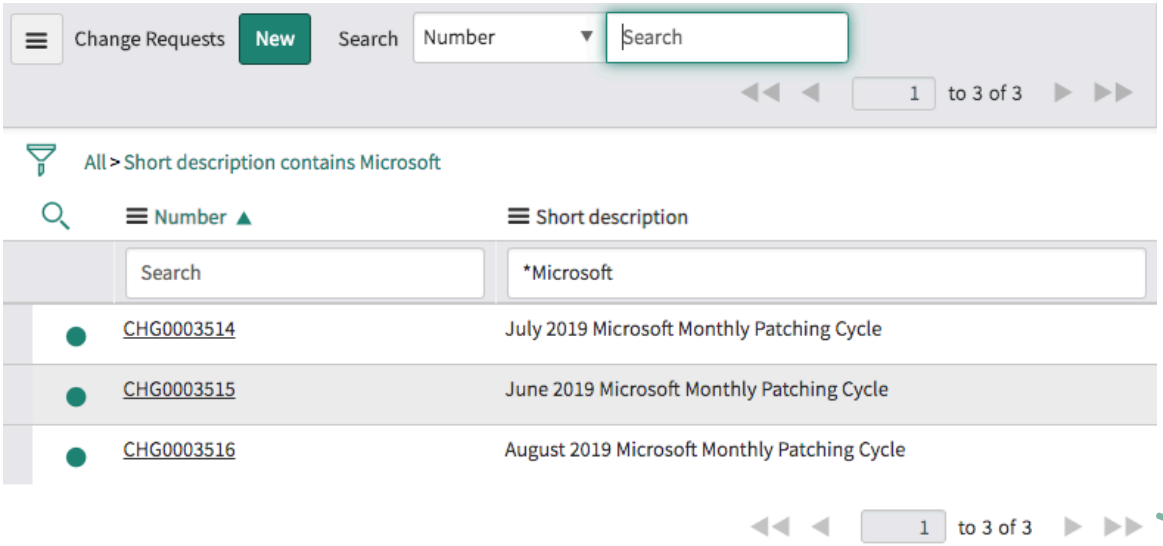
1. Um eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuzuordnen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Suchen Sie die Korrekturaufgabe, an der Sie arbeiten.
3. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** , um das Dashboard „Korrekturübersicht“ anzuzeigen und eine VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
4. Klicken Sie in der Spalte Nummer auf einen VUL-Datensatz, um ihn zu öffnen.
   Der VUL-Datensatz wird angezeigt.
5. Wenn der offene Datensatz angezeigt wird, scrollen Sie, falls er noch nicht angezeigt wurde, zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle mit der VUL verknüpften Change-Anforderungen werden zusammen mit der Schaltfläche **Hinzufügen** angezeigt. In der folgenden Abbildung sind dieser VUL noch keine Change-Anforderungen zugeordnet.




6. Um die VUL einer vorhandenen CHG zuzuordnen, klicken Sie auf **Hinzufügen**.
   Das Formular Vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen wird angezeigt.
7. Klicken Sie im Formular auf das Suchsymbol.
   Eine Listenansicht der vorhandenen Change-Anforderungen wird in einem neuen Fenster angezeigt (siehe folgende Abbildung).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




8. Wählen Sie ein Element aus der angezeigten Liste aus, oder klicken Sie alternativ auf den Filter ( ), und geben Sie Bedingungen ein, um die Suchergebnisse einzuschränken.
9. Wählen Sie für das Kontrollkästchen CIs zu CA hinzufügen eine Option aus, um fortzufahren.

**Hinweis:**
Diese Checkbox wird nur für vorhandene Change Requests im Status Neu angezeigt.

10. Wenn die Nummer der Change-Anforderung im Feld Nach Change-Anforderung suchen angezeigt wird, klicken Sie auf **Absenden**.
Die VUL wird angezeigt. Oben im Datensatz wird eine blaue Bestätigungsmeldung angezeigt, die angibt, dass die von Ihnen ausgewählte Change-Anforderung erfolgreich der VUL zugeordnet wurde.

**Hinweis:**
Bei einer VUL im Status „ Offen “ mit nicht zugewiesenen Feldern „Zuweisungsgruppe“ und „Zugewiesen an“ (leer) wird der aktuell angemeldete Benutzer automatisch der VUL zugewiesen, nachdem Sie auf **Hinzufügen**geklickt haben. Außerdem muss das Kontrollkästchen CIs zu CA hinzufügen aktiviert sein. Oben in der VUL wird eine blaue Bestätigungsmeldung angezeigt, die angibt, dass der aktuelle Benutzer zugewiesen ist.

## Nächste Maßnahme

Überprüfen Sie den VUL-Datensatz. Klicken Sie in der Spalte „Change-Anforderung“ in der zugehörigen Liste „Change-Anforderungen“ auf den Link für das neue CHG, um den CR-Datensatz anzuzeigen. Im geöffneten CHG-Datensatz können Sie den Status der Change-Anforderung überwachen. Die betroffenen Konfigurationselemente (CIs) und die Korrekturaufgaben werden in den zugehörigen Listen Betroffene CIs und Korrekturaufgaben angezeigt.

### Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie als IT-Korrekturbesitzer aus einer vorhandenen Korrekturaufgabe (VUL) eine Teilmenge angreifbarer Elemente (AE), die Sie in eine neue Gruppe verschieben möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

**Hinweis:**

Anwendungsfälle für die Aufteilung von VIs aus vorhandenen VULs in neue Korrekturaufgaben können die folgenden Beispiele umfassen:

- Wenn Sie eine oder mehrere Change-Anforderungen für eine aufgeteilte Aufgabe erstellen möchten.
- Wenn Sie eine Split-Gruppe einem anderen Benutzer in Ihrer Zuweisungsgruppe neu zuweisen.
- Wenn Sie eine Zurückstellung oder Ausnahme für eine aufgeteilte Aufgabe anfordern, da Sie wissen, dass einige Schwachstellen in bestimmten Konfigurationselementen (Configuration Items, CI) nicht in einem bestimmten Zeitrahmen behoben werden können.

Erforderliche Rolle: jeder Benutzer mit der itil-Rolle für die Aufteilung einer VUL.

**Hinweis:**

Die Rolle „sn_vul.remediation_owner“ wird auch automatisch zugewiesen, wenn die Rolle „itil“ einem Benutzer zugewiesen wird.

### Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Aufteilen von Korrekturaufgaben in den Arbeitsbereichen Vulnerability Response finden Sie unter Teilen Sie eine Korrekturaufgabe in auf IT Remediation Workspace.

So teilen Sie eine Korrekturaufgabe in der klassischen Umgebung oder für Versionen von Vulnerability Responseauf.

Sie können vorhandene Korrekturaufgaben mit mehr als einem angreifbaren Element aufteilen, das sich im Status „ Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befindet. Durch die Erstellung einer neuen VUL mit angreifbaren Elementen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe von angreifbaren Elementen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Wenn Sie mit dem Bedingungsgenerator die Bedingungen für die angreifbaren Elemente angeben, die Sie in eine neue Korrekturaufgabe verschieben möchten, werden nur die aktiven AEs, die Ihren Kriterien entsprechen, in die neue Gruppe verschoben.

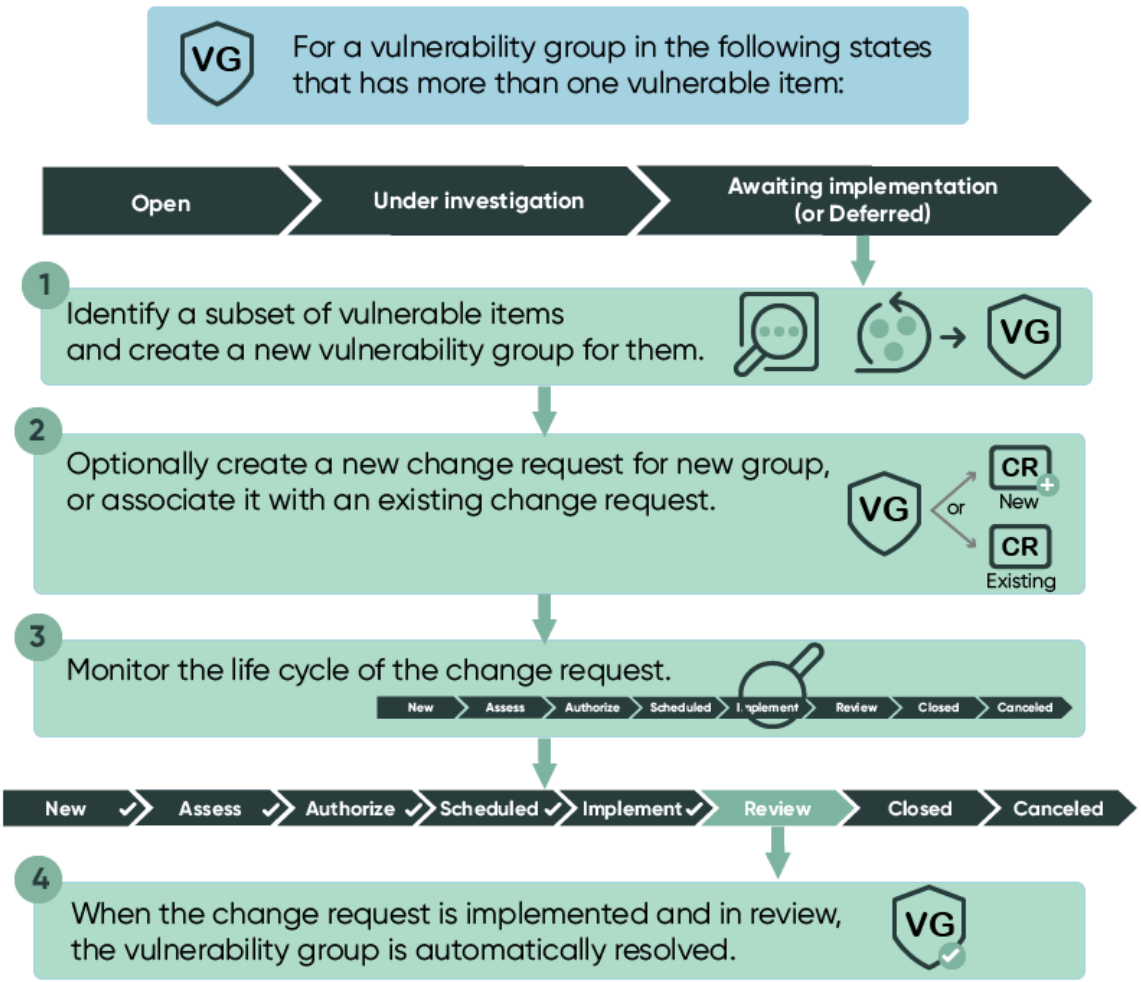
Sie müssen keine Change-Anforderungen (CHG) erstellen, wenn Sie eine VUL aufteilen. Sie haben die Möglichkeit, eine VUL gleichzeitig mit der Erstellung einer Change-Anforderung aufzuteilen, oder Sie können eine VUL aufteilen, ohne eine Change-Anforderung zu erstellen. Die folgende Abbildung zeigt den grundlegenden Flow für die Aufteilung einer Schwachstellengruppe. Die detaillierten Schritte für diesen Flow folgen der Abbildung.

Der Datensatz der Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Bildern ist VG = Korrekturaufgabe oder ein VUL-Datensatz.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

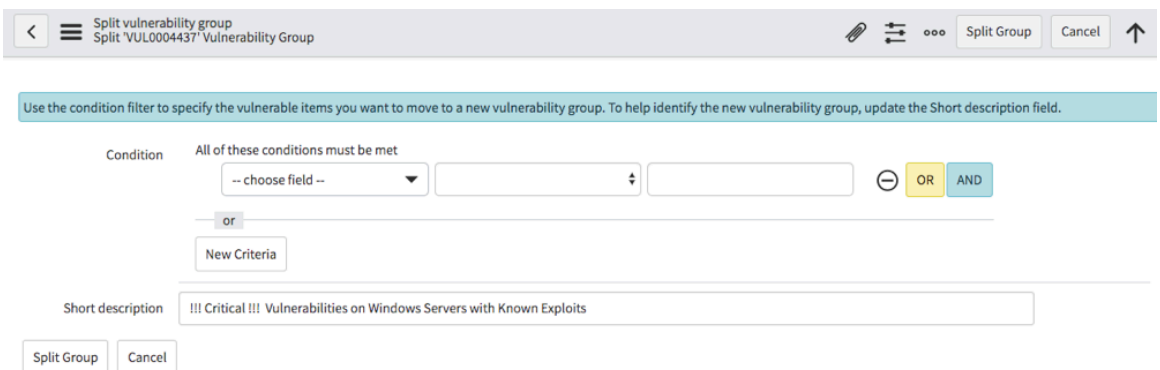
### Workflow zum Aufteilen einer Korrekturaufgabe




Automatische Übersetzung

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**.
   Die Liste der Korrekturaufgaben wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt.
3. Klicken Sie oben rechts in der VUL auf **Aufgabe**teilen.
   Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.



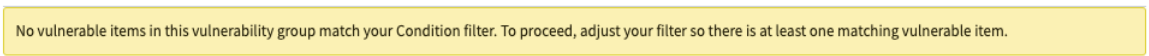

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie bei angezeigtem Bedingungsfilter die Bedingungen für die angreifbaren Elemente an, die Sie in eine neue Aufgabe verschieben möchten.
   Beispielsweise können Sie nur angreifbare Elemente herausfiltern, die den folgenden Bedingungen entsprechen:
   - Im Status „ Offen “.
   - Risikopunktzahlen größer als 80.
   - Konfigurationselemente, die „WINSV“ enthalten.
   - Standort: San Diego

   Für Bedingungen können Sie beispielsweise Folgendes eingeben:
   - Status – ist – Offen
   - Risikopunktzahl – ist größer oder gleich – 80
   - Konfigurationselement. Name – enthält – WINSV
   - Konfigurationselement. Standort ist San Diego

   Wenn angreifbare Elemente Ihrem Filter entsprechen, nachdem Sie die Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der übereinstimmenden angreifbaren Elemente angezeigt.

   **Hinweis:**
   Wenn eine Meldung angezeigt wird, dass keine angreifbaren Elemente Ihrem Filter entsprechen, passen Sie die Bedingungen so an, dass mindestens ein angreifbares Element Ihren Filterkriterien entspricht.

5. **Wahlweise:** Passen Sie den Filter nach Bedarf an.
6. **Wahlweise:** Um die neue VUL nach der Erstellung leichter identifizieren zu können, sollten Sie das Feld Kurzbeschreibung aktualisieren.
   Wenn bearbeitet, verwenden Sie das Kurzbeschreibungsfeld als Suchkriterien für die neue VUL, um sie nach der Erstellung zu finden, z. B.LOCATED IN SAN DIEGO.
7. **Wahlweise:** Um eine Vorschau der Details zu den angreifbaren Elementen anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie die folgenden Schritte aus, bevor Sie auf Aufgabe aufteilen klicken, um die neue **VUL** zu erstellen.
   Diese Details umfassen vorhandene Change-Anforderungen, die dieser Teilmenge bereits zugeordnet sind, und VULs mit diesen angreifbaren Elementen. Wenn Sie diese Informationen in der Vorschau anzeigen, können Sie möglicherweise keine doppelten VULs erstellen.

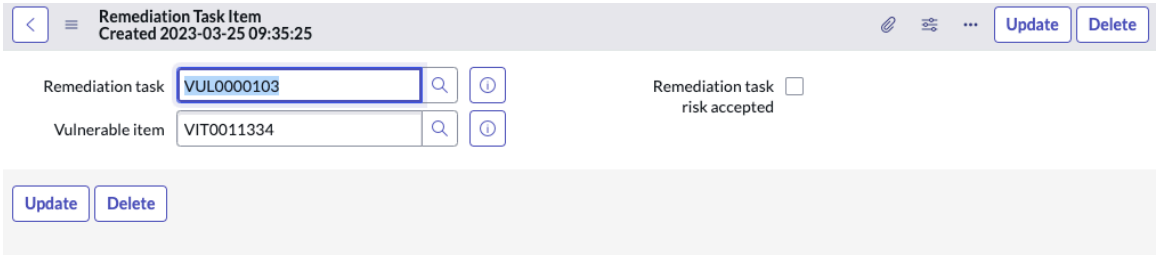
   a. Klicken Sie in der blauen Bestätigungsmeldung im Formular „Korrekturaufgabe aufteilen“ auf **Vorschau für übereinstimmende Elemente**.
      Die Liste „Korrekturaufgabenelement“ wird in einem neuen Fenster in Ihrem Browser mit einer Liste der angreifbaren Elemente angezeigt, die Ihren Bedingungen entsprechen.

   b. Klicken Sie in der Spalte Nummer auf ein Element, um den Datensatz zu öffnen.

   c. Klicken Sie im angezeigten Datensatz rechts neben den Feldern „Schwachstellengruppe“ oder „Schwachstellenelement“ auf das Informationssymbol für das angreifbare Element, um die Datensätze anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**d.** Klicken Sie im angezeigten Dialogfeld auf **Datensatz öffnen**.
Informationen zum Korrekturzieldatum werden angezeigt. Klicken Sie im Abschnitt „Zugehörige Listen“ auf eine zugehörige Liste, um weitere Informationen zum AE anzuzeigen.

**8.** Wenn Sie bereit sind, die neue VUL mit den AEs zu erstellen, die Ihren Bedingungen entsprechen, schließen Sie das Vorschaufenster, um zum Formular „Aufgabe teilen“ im anderen Fenster zurückzukehren, und klicken Sie oben im Formular auf **Aufgabe**teilen.

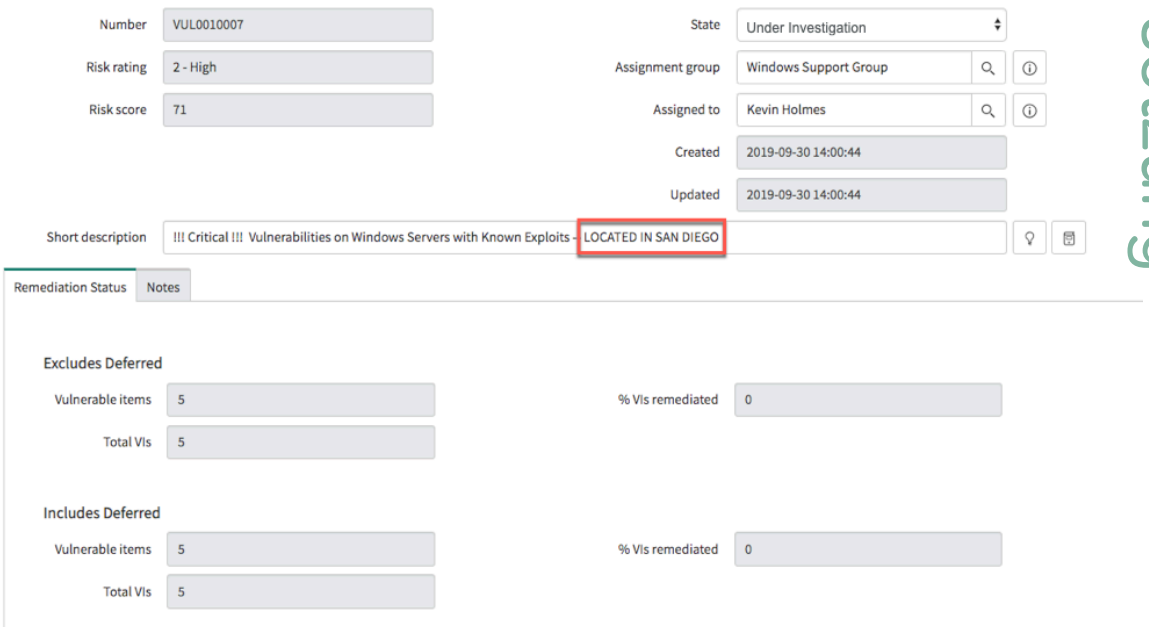
### Hinweis:

Bei weniger als 200 AEs wird der Aufteilungsvorgang synchron ausgeführt.

Bei mehr als 200 VIs wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die VIs in der neuen Gruppe angezeigt werden.

Eine Bestätigungsmeldung wird angezeigt, die alle aktiven AEs anzeigt, die in die neue Gruppe verschoben wurden. Die neue Nummer der Korrekturaufgabe wird ebenfalls angezeigt. Wenn sie sich nicht bereits im Status „Wird untersucht“ befindet, wird die VUL in den Status „Wird untersucht“ verschoben. Überprüfen Sie das Feld Kurzbeschreibung auf den Text, den Sie für die neue VUL in eingegeben haben (BEFINDET SICH SAN DIEGO).

Rollup-Berechnungen für die neue Gruppe werden durchgeführt, um die neue Risikopunktzahl, das Korrekturzieldatum und andere Feldwerte zu berechnen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die angreifbaren Elemente, bevorzugten Lösungen und Change-Anforderungen werden in den zugehörigen Listen am unteren Rand des Datensatzes angezeigt. Verarbeiten und überwachen Sie diese neue Aufgabe wie jede andere Korrekturaufgabe.

9. **Wahlweise:** Scrollen Sie zur zugehörigen Liste **Notizen**, und klicken Sie darauf, um sie auszuwählen. Bestätigen Sie, dass die Anzahl der angreifbaren Elemente aus der ursprünglichen Korrekturaufgabe in die neue Gruppe im Aktivitätenstrom verschoben wurde.
10. **Wahlweise:** Um in der neuen VUL die VIs aus der zugehörigen Liste „Angreifbare Elemente“ auszuwählen und erneut aufzuteilen, scrollen Sie zum Ende des Datensatzes der Schwachstellengruppe, und wählen Sie die VIs, die Sie verschieben möchten, in der Spalte Angreifbares Element der zugehörigen angreifbaren Elemente aus -Liste wählen Sie in der Auswahlliste Aktionen für ausgewählte Zeilen die **Option Aufgabe aufteilen**aus.
    Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.
11. Um die Gruppe erneut aufzuteilen und die ausgewählten Elemente in eine neue Gruppe zu verschieben, klicken Sie auf **Aufgabe**teilen.
    Die ausgewählten AEs werden in eine andere Korrekturaufgabe verschoben, die Bestätigungsmeldung wird angezeigt und die neue Gruppe wird angezeigt.
12. Wählen Sie einen aus, um die Untersuchung oder Korrektur fortzusetzen.

### Nächste Maßnahme

Überwachen Sie den Status der neuen VUL, um die Lösung zu beschleunigen.

#### Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Es besteht eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben (VULs) und den Statusfeldern von Change-Anforderungen (CHG) im Produkt Vulnerability Response. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, wird auch der Status der zugehörigen Korrekturaufgaben automatisch verschoben.

## Übersicht

Der Datensatz der Korrekturaufgabe wird in den folgenden Abschnitten als VUL bezeichnet. In früheren Versionen von Vulnerability Responsewurden Korrekturaufgaben als Schwachstellengruppen (VG) bezeichnet. In den folgenden Bildern ist VG = Korrekturaufgabe oder ein VUL-Datensatz.

Die Statussynchronisierung wird durch eine Systemeigenschaft (sn_vul.cr_state_synch) standardmäßig in Ihrer Instanz aktiviert, wenn Sie die Anwendung Vulnerability Response herunterladen.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG-Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn eine neue CHG für eine Korrekturaufgabe (VUL) erstellt wird und sich diese nicht in „ Warten auf Implementierung“ befindet, wird der VUL-Status in „Warten auf Implementierung“ verschoben.
- Wenn ein vorhandener CHG einer VUL zugeordnet ist und sich dieser nicht in „ Warten auf Implementierung“ befindet, wird der VUL-Status in „Warten auf Implementierung“ verschoben.
- Nachdem die Aufgaben in einem CHG abgeschlossen (Implementiert) sind und das CHG in den Status Überprüfung verschoben wurde, wird die VUL in den Status Gelöstverschoben.



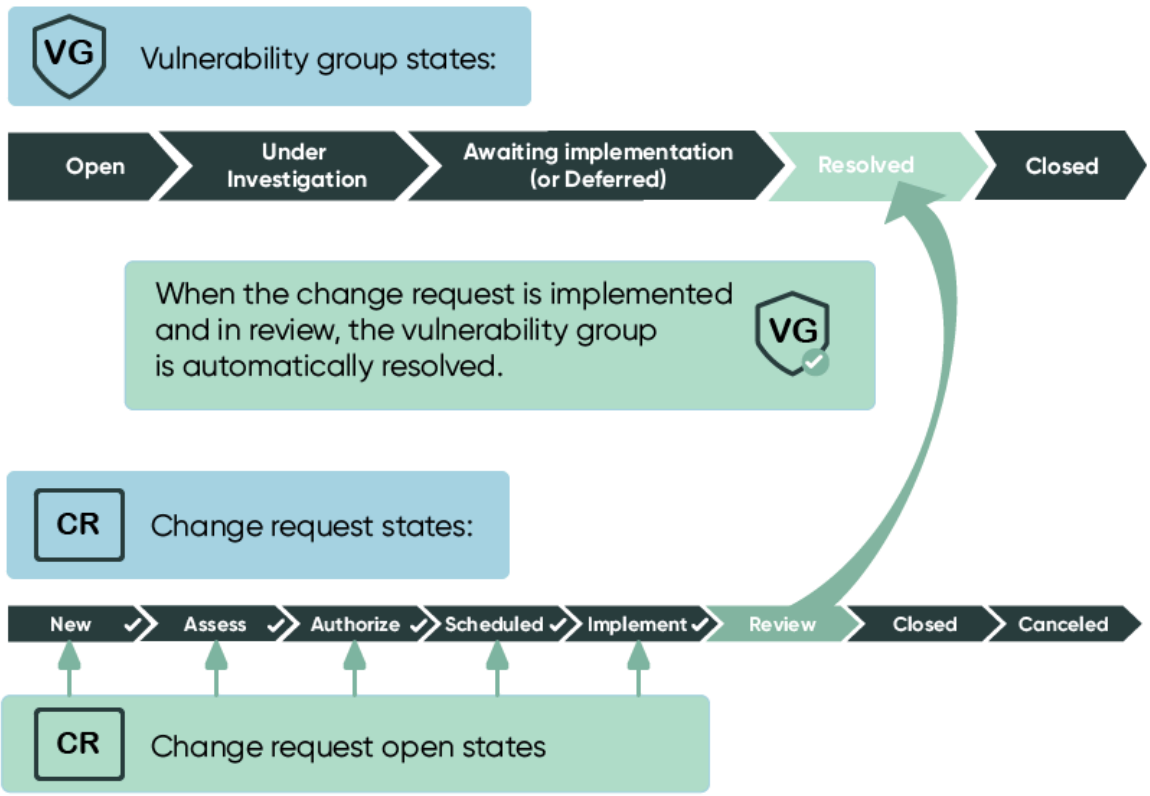
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen und Beispiele für die Statussynchronisierung finden Sie in den folgenden Abschnitten.

**Hinweis:**
Sie können CHGs und VULs weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer VUL entfernen, wird der Status geändert -Synchronisierung kann möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben die VUL jedoch nicht automatisch aus den Status „ Geschlossen “ oder „Zurückgestellt“.

## Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-Status VUL-Status in einem Vorwärtslebenszyklus automatisch verschieben, d. h. von Offen zu Gelöst.




Automatische Übersetzung

Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als Geschlossenerstellen. Die Statussynchronisierung verschiebt die VUL automatisch bidirektional durch die Status „ Offen“, „Wird untersucht“, „ Warten auf Implementierung“ und „ Gelöst “. Diese Verschiebung basiert auf bestimmten Werten des Statusfelds im Change Request. Die Statussynchronisierung zwischen Change-Anforderung und Korrekturaufgabe wird automatisch aufgerufen, es sei denn, das Kontrollkästchen (CIs zu CR hinzufügen) wird in einem Formular angezeigt, und Sie deaktivieren das Kontrollkästchen.

Die VUL wird nicht in den Status „ Gelöst “ versetzt, wenn sich ein CHG im offenen Status befindet. Alle CHGs, die sich in ihrem Lebenszyklus in einem Status vor der Überprüfungbefinden, z. B. „ Neu“, „Bewerten“, „ Autorisieren“, „ Geplant “ oder „ Implementieren “, wie in der vorherigen Abbildung dargestellt, gelten als offene Status für die CHG. Offene Status verschieben das Statusfeld in VUL nicht, da Untersuchungen oder Aufgaben in CHG nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn eine CHG für die VUL erstellt oder ihr zugeordnet wird oder sich der Status einer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorhandenen Beziehung in der CHG ändert. Die abgeschlossenen CHG-Status sind Überprüfen und erfolgreich Geschlossen. Wenn ein CHG erfolgreich geschlossen wird, lauten seine Abschlusscodes: „ Erfolgreich“ oder „ Erfolgreich mit Problemen“. In diesem Fall wird die VUL in den Status „ Gelöst“ verschoben.

### Statussynchronisierung rückwärts

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann er irgendwann abgebrochen werden. In diesem Fall wird die VULautomatisch zurück in den Status „Wird untersucht “ verschoben, wenn CHG Abgebrochenoder Geschlossenist (mit dem Abschlusscode Nicht erfolgreich). Die Schwachstelle wird zurück in den Status „Wird untersucht“ verschoben, da kein aktiver Plan zur Behebung der Schwachstelle vorhanden ist.

Wenn sich eine VUL im Status Gelöst befindet und Sie eine neue CHG erstellen oder sie einer vorhandenen CHG in einem der anfänglichen offenen Status zuordnen, wird die VUL automatisch in den Status „ Warten auf Implementierung“ zurückgesetzt. Die VUL wird in diesen Status zurückgesetzt, da der CHG jetzt mehr Arbeit zugewiesen ist.

### VULs mit mehr als einer CHG

Wenn einer VUL in „ Warten auf Implementierung “ mehr als ein CHG zugeordnet ist, basiert die Statussynchronisierung auf dem Status des CHG im frühesten Status seines Lebenszyklus. Zum Beispiel sind einer VUL vier CHGs zugeordnet: CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle gezeigt.

| CHG-Nummer | CHG-Status |
|---|---|
| 1 | Implementieren |
| 2 | Abgebrochen |
| 3 | Geschlossen (Abschlusscode von Nicht erfolgreich) |
| 4 | Geschlossen (Abschlusscode erfolgreich) |

Die Statussynchronisierung zwischen CHG und VUL basiert in diesem Fall auf CHG1, das sich im frühesten Status der vier CHGs befindet (Implementieren). In diesem Fall bleibt die VUL in „ Warten auf Implementierung“.

In einem anderen Beispiel, wenn sich eine VUL im Status Gelöst befindet und eine vorhandene CHG vorhanden ist, die implementiert wurde und sich im Status Überprüfung befindet, und eine neue CHG erstellt wird, wird die VUL zurück von Gelöst zu Warten auf Implementierungverschoben. Die Statussynchronisierung basiert auf dem CHG im Status Neu, dem CHG im frühesten Status.

| CHG-Nummer | CHG-Status |
|---|---|
| 1 | Prüfung |
| 2 | Neu |

Wenn VULs mehr als eine CHG haben, wechselt der Status der VUL in den folgenden Fällen automatisch:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine CHG zur Überprüfungwechselt und sich alle anderen mit der VUL verknüpften CHGs im Status „ Überprüfen “ oder „ Geschlossen “ befinden (mit einem erfolgreichen Abschlusscode), wird die VUL automatisch in „ Gelöst“ versetzt. Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn eine CHG in den Status „ Abgebrochen “ oder „Geschlossen “ (Abschlusscode von Nicht erfolgreich) verschoben wird und sich alle anderen mit der VUL verknüpften CHGs im selben Status befinden, wird die VUL automatisch in den Status „Wird untersucht“ zurückgesetzt .

Weitere Informationen zu den Status von Korrekturaufgaben und den Möglichkeiten, die Sie in den einzelnen Status haben, finden Sie unter Vulnerability Response Status von Korrekturaufgaben und angreifbaren Elementen.

## Bewerten Sie Ihre Gefährdung durch angreifbare Software

Sie können den Herausgeber und die Produktinformationen im Modul „Risikobewertung“ angeben, um das Zero-Day-Gefahren (aktueller Tag) Ihrer Assets durch angreifbare Software mit der Anwendung ITSM Software Asset Management zu bewerten.

### Vorbereitungen

Weitere Informationen zu Systemanforderungen finden Sie unter Konfigurieren Sie die Risikobewertung.

Zeigen Sie das Software-Risikobewertungsmodul an, und erstellen und bearbeiten Sie Risikobewertungsdatensätze bei Bedarf für angreifbare Software in Ihrer Instanz Now Platform®.

Sie verwalten die Vulnerability Response-Aktivitäten für einen großen Vorgang, der für viele Assets verantwortlich ist. Das Security Operations Center (SOC) in Ihrem Betrieb kontaktiert Sie bezüglich einer Version der Software, von der bekannt wurde, dass sie angreifbar ist. Sie stellen fest, dass ein Scan Ihrer Assets kürzlich abgeschlossen wurde und diese Schwachstelle nicht gefunden wurde. Das SOC-Team hat aus einer zuverlässigen Quelle außerhalb der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder den anderen Bibliotheken von Drittanbietern in Ihrer Instanz von dieser Schwachstelle erfahren, und Sie befürchten, dass Ihr Schwachstellenscanner dies noch nicht getan hat hat das Plugin dafür hinzugefügt.

Sie sind zuversichtlich, dass die Daten für diese Schwachstelle in Kürze im NVD aktualisiert und importiert werden, damit Ihr Scanner diese Schwachstelle beim nächsten Scan erfassen kann. Da Sie jedoch über das Ausmaß Ihrer potenziellen Gefährdung Befürchtungen haben, möchten Sie heute feststellen, ob Sie haben Assets in Ihrem Netzwerk, auf denen diese Software installiert ist.

Erforderliche Rolle: Schwachstellenadministrator (sn_vulnerability_write)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Halten Sie die folgenden Informationen über die angreifbare Software bereit, die Sie bewerten möchten:

- Herausgeber
- Version

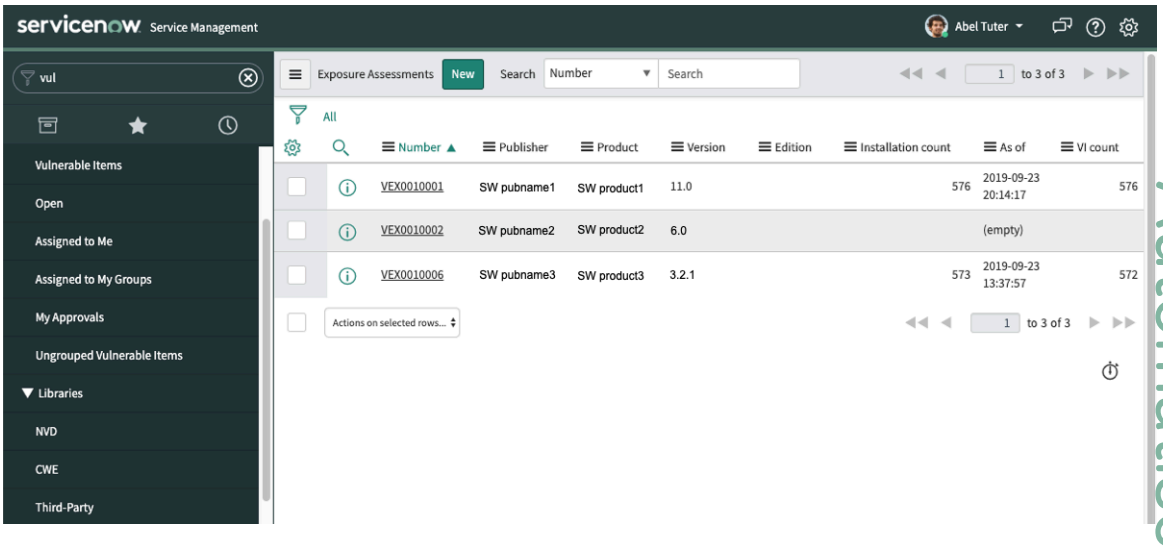


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

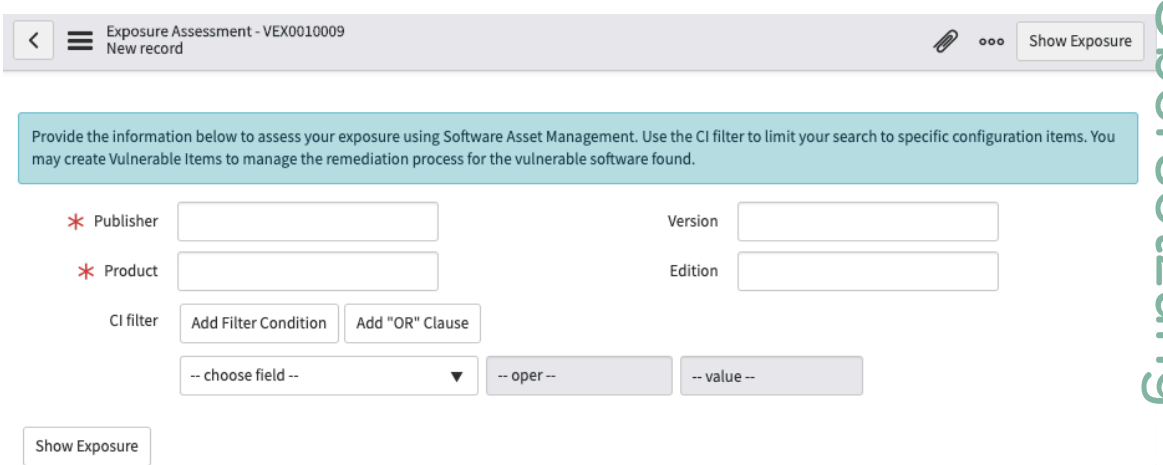
- Produkt
- Edition

### Prozedur

1. Um eine neue Risikobewertung zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Bewertung des Gefahrenpotenzials**.
   Die Liste Risikobewertungen wird angezeigt.




2. Klicken Sie auf **Neu**.
   Das Formular „Risikobewertung“ wird angezeigt.




3. Füllen Sie das Formular aus.

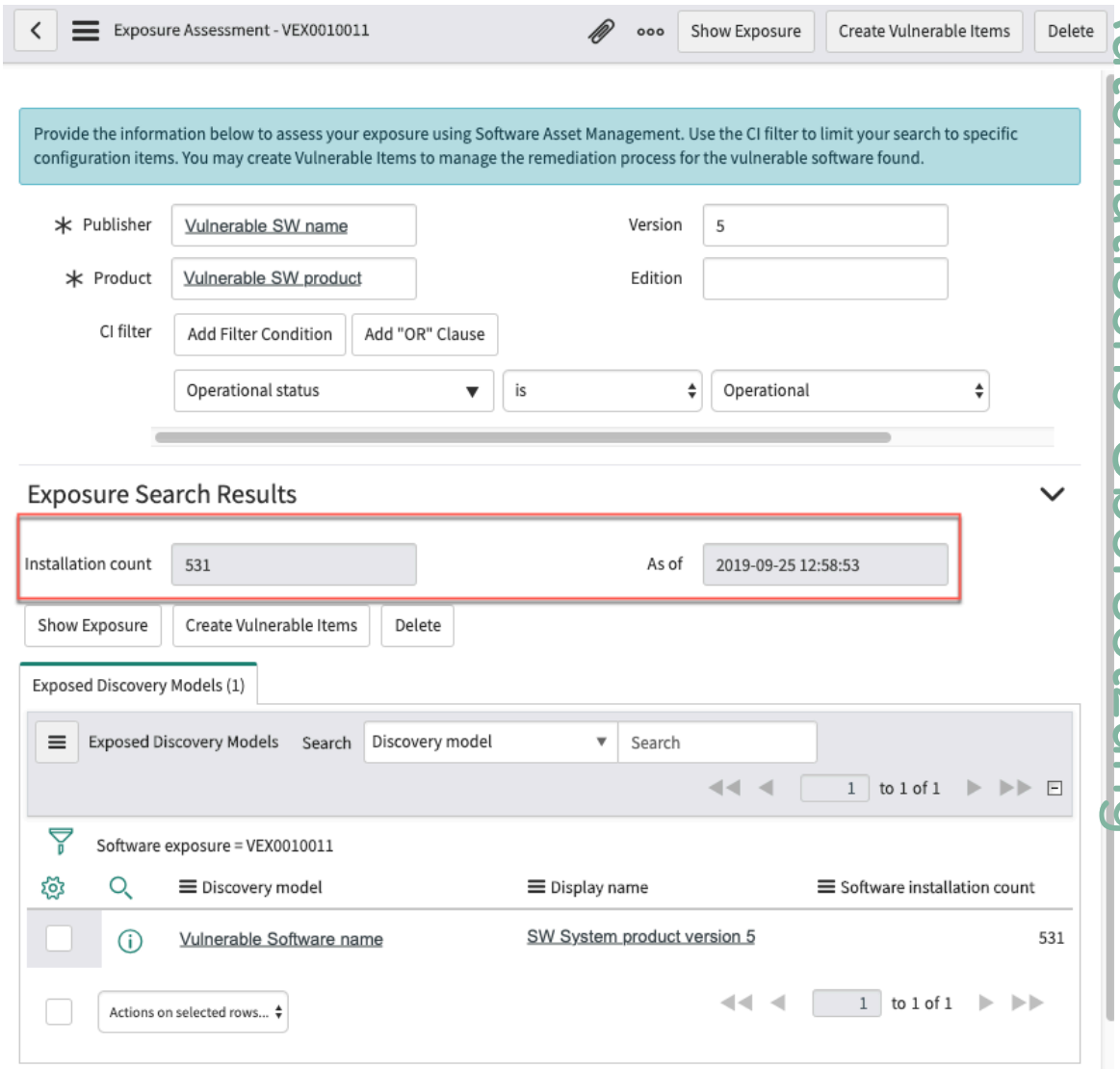
| Feld | Beschreibung |
|---|---|
| Herausgeber | Name des Softwareherausgebers. |
| (Optional) Version | Geben Sie die Versionsnummer ein, um die Suche nach Ihren Assets einzugrenzen. |
| Produkt | Name des Softwareprodukts. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| (Optional) Edition | Geben Sie die Edition ein, um die Suche nach Ihren Assets einzugrenzen. |
| CI-Filter | Verwenden Sie die Auswahllisten für den Configuration Item (CI)-Filter, um Ihre Suche auf bestimmte Konfigurationselemente (Assets) zu beschränken. Sie können beispielsweise eine Abfrage nur für aktive Assets senden, auf denen diese Software möglicherweise installiert ist:<br><br>Betriebsstatus ist „Operativ“. |

4. Klicken Sie **auf Risiko anzeigen**.
   Der Risikobewertungsdatensatz wird mit Ihrem Discovery-Modell und der Anzahl der Softwareinstallationen für Ihre Assets zum angegebenen Datum angezeigt.




5. Wählen Sie eine, um fortzufahren.

6. **Wahlweise:** Erstellen Sie ein angreifbares Element für Ihr Suchergebnis.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Nachdem Sie angreifbare Elemente erstellt haben, können Sie die Suchkriterien für diesen Risikodatensatz nicht mehr ändern.

7. Alternativ können Sie Ihre Filterbedingungen überarbeiten und Ihre Suchergebnisse weiter verfeinern.
8. Führen Sie die folgenden Schritte aus, um angreifbare Elemente zu erstellen:

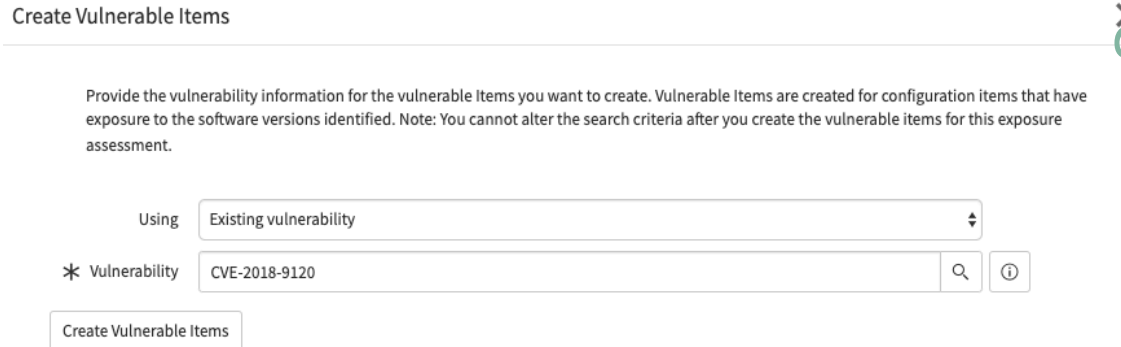
   a. Klicken **Sie auf Angreifbare Elemente erstellen**.
   Das Dialogfeld „Angreifbare Elemente erstellen“ wird angezeigt.

   b. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Arbeiten mit | Wählen Sie aus der Auswahlliste eine Option aus, um fortzufahren.<br>▪ **Vorhandene Schwachstelle**. Klicken Sie rechts neben dem Feld Schwachstelle auf das Suchsymbol. Wählen Sie in der angezeigten Liste die CVE-ID aus, oder geben Sie Suchkriterien ein, um die vorhandene CVE-ID zu finden, z. B. CVE 2018-9120.<br>**Hinweis:** Dies kann eine CVE-ID aus einer anderen Schwachstellendatenbank als dem NVD sein.<br>▪ **Neue Schwachstelle**. Geben Sie die CVE-ID für Ihre neue Schwachstelle im Format xxxx-xxxx, xxxx-xxxxx oder xxxx-xxxxxxx ein. |
| Schwachstellenübersicht (nur für neue Schwachstelle) | Geben Sie eine Zusammenfassung für die neue Schwachstelle ein, z. B. Ein Angreifer kann ein Skript im Browser eines ahnungslosen Benutzers ausführen. |

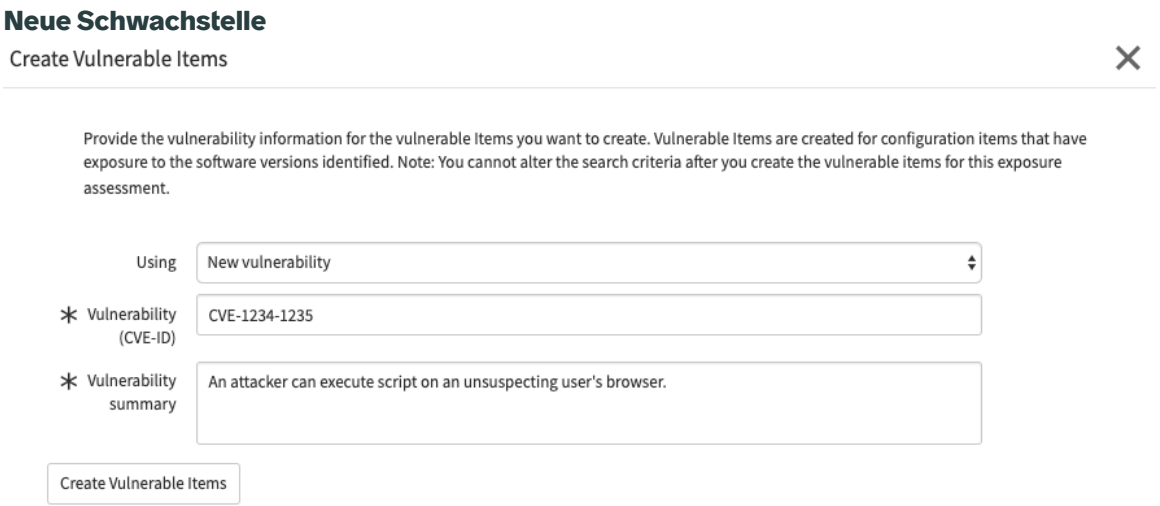
Die folgenden Abbildungen zeigen Beispiele des ausgefüllten Formulars für eine vorhandene und eine neue Schwachstelle.

**Vorhandene Schwachstelle**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



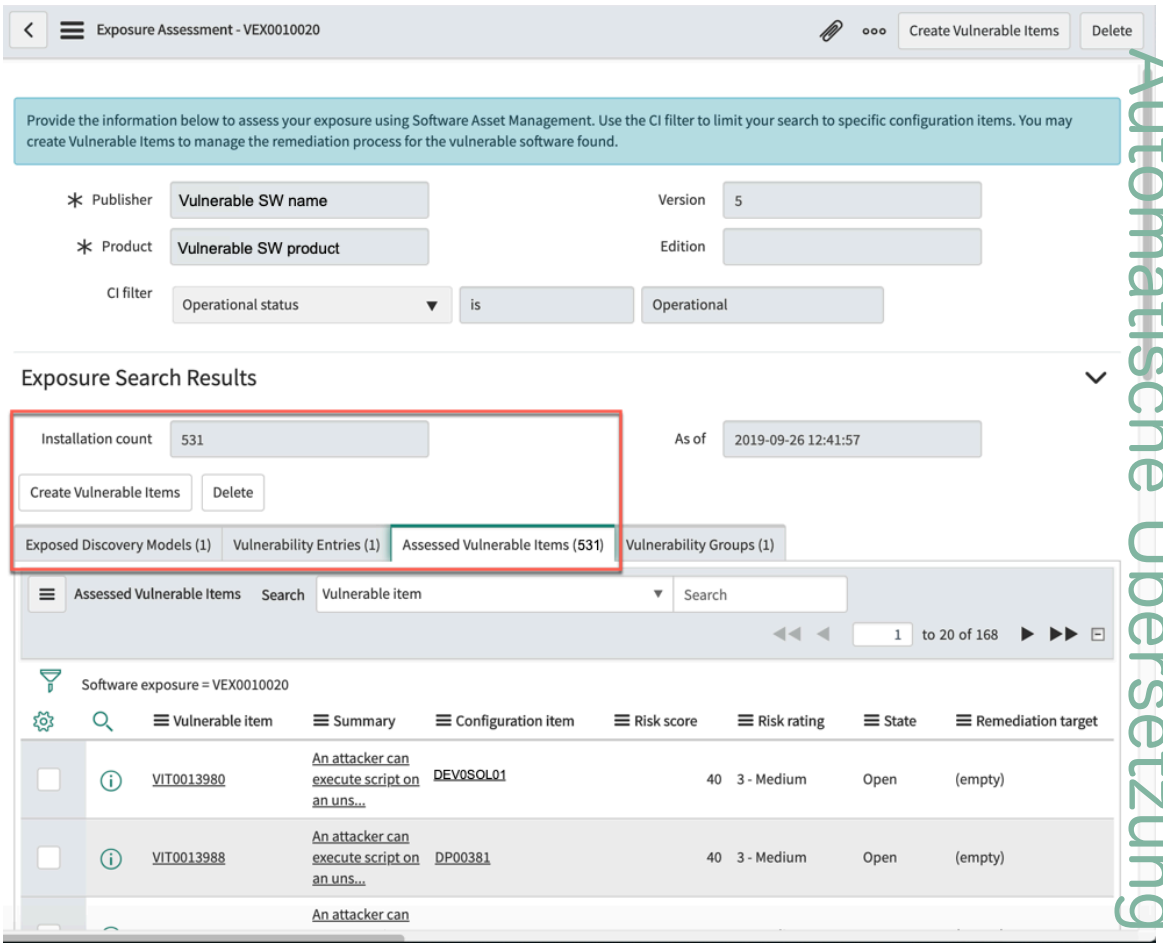

**c.** Klicken **Sie auf Angreifbare Elemente erstellen**.
Der Datensatz „Risikobewertung“ wird mit einer Statusmeldung angezeigt, die angibt, dass angreifbare Elemente erstellt werden.

**d.** Klicken Sie nach einigen Sekunden oben im Formular mit der rechten Maustaste auf das graue Banner, um die Seite neu zu laden.
Die neuen angreifbaren Elemente werden wie in der folgenden Abbildung auf der Registerkarte „Bewertete angreifbare Elemente“ (531) angezeigt. Die für diese angreifbaren Elemente erstellte neue Korrekturaufgabe wird auf der Registerkarte „Korrekturaufgabe“ (1) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
In diesem Beispiel wird eine Korrekturaufgabe gemäß den Gruppenregeln und Bedingungen aus der Regel für Korrekturaufgaben mit der Bezeichnung Schwachstelle erstellt. Diese Gruppenregel ist die Standardregel für Korrekturaufgaben, die mit dem Vulnerability Response-Produkt in Ihrer Now Platform® -Instanz installiert wird. In diesem Beispiel wurden durch die Bedingungen dieser Gruppenregel alle angreifbaren Elemente in einer einzigen Korrekturaufgabe zusammengefasst. Wenn Sie es vorziehen, mehr als eine Korrekturaufgabe für die angreifbaren Elemente zu erstellen, die den Suchergebnissen der Risikobewertung entsprechen, ziehen Sie es möglicherweise vor, zusätzliche Regeln für Korrekturaufgaben einzurichten. Durch das Erstellen weiterer Korrekturaufgaben können Sie die Erstellung von Korrekturaufgaben mit einer großen Anzahl angreifbarer Elemente verhindern. Weitere Informationen zu Regeln für Korrekturaufgaben finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgaben.

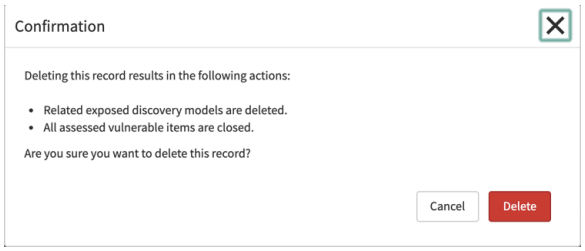



Automatische Übersetzung

**9.** Wählen Sie eine, um fortzufahren.

| Option | Beschreibung |
|---|---|
| Korrekturaufgaben | Klicken Sie bei ausgewählter Registerkarte Korrekturaufgaben in der Nummernspalte auf den Datensatz, um die Aufgabe zu überprüfen und zuzuweisen. Weitere Informationen zu Zuweisungsgruppen finden Sie unter Creating groups . |
| Bewertete angreifbare Elemente | Klicken Sie bei ausgewählter Registerkarte Bewertete angreifbare Elemente in der Spalte Angreifbares Element auf, um die Datensätze |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | zu öffnen und einzelne angreifbare Elemente zu überprüfen und zuzuweisen. |
| Löschen | Löschen Sie den Risikobewertungsdatensatz. Ein Bestätigungsdialogfeld wird angezeigt.<br>**Hinweis:**<br>Wenn Sie den Gefährdungsdatensatz löschen, nachdem Sie angreifbare Elemente erstellt haben, werden alle angreifbaren Elemente, die Sie für diesen Datensatz erstellen und die sich nicht auf einen anderen Gefährdungsdatensatz beziehen, automatisch in den Status Geschlossen verschoben. Der Grund für die Schließung ist Abgebrochen. |
| |  |

### Nächste Maßnahme

Reagieren Sie auf Zero-Day-Bedrohungen (aktueller Tag) basierend auf Ihrer Gefährdungsbewertung. Weitere Informationen zu Korrekturaufgaben und Change Management für Vulnerability Responsefinden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Change Management für Vulnerability Response.

## Zuweisungsempfehlungen anzeigen

Eine Zuweisungsgruppe wird normalerweise mithilfe von Zuweisungsregeln einem angreifbaren Element zugewiesen. Diese Regeln werden vom Schwachstellenadministrator konfiguriert, um die richtigen Zuweisungsgruppen zuzuweisen, die auf den Daten basieren, die von Scannern von Drittanbietern empfangen wurden.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Wenn eine übereinstimmende Zuweisungsgruppe nicht verfügbar oder falsch ist, können Sie Empfehlungen für die Zuweisung von Schwachstellen verwenden, um alternative Zuweisungsgruppen anzuzeigen.

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen, um die folgenden Aktionen auszuführen:

- Fordern Sie Zuweisungsgruppenempfehlungen für ein angreifbares Element anan.
- Fordern Sie Zuweisungsgruppenempfehlungen für mehrere angreifbare Elemente an.
- Fordern Sie Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe an.

### Fordern Sie Zuweisungsgruppenempfehlungen für ein angreifbares Element an

Fordern Sie Empfehlungen für die Zuweisung von Schwachstellen an, damit Sie Zuweisungsgruppenempfehlungen anzeigen können. Sie können Empfehlungen anfordern,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wenn eine übereinstimmende Zuweisungsgruppe für ein angreifbares Element (AE) nicht verfügbar oder falsch ist.

### Vorbereitungen
Erforderliche Rolle: sn_vul.remediation_owner

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** und öffnen Sie eine VI.
   Das Element muss sich im Status „Offen“, „Zurückgestellt“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld **Zuweisungsgruppe,** um Zuweisungsvorschläge für diesen VI anzuzeigen.
3. Wählen Sie im Dialogfeld „Zuweisungsgruppenempfehlungen“ eine Empfehlung aus, die auf der Konfidenzpunktzahl basiert.
   Die Konfidenzpunktzahl sagt voraus, wie relevant die Übereinstimmung für den VI ist. Weitere Informationen finden Sie unter Lösungen für maschinelles Lernen für Vulnerability Response.
4. Klicken Sie auf **Zuweisen**.

### Ergebnisse
Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt, und der Zuweisungstyp ändert sich in Empfehlung.

## Fordern Sie Zuweisungsgruppenempfehlungen für mehrere angreifbare Elemente an

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen, um die Zuweisungsgruppenempfehlungen für mehrere angreifbare Elemente (VIs) mithilfe einer Massenbearbeitung anzuzeigen. Wenn mehrere VIs ausgewählt sind, wird eine Vorhersage für eine Zufallsstichprobe der ausgewählten VIs durchgeführt.

### Vorbereitungen
Erforderliche Rolle: sn_vul.remediation_owner

### Warum und wann dieser Vorgang ausgeführt wird
Die Empfehlungen und ihre Konfidenzwerte können sich je nach den aus den ausgewählten AEs entnommenen Beispielen geringfügig unterscheiden. Die Konfidenzpunktzahl wertet aus, ob das System davon ausgeht, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Verwenden Sie die Systemeigenschaft „ `assignment_recommendation_batchsize` “, um die Batch-Größe festzulegen, wenn Sie Empfehlungen für die Zuweisung von Schwachstellen für Korrekturaufgaben (VULs) und VIs mithilfe der Massenbearbeitungsoption anfordern. Der Standardwert dieser Systemeigenschaft ist auf eine optimale Vorhersageleistung festgelegt.

**Hinweis:**
Wenn Sie den Standardwert erhöhen, kann sich die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen für diese Fälle ändern.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbares Element** und wählen Sie mehrere AEs aus.
   Die Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie **auf Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Massenangreifbare Elemente“

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Datensätze, die für die Massenbearbeitung ausgewählt werden sollen. |
| Zuweisungsgruppe | Zuweisungsgruppe, die für die ausgewählten angreifbaren Elemente festgelegt werden soll. Um die empfohlenen Zuweisungsgruppen anzuzeigen, klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld. Wählen Sie eine Empfehlung aus, die auf der Konfidenzpunktzahl basiert, und klicken Sie auf **Zuweisen**. |
| Arbeitsnotizen | Notizen, die hinzugefügt werden sollen. |

4. Klicken Sie auf **OK**.

## Ergebnisse
Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt, und der Zuweisungstyp ändert sich für alle ausgewählten AEs in Empfehlung.

### Fordern Sie Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe an

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen, um Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe (VUL) anzuzeigen.

## Vorbereitungen
Erforderliche Rolle: sn_vul.remediation_owner

## Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die Systemeigenschaft „ assignment_recommendation_batchsize “, um die Batch-Größe festzulegen, wenn Sie Empfehlungen für die Zuweisung von Schwachstellen für VULs und angreifbare Elemente (AEs) mithilfe der Massenbearbeitungsoption anfordern. Der Standardwert dieser Systemeigenschaft ist auf eine optimale Vorhersageleistung festgelegt.

**Hinweis:**
Wenn Sie den Standardwert erhöhen, kann sich die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen für diese Fälle ändern.

## Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** und wählen Sie eine VUL aus.
   Die Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) neben dem Feld **Zuweisungsgruppe** für die Zuweisungsgruppenempfehlungen für die ausgewählte VUL.
   Im Dialogfeld „Zuweisungsgruppenempfehlungen“ werden die empfohlenen Zuweisungsgruppen mit der durchschnittlichen Konfidenzpunktzahl für alle AEs in dieser Gruppe angezeigt.
3. Wählen Sie eine Empfehlung aus der Liste Zuweisungsgruppe basierend auf der Konfidenzpunktzahl aus.
   Die Konfidenzpunktzahl sagt voraus, wie relevant die Übereinstimmung für die ausgewählte VUL ist.
4. Klicken Sie auf **Zuweisen**.
   Die ausgewählte Gruppe wird im Feld **Zuweisungsgruppe** angezeigt.
5. Speichern Sie die Korrekturaufgabe mit den aktualisierten Informationen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse
Alle VIs mit derselben Zuweisungsgruppe wie die VUL werden der ausgewählten Zuweisungsgruppe zugewiesen. Der Zuweisungstyp ändert sich in Empfehlung für die VUL sowie für alle geänderten AEs.

## Eine Ausnahme anfordern und genehmigen

Sie können anfordern, dass die Korrektur eines angreifbaren Elements oder einer Korrekturaufgabe für einen bestimmten Zeitraum zurückgestellt wird. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen von anderen Benutzern genehmigen.

Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

- Fordern Sie eine Ausnahme für ein angreifbares Element an
- Fordern Sie eine Ausnahme für eine Korrekturaufgabe an
- Fordern Sie eine Massenausnahme an

Sie können Richtlinienausnahmen auch mit GRC: Policy and Compliance Managementanfordern:

- Fordern Sie eine Ausnahme mit an GRC: Policy and Compliance Management
- Fordern Sie eine Massenausnahme mit an GRC: Policy and Compliance Management

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Fordern Sie eine Ausnahme für ein angreifbares Element an

Fordern Sie eine Ausnahme für ein angreifbares Element (AE) an, das nicht sofort korrigiert werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.remediation_owner

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Sie können auch Ausnahmen für AEs in der klassischen Umgebung anfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

## Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle**.
2. Wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Klicken Sie im Formular „Angreifbares Element“ auf **Ausnahme anfordern**.
4. Wenn Vulnerability Response im Bildschirm „Exception Management“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der im ausgewählten Zeitraum liegen **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** -Bildschirm.<br><br>Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „Offen“ zurück.<br><br>**Hinweis:**<br>Wenn ab Version 18.0 von Vulnerability Response (VR) die Korrektur eines angreifbaren Elements mithilfe der Ausnahmeverwaltungsfunktion zurückgestellt wurde, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum im Falle einer erneuten Öffnung durch den Scanner erhalten. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vul.auto_defer_vit_in_active_exception_win` auf „true“ fest. Außerdem bleibt das zurückgestellte **Bis** -Datum bestehen, auch nachdem das angreifbare Element geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle ist sn_vul.manage_exception_configuration für Lese- und Schreibvorgänge. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Grund | Grund für die Anforderung. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Behebung nicht verfügbar<br>○ Ausgleichende Steuerung vorhanden<br>○ Sonstige<br>Informationen zum Hinzufügen neuer Grundoptionen finden Sie unter Definieren Sie die Ursachenzuordnung für Richtlinien. |
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer aktualisiert werden. |

5. Senden Sie die Ausnahmeanforderung, indem Sie auf **Genehmigung**anfordern klicken.

### Ergebnisse
Der Status des angreifbaren Elements ändert sich in Wird überprüft. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

## Fordern Sie eine Ausnahme für eine Korrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

### Vorbereitungen
Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können auch Ausnahmen für Korrekturaufgaben in der klassischen Umgebung anfordern.

### Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Wählen Sie im Datensatz der Korrekturaufgabe (VUL) die Option **Ausnahme anfordern**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist. |
| Grund | Begründung für die Anforderung einer Ausnahme. |
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden. |

5. Klicken Sie auf **Genehmigungs-Engine**.

### Fordern Sie eine Massenausnahme an

Verwenden Sie die Massenbearbeitungsoption, um eine Ausnahme für mehrere angreifbare Elemente (VIs) anzufordern, anstatt jedes Element manuell auszuwählen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_analyst

Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn mehrere VIs ausgewählt sind, wird eine Korrekturaufgabe (VUL) mit diesen Elementen gebildet. Weitere Informationen zum Bearbeiten mehrerer VIs finden Sie unter Bearbeiten Sie angreifbare Elemente im Massenvorgang in Vulnerability Response.

#### Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Elemente aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie **auf Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Massenbearbeitung für angreifbares Element“.**

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben. |
| Status | Status des angreifbaren Elements. Wählen Sie den Status Zurückgestellt aus, um eine Ausnahme für die ausgewählten Elemente anzufordern. |
| Grund | Substatus für den von Ihnen ausgewählten Status. |
| Kurzbeschreibung | Name der Korrekturaufgabe, die Sie erstellen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Bis | Enddatum, das Sie für Ihre Ausnahmeanforderung angeben. |
| Zusätzliche Informationen | Weitere Details, die Sie angeben möchten, um den Genehmiger über die Gründe für Ihre Anforderung zu informieren. |
| Bevorzugte Lösung | Lösung, die auf die Korrektur aller angreifbaren Elemente abzielt, die Sie für eine Massenbearbeitung ausgewählt haben. |
| Zuweisungsgruppe | Zuweisungsgruppe für die VI. Sie können eine Gruppe manuell auswählen oder Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist. |
| Arbeitsnotizen | Notizen, die hinzugefügt werden sollen. |

4. Klicken Sie auf **OK**.
   Eine Korrekturaufgabe mit den von Ihnen ausgewählten VIs wird erstellt. Diese Korrekturaufgabe wird zur Genehmigung übermittelt.

### Fordern Sie eine Ausnahme mit an GRC: Policy and Compliance Management

Fordern Sie Richtlinienausnahmen mit der Funktion GRC zur Verwaltung von Richtlinienausnahmen in der Anwendung Policy and Compliance Management aus Vulnerability Responsean.

## Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Policy and Compliance Management aus dem ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Benutzeroberfläche anfordern:

## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** (oder **Korrekturaufgaben**)>**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme anfordern**.
3. Füllen Sie die Felder des Formulars aus.

### Formular „Ausnahme anfordern“.

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Kontrollziel | Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und sich der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ ändert.<br>**Hinweis:**<br>Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in Policy and Compliance festgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen. |
| Grund | Grund für die Anforderung einer Ausnahme. |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden. |

4. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management.

### Fordern Sie eine Massenausnahme mit an GRC: Policy and Compliance Management

Wählen Sie eine Gruppe angreifbarer Elemente aus, und übermitteln Sie eine Massenausnahme.

#### Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen zum Anfordern von Massenausnahmen verwenden können, müssen Sie die Anwendung GRC: Policy and Compliance Management aus dem ServiceNow Storeherunterladen.

**Hinweis:**
Um diese Funktion zu verwenden, müssen Sie GRC: Policy and Compliance Management vor dem Upgrade von Vulnerability Response] aktualisieren. Wenn Sie Vulnerability Response bereits vor GRC: Policy and Compliance Managementaktualisiert haben und diese Funktion verwenden möchten, müssen Sie die Upgrade-Verfahren in der richtigen Reihenfolge erneut ausführen.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Umgebung in Vulnerability Responseanfordern.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Elemente aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen den Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ aufweisen.
2. Klicken Sie **auf Massenbearbeitung**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Massenbearbeitung für angreifbares Element“.**

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben. |
| Status | Status des angreifbaren Elements. Wählen Sie den Status Zurückgestellt aus, um eine Ausnahme für die ausgewählten Elemente anzufordern. |
| Kurzbeschreibung | Name der Aufgabe, die Sie erstellen. |
| Bevorzugte Lösung | Lösung, die Sie zur Korrektur aller angreifbaren Elemente anstreben, die Sie für die Massenbearbeitung ausgewählt haben. |
| Zuweisungsgruppe | Zuweisungsgruppe für die VI. Sie können eine Gruppe manuell auswählen oder Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist. |
| Arbeitsnotizen | Notizen, die hinzugefügt werden sollen. |

4. Klicken Sie auf **OK**.
   Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt.
5. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |
| Kontrollziel | Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und sich der Status des angreifbaren Elements oder |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ ändert.<br><br>**Hinweis:**<br>Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in GRC: Policy and Compliance Managementfestgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen . |
| Grund | Grund für die Anforderung einer Ausnahme. |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden. |

6. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management .

### Genehmigen Sie eine Ausnahmeanforderung in Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Elemente oder Korrekturaufgaben, die nicht sofort korrigiert werden können. Sie müssen diese Anforderungen auf Risiken bewerten und sie dann zur Zurückstellung genehmigen, bis sie korrigiert werden können.

#### Vorbereitungen

Sie können Ausnahmen und falsch positive Anforderungen im Vulnerability Response -Arbeitsbereich genehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

Erforderliche Rolle: sn_vul.exception_approver

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen.

**Hinweis:**

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

## Arbeiten mit einer Ausnahmeregel

Sie können eine Ausnahme für Schwachstellen, angreifbare Elemente (VIs) oder Konfigurationselemente (CIs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch die Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden VIs basierend auf der Regel zurückstellen, wenn das System sie identifiziert.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Ausnahmeregel erstellen
- Antrag auf Ausnahmeregel genehmigen
- Ausnahmeregel aktivieren
- Öffnen Sie eine Ausnahmeregel erneut
- Aktualisieren Sie eine genehmigte Ausnahmeregel
- Ausnahmeregel löschen

### Hinweis:

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Ausnahmeregel erstellen

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Elementen (VIs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser VIs basiert. Mit dieser Regel können Sie neue und vorhandene AEs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Die Regel wird vom „Gültig ab“-Datum bis zum „Gültig bis“-Datum angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die Gruppierungsmethode für diese VUL wird als Ausnahmeregel bezeichnet. Die VUL wird im Status „Zurückgestellt“ erstellt. Sie können diese VUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete AEs werden zurückgestellt und dieser VUL ab dem „Gültig ab“-Datum hinzugefügt, bis die Gruppe am „Gültig bis“-Datum abläuft.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

**Hinweis:**

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann zur Genehmigung erneut übermitteln.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Klicken Sie auf der Seite „Ausnahmeregel für neuen Datensatz“ auf **Neu**, um eine Regel zu erstellen.
3. Füllen Sie die Felder des Formulars aus.

#### Formular „Ausnahmeregel“

| Feld | Beschreibung |
|---|---|
| Name | Name der Ausnahmeregel. |
| Gültig ab | Datum, ab dem diese Regel aktiv ist, um die AEs zurückzustellen. |
| Gültig bis | Datum, ab dem die Korrekturaufgabe keine neuen VIs mehr akzeptiert. |
| Grund | Grund für die Erstellung dieser Ausnahmeregel. |
| Zuweisungsgruppe | Gruppe, der die Korrekturaufgabe zugewiesen ist, die für die Nachverfolgung der zurückgestellten VIs erstellt wurde. |
| Zusätzliche Informationen | Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen. |
| Bedingung | Filterbedingung für die VIs, die während der Verarbeitung der VIs definiert werden kann. |
| Für vorhandene Daten ausführen | Option, mit der Sie diese Regel für vorhandene Daten ausführen können, wenn sie zum ersten Mal ausgeführt wird. |
| Workflow-Phase | Aktueller Genehmigungsstatus der Ausnahmeregel. |
| Status | Status der Ausnahmeregel. |
| Ausführungsbefehl | Eindeutige Reihenfolge für jede Ausnahmeregel. |
| Zurückgestellt bis | Datum, bis zu dem die VULs und VIs zurückgestellt werden. An diesem Datum wird die erstellte VUL geschlossen, alle AEs werden aus der Gruppe verschoben und die Gruppenregeln werden erneut angewendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Senden Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in Wird überprüft. Bis Sie die Ausnahmeregel absenden, bleibt sie im Status Entwurf.

### Antrag auf Ausnahmeregel genehmigen

Bewerten Sie Ausnahmeregelanforderungen von Benutzern, damit Sie diese Anforderungen genehmigen oder ablehnen können.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

Mitglieder der Benutzergruppe des Ausnahmegenehmigers der Ebene 1 können Ausnahmeregelanforderungen der Ebene 1 genehmigen. Ebenso können Benutzergruppenmitglieder von Ausnahmegenehmigern der Ebene 2 Ausnahmeregelanforderungen der Ebene 2 genehmigen. Beide Benutzergruppen erben standardmäßig die Rolle des Ausnahmegenehmigers.

**Hinweis:**

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit ab, und erläutern Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe (RT) im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird diese Regel für alle erstellten AEs sowie für AEs ausgeführt, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. AEs, die den definierten Bedingungen entsprechen, werden dem RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   **Hinweis:**
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann zur Genehmigung erneut übermitteln.

### Ausnahmeregel aktivieren

Eine Regel wird an ihrem „Gültig ab“-Datum aktiviert. Nach der Aktivierung wird der Ausnahmeprozess für angreifbare Elemente (AEs) automatisiert.

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen angreifbaren Elemente (AEs), die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten AEs, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird geändert zu Zurückgestellt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wenn ein neu erstellter VI mit der Ausnahmeregelbedingung übereinstimmt, wird er in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht darauf ausgeführt.
3. Am Datum „Gültig ab“ werden vorhandene VIs hinzugefügt, wenn Sie die Option Für vorhandene Daten ausführen aktivieren.
4. Die RT akzeptiert keine neuen AEs mehr, wenn die Regel am „Gültig bis“-Datum abläuft. Die RT bleibt bis zum Datum „Zurückgestellt bis“ bestehen.
5. Die Ausnahmeregel läuft am „Gültig bis“-Datum ab.

### Fordern Sie eine Verlängerung für eine Ausnahmeregel an

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie ihr Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein.<br>Zur Auswahl stehen:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.
- Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Öffnen Sie eine Ausnahmeregel erneut

Öffnen Sie eine abgelehnte Ausnahmeregel erneut, die Sie jedoch erneut übermitteln möchten. Wenn Sie die Regel erneut öffnen, wird sie in den Status „Entwurf“ versetzt.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Anschließend können Sie die Regel aktualisieren und erneut zur Genehmigung übermitteln.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut**öffnen.
3. Aktualisieren Sie das Formular, und übermitteln Sie es erneut zur Genehmigung.

### Aktualisieren Sie eine genehmigte Ausnahmeregel

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Datumsangaben ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Elemente (AEs) in den Status „Offen“ versetzt werden.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Gruppenregeln werden auf diese AEs erneut angewendet. Senden Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie den Genehmigungsprozess erneut durchläuft.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im Dialogfeld „Regel abbrechen“ auf **Regel abbrechen**.
   Die Regel wird wieder in den Status „Entwurf“ verschoben, und die zugehörige VUL wird gelöscht. Die zugehörigen AEs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen AEs angewendet.

### Ausnahmeregel löschen

Löschen Sie eine Ausnahmeregel, die nicht mehr benötigt wird. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Element (AE) während der Erfassung nicht zurückstellen möchten.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Durch das Löschen einer Regel wird die zugeordnete Korrekturaufgabe (VUL) abgebrochen. Die zugehörigen AEs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen AEs angewendet.

#### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie im Dialogfeld „ **Regel** löschen“ auf Regel löschen, um die ausgewählte Regel zu löschen.
   Die zugeordnete Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen AEs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen AEs angewendet.

## Falsch positive Meldungen markieren und genehmigen

Angreifbare Elemente (AEs) und Korrekturaufgaben (VULs) können als falsch positive Meldungen markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Benutzern genehmigen.

- Als falsch positiv markieren
- Massenbearbeitung für falsch positive Ergebnisse
- Genehmigen Sie ein falsch positives Ergebnis

### Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise ein VI oder eine Korrekturaufgabe als falsch positiv markiert wird, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail mit der Nachricht, dass ein VI oder eine Korrekturaufgabe als falsch positiv markiert wurde.

Ab v21.0 von Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Als falsch positiv markieren

Markieren Sie ein angreifbares Element (VI) oder eine Korrekturaufgabe (VUL) als falsch positiv, wenn die vom Scanner ausgegebene Warnung kein tatsächliches Problem ist. Beispiel: Wenn ein Konfigurationselement außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit verbundenes Problem auslöst, markieren Sie es als falsch positiv.

#### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Sie können falsch positive Meldungen aus den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie ein falsch positives Ergebnis in an IT Remediation Workspace.

Sie können Falschmeldungen auch in der klassischen Umgebung anfordern:

#### Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente (oder Korrekturaufgaben)** > **Alle**.
2. Öffnen Sie den VI oder **VUL**, den Sie als falsch positiv markieren möchten, und klicken Sie auf Als falsch positiv markieren.
   Die VI oder VUL muss sich im Status „ **Offen** “ befinden.
3. Geben Sie im Formular „Falsch positiv“ Details in **Zusätzliche Informationen** ein, und klicken Sie auf **Genehmigung anfordern**.
   Die Genehmigungsanforderung wird gesendet, und der Status des VI oder VUL ändert sich in Wird **überprüft**.

### Massenbearbeitung für falsch positive Ergebnisse

Verwenden Sie die Massenbearbeitung, um mehrere angreifbare Elemente (AEs) als falsch positiv zu kennzeichnen. Wenn mehrere VIs ausgewählt sind, wird eine Korrekturaufgabe mit diesen Elementen gebildet.

#### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

. Informationen zum Anfordern eines falsch positiven Ergebnisses aus den Arbeitsbereichen für Schwachstellen Vulnerability Response finden Sie unter Fordern Sie ein falsch positives Ergebnis in an IT Remediation Workspace. Sie können Falschmeldungen auch in der klassischen Umgebung anfordern:

#### Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** und wählen Sie die Elemente aus, die Sie als falsch positiv markieren möchten.
   Die ausgewählten Elemente müssen den Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ aufweisen.
2. Klicken Sie **auf Massenbearbeitung**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder des Formulars aus.

**Formular „Massenbearbeitung für angreifbares Element“.**

| Feld | Beschreibung |
|---|---|
| Datensatzauswahl | Datensätze, die für die Massenbearbeitung ausgewählt werden sollen. |
| Status | Status der angreifbaren Elemente. Wählen Sie Geschlossen aus, um ihn als falsch positiv zu kennzeichnen. |
| Grund | Substatus für den ausgewählten Status. Wenn Sie Geschlossen als Status ausgewählt haben, wählen Sie hier Falsch positiv aus, um dies als falsch positiv zu markieren. |
| Zuweisung aufheben | Senden Sie eine Anforderung zum Löschen der Felder Zugewiesen an und Zuweisungsgruppe. |
| Bevorzugte Lösung | Lösung, die auf die Korrektur aller für die Massenbearbeitung ausgewählten angreifbaren Elemente ausgerichtet ist. |
| Zuweisungsgruppe | Zuweisungsgruppe für die VI. Wählen Sie manuell aus, oder verwenden Sie Zuweisungsempfehlungen, wenn diese Option aktiviert ist. |
| Arbeitsnotizen | Notizen, die hinzugefügt werden sollen. |

4. Klicken Sie auf **OK**.
   Eine neue Korrekturaufgabe mit den ausgewählten AEs wird erstellt und zur Genehmigung gesendet.

## Genehmigen Sie ein falsch positives Ergebnis

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Benutzern genehmigen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.false_positive_approver oder sn_vul.app_false_positive_approver

Sie können Ausnahmen und falsch positive Anforderungen im Vulnerability Response -Arbeitsbereich genehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

Sie können Ausnahmen und falsch positive Anforderungen auch in der klassischen Umgebung genehmigen.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellen** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

**Hinweis:**
Ein falsch positives Ergebnis kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Analytics- und Reporting-Lösungen für Vulnerability Response

Die Überwachung der Schwachstellenkorrektur umfasst das Anzeigen von Trends, das Verwalten von Risiken und das Überwachen von Zuweisungsgruppen. Sie können Probleme mit hohem Risiko, Arbeitsauslastungen von Zuweisungsgruppen, Zurückstellungen und wiederkehrende Schwachstellen überprüfen. Vulnerability Response bietet Tools, Berichte und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

Schwachstellenanalysten können in auch Standarddashboards Vulnerability Response verwenden **Alle** > **Vulnerability Response** > **Übersicht**.

Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards in Vulnerability Manager Workspace und Dashboards in IT Remediation Workspace.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

## Vulnerability Response Korrekturprozess

Die meisten Schwachstellenkorrekturen werden über den Datensatz der Korrekturaufgabe in den Vulnerability Response Arbeitsbereichen durchgeführt. Über die Korrekturaufgaben (Remediation Tasks, RTs) im Status Wird untersucht können Sie mehrere Aufgaben ausführen.

- Erstellen Sie Change-Anforderungen.
- Fügen Sie Arbeitsnotizen und Beschreibungen von Schwachstellen innerhalb der Korrekturaufgabe hinzu.
- Verschieben Sie die Korrekturaufgabe und die darin enthaltenen angreifbaren Elemente auf einen späteren Zeitpunkt.
- Schließen Sie die Korrekturaufgabe.
- Verfolgen Sie neue regulatorische Compliance-Verpflichtungen nach, die in der Regel zeitkritisch sind.

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Überprüfen Sie Ihr Schwachstellenmanagement sowie Dashboards und Berichte von Drittanbietern, um Problembereiche zu lokalisieren. Zeigen Sie beispielsweise Dashboards an, die die Alterung der Korrekturaufgabe (RT) nach Status oder angreifbare Elemente mit hohem Risiko (AEs) nach ihrem Korrekturzieldatum anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie den Status der Korrekturaufgaben in der Reihenfolge des Risikos.
- Überarbeiten Sie die Priorisierung für die Aufgaben, indem Sie die Risikopunktzahl-Rechner anpassen, wenn die Risikopunktzahl nicht korrekt berechnet wird oder wenn AEs oder AEs nach Bedarf zurückgestellt werden. Weitere Informationen zu diesen Optionen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln oder Korrekturaufgabe zurückstellen.
- Überprüfen Sie zurückgestellte angreifbare Elemente, die kurz vor der erneuten Öffnung stehen, und ergreifen Sie nach Bedarf weitere Maßnahmen. Wenn Sie Change-Aktivitäten für Ihre Assets, Korrekturaufgaben und die entsprechenden angreifbaren Elemente initiieren und nachverfolgen möchten, finden Sie weitere Informationen unter Change Management für Vulnerability Response.
- Überprüfen Sie das Feedback von IT Operations.

  Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, warten Sie auf den nächsten Scan. Scans werden automatisch durch den im Setup-Assistenten konfigurierten Importzeitplan für Drittparteien ausgelöst.
- Wenn nach einem Scan der Status „Fest“ lautet, werden angreifbare Elemente während des Imports automatisch geschlossen. Die Gruppe wird geschlossen, wenn alle angreifbaren Elemente in der Gruppe repariert sind.
- Wenn der Status nach dem Scan nicht „Fest“ lautet, wird die VI automatisch zurück in „Wird untersucht“ verschoben.
- Angreifbare Elemente, die in Ihrer Instanz auf „Gelöst“ festgelegt, aber von den Integrationsausführungen der Drittpartei nicht auf „Geschlossen/Korrigiert“ gesetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

  Wenn der Scanner bei Erkennungen von Qualys weiterhin VIs findet, die auf „Gelöst“ festgelegt wurden, dann aber durch nachfolgende Scans nicht in „Geschlossen/Korrigiert“ geändert wurden, werden diese VIs wieder in den Status „Offen“ verschoben, wenn das Datum des letzten Funds nach dem liegt Datum der Lösung.

  Für Rapid7 -Erkennungen ist jetzt auf der Konfigurationsseite Rapid7 in Ihrer Instanz eine Option verfügbar, um aufgelöste AEs nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIs, die auf „Gelöst“ gesetzt sind, aber dann nicht durch nachfolgende Scans auf „Geschlossen/Korrigiert“ gesetzt wurden, nach der von Ihnen eingegebenen Anzahl von Tagen wieder auf „Offen“ gesetzt.



## Vulnerability Solution Management Fortschritt der Bereitstellung

Umfassende Bereitstellungsmetriken für Korrekturaufgaben und Schwachstelleneinträge sind in Vulnerability Solution Management unter **Korrekturstatus** in Schwachstellen, angreifbare Elemente enthalten. Identifizieren Sie einfach, welche Korrekturaufgabe oder Schwachstelle den Lösungsfortschritt verlangsamt. Zeigen Sie Detailinformationen dazu an, wie die Schwachstelle identifiziert wurde oder welche Aspekte der betroffenen Assets das Korrekturproblem verursachen könnten. Aktualisieren Sie den Status Ihrer Metriken mithilfe des zugehörigen Links **Status** aktualisieren in den Formularen für Schwachstellen, Lösungen und Korrekturaufgaben.

## Standardmäßige Dashboards Vulnerability Response werden verwendet

Das Übersichts-Dashboard Vulnerability Response (Schwachstellenmanagement) bietet einen Überblick über Schwachstellen und angreifbare Elemente und hilft dem Schwachstellenadministrator, Problembereiche schnell zu erkennen. Das Korrektur-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard Vulnerability Response (Schwachstellenkorrektur) ermöglicht es einem Korrekturspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, die er besitzt.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

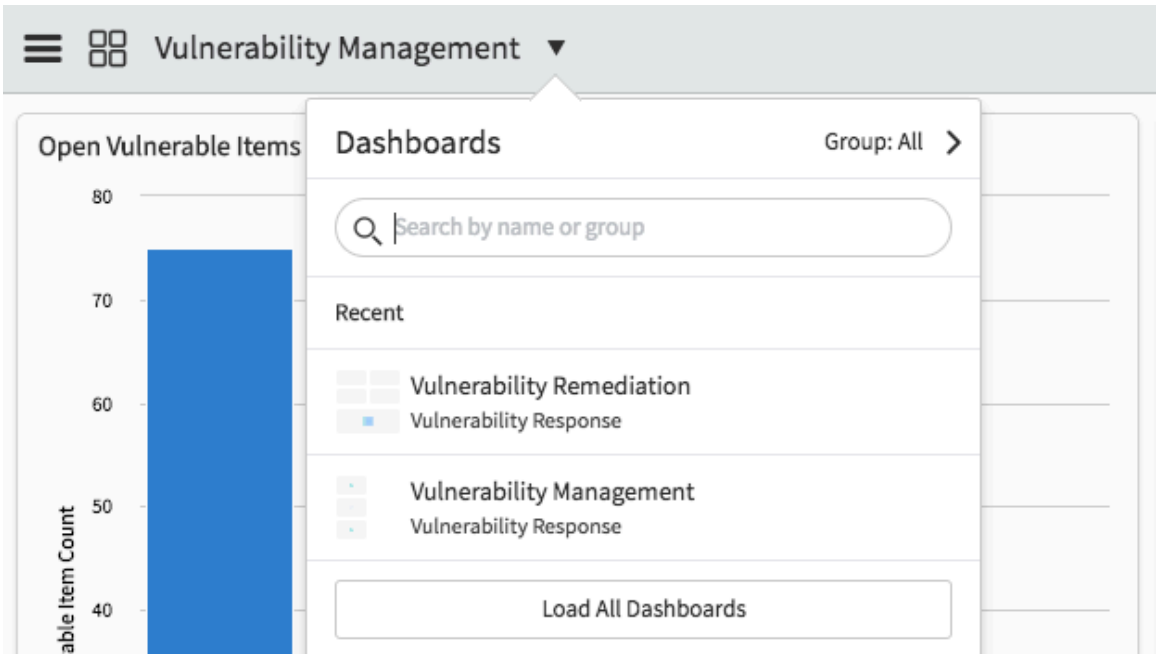
Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

Schwachstellenanalysten können auch Standarddashboards Vulnerability Response verwenden.

Erforderliche Rollen: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst und Benutzer mit sn_vul.vulnerability_read (oder die die Rolle sn_vul.vulnerability_read erben) und pa_viewer.

## Die standardmäßigen Vulnerability Response Dashboards in der veralteten -Umgebung

Diese Berichte sind als Teil der Anwendung Performance Analytics for Vulnerability Response enthalten und erfordern kein separates Abonnement. Um eines zu öffnen, wählen Sie die Auswahlliste aus, um sie zu erweitern, und wählen Sie ein Dashboard aus. Alternativ können Sie den Namen eines Dashboards in das Suchfeld eingeben.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Wenn die Anwendung Performance Analytics Content Pack for Vulnerability Response installiert und aktiviert ist, wird das Dashboard für Schwachstellenmanagement (PA) automatisch im -Übersichtsmodul angezeigt. Dieses Dashboard enthält Berichte, die alle Phasen des Lebenszyklus des Schwachstellenmanagements abdecken.

Weitere Informationen zu den Berichten, die im Performance Analytics Content Pack für Vulnerability Responseenthalten sind, finden Sie unter Dashboard für Schwachstellenmanagement [PA].

Weitere Informationen zum CISO-Dashboard und zu Berichten zur Scan-Abdeckung finden Sie unter Vulnerability Management CISO-Dashboard.

## Schwachstellenmanagement-Dashboard

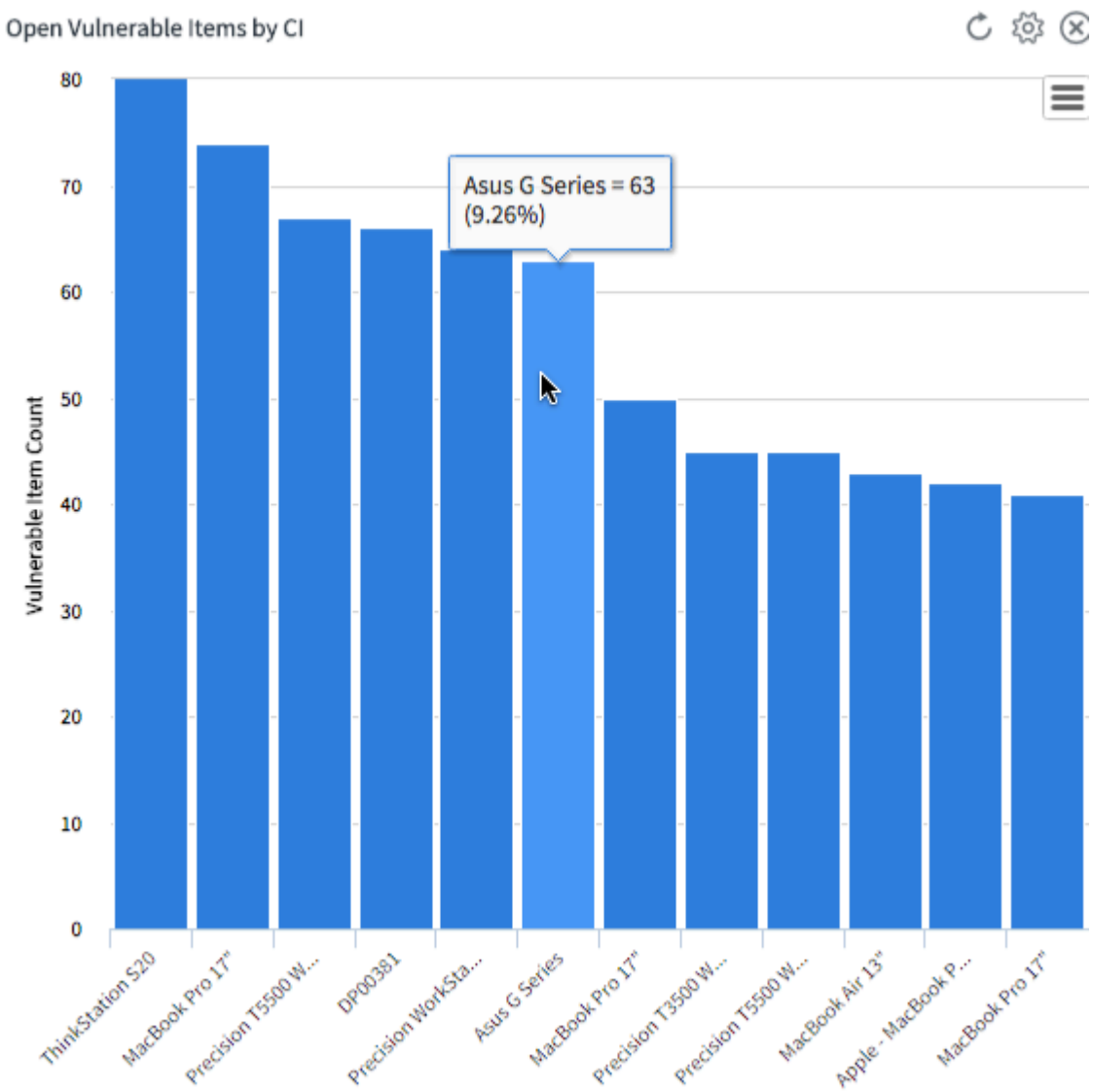
In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt usw.) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

**Hinweis:**

Wenn benutzerdefinierte Dashboards benötigt werden, finden Sie weitere Informationen unter Dashboards erstellen und verwenden .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Schwachstellenübersichtsberichte

| Name | Visuell | Beschreibung |
|---|---|---|
| Offene angreifbare Elemente nach CI | Balkendiagramm | Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes Konfigurationselement (CI) aufgezeichnet wurden, von den meisten bis zu den wenigsten. |
| Angreifbare Elemente nach Korrekturzielstatus | Balkendiagramm | Zeigt die Anzahl der angreifbaren Elemente an, die sich dem Ziel nähern, sich in der Ausführung befinden und das Ziel überschritten haben.<br>**Hinweis:**<br>Elemente im Status „Zurückgestellt“, „Gelöst“ oder „Geschlossen“ sind nicht enthalten. |
| Zurückgestellte angreifbare Elemente, die diese Woche ablaufen | Diagramm | Zeigt die Anzahl der zurückgestellten angreifbaren Elemente an, die innerhalb von sieben Tagen reaktiviert werden sollen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Schwachstellenübersichtsberichte (Fortsetzung)**

| Name | Visuell | Beschreibung |
|---|---|---|
| Offene angreifbare Elemente nach Schwachstelle | Balkendiagramm | Zeigt die Anzahl der offenen angreifbaren Elemente für jede Schwachstelle an, von den meisten bis zu den wenigsten. |
| Schwachstellen nach Modell | Balkendiagramm | Zeigt die Anzahl der für jedes Modell (CI-Klasse) aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten. |
| Schwachstellen nach Woche | Trend | Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an. |
| Modelle mit den meisten Schwachstellen | Ring | Zeigt Modelle (CI-Klassen) mit den angreifbarsten Elementen an. |
| Schwachstellen nach Herausgeber | Balkendiagramm | Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten. |
| Schwachstellen nach Impact | Balkendiagramm | Zeigt die Anzahl der Schwachstelleneinträge für betroffene Netzwerktypen an. |
| Herausgeber mit den meisten Schwachstellen | Ring | Zeigt Herausgeber mit den angreifbarsten Elementen an. |
| CIs mit den meisten Schwachstellen | Ring | Zeigt CIs mit den angreifbarsten Elementen an. |
| Schwachstellen nach Punktzahl | Balkendiagramm | Zeigt die Anzahl der Schwachstelleneinträge nach Schwachstellenpunktzahlen an. |
| Erneut geöffnete angreifbare Elemente | Liste | Listet die erneut geöffneten angreifbaren Elemente und deren Alter auf. |
| CIs mit den meisten Schwachstellen nach Klasse | Ring | Zeigt CIs mit den angreifbarsten Elementen an. |
| Alter des angreifbaren Elements | Liste | Listet die Anzahl der Tage seit dem letzten Öffnen von angreifbaren Elementen auf. |
| CIs mit Schwachstelle nach Datum | Liste | Listet Konfigurationselemente auf, die innerhalb der letzten 30 Tage gescannt wurden. |
| CIs nicht gescannt | Liste | Listet Konfigurationselemente auf, die noch nie auf Schwachstellen gescannt wurden. |



## Dashboard für Schwachstellenkorrekturen

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

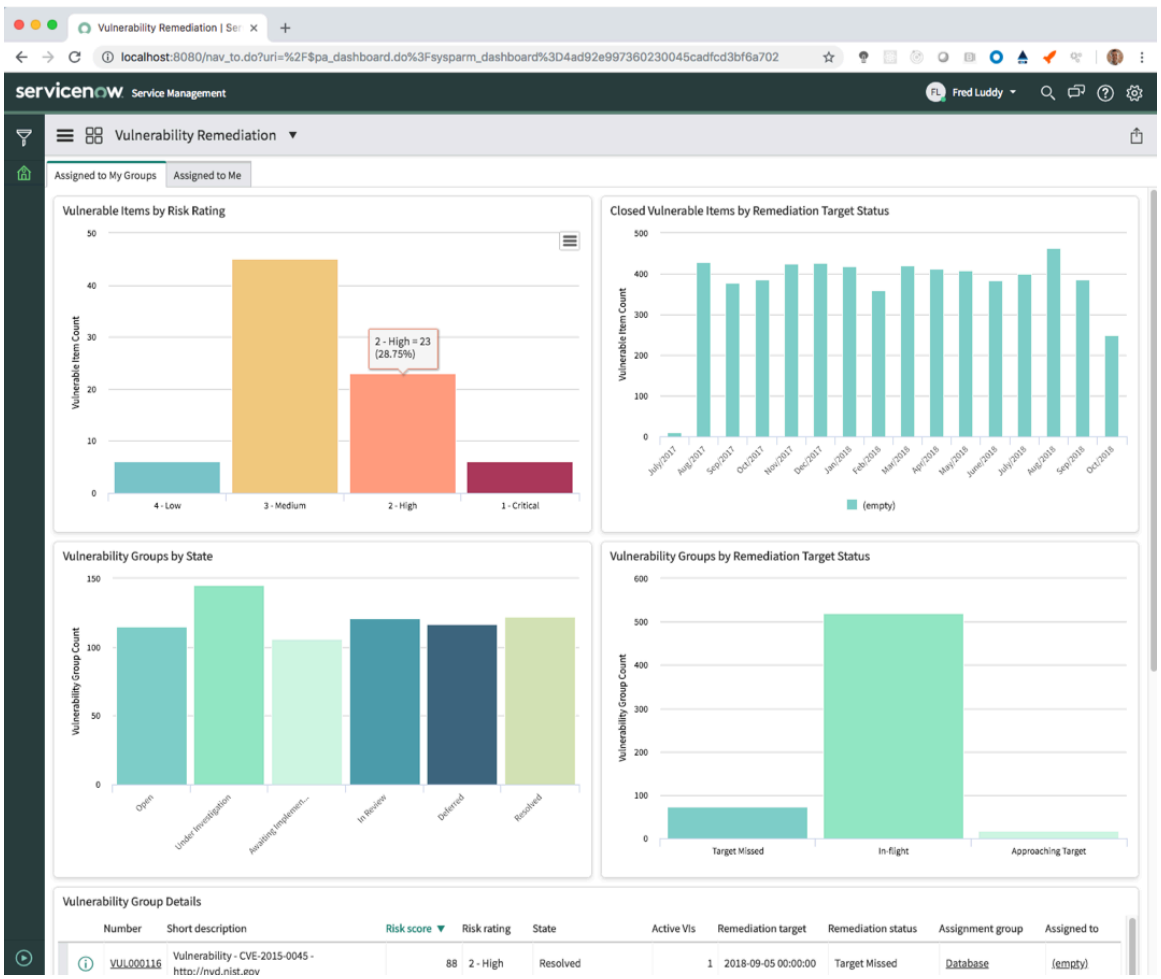
**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

Das Dashboard „Schwachstellenkorrektur“ enthält die folgenden Registerkarten: **Meinen Gruppenzugewiesen, Mir zugewiesen**und **Von mir angefordert**. Die Registerkarten Meinen Gruppen zugewiesen und Mir zugewiesen zeigen dieselben Berichte an. Erstere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkartenberichte nach den Zuweisungsgruppen, denen Sie angehören, und letztere nach angreifbaren Elementen oder Korrekturaufgaben, die Ihnen zugewiesen sind. Auf der Registerkarte Von mir angefordert werden die von Ihnen angeforderten Fehlalarme und Ausnahmen angezeigt.

## Dashboard für Schwachstellenkorrekturen




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Berichte

### Meinen Gruppen zugewiesen und Mir zugewiesen

| Name | Visuell | Beschreibung |
|---|---|---|
| Angreifbare Elemente nach Risikobewertung | Balken | Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne. |
| Geschlossene angreifbare Elemente nach Korrekturzielstatus | Balken | Anzahl der geschlossenen angreifbaren Elemente, gruppiert nach Nachbesserungszielstatus für die ausgewählte Zeitspanne. |
| Korrekturaufgaben nach Status | Balken | Anzahl der aktiven Korrekturaufgaben (RTs), gruppiert nach Status. |
| Korrekturaufgaben nach Status des Korrekturziels | Balken | Anzahl der aktiven RTs, gruppiert nach Status des Korrekturziels.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |
| Details zur Korrekturaufgabe | | Datensatzdetails der Korrekturaufgabe in einer Liste. |

### Angefordert von mir

| Name | Visuell | Beschreibung |
|---|---|---|
| Status von Ausnahme- und falsch positiven Anforderungen | Balken | Anzahl der aktiven Anforderungen von Ihnen. |
| Ablaufende zurückgestellte und falsch positive Korrekturaufgaben | Balken | Anzahl der zurückgestellten und falsch positiven Korrekturaufgaben (RTs), gruppiert nach Bis-Datum. |

## Dashboard „Schwachstellengenehmigungen“.

Das Dashboard „Schwachstellengenehmigungen“ enthält die folgenden Berichte für Ausnahmegenehmiger und falsch positive Genehmiger.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

| Name | Visuell | Beschreibung |
|---|---|---|
| Ausnahme- und falsch positive Anforderungen nach Alter meiner ausstehenden Genehmigungen | Balken | Anzahl der für Sie ausstehenden Genehmigungen, gruppiert nach Erstellungsdatum. |
| Meine Genehmigung und abgelehnte Ausnahmen und falsch positive Anforderungen | Balken | Anzahl der genehmigten oder abgelehnten Genehmigungsanforderungen, gruppiert nach Genehmigungsstatus. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Visuell | Beschreibung |
|---|---|---|
| Alle Korrekturaufgaben nach Risikobewertung – Genehmigung ausstehend | Balken | Anzahl der ausstehenden Genehmigungen für Korrekturaufgaben, gruppiert nach Risikobewertung. |
| Alle ausstehenden und falsch positiven Genehmigungsanforderungen, gruppiert nach Grund | Balken | Anzahl der ausstehenden Genehmigungsanforderungen, gruppiert nach Grund. |

## Platform Analytics-Lösungen für Schwachstellenmanagement

Platform Analytics-Lösungen enthalten vorverpackte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Mit dieser Analytics and Reporting-Lösung können Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nachverfolgen. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

Das Inhaltspaket Performance Analytics for Vulnerability Response wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Sie ist im ServiceNow Store als separates Abonnement verfügbar.

Performance Analytics for Vulnerability Response enthält zwei Dashboards:

- Dashboard „Schwachstellenmanagement“ (PA).
- Vulnerability Management Chief Information Security Officer (CISO) Dashboard

## Erforderliche Rollen, Installation und Anzeigen der Dashboards

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Informationen zur Installation dieser Anwendung finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

**Hinweis:**
Richten Sie Analytics and Reporting-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie sie, bevor Sie sie in der Produktion aktivieren.

Lösungen für Analytik und Berichterstellung bieten alle für die Analyse von Standardanwendungen erforderlichen Konfigurationsdatensätze. Passen Sie diese Datensätze zur Verwendung in Ihrer Produktionsumgebung an. Weitere Informationen finden Sie unter Analytics and Reporting-Lösungen konfigurieren .

Um das Schwachstellenmanagement-Dashboard (PA) anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Übersicht** > **.**

Um das CISO-Dashboard von Vulnerability Management anzuzeigen, navigieren Sie zu **Vulnerability Response** > **CISO-Dashboard** > **.**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Wichtige Begriffe

**Performance Analytics (PA)**

Lösung, die Management-Dashboards, Berichte zu KPIs und Metriken erstellt und wichtige Geschäftsfragen beantwortet, um die Qualität zu steigern und die Kosten zu senken.

**Angreifbares Element (AE)**

Eine Sicherheitsschwachstelle, die von einem Schwachstellenscanner einer Drittpartei gemeldet wurde und in einem Konfigurationselement (Configuration Item, CI) vorhanden ist

**Korrekturaufgabe**

Korrekturaufgaben werden basierend auf der Gruppe, die den angreifbaren Elementen in einer Korrekturmaßnahme zugeordnet ist, erstellt und automatisch IT-Teams zugewiesen. IT-Teams und Korrekturverantwortliche zeigen Korrekturaufgaben im IT-Korrekturarbeitsbereich an. Weitere Informationen finden Sie unter Vulnerability Response Arbeitsbereiche.

.

**PA-Indikator**

Definiert eine Leistungsmessung, die in regelmäßigen Abständen für einen Business Service, eine Aktivität oder ein Organisationsverhalten durchgeführt wird, z. B. Nicht zurückgestellte überfällige kritische angreifbare Elemente.

**PA-Indikatorquelle**

Datensätze, die Datensätze aus einer Tabelle oder Datenbankansicht filtern, z. B. VI aktiv.

## Zeigen Sie Datenvisualisierungen in Echtzeit an

Um zu sehen, was heute mit den wichtigsten Elementen in Ihrer Vulnerability Response -Anwendung geschieht, können Sie bestimmte Berichte im Dashboard für Schwachstellenmanagement (PA) in Echtzeit anzeigen. Wenn Sie diese Berichte in Echtzeit anzeigen, können Sie Ihre wichtigsten angreifbaren Elemente (AEs) verwalten und schnell beheben. Sie können die folgenden Berichte in Echtzeit anzeigen:

- Registerkarte „Übersicht“ – Angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „Angreifbare CIs“
  - Angreifbare Konfigurationselemente (CIs) ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte Ausnahmen
  - Zurückgestellte angreifbare Elemente nach Grund
  - In Kürze ablaufende Zurückstellungsanforderungen
  - Zurückgestellte angreifbare Elemente nach CIO-Manager
- Registerkarte „Korrektur“ – Nicht zugewiesene angreifbare Elemente

Weitere Informationen finden Sie unter Performance Analytics für Vulnerability Response-Berichte [PA] in Echtzeit anzeigen.

**Zugehörige Informationen**

Analytics- und Reporting-Lösungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vulnerability Management CISO- Dashboard

Mit dem Vulnerability Management CISO -Dashboard können Sie Daten wie Key Performance Metrics (KPIs) für die Schwachstellenkorrektur anzeigen, die höchsten Risiken anzeigen, die Scan-Abdeckung überprüfen und erfahren, wie Risiken reduziert werden können.

## Erforderliche Now Platform-Rollen

- sn_vul.vulnerability_ciso, um das Dashboard anzuzeigen.
- sn_vul.ciso_write, um das Dashboard zu bearbeiten.

## CISO-Dashboard wird aktiviert

Um das CISO-Dashboard zu aktivieren, müssen Sie Performance Analytics für Vulnerability Response installieren und den entsprechenden Performance Analytics-Job aktivieren. Weitere Informationen finden Sie unter Analytics and Reporting-Lösungen für Vulnerability Response.

## Anwendungsfälle

| Anwender | Dashboard-Verwendung |
|---|---|
| Chief Information Security Officers (CISOs) | Chief Information Security Officers (CISOs) können das CISO-Dashboard verwenden, um Einblicke in das Schwachstellenmanagementprogramm ihrer Organisation zu erhalten.<br><br>Das Dashboard stellt Daten bereit, mit denen sie Daten auf einen Blick identifizieren können, mit denen sie die Schwachstellen in ihren Umgebungen verringern können. |

## Verwenden des CISO-Dashboards

Ausführende Benutzer, wie die Chief Information Security Officers (CISOs) in Ihrer Organisation, können das CISO-Dashboard für Vulnerability Response anzeigen, um nachzuvollziehen, wie effektiv ihr Schwachstellenmanagementprogramm ist. Sie können das CISO-Dashboard anzeigen, indem Sie zu navigieren **Vulnerability Response** > **CISO-Dashboard**. Verwenden Sie die Filter der obersten Ebene, um Berichte nach Risikobewertung, Altersbereich oder Internetverbindung zu filtern. Einige Berichte zeigen Trenddaten über einen bestimmten Zeitraum an. Sie können die regelmäßigen Trends der wichtigen Metriken anzeigen, das allgemeine Sicherheitsrisiko des Unternehmens analysieren und die Bereiche identifizieren, die verbessert werden müssen.

Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards in Vulnerability Manager Workspace und Dashboards in IT Remediation Workspace.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Die geplanten Aufgaben werden ausgeführt

Führen Sie die geplanten Aufgaben in der folgenden Reihenfolge aus, um die Daten in den Berichten zu aktualisieren:

1. Aktualisieren Sie Dashboard-Tabellen
2. [PA VR] CISO-Dashboard

### Geplante Aufgaben für das CISO-Dashboard

| Name der geplanten Aufgabe | Beschreibung |
|---|---|
| Aktualisieren Sie Dashboard-Tabellen | Tägliche geplante Aufgabe, die Sie vor der [PA VR] CISO Dashboard-Aufgabe ausführen müssen, damit Sie die CISO-Daten erfassen können. Durch Ausführen dieser regelmäßigen Aufgabe aktualisieren Sie die Berichte zur Scan-Abdeckung.<br><br>Die aktualisierten Informationen umfassen die operativen Konfigurationselemente (CIs), die in den letzten 90 Tagen gescannt wurden, ihre Klassen und die Gesamtzahl der operativen CIs, die diesen Klassen entsprechen. Durch die Ausführung dieser regelmäßigen Aufgabe werden auch die Berichte auf der Registerkarte **„Empfohlene Aktionen** “ aktualisiert.<br><br>**Hinweis:**<br>Operative CIs beziehen sich auf die CIs, die den Betriebsstatus „ Operativ“ haben. |
| [PA VR] CISO-Dashboard | Nachdem die regelmäßige Aufgabe „Dashboard-Tabellen aktualisieren“ abgeschlossen ist, führen Sie diese regelmäßige Aufgabe aus, um alle Berichte auf der Registerkarte **„CISO-Übersicht“** auszufüllen. |

## CISO-Dashboard-Registerkarten

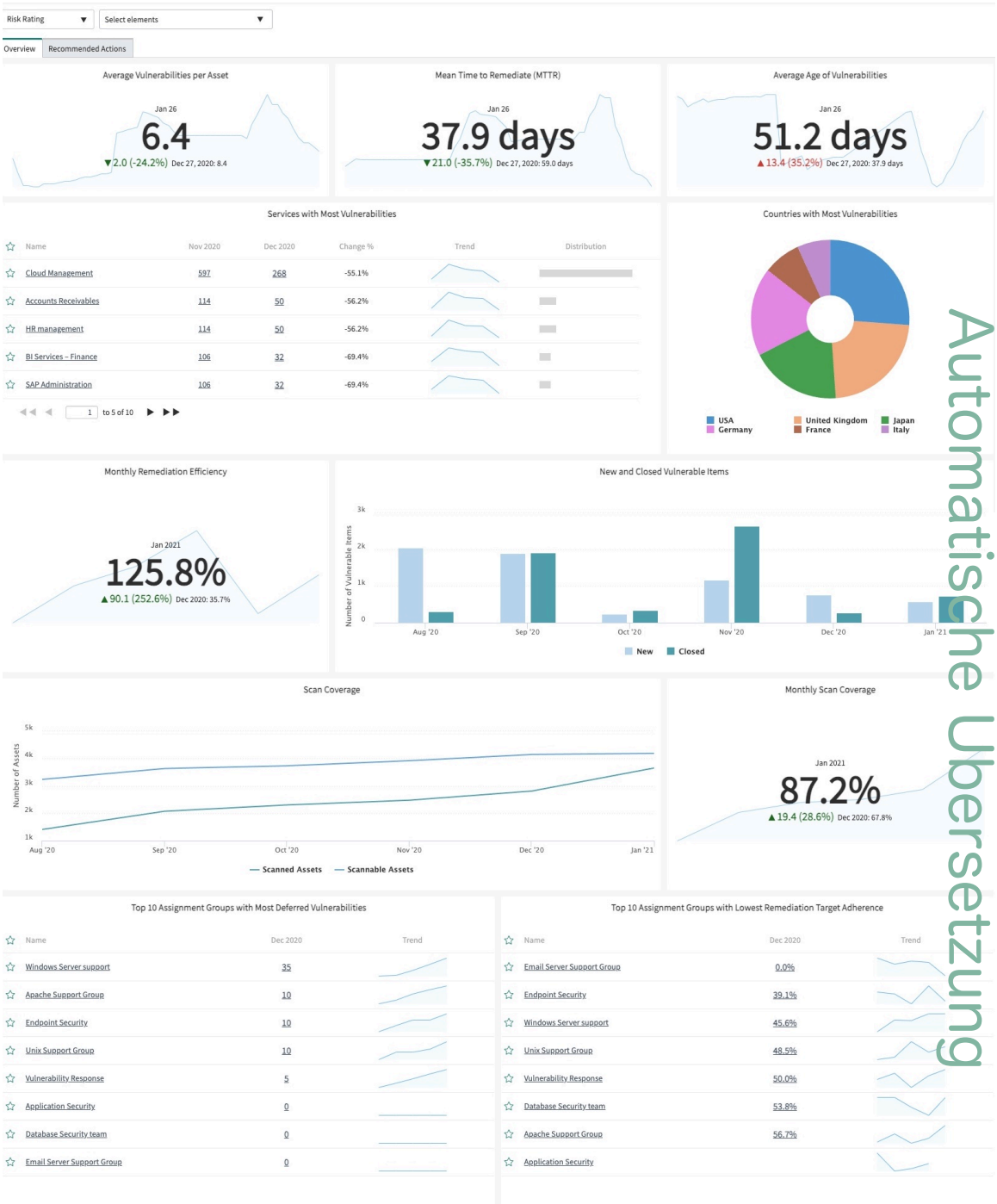
Dieses Dashboard bietet Einblicke in die Risiken in Vulnerability Management. Sie können Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Übersicht“

Die Registerkarte Übersicht enthält Berichte, die den Sicherheitsstatus Ihrer Organisation auf einen Blick bereitstellen.



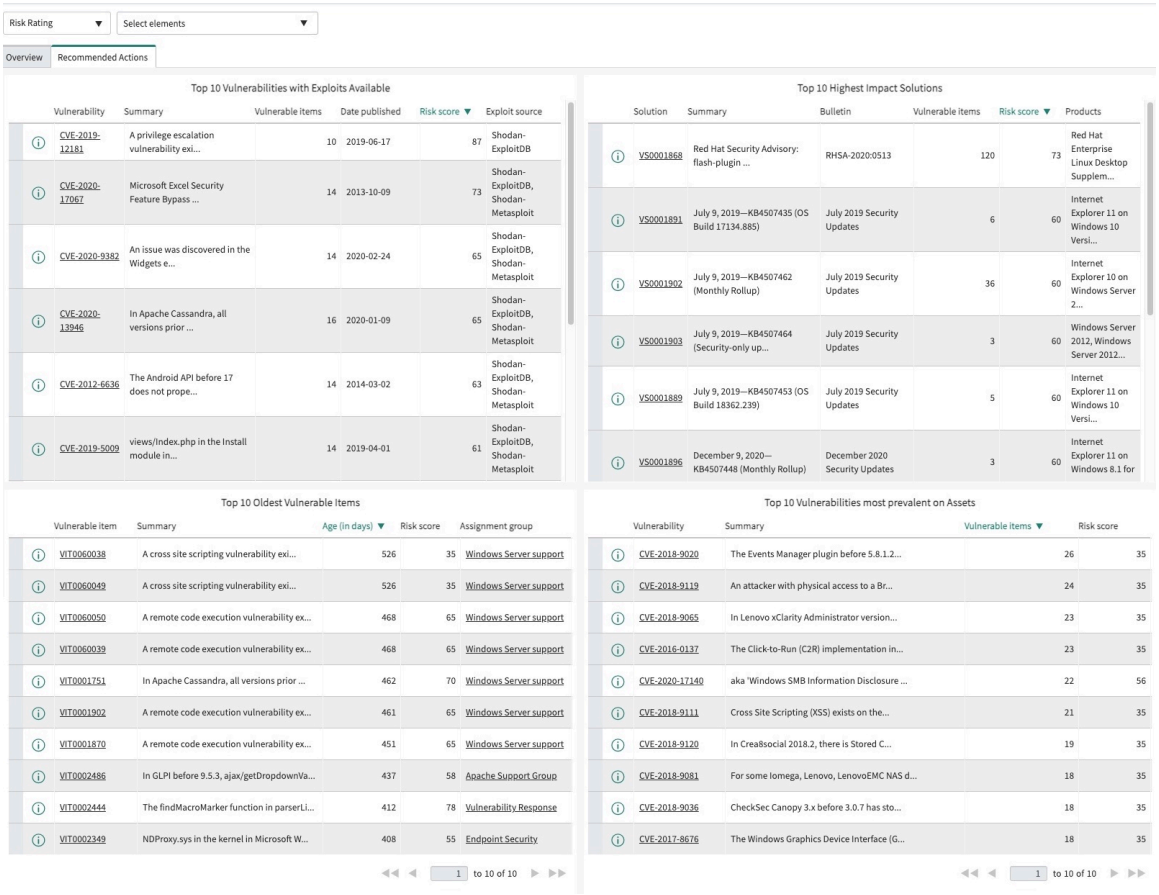

Automatische Übersetzung

**Hinweis:**
Der Filter auf oberster Ebene kann nur für einige Berichte verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Empfohlene Aktionen“

Die Registerkarte „Empfohlene Aktionen“ enthält Berichte, die Einblicke in ausnutzbare, veraltete und weit verbreitete Schwachstellen bieten. Sie enthält auch Lösungen, die Aktionen zur Reduzierung der Risiken empfehlen. Führen Sie die regelmäßige Aufgabe **„CISO-Dashboard-Tabellen** aktualisieren“ aus, um die Berichte auf dieser Registerkarte zu aktualisieren.




## Indikatoren

Um die Indikatoren anzuzeigen, navigieren Sie zu **Performance Analytics** > **Indikatoren**.

1. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem Namen des erforderlichen Indikators.
2. Klicken Sie auf den Indikatornamen, um den Datensatz zu öffnen und seine Details anzuzeigen.

   Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze sammeln, indem Sie das Kontrollkästchen Datensätze sammeln aktivieren.

#### Summierte Dauer der geschlossenen angreifbaren Elemente

Die Gesamtdauer der geschlossenen AEs wird täglich in Tagen gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

#### Scannbare Assets

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

#### Services mit den meisten Schwachstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.


Automatische Übersetzung

„Services mit den meisten Schwachstellen“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

**Durchschnittliche Schwachstellen pro Asset**

[[Aktive angreifbare Elemente]] / [[Aktive angreifbare Konfigurationselemente]

**Geschlossene angreifbare Elemente**

„Geschlossene angreifbare Elemente“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

**Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente**

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

**Aktuelle Scan-Abdeckung**

Berechnet die aktuelle Scan-Abdeckung als Prozentsatz.

**Gescannte Assets**

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

**Geschlossene angreifbare Elemente (Ziel erfüllt)**

„Geschlossene angreifbare Elemente (Ziel erfüllt)“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

**% der geschlossenen angreifbaren Elemente, die das Ziel erfüllt haben**

[[Geschlossene angreifbare Elemente (Ziel erfüllt) / Nach Monat SUM]] / [[Geschlossene angreifbare Elemente / Nach Monat SUM]] *100

**Aktive angreifbare Elemente**

„Aktive angreifbare Elemente“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

**Durchschnittliches Alter der angreifbaren Elemente**

Das durchschnittliche Alter aktiver AEs wird täglich als Einheit „Tage“ gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

**Aktive angreifbare Konfigurationselemente**

„Aktive angreifbare CIs“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

**Effizienz der monatlichen Fehlerbehebung**

[Anzahl der während eines Monats geschlossenen angreifbaren Elemente] / [Anzahl neuer oder erneut geöffneter angreifbarer Elemente im selben Monat]

**Neue angreifbare Elemente**

„Neue angreifbare Elemente“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

**Zurückgestellte angreifbare Elemente**

„Zurückgestellte AEs“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

## BreakdownsAufgliederungen

- Zuweisungsgruppe: Gilt für einige VI-Berichte.
- Risikobewertung: Gilt für VI-Berichte.
- Altersbereich: Gilt für VI-Berichte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschlossen-Alter: Gilt für Berichte für geschlossene AEs.
- Mit Internetverbindung: Gibt an, ob das CI zur Hardwareklasse gehört und mit dem Internet verbunden ist.
- Region: Der verwendete CMDB-CI-Parameter ist Location. Dieser Speicherort gibt das Ursprungsland des Konfigurationselements an.

## Datenvisualisierungen

| Name | Typ | Beschreibung |
|---|---|---|
| Durchschnittliche Schwachstellen pro Asset | Einzelne Punktzahl | Durchschnittliche Anzahl aktiver angreifbarer Elemente pro Konfigurationselement. |
| Durchschnittliche Zeit bis zur Nachbesserung (MTTR) | Einzelne Punktzahl | Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt.<br>**Hinweis:**<br>Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „Zuletzt geöffnet“ und dem Datum und der Uhrzeit der Erfassungsaufgabe. |
| Durchschnittliches Alter von Schwachstellen | Einzelne Punktzahl | Durchschnittliches Alter aktiver angreifbarer Elemente in Tagen. |
| Services mit den meisten Schwachstellen | Liste und | Monatlicher Durchschnitt der aktiven angreifbaren Elemente für Services in der Organisation.<br>**Hinweis:**<br>Informationen zum Definieren der Serviceklassifizierungen, die Sie in Vulnerability Response-Berichten und zugehörigen Listen anzeigen möchten, finden Sie auf der Registerkarte Services im Dashboard von Vulnerability Management [PA]. |
| Länder mit den meisten Schwachstellen | Ring | Top 10 der Länder mit der höchsten Anzahl angreifbarer Elemente. |
| Effizienz der monatlichen Fehlerbehebung | Einzelne Punktzahl | Prozentsatz geschlossener angreifbarer Elemente geteilt durch neue angreifbare Elemente im aktuellen Monat. |
| Neue und geschlossene angreifbare Elemente | Balken | Anzahl der neuen angreifbaren Elemente, die in einem Monat importiert wurden, und Anzahl der geschlossenen angreifbaren Elemente. |
| Scan-Abdeckung | Linie | Anzahl der gescannten Assets im Vergleich zur Gesamtzahl der scannbaren Assets im Zeitverlauf. Die im Widget enthaltenen CI-Klassen werden im Modul „Konfiguration der Scan-Abdeckung“ angegeben.<br>Informationen zum Konfigurieren des Moduls „Scan-Abdeckung“ finden Sie unter Scan-Abdeckungsberichte konfigurieren. |
| Monatliche Scan-Abdeckung | Einzelne Punktzahl | Prozentsatz der gescannten Assets geteilt durch die Gesamtzahl der scannbaren Assets für den aktuellen Monat. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
|---|---|---|
| | | Informationen zum Konfigurieren des Moduls „Scan-Abdeckung“ finden Sie unter Scan-Abdeckungsberichte konfigurieren |
| Top 10 der Zuweisungsgruppen mit den meisten zurückgestellten Schwachstellen | Liste und | Top-10-Zuweisungsgruppen mit der höchsten Anzahl zurückgestellter angreifbarer Elemente, zurückgestellt basierend auf dem monatlichen Durchschnitt. |
| Top 10 der Zuweisungsgruppen mit den der niedrigsten Einhaltung des Nachbesserungsziels | Liste und | Top-10-Zuweisungsgruppen, deren angreifbare Elemente die niedrigste Einhaltung ihrer Korrekturziele aufweisen. |

### Empfohlene Aktionen

| Name | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Die 10 häufigsten Schwachstellen mit verfügbaren Exploits | | Häufigstes Schwachstellenelement [sn_vul_analytics_top_item] | Aktive Schwachstellen mit Exploits, die für alle Threat Intelligence-Anbieter verfügbar sind, die das VR-Exploit-Framework verwenden. |
| Top 10 der Lösungen mit den höchsten Auswirkungen | | Häufigstes Schwachstellenelement [sn_vul_analytics_top_item] | Bevorzugte Lösungen oder Patches mit den höchsten Risikopunktzahlen für aktive angreifbare Elemente. Dieser Bericht verwendet die Funktionen von Vulnerability Solution Management (VSM), das Patches von Microsoft und Red Hat mit Schwachstellen in der -Umgebung korreliert. VSM hilft bei der Identifizierung der bevorzugten Lösung für Schwachstellen. |
| Top 10 der ältesten angreifbaren Elemente | | Häufigstes Schwachstellenelement [sn_vul_analytics_top_item] | Aktive angreifbare Elemente mit dem höchsten Alter. Lösen Sie diese Elemente, um das durchschnittliche Alter von Schwachstellen auf der Registerkarte „Übersicht“ zu senken. |
| Top 10 der häufigsten Schwachstellen in Assets | | Häufigstes Schwachstellenelement [sn_vul_analytics_top_item] | Aktive angreifbare Elemente, die für die höchste Anzahl von Assets verfügbar sind. |

### Konfigurieren Sie die Berichte zur Scan-Abdeckung

Ermöglichen Sie Ihren Benutzern, Berichte zur Scan-Abdeckung über das CISO-Dashboard auszuführen. Mit diesen Berichten können Ihre Benutzer sehen, wie hoch die Scan-Abdeckung der Organisation über einen bestimmten Zeitraum ist.

**Vorbereitungen**

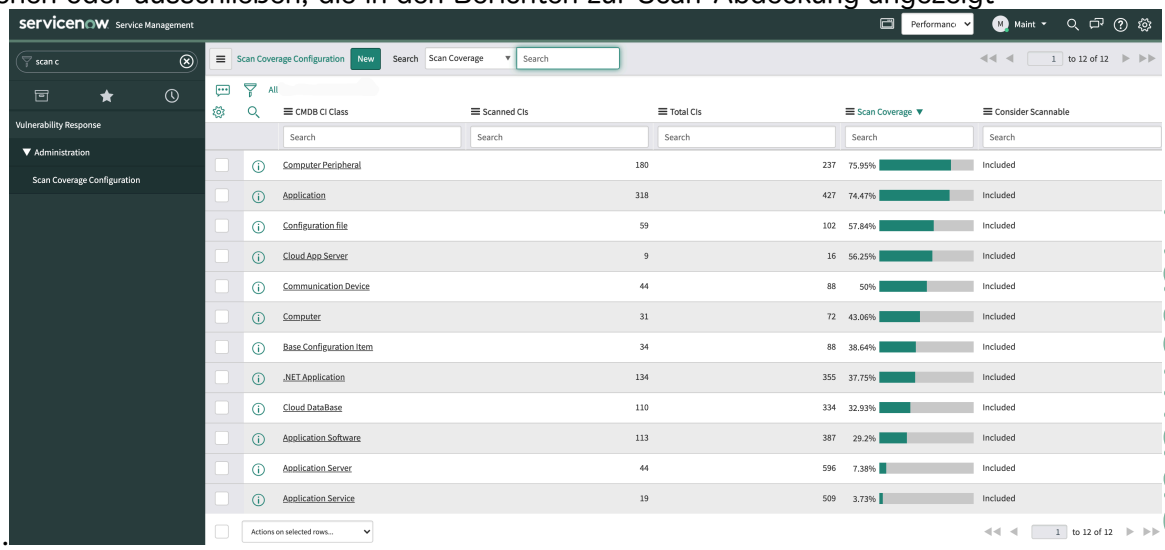
Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Die Scan-Abdeckung zeigt die Anzahl der Assets an, die in den letzten 90 Tagen von den Schwachstellenscannern für die verschiedenen Klassen gescannt wurden. Diese Assets werden mit der Anzahl der durchsuchbaren Assets im Configuration Management Database (CMDB)verglichen. Standardmäßig enthält das Modul „Konfiguration der Scan-Abdeckung CMDB “ CI-Klassen, mit denen mindestens ein gescanntes Asset abgeglichen wurde. Sie können dem Bericht „Scan-Abdeckung“, der im CISO-Dashboard angezeigt wird, eine CI-Klasse aus CMDB hinzufügen. Sie können CMDB CI-Klassen einbeziehen oder ausschließen, die in den Berichten zur Scan-Abdeckung angezeigt werden.




### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Konfiguration der Scan-Abdeckung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

#### Formular „Konfiguration der Scan-Abdeckung“

| Feld | Beschreibung |
|---|---|
| CMDB-CI-Klasse | CI-Klasse, die dem Scan-Abdeckungsbericht im CISO-Dashboard hinzugefügt werden muss.<br>**Hinweis:**<br>Wenn im Modul „Konfiguration der Scan-Abdeckung“ bereits eine CI-Klasse vorhanden ist, wird sie nicht in diese Liste aufgenommen. |
| Als scannbar betrachten | Option zum Definieren, ob die CI-Klasse enthalten sein muss oder nicht. Schließen Sie eine CI-Klasse ein, wenn deren Daten den Berichten zur Scan-Abdeckung hinzugefügt werden sollen. Wenn ausgeschlossen, werden die Daten für diese CI-Klasse nicht hinzugefügt. |

4. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Konfigurieren Sie die PA-Indikatoren für das CISO-Dashboard

Überwachen Sie die automatisierten und formulierten CISO-Indikatoren, damit Sie die Schwachstellendaten in Ihrer Instanz verwalten können.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

## Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response verfügt sowohl über automatisierte als auch über formulierte Indikatoren.

### Wichtige Begriffe

**Indikator**

Definiert eine Leistungsmessung, die in regelmäßigen Abständen für einen Business Service, eine Aktivität oder ein Organisationsverhalten durchgeführt wird. Ein Beispiel ist ein aktives angreifbares Element.

**Indikatorquelle**

Datensätze, die aus Datensätzen bestehen, die aus einer Tabelle oder Datenbankansicht gefiltert wurden, um die Effizienz zu erhöhen. Ein Beispiel ist AE.Aktiv (mit Internetverbindung).

**BreakdownsAufgliederungen**

Aufgliederungen filtern und gruppieren Indikatorpunktzahlen anhand qualitativer Attribute wie Priorität, Kategorie und Zuweisungsgruppe.

**Geplante Aufgaben**

Geplante Aufgaben werden ausgeführt, um die Indikatorquelldaten auszufüllen. Die tägliche geplante Aufgabe [PA VR] CISO-Dashboard ist standardmäßig deaktiviert. Sie müssen sie aktivieren, um Indikatorpunktzahlen für das CISO-Dashboard zu sammeln.

## Prozedur

1. Navigieren zu **Alle** > **Performance Analytics** > **Indikatoren** und wählen Sie eine der folgenden Optionen aus:
   - Automatisierte Indikatoren
   - Formelindikatoren

   Weitere Informationen zu Indikatoren finden Sie unter Performance Analytics-Indikatoren .
2. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem Namen des erforderlichen Indikators.
3. Klicken Sie auf den Indikatornamen, um den Datensatz zu öffnen und seine Details anzuzeigen.

   Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze sammeln, indem Sie das Kontrollkästchen **Datensätze** sammeln aktivieren.

   **Hinweis:**
   Das Aktivieren von Datensätzen in einem Indikator kann zu Leistungsproblemen führen, z. B., dass viel mehr Zeit und Arbeitsspeicher benötigt wird, die für die Ausführung der Datenerfassungsaufgabe erforderlich sind.

   Die maximale Anzahl von Zeilen, die Sie für eine Indikatorquelle abrufen können, beträgt 1.000.000.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Dashboard „SecOps Vulnerability Response-Integrität“.

Das Vulnerability Response-Integritäts-Dashboard ist ein Tool, mit dem Unternehmen umfassende Einblicke in die Implementierung und Verwendung ihrer Vulnerability Response-Anwendungen erhalten.

Die Gesamtintegritätsbewertung wird durch die Zusammenfassung verschiedener kritischer Faktoren für Konfiguration, Implementierung, Integration, Leistung, Daten und Prozess bestimmt. Zeigen Sie das zusammengefasste Dashboard für jede Kategorie für die folgenden Anwendungen an:

- Vulnerability Response
- Vulnerability Response auf Anwendungsebene
- Container Vulnerability Response
- Konfigurations-Compliance

## Installation des SecOps Vulnerability Response-Integritäts-Dashboards

Um das SecOps Vulnerability Response Health Dashboard für Vulnerability Response -Anwendungen in Ihrer Now Platform-Instanz zu installieren und zu konfigurieren, navigieren Sie zu ServiceNow® Store, und aktivieren Sie das Plugin „SecOps Health Analytics“ (sn_sec_analytics).

## Erforderliche Now Platform-Rollen

Erforderliche Rollen: sn_sec_analytics.admin, sn_sec_analytics.read

## Regelmäßige Aufgabe

Um die geplante Aufgabe anzuzeigen, navigieren Sie zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben** > **Erfasst Integritäts-Dashboard-Metriken**. Die geplante Aufgabe „Integritäts-Dashboard-Metriken erfassen“ wird täglich um 00:00 Uhr ausgeführt. Sie generiert die Daten für das Dashboard „SecOps Vulnerability Response-Integrität“. Sie können die geplante Aufgabe auch manuell ausführen.

## Anwendungsfälle

Beispiele dafür, wie Mitarbeiter in Ihrer Organisation dieses Dashboard verwenden können, finden Sie in diesen Anwendungsfällen.

| Anwender | Dashboard-Verwendung |
|---|---|
| Schwachstellenadministrator | Hilft Ihnen, die Integritätspunktzahl der Vulnerability Response -Anwendungen nachzuvollziehen. Es ist auch hilfreich, die Bereiche hervorzuheben, die verbessert werden müssen.<br><br>Das Vulnerability Response-Integritäts-Dashboard befasst sich nur mit der Implementierungs- und Nutzungsintegrität. Sie hilft nicht bei der Verwaltung von Schwachstellen oder Assets. |
| Supportadministrator | Hilft Ihnen, Leistungs-, Anpassungs- und Konfigurationsprobleme mithilfe von KPIs zu identifizieren. Basierend auf der Anwendungsintegrität können Sie eine zusätzliche |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwender | Dashboard-Verwendung |
|---|---|
| | Analyse durchführen oder den Benutzern eine Empfehlung geben. |
| Implementierungspartner | Hilft Ihnen, die Implementierungsintegrität von Vulnerability Response für Konfigurationen, Add-ons, Anpassungen und Integrationen zu bewerten und Verbesserungsvorschläge für die Benutzer bereitzustellen. |

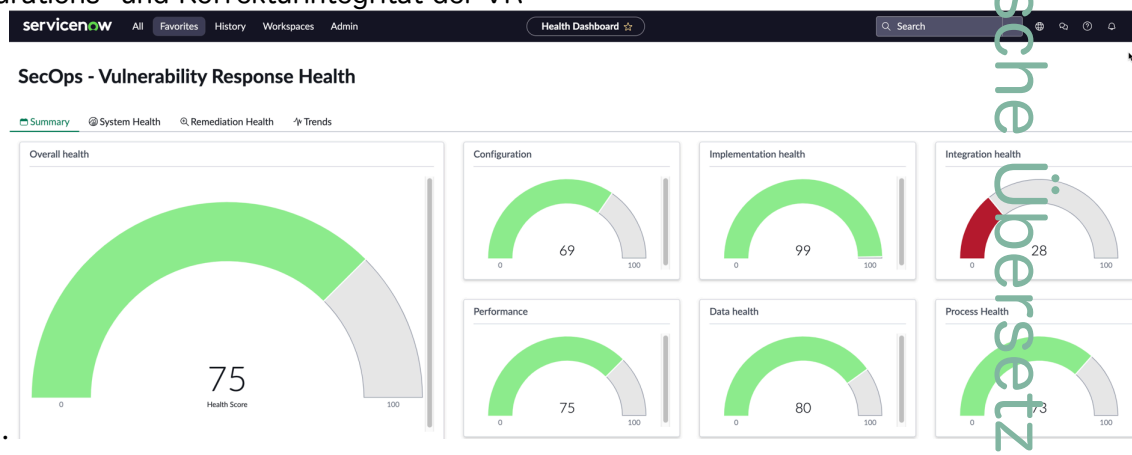
## Die Registerkarten des SecOps Vulnerability Response-Integritäts-Dashboards

Um das Dashboard „SecOps Vulnerability Response-Integrität“ anzuzeigen, navigieren Sie zu **Security Operations-Integrität** > **Vulnerability Response-Integrität**. Jede Farbe im Dashboard stellt Folgendes dar:

- Grün: Sicher
- Gelb: Warnung
- Rot: Kritisch

### Registerkarte „Zusammenfassung“

Dieses Dashboard kommuniziert die Gesamtintegritätspunktzahl für die Konfigurations- und Korrekturintegrität der VR-Anwendungen.

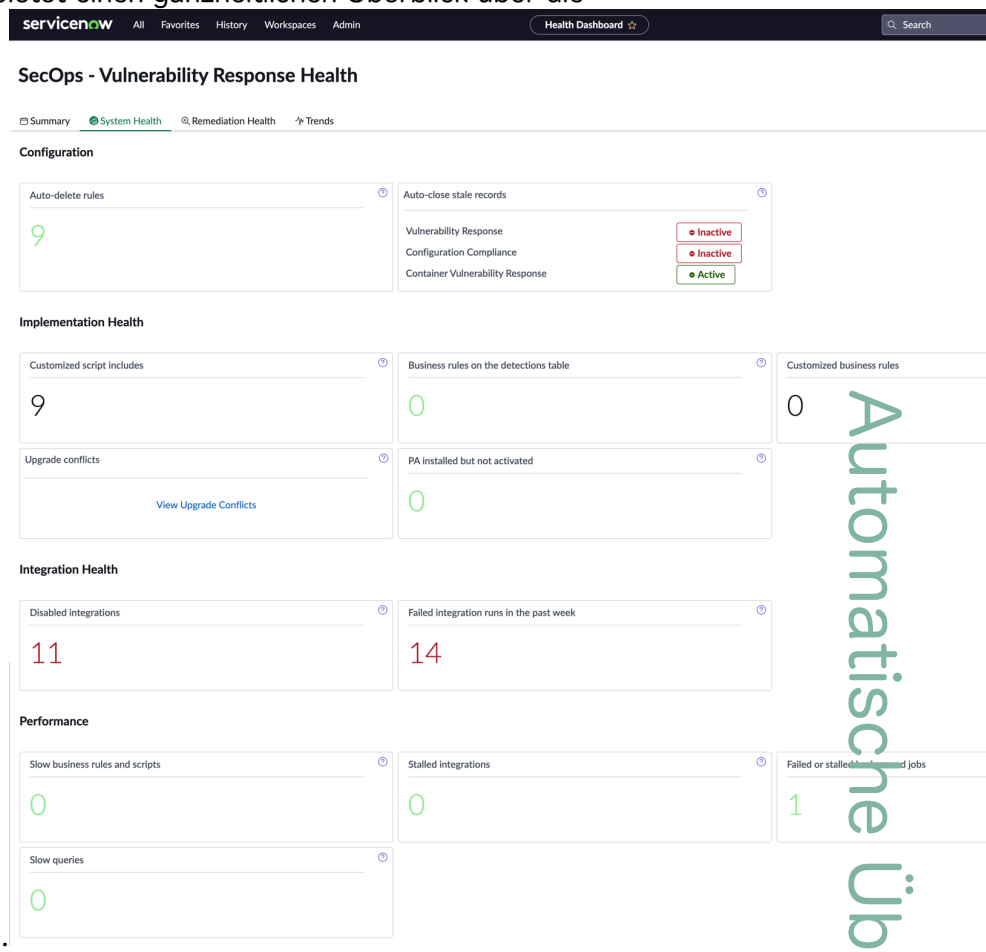



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte Systemintegrität

Dieses Dashboard zeigt die Konfigurations- und Integrationsintegrität Ihrer Implementierung an. Sie bietet einen ganzheitlichen Überblick über die Implementierungsleistung.

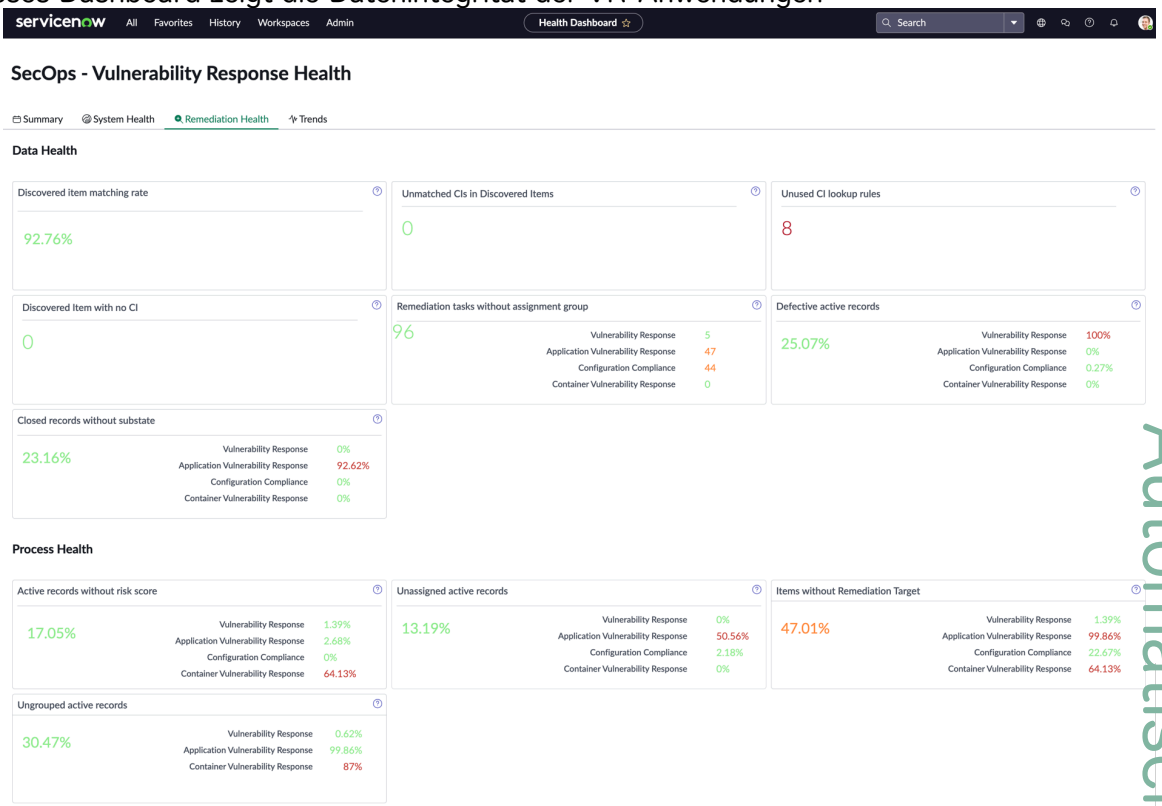



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Korrekturintegrität“

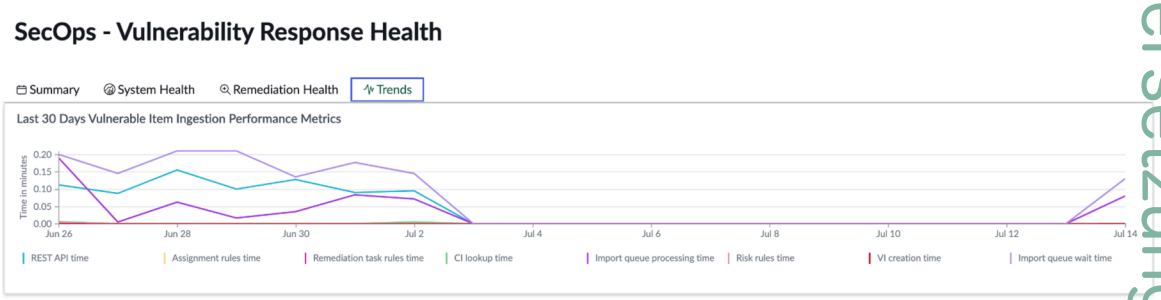
Dieses Dashboard zeigt die Datenintegrität der VR-Anwendungen




an.

### Registerkarte „Trends“.

Dieses Dashboard zeigt die Trends für die Leistungsmetriken der Erfassung angreifbarer Elemente für die letzten 30 Tage für die VR-Anwendungen




an.

## Berichte

**Hinweis:**
Die Schwellenwerte sind Teil des Basissystems. Sie können die Werte basierend auf Ihren Anforderungen konfigurieren.

### Zusammenfassung

| Titel | Beschreibung |
|---|---|
| Integrität gesamt | Gesamtintegritätspunktzahl für die VR-Anwendungen. Weitere Informationen finden Sie in den Berichten für die Metriken. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zusammenfassung (Fortsetzung)

| Titel | Beschreibung |
|---|---|
| Konfiguration | Gesamtkonfigurationsintegrität der VR-Anwendungen. |
| Integrität der Implementierung | Gesamtintegrität der Implementierung der VR-Anwendungen. |
| Integrität der Integration | Gesamtintegrität der VR-Anwendungen. |
| Leistung | Gesamtpunktzahl der Leistungsintegrität der VR-Anwendungen. |
| Datenintegrität | Gesamtdatenintegrität der VR-Anwendungen. |
| Prozessintegrität | Gesamtpunktzahl der Prozessintegrität der VR-Anwendungen. |

### Systemintegrität

| Titel | Beschreibung | Überlegungen zur Verbesserung der Leistung | Schwellenwertwarn | Schwellenwert kritisch |
|---|---|---|---|---|
| Konfiguration | | | | |
| Regeln für automatische Löschung | Zeigt die Anzahl der aktivierten Regeln für die automatische Löschung an. | Überprüfen und beheben Sie die inaktiven Regeln für die automatische Löschung. | 3 | 1 |
| Veraltete Datensätze automatisch schließen | Schließt veraltete Erkennungen automatisch. Weitere Informationen finden Sie im Thema „Veraltete Erkennungen in Vulnerability Response automatisch schließen“ in docs.servicenow.com. | Reduzieren Sie die Menge der veralteten Erkennungen. Aktivieren Sie diese Option, um veraltete Erkennungen zu schließen, die nicht von den Scannern geschlossen werden. | 3 | 1 |
| Integrität der Implementierung | | | | |
| Benutzerdefinierte Skripteinbindungen | Anzahl der angepassten „Skripteinbindungen“. | Minimieren Sie benutzerdefinierte Skripteinbindungen, um Upgrades zu erleichtern. | 10 | 12 |
| Business-Regeln in der Erkennungstabelle | Anzahl der benutzerdefinierten Business | Minimieren Sie Geschäftsregeln, um Upgrades zu erleichtern. | 4 | 8 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Systemintegrität (Fortsetzung)

| Titel | Beschreibung | Überlegungen zur Verbesserung der Leistung | Schwellenwertwarn | Schwellenwert kritisch |
|---|---|---|---|---|
| | Rules in der Erkennungstabelle. | | | |
| Benutzerdefinierte Geschäftsregeln | Anzahl der benutzerdefinierten Geschäftsregeln vor der Erstellung von Datensätzen in der CMDB. | Verwenden Sie die Standardgeschäftsregeln für Datensätze. | 5 | 8 |
| Upgrade-Konflikte | Konflikte wie Business Rules und Skripts, die bei einem Upgrade identifiziert wurden | Überprüfen und lösen Sie die Upgrade-Konflikte. | 10 | 15 |
| PA installiert, aber nicht aktiviert | Gibt an, ob das Performance Analytics-Dashboard nicht aktiviert ist. | Aktivieren Sie das PA-Dashboard. | 10 | 15 |
| Integrität der Integration | | | | |
| Deaktivierte Integrationen | Anzahl der Integrationen, die deaktiviert wurden. | Überprüfen und aktivieren Sie die erforderlichen Integrationen. | 6 | 9 |
| Fehlgeschlagene Integrationsausführungen in der letzten Woche | Anzahl der Integrationsausführungen, die in der letzten Woche nicht erfolgreich waren. | Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Integrationsausführungen. | 9 | 12 |
| Leistung | | | | |
| Langsame Geschäftsregeln und Skripts | Business Rules und Skripts mit einer durchschnittlichen Ausführungszeit von mehr als 10 ms und einer Ausführungsanzahl von mehr als 10.000. | Überprüfen und beheben Sie die langsam ausgeführten Geschäftsregeln. | 10 | 15 |
| Angehaltene Integrationen | Anzahl der Integrationen, bei denen vor dem Abschluss eine Zeitüberschreitung aufgetreten ist. | Überprüfen und beheben Sie die Ursache der blockierten Integrationen. | 10 | 15 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Systemintegrität (Fortsetzung)

| Titel | Beschreibung | Überlegungen zur Verbesserung der Leistung | Schwellenwertwarn | Schwellenwert kritisch |
|---|---|---|---|---|
| Hintergrundaufträge fehlgeschlagen oder angehalten | Fehlgeschlagene oder abgelaufene Hintergrundaufträge in der letzten Woche. | Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Aufträge. | 5 | 10 |
| Langsame Abfragen | Abfragen mit einer durchschnittlichen Ausführungszeit von mehr als 10 ms und einer Ausführungsanzahl von mehr als 10.000. | Überprüfen und beheben Sie die langsam ausgeführten Geschäftsregeln. | 10 | 15 |

### Integrität der Korrektur

| Titel | Beschreibung | Überlegungen zur Verbesserung der Leistung | Schwellenwertwarn | Schwellenwert kritisch |
|---|---|---|---|---|
| Datenintegrität | | | | |
| Übereinstimmungsrate des erkannten Elements | Anzahl der erkannten Elemente, die mit vorhandenen CIs übereinstimmen. | Überprüfen Sie die Integrität Ihrer CMDB und die Logik der CI-Suchregeln. | 50 | 20 |
| Nicht abgeglichene CIs in erkannten Elementen | Erkannte Elemente in nicht abgeglichenem Status. | Überprüfen Sie die Integrität Ihrer CMDB und die Logik der CI-Suchregeln. | 9 | 12 |
| Nicht verwendete CI-Suchregeln | CI-Suchregeln, die keinem erkannten Element zugeordnet sind. | Ändern Sie den Status der nicht verwendeten CI-Suchregeln in „inaktiv“. | 4 | 6 |
| Erkanntes Element ohne CI | Erkanntes Element ohne Konfigurationselement. | Überprüfen Sie die CI-Suchregeln, und wenden Sie sie erneut an. | 9 | 12 |
| Fehlerhafte aktive Datensätze | Datensätze ohne Konfigurationselement oder Schwachstelle. | CIs mithilfe der CMDB CI Lifecycle Management-Option löschen. | 40 | 60 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Integrität der Korrektur (Fortsetzung)

| Titel | Beschreibung | Überlegungen zur Verbesserung der Leistung | Schwellenwertwarn | Schwellenwert kritisch |
|---|---|---|---|---|
| | | **Hinweis:** Das direkte Löschen von CIs kann zu verwaisten VITs führen. | | |
| Korrekturaufgaben ohne Zuweisungsgruppe | Aktive Korrekturaufgaben, deren Zuweisungsgruppe noch zugewiesen werden muss. | Weisen Sie einer Zuweisungsgruppe Korrekturaufgaben zu, und überprüfen Sie die vorhandenen Zuweisungsregeln. | 40 | 60 |
| Geschlossene Datensätze ohne Substatus | Datensätze, die ohne Substatus geschlossen werden. | Geben Sie beim Schließen der Datensätze Informationen im Feld Grund an. | 40 | 50 |
| Prozessintegrität | | | | |
| Aktive Datensätze ohne Risikopunktzahl | Aktive Datensätze mit einer Risikopunktzahl von 0 oder ohne zugewiesene Risikopunktzahl. | Überprüfen und lösen Sie die Risikoregeln. | 40 | 60 |
| Nicht zugewiesene aktive Datensätze | Datensätze ohne Zuweisungsgruppe. | Weisen Sie den Datensätzen eine Gruppe zu, und überprüfen Sie die vorhandenen Zuweisungsregeln. | 30 | 50 |
| Elemente ohne Korrekturziel | Elemente ohne Korrekturzieldatum. | Überprüfen und lösen Sie die Korrekturzielregeln. Diese Regeln müssen alle Datensätze enthalten. | 30 | 50 |
| Nicht gruppierte aktive Datensätze | Datensätze, die nicht in einer Regel für Korrekturaufgaben enthalten sind. | Überprüfen Sie die Regeln für Korrekturaufgaben. | 40 | 60 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Trends

| Titel | Beschreibung |
|---|---|
| Leistungsmetriken zur Erfassung angreifbarer Elemente der letzten 30 Tage | Durchschnittliche Zeit, die in den letzten 30 Tagen für die Erfassung angreifbarer Elemente und die Verarbeitung mehrerer Regeln benötigt wurde. |

### Ändern der Schwellenwerte

Sie können die Schwellenwerte für die Daten im Dashboard „SecOps VR-Integrität“ nach Ihren Wünschen ändern.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren zu **Security Operations-Integrität** > **Konfiguration** > **Metriken**.
2. Öffnen Sie auf der Seite „Integritäts-Dashboard-Daten“ den Datensatz, den Sie ändern möchten.
3. Aktualisieren Sie den Datensatz, und speichern Sie ihn.

## Vulnerability Management (PA) -Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach. Sie können Berichte beispielsweise nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern. Erhalten Sie schnell Einblick in Ihr Schwachstellenrisiko und die betroffenen Business Services.

### Erforderliche Now Platform-Rollen

Erforderliche Rolle: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst und Benutzer mit sn_vul.vulnerability_read (oder die die Rolle sn_vul.vulnerability_read erben) und pa_viewer.

### Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

| Anwender | Dashboard-Verwendung |
|---|---|
| IT-Manager, IT-Analysten, Schwachstellenkorrektur-Besitzer | Unterstützen Sie Ihr Unternehmen bei der Bewältigung der steigenden Anzahl von Security Incidents aufgrund von ausgenutzten Schwachstellen, indem Sie effizient bestimmen, welche angreifbaren Elemente das höchste Risiko darstellen. Diese Dashboards bieten eine grafische Ansicht der Aktivität angreifbarer Elemente und helfen beim Entwerfen von Korrekturplänen und Statusfortschritten. Sie können sich auf die KPIs konzentrieren, die kritischen betroffenen Assets und Schwachstellen mit hoher Transparenz zugeordnet sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um das Dashboard für Schwachstellenmanagement (PA) anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Übersicht**.

Sehen Sie sich Berichte an, die Trenddaten im Zeitverlauf anzeigen. Berichte mit Echtzeitdaten sind unten aufgeführt. Zeigen Sie regelmäßig Trends wichtiger Metriken an, um Ihre gesamten Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

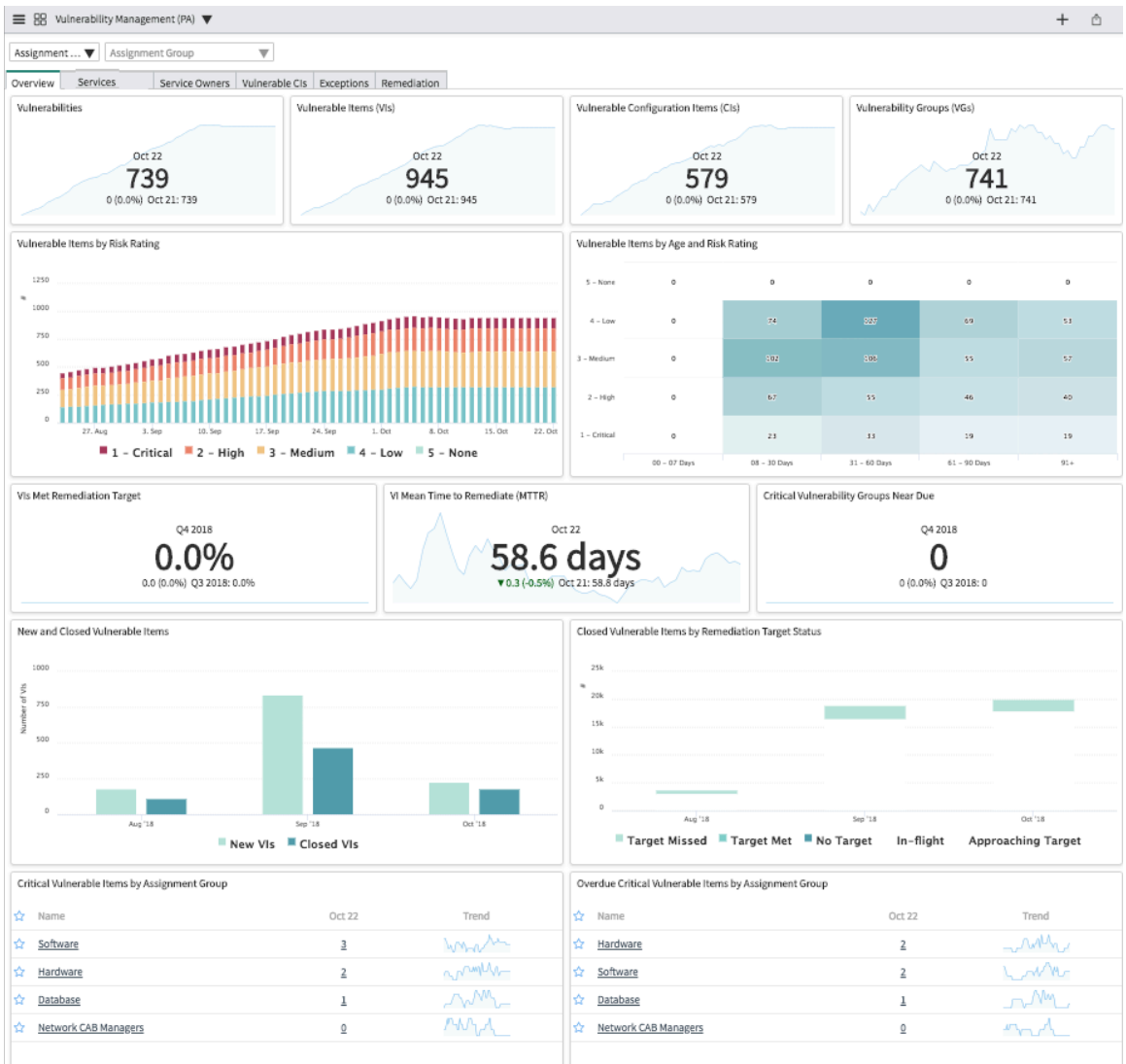
Weitere Informationen zum Anzeigen Ihrer PA-Berichte mit Echtzeitpunktzahlen finden Sie unter Performance Analytics für Vulnerability Response-Berichte [PA] in Echtzeit anzeigen.

## Die Registerkarten des Schwachstellenmanagement-Dashboards [PA].

### Registerkarte „Übersicht“

Dieses Dashboard kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Assets, Einhaltung der Korrekturziele und Fortschritt der Korrektur.

Auf der Registerkarte Übersicht können Sie den Bericht „Kritische angreifbare Elemente nach Zuweisungsgruppe“ anzeigen, der basierend auf der geplanten Aufgabe ausgeführt wird.



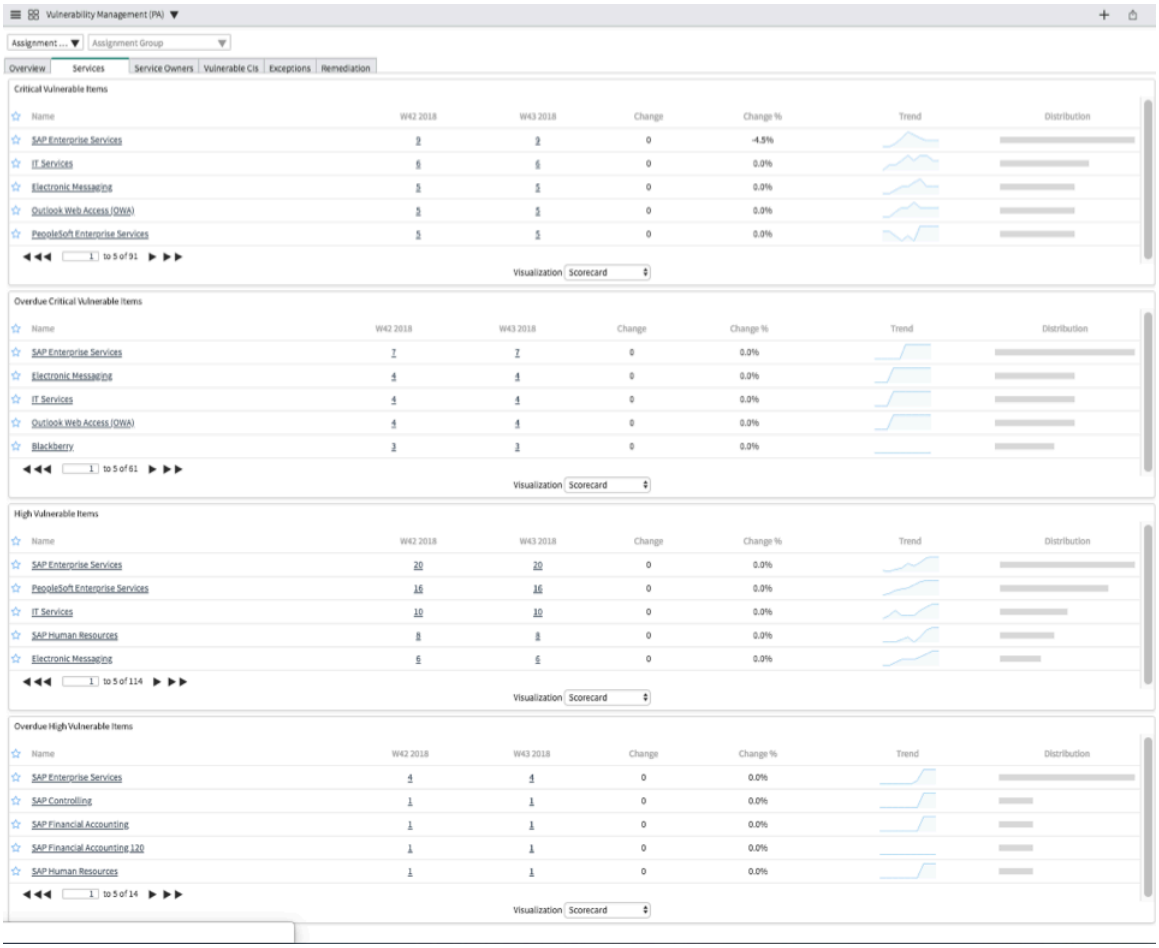

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Business Services“

Dieses Dashboard macht Schwachstellenrisiken auf Geschäftsserviceebene verfügbar. Die Weitergabe dieser Informationen im gesamten Unternehmen kann Servicemanager dabei unterstützen, Schwachstellen schnell und proaktiv zu beheben, und die Organisation in Richtung eines Modells der Informationssicherheit mit gemeinsamer Verantwortung führen.

Sie können die Serviceklasse mithilfe der Systemeigenschaft sn_vul.service_classificationsin technische Services oder Anwendungsservices ändern.

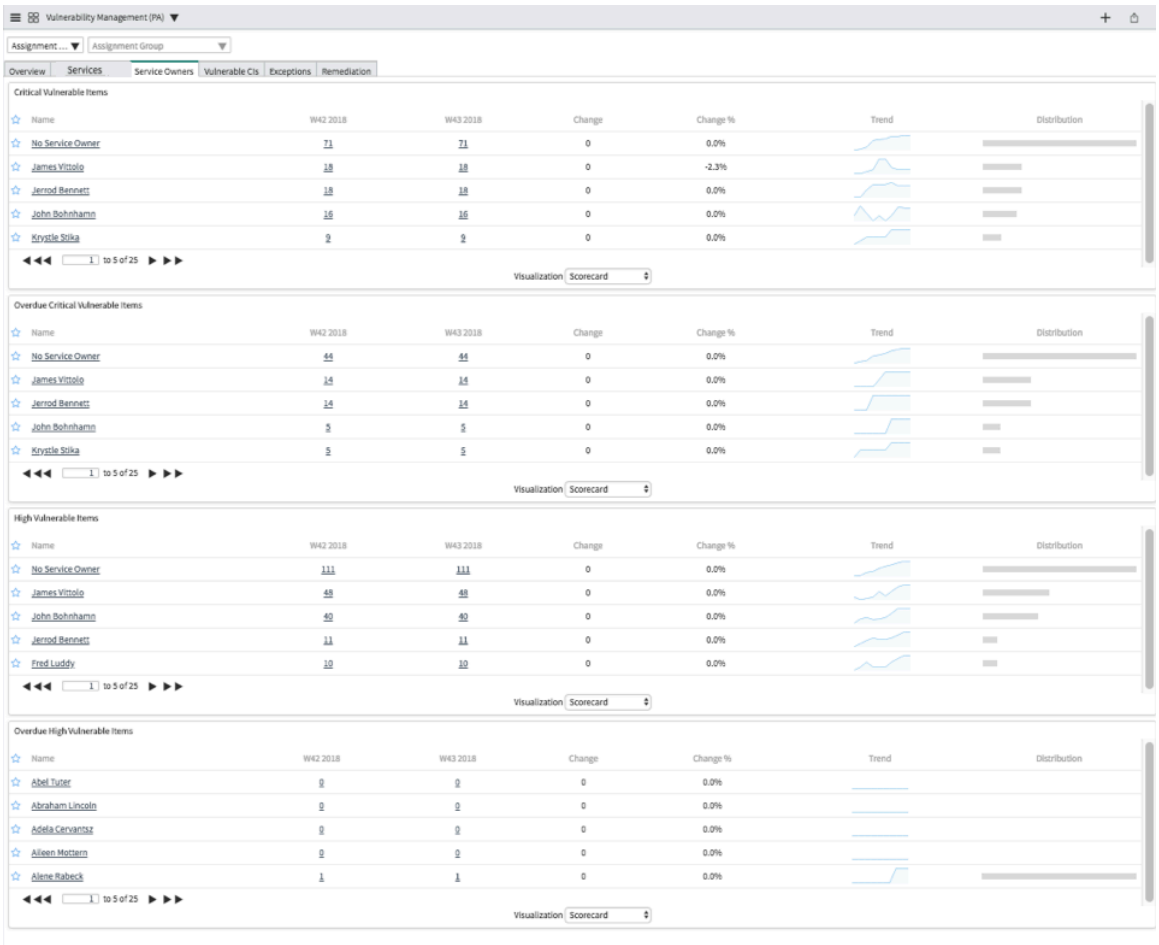



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte Serviceverantwortliche

Dieses Dashboard fasst das Schwachstellenrisiko vom Business Service-Level bis hin zu den Serviceverantwortlichen zusammen – den Führungskräften, die für diese Business Services verantwortlich sind. Sie zeigt, welche Führungskräfte das höchste Schwachstellenrisiko eingehen und welche möglicherweise die meiste Hilfe benötigen, um sofortige Korrekturmaßnahmen zu fördern.



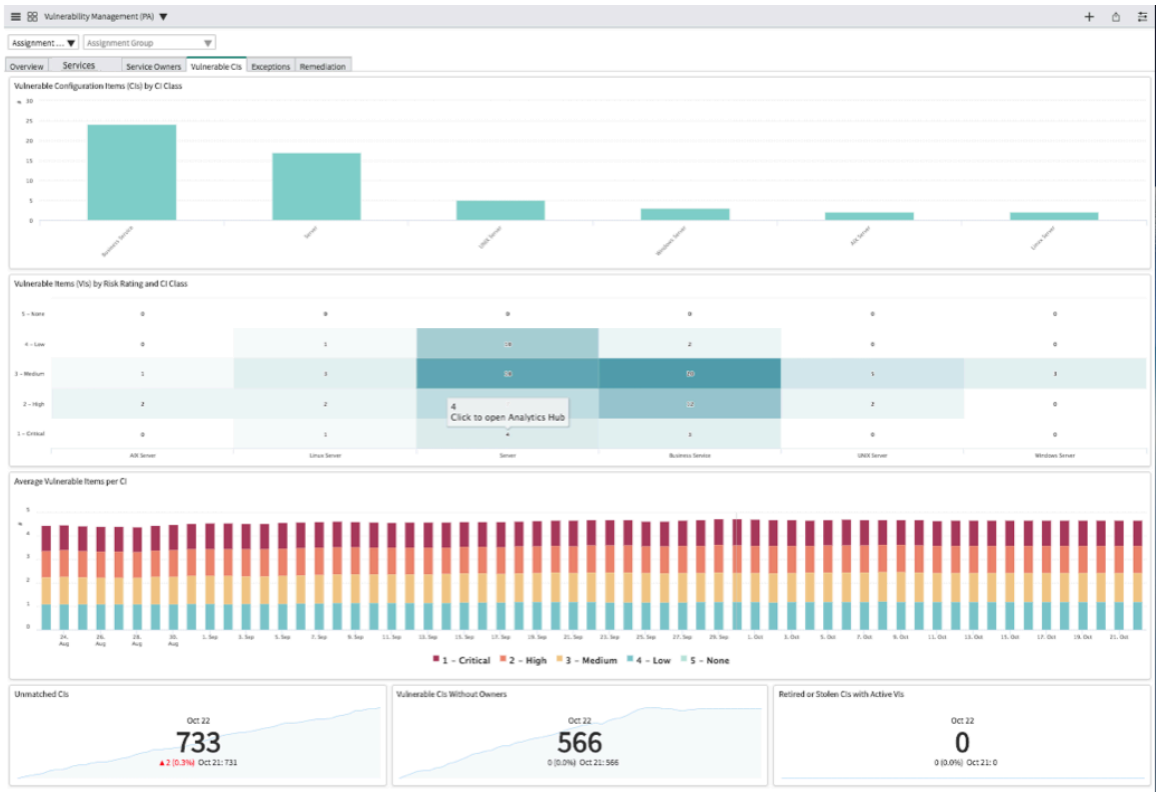

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Registerkarte „Angreifbare CIs“

Dieses Dashboard zeigt Umfang und Zusammensetzung von CIs mit aktiven Schwachstellen und welche Kategorien von CIs die meiste Aufmerksamkeit erfordern. Identifizieren Sie stillgelegte Assets mit aktiven angreifbaren Elementen, und bestätigen Sie, dass die Assets stillgelegt wurden. Zeigen Sie die Anzahl der angreifbaren CIs an, für die keine Besitzerinformationen vorhanden sind, damit Sie Besitzer für diese Assets proaktiv identifizieren können, bevor eine kritische Schwachstelle diese Systeme betrifft.

Auf der Registerkarte „Angreifbare CIs“ können Sie die Berichte „Angreifbare CIs ohne Besitzer“ und „Stillgelegte oder gestohlene CIs mit aktiven VIs“ in Echtzeit anzeigen.



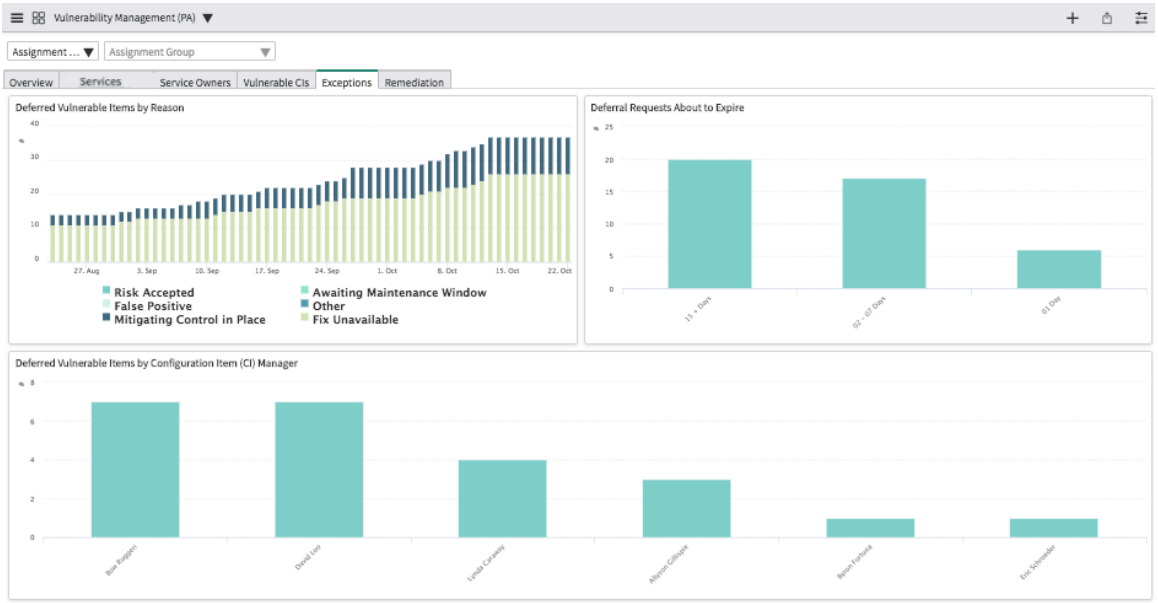

### Registerkarte Ausnahmen

Dieses Dashboard hilft Ihnen zu verstehen, wo Ihr Unternehmen aufgrund potenziell übermäßiger Zurückstellungen Risiken eingeht, und hilft Ihnen, die Korrekturoptionen zu überdenken.

Sie können die Berichte „Zurückgestellte angreifbare Elemente nach Grund“, „Ablaufende Zurückstellungsanforderungen“, „Ausnahmen für kritische angreifbare Elemente nach Zuweisungsgruppe“ und „Ausnahmeanforderungen nach anfordernder Person“ anzeigen.



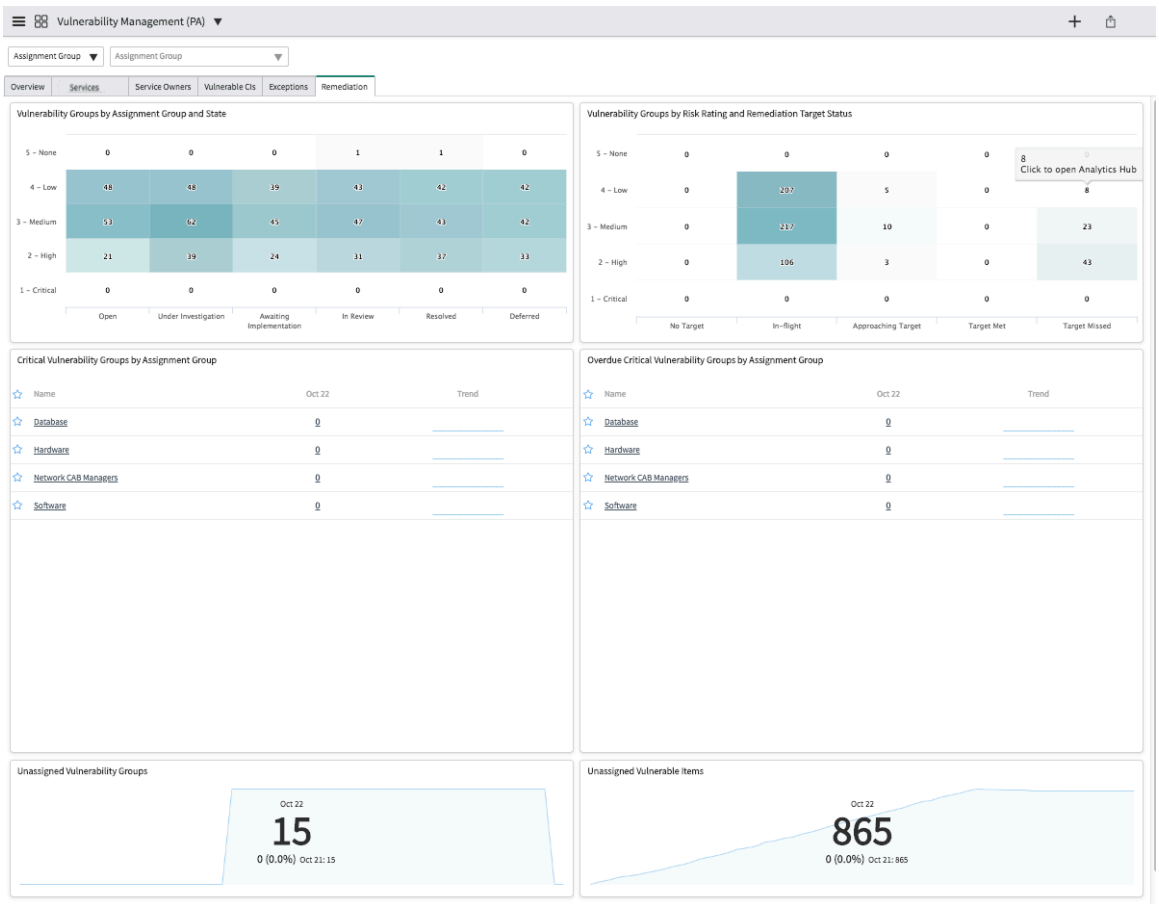
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Registerkarte „Remediation“

Dieses Dashboard hilft Ihnen, den Fortschritt Ihrer Korrekturmaßnahmen nachzuvollziehen und festzustellen, welche Support-Teams bei deren Abschluss die meiste Unterstützung benötigen.

Auf der Registerkarte „Korrektur“ können Sie den Bericht „Nicht zugewiesene angreifbare Elemente“ in Echtzeit anzeigen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Indikatoren

### Vulnerability Response – Indikatoren

Es gibt eine Reihe von Indikatoren, mit denen Sie den Fortschritt der Korrektur von Schwachstellen in der Anwendung Vulnerability Response messen und nachverfolgen können.

Die Option zum Sammeln von Datensätzen für die Indikatoren ist für die Anwendung Vulnerability Response standardmäßig deaktiviert. Diese Option ist deaktiviert, sodass bestimmte Berichte in Echtzeit angezeigt werden können. Die von diesen Indikatoren verwendeten Trendinformationen sind weiterhin verfügbar, wenn Sie das Sammeln von Datensätzen manuell aktivieren und die Datensätze anzeigen möchten, aus denen die Punktzahlen bestehen.

**Eindeutige Schwachstellen**

Eindeutige Schwachstellen mit count_active_vi > 0. Ziel ist die Minimierung.

**Nicht zurückgestellte überfällige kritische angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**% der angreifbaren Elemente mit erfülltem Nachbesserungsziel**

([[Geschlossene angreifbare Elemente > Korrekturziel = Ziel erfüllt]] / [[Geschlossene angreifbare Elemente]]) * 100. Ziel ist die Maximierung.

**Nicht zugewiesene angreifbare Elemente**

Alle aktiven angreifbaren Elemente, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist die Minimierung.

**Kritische angreifbare Elemente (Services)**

Dies ist die Anzahl in der Datenquelle „Aktive AEs (Services)“, die die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

**Weit überfällige angreifbare Elemente (Services)**

Dies ist die Anzahl in der Datenquelle „Aktive AEs (Services)“, die die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

**Nicht zugewiesene Korrekturaufgaben**

Alle aktiven Korrekturaufgaben, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist die Minimierung.

**Kritische angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Neue angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Neu“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Angreifbare Konfigurationselemente**

Dies ist die eindeutige Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Summierte Dauer der geschlossenen angreifbaren Elemente**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies ist die Summe in der Datenquelle „AE.Geschlossen“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Nicht zurückgestellte Korrekturaufgaben**

Dies ist die Anzahl in der Datenquelle „VG.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerability. Ziel ist die Minimierung.

**Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente**

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

**Kritische überfällige angreifbare Elemente (Services)**

Dies ist die Anzahl in der Datenquelle „Aktive AEs (Services)“, die die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

**Stillgelegte Konfigurationselemente**

Dies ist die eindeutige Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Zurückstellungsanforderungen**

Dies ist die Anzahl in der Datenquelle „Aktive Zurückstellungsanforderungen“, die die folgende Tabelle verwendet: sn_vul_change_approval. Ziel ist die Minimierung.

**Angreifbare Elemente nach Konfigurationselementen**

Dies ist die Anzahl in Datenquellen-CIs mit aktiven AEs, die die folgende Tabelle verwendet: sn_vul_analytics_vi_ci_class. Ziel ist die Minimierung.

**Geschlossene angreifbare Elemente**

„Geschlossene angreifbare Elemente“ wird täglich als Anzahl von Einheiten gemessen. Das Ziel besteht in der Maximierung.

**Nicht abgeglichene Konfigurationselemente**

Listet die Hosts auf, die von Schwachstellenscannern einer Drittpartei erkannt wurden und keinen vorhandenen CIs in der CMDB entsprechen.

**Nicht zurückgestellte überfällige kritische Korrekturaufgaben**

Dies ist die Anzahl in der Datenquelle „VG.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerability. Ziel ist die Minimierung.

**Angreifbare Konfigurationselemente ohne Supportgruppe**

Dies ist die Anzahl in der Datenquelle „AE.Offen“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Nicht zurückgestellte kritische Korrekturaufgaben**

Dies ist die Anzahl in der Datenquelle „VG.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerability. Ziel ist die Minimierung.

**Zurückgestellte angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Hoch angreifbare Elemente (Services)**

Dies ist die Anzahl in der Datenquelle „Aktive AEs (Services)“, die die folgende Tabelle verwendet: sn_vul_analytics_business_services_vi. Ziel ist die Minimierung.

**Eindeutige Konfigurationselemente mit aktiven angreifbaren Elementen**

Dies ist die eindeutige Anzahl in Datenquellen-CIs mit aktiven AEs, die die folgende Tabelle verwendet: sn_vul_analytics_vi_ci_class. Ziel ist die Minimierung.

**Durchschnittliche Anzahl angreifbarer Elemente pro Konfigurationselement.**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[Aktive angreifbare Elemente]] / [[angreifbare CIs]]. Ziel ist die Minimierung.

**Korrekturaufgaben**

Dies ist die Anzahl in der Datenquelle „VG.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerability. Ziel ist die Minimierung.

**Kritische zurückgestellte angreifbare Elemente**

Dies ist die Anzahl in der Datenquelle „AE.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_vulnerable_item. Ziel ist die Minimierung.

**Zurückstellungsanforderungen (erstellt)**

Dies ist die Anzahl in der Datenquelle „Closed.Requests“, welche die folgende Tabelle verwendet: sn_vul_change_approval. Ziel ist die Minimierung.

## BreakdownsAufgliederungen

Die folgenden Aufgliederungsnamen gelten für die Indikatoren im Dashboard:

- Alter
- Geschlossen mit Alter
- Zuweisungsgruppe
- CI-Klasse
- CI-Manager
- Zurückstellungsalter
- Aufschiebungsgrund
- Ausnahme für anfordernde Person
- Exploit-Angriffsvektor
- Exploit vorhanden
- Exploit-Kompetenzniveau
- Korrekturzielregel
- Nachbesserungszielstatus
- Nachbesserungszielstatus (geschlossen)
- Risikobewertung
- Service
- Servicerelevanz
- Serviceverantwortlicher
- Schweregrad
- Status

Aufgliederungsquelle

- Zuweisungsgruppe: Gilt für VI- oder und RT-Berichte
- Exploit vorhanden: Gilt für VI-Berichte.
- Exploit-Angriffsvektor: Gilt für VI-Berichte.
- Exploit-Kompetenzniveau: Gilt für VI-Berichte.
- Status des Korrekturziels: Gilt für VI- und RT-Berichte.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Risikobewertung: Gilt für VI- und RT-Berichte.
- Status: Gilt für VI- und RT-Berichte.

## Datenvisualisierungen

| Titel | Typ | Beschreibung |
|---|---|---|
| Schwachstellen | Einzelne Punktzahl | Anzahl der Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Elementen verknüpft sind. |
| Angreifbare Elemente (AEs) | Einzelne Punktzahl | Anzahl der aktiven (nicht geschlossenen) angreifbaren Elemente. |
| Angreifbare Konfigurationselemente (CIs) | Einzelne Punktzahl | Anzahl der Konfigurationselemente (CIs), die mindestens einem aktiven angreifbaren Element zugeordnet sind. |
| Korrekturaufgaben | Einzelne Punktzahl | Anzahl der aktiven (nicht geschlossenen) Korrekturaufgaben. |
| Angreifbare Elemente nach Risikobewertung | Balken | Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne. |
| Angreifbare Elemente nach Alter und Risikobewertung | Heatmap | Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung und Alter (in Tagen). |
| AEs mit erfülltem Nachbesserungsziel | Einzelne Punktzahl | Prozentsatz der geschlossenen angreifbaren Elemente, deren Korrekturzieldaten im aktuellen und vorherigen Quartal eingehalten wurden.<br>Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. |
| Durchschnittliche Zeit bis zur Korrektur (MTTR) für AEs | Einzelne Punktzahl | Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Titel | Typ | Beschreibung |
|---|---|---|
| | | **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe. |
| Kritische Korrekturaufgaben kurz vor der Fälligkeit | Einzelne Punktzahl | Anzahl der aktiven Korrekturaufgaben, die sich ihrem Korrekturzieldatum nähern.<br><br>Das Korrekturzieldatum einer Korrekturaufgabe wird auf das nächste Fälligkeitsdatum festgelegt, das zu einem aktiven angreifbaren Element in der Gruppe gehört.<br><br>Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.<br><br>Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus. |
| Neue und geschlossene angreifbare Elemente | Balken | Anzahl neuer und geschlossener angreifbarer Elemente über die ausgewählte Zeitspanne.<br><br>**Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe. |
| Geschlossene angreifbare Elemente nach Korrekturzielstatus | Balken | Anzahl der geschlossenen angreifbaren Elemente, gruppiert nach Nachbesserungszielstatus für die ausgewählte Zeitspanne. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Titel | Typ | Beschreibung |
|---|---|---|
| | | **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe. |
| Kritische angreifbare Elemente nach Zuweisungsgruppe | Liste und | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Zuweisungsgruppe. |
| Überfällige kritische angreifbare Elemente nach Zuweisungsgruppe | Liste und | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Zuweisungsgruppe.<br><br>Korrekturziele werden aus dem Datum von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |

### Business-Services

| Name | Typ | Beschreibung |
|---|---|---|
| Kritische angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. |
| Überfällige kritische angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Business-Service. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Business-Services (Fortsetzung)

| Name | Typ | Beschreibung |
|---|---|---|
| | | Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |
| Hoch angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, gruppiert nach Business-Service.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. |
| Überfällige hoch angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Business-Service.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |

### Serviceverantwortliche

| Name | Typ | Beschreibung |
|---|---|---|
| Kritische angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service-Besitzer.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. |
| Überfällige kritische angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Business-Service-Besitzer. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Serviceverantwortliche (Fortsetzung)

| Name | Typ | Beschreibung |
|---|---|---|
| | | Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |
| Hoch angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, gruppiert nach Business-Service-Besitzer.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. |
| Überfällige hoch angreifbare Elemente | Liste, Linie und Verteilungsleiste | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Business-Service-Besitzer.<br><br>Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche an, die Differenz zwischen den zwei Wochen (in Anzahl und Prozent) und einen Trend.<br><br>Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |

### Angreifbare CIs

| Name | Typ | Beschreibung |
|---|---|---|
| Angreifbare Konfigurationselemente (CIs) nach CI-Klasse | Balken | Anzahlen der Konfigurationselemente mit aktiven Schwachstellen, gruppiert nach CI-Klasse in der CMDB. |
| Angreifbare Elemente (AEs) nach CI-Klasse | | Anzahl der aktiven AEs aufgeschlüsselt nach CI-Klasse. |
| Durchschnittliche angreifbare Elemente pro CI | Balken | Durchschnittliche Anzahl von angreifbaren Elementen, die zu einem Konfigurationselement gehören, gruppiert nach Risikobewertung. |
| Nicht abgeglichene CIs | Einzelne Punktzahl | Anzahl der importierten Konfigurationselemente, die keinem vorhandenen CI in der CMDB entsprechen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Angreifbare CIs (Fortsetzung)

| Name | Typ | Beschreibung |
|---|---|---|
| Angreifbare CIs ohne Supportgruppe | Einzelne Punktzahl | Anzahl der angreifbaren Konfigurationselemente, denen keine Supportgruppe zugewiesen ist. |
| Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs | Einzelne Punktzahl | Anzahl der Konfigurationselemente, die in der CMDB als „**Stillgelegt**“ oder „**Gestohlen** “ markiert sind und aktive angreifbare Elemente aufweisen. |

### Ausnahmen

| Name | Typ | Beschreibung |
|---|---|---|
| Zurückgestellte angreifbare Elemente nach Grund | Balken | Anzahl der zurückgestellten angreifbaren Elemente, gruppiert nach Zurückstellungsgrund. |
| In Kürze ablaufende Zurückstellungsanforderungen | Balken | Anzahl der Zurückstellungsanforderungen, die Korrekturaufgaben oder angreifbaren Elementen zugeordnet sind, die kurz vor der erneuten Öffnung zur Überprüfung stehen. Sie werden nach der Anzahl der verbleibenden Tage gruppiert, bis sie erneut geöffnet werden.<br><br>Wenn E-Mail-Benachrichtigungen definiert sind, wird eine E-Mail gesendet. |
| Zurückgestellte angreifbare Elemente nach Configuration Item (CI)-Manager | Balken | Anzahl der zurückgestellten angreifbaren Elemente, die vom Manager für das zugehörige Konfigurationselement gruppiert wurden. |

### Korrektur

| Name | Typ | Beschreibung |
|---|---|---|
| Korrekturaufgaben nach Risikobewertung und Status | Heatmap | Anzahl der aktiven Korrekturaufgaben, gruppiert nach Risikobewertung und Status. |
| Korrekturaufgaben nach Risikobewertung und Status des Korrekturziels | Heatmap | Anzahl der aktiven Aufgaben, gruppiert nach Risikobewertung und Status des Korrekturziels.<br><br>Dieser Bericht schließt zurückgestellte angreifbare Elemente aus. |
| Kritische Korrekturaufgaben nach Zuweisungsgruppe | Liste und | Anzahl der aktiven Korrekturaufgaben mit kritischer Risikobewertung, gruppiert nach Zuweisungsgruppe.<br><br>Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus. |
| Überfällige kritische Korrekturaufgaben nach Zuweisungsgruppe | Liste und | Anzahl der aktiven Korrekturaufgaben mit kritischer Risikobewertung, deren Korrekturzieldatum verstrichen ist, gruppiert nach Zuweisungsgruppe. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Korrektur (Fortsetzung)**

| Name | Typ | Beschreibung |
|---|---|---|
| | | Dieser Bericht schließt zurückgestellte Korrekturaufgaben aus. |
| Nicht zugewiesene Korrekturaufgaben | Einzelne Punktzahl | Anzahl der aktiven Korrekturaufgaben ohne einen Beauftragten oder eine Zuweisungsgruppe. |
| Nicht zugewiesene angreifbare Elemente | Einzelne Punktzahl | Anzahl der aktiven angreifbaren Elemente ohne einem Beauftragten oder einer Zuweisungsgruppe. |

### Zeigen Sie Performance Analytics for Vulnerability Response [PA]-Berichte in Echtzeit an

Um Ihre wichtigsten angreifbaren Elemente (AEs) zu verwalten und sie schnell zu beheben, können Sie Berichte bei Bedarf in Echtzeit im Dashboard „Schwachstellenmanagement“ (PA) anzeigen. Die Anwendung Performance Analytics for Vulnerability Response ist mit einem separaten Abonnement von ServiceNow Storeverfügbar.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Weitere Informationen zu den Berichten für Performance Analytics for Vulnerability Responsefinden Sie unter Dashboard für Schwachstellenmanagement [PA].

Weitere Informationen zum Setup und zur Installation der Anwendung Performance Analytics for Vulnerability Response finden Sie unter Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA]..

Wenn nicht angezeigt, navigieren Sie zum Anzeigen des Dashboards zu **Vulnerability Response** > **Übersicht**. Oben im Dashboard werden die Berichtsregisterkarten angezeigt.

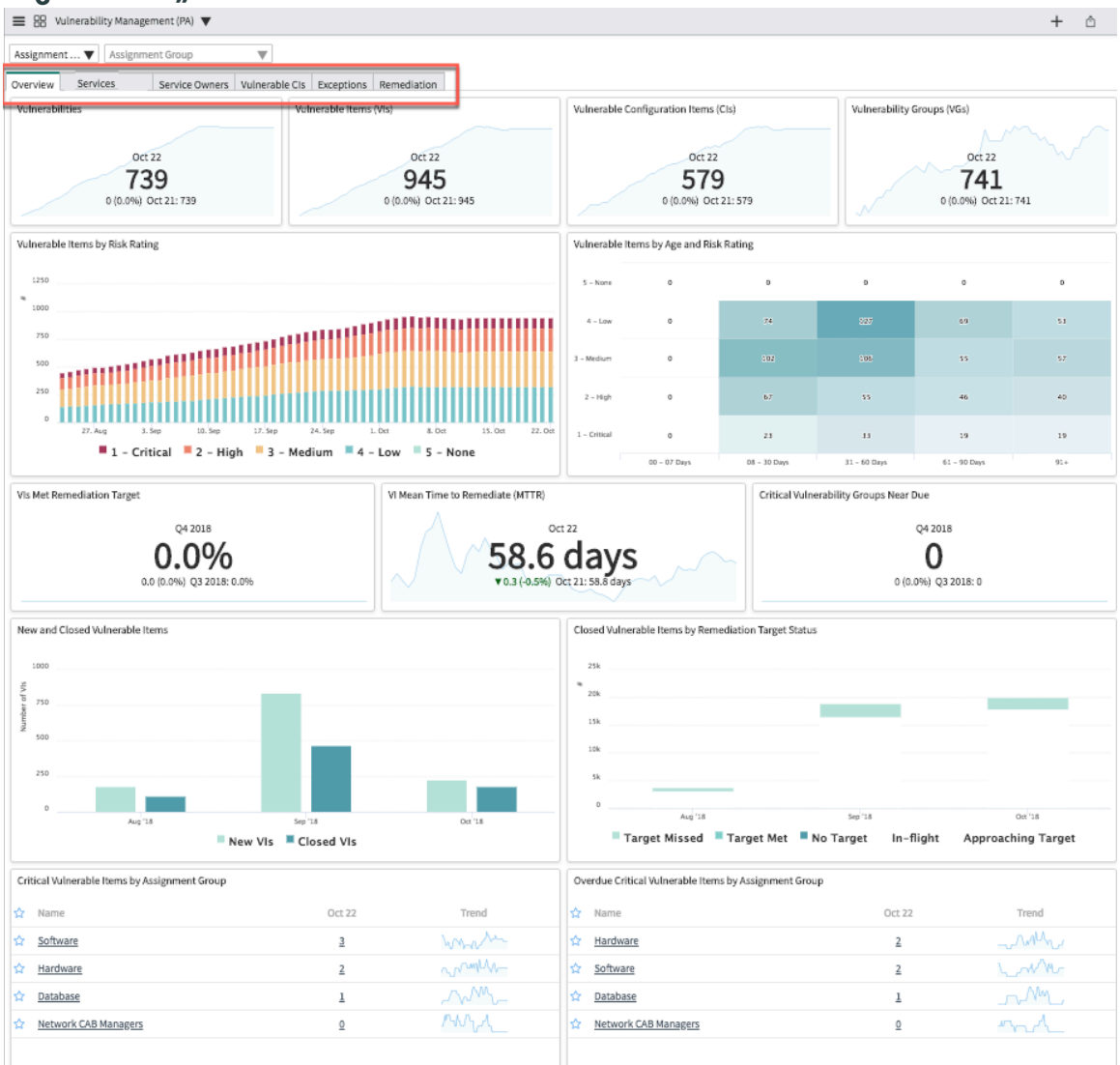
Ab Version 19.0 von Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards in Vulnerability Manager Workspace und Dashboards in IT Remediation Workspace.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Übersicht“




Zeigen Sie die folgenden Berichte auf den Registerkarten des Dashboards für Schwachstellenmanagement (PA) in Echtzeit an.

- Registerkarte „Übersicht“
  - Kritische angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „Angreifbare CIs“:
  - Angreifbare CIs ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte „Ausnahmen“:
  - Zurückgestellte angreifbare Elemente nach Grund
  - In Kürze ablaufende Zurückstellungsanforderungen
  - Zurückgestellte angreifbare Elemente nach CIO-Manager
- Registerkarte „Korrektur“:
  - Nicht zugewiesene angreifbare Elemente

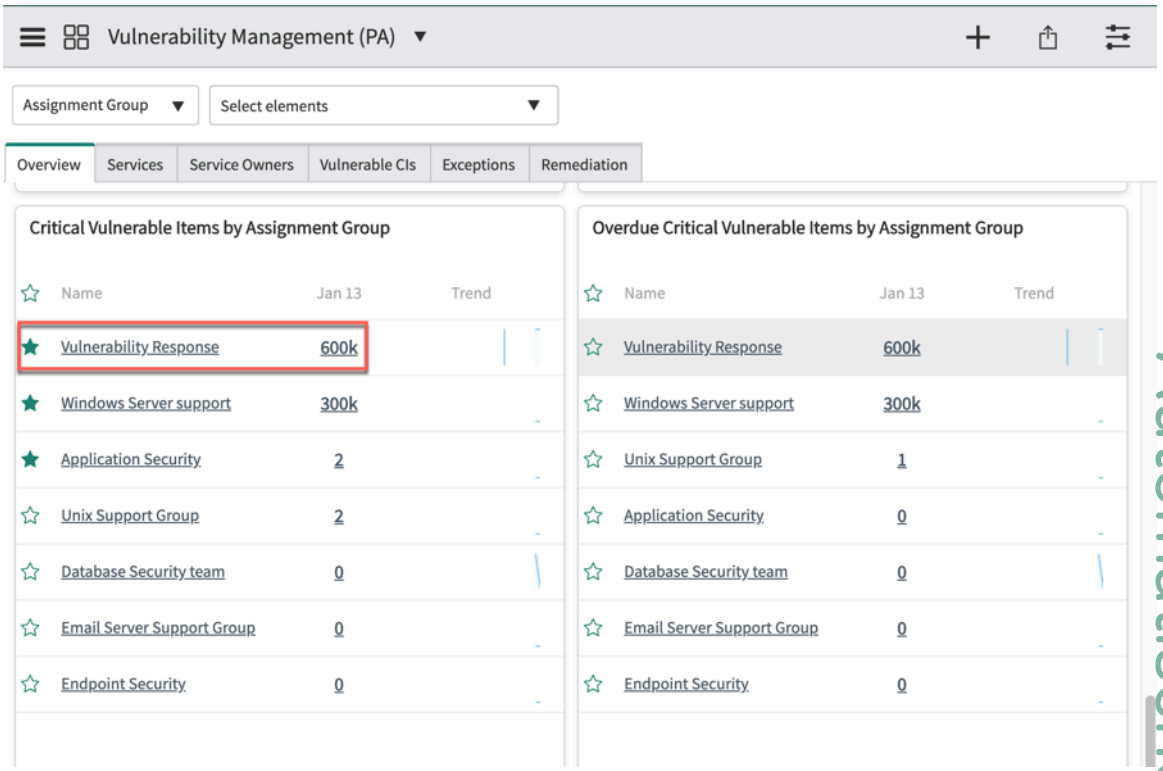
Um Echtzeitpunktzahlen anzuzeigen, führen Sie die folgenden Schritte aus, wenn Sie eine der Registerkarten ausgewählt haben, die Echtzeitberichte enthält:

Automatische Übersetzung

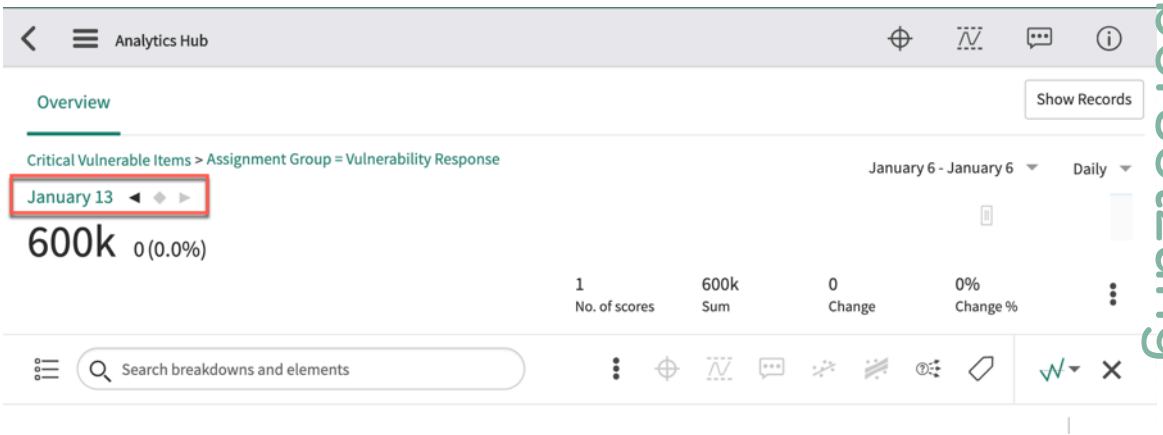
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Klicken Sie im Bericht, z. B. Kritische angreifbare Elemente nach Zuweisungsgruppe, auf einen der angezeigten Links.




2. Klicken Sie im angezeigten Datensatz auf das Datum.

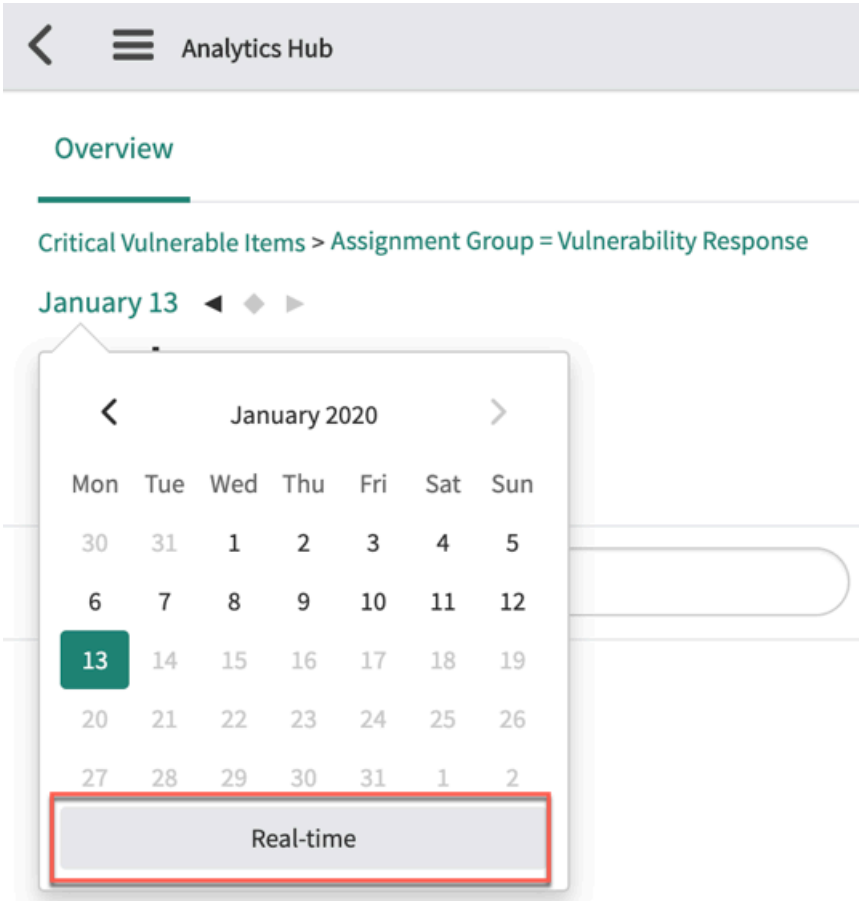



3. Klicken Sie im angezeigten Kalender auf Echtzeit.

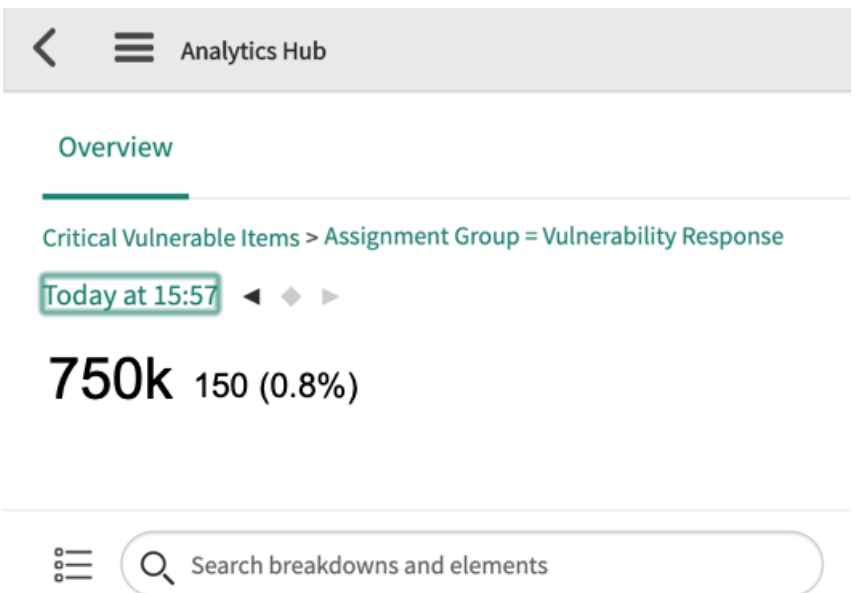
   Wenn ein Bericht keine Echtzeitpunktzahl unterstützt, wird die Schaltfläche Echtzeit nicht im Kalender angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Es kann einen Moment dauern, bis der Wert aktualisiert wird. Das aktuelle Datum, die Datensätze, die Anzahl der neuen Datensätze seit dem letzten Bericht und die prozentuale Änderung gegenüber dem letzten Bericht werden ebenfalls angezeigt.




4. **Wahlweise:** Um die Datensätze anzuzeigen, aus denen der Bericht besteht, klicken Sie bei angezeigtem Echtzeitbericht oben rechts auf **Datensätze**anzeigen.
   Eine Liste der Datensätze, aus denen die Punktzahl besteht, wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Indikatoren [ Performance Analytics für Vulnerability Response [PA] anzeigen

Zeigen Sie automatisierte und formulierte Performance Analytics Indikatoren an, die die Schwachstellendaten in Ihrer Instanz darstellen.

## Vorbereitungen

Die Option zum Sammeln von Datensätzen für die Indikatoren ist für die Anwendung Performance Analytics - Content Pack Vulnerability Response standardmäßig inaktiv. Diese Option ist deaktiviert, sodass bestimmte Berichte in Echtzeit angezeigt werden können. Die von diesen Indikatoren verwendeten Trendinformationen sind weiterhin verfügbar, wenn Sie das Sammeln von Datensätzen manuell aktivieren und die Datensätze anzeigen möchten, aus denen die Punktzahlen bestehen.

**Hinweis:**
Die Aktivierung von Datensätzen erfassen in einem Indikator kann sich auf Ihre Leistung auswirken und die Zeit und den Arbeitsspeicher, die für die Ausführung der Datenerfassungsaufgabe erforderlich sind, erheblich verlängern.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) oder pa.viewer

## Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response verfügt sowohl über automatisierte als auch über formulierte Indikatoren.

## Wichtige Begriffe

**PA-Indikator**

Definiert eine Leistungsmessung, die in regelmäßigen Abständen für einen Business Service, eine Aktivität oder ein Organisationsverhalten durchgeführt wird, z. B. Nicht zurückgestellte überfällige kritische angreifbare Elemente.

**PA-Indikatorquelle**

Datensätze, die Datensätze aus einer Tabelle oder Datenbankansicht filtern, z. B. VI aktiv.

**Datensätze erfassen**

Wenn diese Option aktiviert ist, werden Datensätze im Speicher gespeichert und Zugriff auf Analytics Hub gewährt.

**BreakdownsAufgliederungen**

Aufgliederungen filtern und gruppieren erfasste Datensätze. Aufgliederungen können die Speichernutzung erhöhen, insbesondere wenn ihre Anzahl und Vielfalt zunimmt.

**Aufgliederungsausschlüsse**

Ausschlüsse entfernen bestimmte Aufgliederungen, wodurch der Speicherverbrauch reduziert werden kann

## Prozedur

1. Navigieren Sie für automatisierte Indikatoren zu **Performance Analytics** > **Indikatoren** > **Automatisierte Indikatoren**.
2. Navigieren Sie für formulierte Indikatoren zu **Performance Analytics** > **Formelindikatoren**.

Ausführliche Informationen zu Indikatoren finden Sie unter Performance Analytics-Indikatoren .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

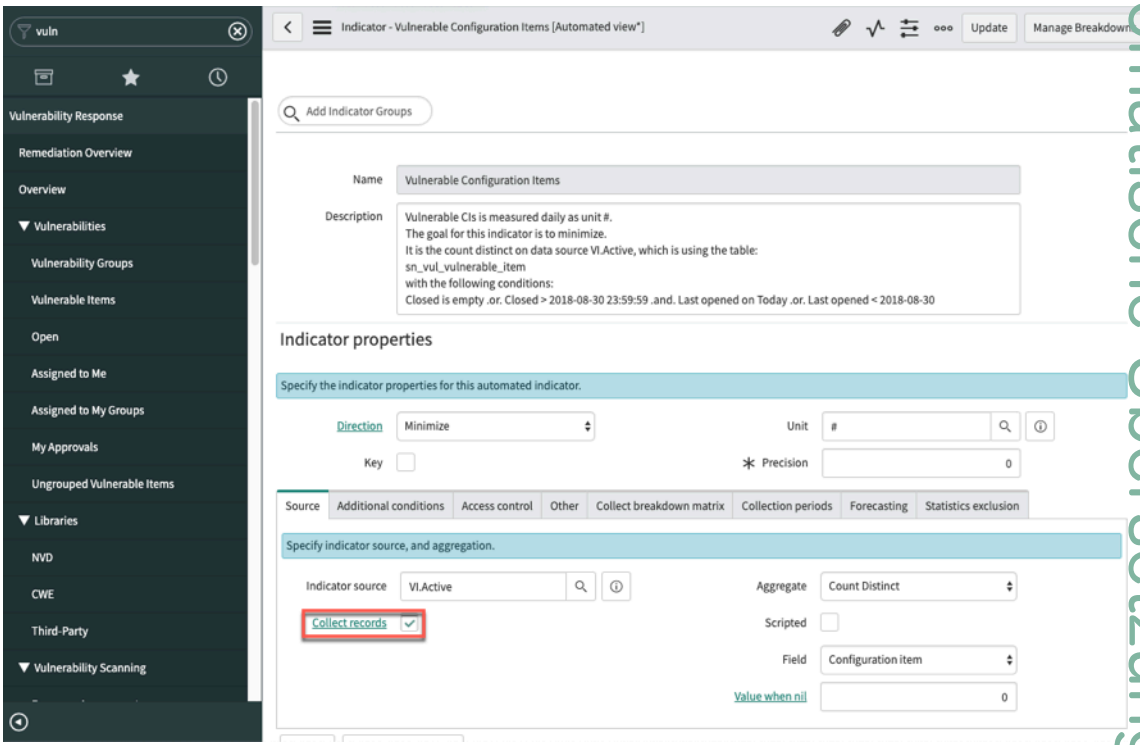
3. Suchen Sie in beiden Fällen nach **Anwendung** > **Performance Analytics**.

**Hinweis:**
Wenn sie sich nicht in Ihrer Standardansicht befindet, fügen Sie die Spalte **Anwendung** mithilfe des Zahnradsymbols ( ) in der oberen linken Ecke der Seite hinzu. Die Spalte Anwendung wird dann im Dropdown-Menü „Suche“ angezeigt.

4. **Wahlweise:** Führen Sie die folgenden Schritte aus, um Datensätze erfassen für einen Performance Analytics-Indikator für Vulnerability Response zu aktivieren:

a. Wenn die Liste der automatisierten Indikatoren angezeigt wird, klicken Sie in der Spalte Name auf den Indikator, für den Sie das Sammeln von Datensätzen aktivieren möchten.
Der Indikatordatensatz wird angezeigt.

b. Aktivieren Sie im Abschnitt „Indikatoreigenschaften“ auf der Registerkarte Quelle das Kontrollkästchen Datensätze sammeln.




Automatische Übersetzung

c. Wählen Sie eine, um fortzufahren.

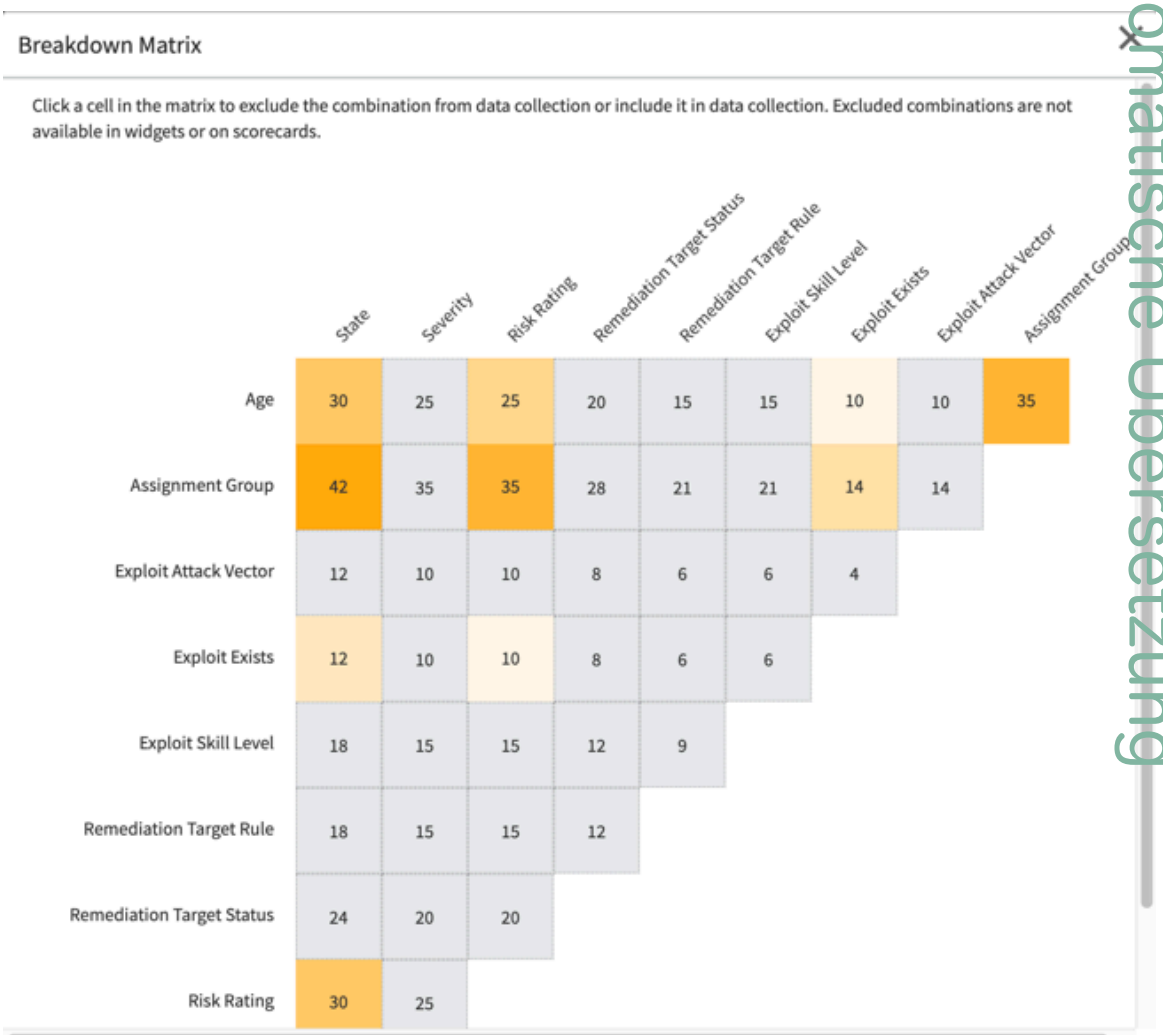
| Option | Beschreibung |
|---|---|
| **Aktualisieren** | Speichern Sie Ihre Änderungen, und kehren Sie zur Liste der Indikatoren zurück. |
| **Aufgliederungen verwalten**<br>**Hinweis:**<br>Wenn Sie Aufgliederungen der zweiten Ebene erneut aktivieren, können Sie den Speicherverbrauch erheblich erhöhen und die Datenerfassungsaufgabe verlangsamen. | Reaktivieren Sie Aufgliederungen der zweiten Ebene für die aufgelisteten Indikatoren, oder bearbeiten Sie Aufgliederungen für andere Indikatoren.<br>(Optional) Weitere Informationen zu Performance Analytics-Aufgliederungen |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| Standardmäßig wurden Aufgliederungsausschlüsse der zweiten Ebene auf die folgenden Indikatoren angewendet:<br>▪ Angreifbare Konfigurationselemente<br>▪ Außer Kraft gesetzte CIs<br>▪ Zurückgestellte AEs | finden Sie unter Performance Analytics-Aufgliederungen. |

**d.** Klicken Sie auf **Aufgliederungen verwalten**.

**e.** Klicken Sie im angezeigten Formular auf **Konfigurieren Aufgliederungsmatrix**.
Das Formular „Aufgliederungsmatrix“ wird angezeigt. Ausgeschlossene Kombinationen werden ausgewählt und mit Farben angezeigt, wie in der folgenden Abbildung dargestellt.




**f.** Um den Ausschluss zu entfernen und eine ausgeschlossene Kombination erneut zu aktivieren, klicken Sie auf eine ausgewählte Zelle.

**g.** Klicken Sie oben rechts im Formular auf **Schließen**, um zum Formular „Aufgliederung verwalten“ zurückzukehren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**h.** Klicken Sie auf den Zurück-Pfeil, um zum Indikatordatensatz zurückzukehren.

**i.** Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Liste der Indikatoren zurückzukehren.

## Vulnerability Response Referenzinformationen

Die folgenden Themen enthalten Links, Referenzinformationen, Problembehandlung und Wissensartikel sowie Felddaten in den Formularen und Datensätzen in Vulnerability Response.

Nachfolgend sind einige Links zu anderen Ressourcen aufgeführt, die für Sie hilfreich sein könnten, beginnend mit einem Link zu den Knowledge Base-Links für den Artikel Support und Problembehandlung für VR/CC in der HI Knowledge Base.

- Knowledge Base-Links für Support und Problembehandlung für VR/CC
- Weitere Informationen zu Anwendungen und Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes .
- Videos zu Security Operations
- Entwicklerschulungen
- Entwicklerdokumentation
- Arbeiten Sie mit einem Implementierungsspezialisten zusammen, um mit dem Customer Success Center die gewünschten Geschäftsergebnisse zu erzielen.
- Nehmen Sie an einem Vulnerability Response-Kurs teil, um Fachwissen aufzubauen und den ROI schneller zu erzielen. Besuchen Sie zur Anmeldung die ServiceNow-Schulungs- und -Zertifizierungs-Website .
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden
- Orchestration für Vulnerability Response
- Tipps zum Schreiben von Integrationen
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Implementierungsprüfliste für die Anwendung Vulnerability Response .

Diese Prüfliste listet die Schritte auf, die für eine grundlegende Implementierung der Anwendung Now Platform®Vulnerability Response in Ihrer Instanz von [] erforderlich sind. Wenn Sie diese Aufgaben abgeschlossen haben, ist das Basissystem betriebs- und verifizierungsbereit.

#### Vorbereitungen

Erforderliche Rollen: admin zum Herunterladen und Aktivieren von Anwendungen und Zuweisen von Rollen, sn_vul.vulnerability_admin zum Konfigurieren von Vulnerability Response.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Erwägen Sie das Erstellen und Drucken einer PDF-Datei dieser Prüfliste, damit Sie Aufgaben nach Abschluss abhaken können.
2. Um eine PDF-Datei zu generieren, klicken Sie oben im Thema auf das Symbol „ **Als PDF speichern** “ ( ) und dann auf Ausgewähltes Thema.

#### Vulnerability Response Prüflistenaufgaben für grundlegende Implementierungen für Administratoren

| Element | Beschreibung |
|---|---|
| ☐ | Stellen Sie als Benutzer mit der Administratorrolle sicher, dass Sie Berechtigungen erworben und die folgenden Anwendungen aus ServiceNow® Store in Ihre Instanz von Now Platform ] heruntergeladen (**installiert**) haben:<br>○ Vulnerability Response<br>○ Vulnerability Response Integration mit der NIST National Vulnerability Database<br>○ Qualys Integration for Security Operations<br>**a.** Um zu überprüfen, ob die Anwendungen in Ihrer Instanz verfügbar sind, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie nach [sn_vul], [sn_vul_nvd] und [sn_vul_qualys].<br>**b.** Wenn Sie die Anwendungen nicht finden können, finden Sie unter Security Operations und ServiceNow Store weitere Informationen zum Erhalten der -Berechtigung und zum Herunterladen der Anwendungen. |
| ☐ | Navigieren Sie als Benutzer mit der Administratorrolle **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** und aktivieren (**installieren**) Sie die Anwendung Vulnerability Response zusammen mit ihren Abhängigkeiten von Ihrer Now Platform -Instanz. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Während der Installation der Anwendung Vulnerability Response haben Sie die Möglichkeit, Demodaten zu installieren.<br><br>Demodaten sind erforderlich, wenn Sie automatisierte Tests ausführen möchten, um sicherzustellen, dass Ihre Instanz nach der Installation funktioniert. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus, um Datenbeschädigungen und -ausfälle zu vermeiden. Wenn Demodaten oder Demokonten erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.<br><br>Der Setup-Assistent für Vulnerability Response wird automatisch zusammen mit der Anwendung installiert. Der Setup-Assistent ist erforderlich, um die Anwendung Vulnerability Response zu konfigurieren. Darüber hinaus wird es verwendet, um die in diesem Beispiel verwendete Anwendung Qualys Integration for Security Operations zu installieren und zu konfigurieren, sowie andere Anwendungen, die Vulnerability Responseunterstützen und mit ihnen kompatibel sind.<br><br>Weitere Informationen zur Installation der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. |
| ☐ | Navigieren Sie als Benutzer mit der Administratorrolle im Setup-Assistenten zu **Alle** > **Vulnerability Response-Anwender und -Gruppen** und weisen Benutzern die erforderlichen Vulnerability Response Persona-Rollen zu.<br><br>**a.** Zeigen Sie im Setup-Assistenten vorhandene Benutzer und alle Rollen an, die bereits zugewiesen sind, indem Sie auf den Link für das **Benutzeradministrationsmodul** klicken.<br><br>**b.** Klicken Sie in der Liste auf einen Benutzernamen, um den Datensatz zu öffnen, und klicken Sie auf die zugehörige Liste **Rollen**. Alle diesem Benutzer zugewiesenen Rollen werden angezeigt.<br><br>**c.** Navigieren Sie zurück zu **Vulnerability Response-Anwender und -Gruppen** im Setup-Assistenten, und befolgen Sie die Anweisungen, um die Rolle sn_vul.vulnerability_admin zuzuweisen.<br><br>**Hinweis:**<br>Die Rolle sn_vul.vulnerability_admin ist erforderlich, um mit der Konfiguration fortzufahren. Alternativ können Sie mit der Konfiguration als Benutzer mit der Administratorrolle fortfahren.<br><br>(Optional) Sie können auch die Rollen Configuration Item (CI)-Manager [sn_vul.ci_manager] und Ausnahmegenehmiger [sn_vul.exception_approver] zuweisen, aber diese Personas sind für die verbleibenden Setupaufgaben nicht erforderlich.<br><br>Weitere Informationen zum Zuweisen der Persona-Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
| --- | --- |
| | Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration. |
| ☐ | **a.** Navigieren zu **Alle** > **Administration** > **Integrationen** und stellen Sie sicher, dass die **CWE Comprehensive 2000-Integration** aktiviert ist, und führen Sie die geplante Aufgabe aus, um Daten zu importieren.<br>**b.** Navigieren Sie als Benutzer mit der Administratorrolle zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** und aktivieren (**installieren**) Sie die Anwendung Vulnerability Response Integration with NVD.<br><br>Führen Sie die NVD- und CWE-Integrationen als Teil der Ersteinrichtung von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren.<br><br>Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern und Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus. |
| ☐ | Navigieren Sie als Benutzer mit der Administratorrolle **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** und aktivieren Sie die Anwendung Qualys Integration for Security Operations. Bevor Sie ein Scannerprodukt einer Drittpartei wie Qualys mit einer Bibliothek installieren und ausführen, müssen Sie zuerst die NVD- und CWE-Integrationen installieren und ausführen, um Schwachstellendaten zu erfassen.<br><br>Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten. |
| ☐ | (Optional) Wenn Sie als Benutzer mit der Administratorrolle Demodaten mit der Anwendung Vulnerability Response installiert haben, können Sie die ATF-Test-Suite Vulnerability Response ausführen, um zu überprüfen, ob die Anwendungen erfolgreich installiert wurden.<br><br>**Hinweis:**<br>Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus, um Datenbeschädigungen und -ausfälle zu vermeiden.<br><br>Weitere Informationen finden Sie unter Führen Sie die Test-Suite Automated Test Framework (ATF) für aus Vulnerability Response.<br><br>Weitere Informationen zu automatisierten Tests finden Sie unter Automated Test Framework (ATF). |

**3.** Fahren Sie mit der Konfiguration der Anwendungen fort, beginnend im Abschnitt Vulnerability Response-Einstellungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie diese Einstellungen überprüfen, können Sie besser verstehen, wie Vulnerability Response funktioniert, während Sie mit der Einrichtung Ihrer Umgebung fortfahren. Für die in diesem Beispiel verwendete Scanner-Integration müssen Sie die Einstellungen bearbeiten.

Die Konzepte, die Sie in diesem Konfigurationsbeispiel für das Produkt Qualys verwenden, gelten auch für andere Scanner-Anwendungen.

Zum Konfigurieren der Anwendung sind Ihre Qualys -Anmeldeinformationen erforderlich. Vergewissern Sie sich, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für die Produkte von Qualys erforderlich sind, damit Sie darauf zugreifen können.

Erforderliche Rolle: sn_vul.vulnerability_admin oder alternativ admin.

**Vulnerability Response Prüflistenaufgaben für grundlegende Implementierungen für Schwachstellenadministratoren**

| Aufgabe | Beschreibung |
|---|---|
| ☐ | Überprüfen Sie die Zuweisungsregeln für Schwachstellen.<br><br>Zuweisungsregeln weisen angreifbare Elemente (AEs) automatisch der entsprechenden Zuweisungsgruppe zu. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.<br><br>Weitere Informationen zum Konfigurieren von Vulnerability Response mit dem Setup-Assistenten finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren. |
| ☐ | Überprüfen Sie die Regeln für Korrekturaufgaben.<br><br>Regeln für Korrekturaufgaben gruppieren angreifbare Elemente (AEs) automatisch, wenn sie basierend auf bestimmten Bedingungen importiert werden. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln. |
| ☐ | Überprüfen Sie die Risikorechner.<br><br>Risikorechner bewerten angreifbare Elemente für die Priorisierung. Sie können Rechner so konfigurieren, dass Merkmale des Konfigurationselements (CI), der Exploit-Verfügbarkeit und des Schwachstellenschweregrads berücksichtigt werden, die von Ihrem Anbieter von Schwachstellenbewertungen (Scannern) gemeldet werden. Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln. |
| ☐ | Überprüfen Sie die Korrekturzielregeln.<br><br>Korrekturzielregeln definieren Korrekturzeitleisten für AEs und Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| ☐ | Überprüfen Sie im Abschnitt „Integrationskonfiguration“ die Anwendungseinstellungen Qualys, und definieren und planen Sie Ihre Datenimporte.<br>**a.** Klicken Sie **auf Scanner-Integrationen**.<br>**b.** Klicken Sie auf der Seite „Installierte Anwendungen“ auf **Bearbeiten**.<br>**c.** Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie auf **Weiter**.<br>**d.** Lesen Sie die Beschreibungen für die KnowledgeBase-Konfiguration.<br>**e.** Überprüfen Sie die Seite „Hosterkennungskonfiguration“ auf Importeinstellungen, CI-Suchregeln und Importzeitpläne.<br>**f.** Wenn Sie mit den Einstellungen auf dieser Seite zufrieden sind, klicken Sie auf **Jetzt ausführen**, um Daten zu importieren. Klicken Sie auf den angezeigten Link **Details** anzeigen, um den Ausführungsstatus der Schwachstellenintegration anzuzeigen.<br>**g.** (Optional) Setzen Sie die Bearbeitung der Konfigurationseinstellungen fort.<br>**h. Klicken** Sie auf Fertigstellen, um die Installation und Konfiguration im Setup-Assistenten abzuschließen.<br>Weitere Informationen zum Konfigurieren der Anwendung Qualys finden Sie unter Konfigurieren Sie Qualys Vulnerability Integration mit dem Setup-Assistenten. |

### Nächste Maßnahme

Herzlichen Glückwunsch! Sie haben die Anwendung Vulnerability Response erfolgreich installiert und sie und eine Scanner-Anwendung mit dem Setup-Assistenten konfiguriert. Das Basissystem ist jetzt betriebsbereit.

Befolgen Sie dieselben Schritte und Konzepte, die Sie für die vorherige Prüfliste ausgeführt haben, um andere Anwendungen für Vulnerability Responseherunterzuladen, zu installieren und zu konfigurieren. Weitere Informationen finden Sie in den spezifischen Themen, die für jede Anwendung bereitgestellt werden.

Weitere Informationen zu unterstützten Anwendungen, die Ihnen über ServiceNow Store für Vulnerability Responsezur Verfügung stehen, finden Sie unter Installation von Vulnerability Response und unterstützten Anwendungen.

Weitere Informationen zur Verwendung von Vulnerability Responsefinden Sie unter Die Anwendung Vulnerability Response erkunden.

## Vulnerability Response Status der Korrekturaufgabe

Integrationen von Drittanbietern importieren Erkennungsdaten für angreifbare Elemente, die neue angreifbare Elemente (AEs) erstellen oder vorhandene AEs aktualisieren. Erkennungsstatus aktualisieren VI-Status, sofern sie „Offen“ oder „Geschlossen“ sind. Weitere Informationen finden Sie im Abschnitt „Erkennungen, Korrekturaufgaben und angreifbare Elemente“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Change Management für Vulnerability Responsebesteht eine synchronisierte Beziehung zwischen den Statusfeldern der Korrekturaufgaben und den Statusfeldern der Change-Anforderungen (CHG) im Vulnerability Response-Produkt. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, wird auch der Status der zugehörigen Korrekturaufgaben automatisch verschoben. Nachdem eine Change-Anforderung implementiert wurde, wird die Korrekturaufgabe automatisch gelöst. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

In der folgenden Tabelle werden die Korrekturaufgabenstatus und die Aktionen aufgelistet, die Sie für eine Korrekturaufgabe im jeweiligen Status ausführen können:

**Status der Korrekturaufgabe**

| Status | Beschreibung |
|---|---|
| Offen | Status bei Erstellung. In diesem Status können Sie:<br>**Doppelte VIs anzeigen**<br>Identifizieren Sie doppelte VIs, die von mehreren Scannern im System gemeldet wurden. Sie können die doppelte VI als Gelöst oder Geschlossen markieren. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mit Common Vulnerabilities and Exposures (CVE)erstellt wird. Weitere Informationen finden Sie unter Vulnerability Response Status von Korrekturaufgaben und angreifbaren Elementen.<br>**Untersuchung starten**<br>Weisen Sie diese Korrekturaufgabe einer Person oder Gruppe zu, um mit der Untersuchung zu beginnen.<br>**Als falsch positiv markieren**<br>Markieren Sie ein Element oder eine Gruppe als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, aber tatsächlich keine Schwachstelle vorhanden ist.<br>**Ausnahme anfordern**<br>Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und einen Grund an, und geben Sie optional zusätzliche Informationen an. Die Korrektur des Elements oder der Gruppe wird bis zu dem Datum zurückgestellt, an dem eine Ausnahme angefordert wird.<br>**Lösen**<br>Als Gelöst markieren, um das Element oder die Gruppe in einen gelösten Status zu verschieben.<br>**Change erstellen**<br>Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu.<br>**Split-Korrekturaufgabe**<br>Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Status der Korrekturaufgabe (Fortsetzung)**

| Status | Beschreibung |
| --- | --- |
| | verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe in auf IT Remediation Workspace.<br>**Zurückstellen**<br>Wählen Sie den Status Zurückgestellt, ein Wiedereröffnungsdatum und einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung.<br>**Schließen**<br>Wählen Sie den Status Geschlossen aus, wählen Sie einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Gruppe.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. |
| Wird untersucht | Wird durch die Schaltfläche **„Untersuchung starten“** ausgelöst. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Change erstellen**<br>Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu.<br>**Aufgabe teilen**<br>Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf.<br>**Erstellen Sie eine Change-Anforderung**<br>Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe.<br>**Warten auf Implementierung**<br>Ändert den Status in „Warten auf Implementierung“. Dieser Status gibt an, dass Korrekturaufgaben außerhalb eines Vulnerability Responseverwiesen wurden.<br>**Zurückstellen**<br>Wählen Sie den Status Zurückgestellt, ein Datum für die Wiedereröffnung, einen Grund und optional zusätzliche Informationen aus. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung.<br>**Schließen** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Status der Korrekturaufgabe (Fortsetzung)**

| Status | Beschreibung |
|---|---|
| | Wählen Sie den Status Geschlossen aus, wählen Sie einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Korrekturaufgabe.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. |
| Zurückgestellt | Ausgelöst durch die Schaltfläche **Ausnahme anfordern**. Als Teil des Genehmigungs-Workflows lautet der Status „Zurückgestellt“ In Überprüfung und kann erst nach Genehmigung geschlossen werden.<br>In diesem Status können Sie:<br>**Change erstellen**<br>Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu.<br>**Aufgabe teilen**<br>Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Schwachstellengruppe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue VG verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf.<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.<br>**Schließen**<br>Wählen Sie den Status Geschlossen aus, wählen Sie einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Korrekturaufgabe.<br>Informationen zum Aufschub werden auf der Registerkarte **Schließen/Zurückstellen** angezeigt. Am Zurückstellungsdatum wird die Gruppe erneut zur Korrektur geöffnet. |
| Warten auf Implementierung | Ausgelöst durch die Schaltfläche **„Warten auf Implementierung** “. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Change erstellen**<br>Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Status der Korrekturaufgabe (Fortsetzung)**

| Status | Beschreibung |
| --- | --- |
| | Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu.<br>**Aufgabe teilen**<br>Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Schwachstellengruppe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf.<br>**Erstellen Sie eine Change-Anforderung**<br>Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe.<br>**Zurückstellen**<br>Wählen Sie den Status Zurückgestellt, ein Wiedereröffnungsdatum und einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung.<br>**Schließen**<br>Wählen Sie den Status Geschlossen aus, wählen Sie einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Korrekturaufgabe.<br>**Lösen**<br>Fügen Sie Notizen hinzu. Der Status wird zu Gelöst. Notizen werden auf der Registerkarte **Auflösung** angezeigt.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. |
| Gelöst | Wird über die **Schaltfläche „Lösen** “ ausgelöst. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Change erstellen**<br>Erstellen Sie eine Change-Anforderung, oder ordnen Sie eine Schwachstellengruppe einer vorhandenen Change-Anforderung zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu.<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Schließen**<br>Wählen Sie den Status Geschlossen aus, wählen Sie einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt die Gruppe.<br>**Löschen** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Status der Korrekturaufgabe (Fortsetzung)**

| Status | Beschreibung |
|---|---|
| | Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.<br><br>Notizen werden auf der Registerkarte **Notizen** angezeigt. Auflösungsinformationen werden auf der Registerkarte **Auflösung** angezeigt. |
| Geschlossen | Ausgelöst durch die Schaltfläche **Schließen**. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.<br><br>Abschlussinformationen werden auf der Registerkarte **Schließen/ Zurückstellen** angezeigt. |

- Der Korrekturbesitzer kann nur ein angreifbares Element oder eine Korrekturaufgabe als gelöst markieren. Basierend auf der Bestätigung des Scanners kann dieses gelöste Element oder diese Korrekturaufgabe als Geschlossen oder erneut geöffnet markiert werden.
- Während die Option Schließen nur für Schwachstellenanalysten verfügbar ist, ist Löschen für den Administrator verfügbar, wenn mehrere angreifbare Elemente manuell erstellt wurden und diese geschlossen oder gelöscht werden müssen.
- Wenn Sie feststellen, dass die Elemente ein geringes Risiko aufweisen und auf ein Change-Zeitfenster oder einen Patch warten, können Sie die Korrekturaufgabe für eine bestimmte Zeit in den Status Zurückstellen ändern oder die Gruppe sofort schließen. Sie können eine Ausnahme mit der Option Ausnahme anfordern anfordern.

  **Hinweis:**
  Wenn Korrekturaufgaben zurückgestellt oder geschlossen werden, können Sie Lösungen angeben, um die Gründe dafür weiter zu definieren.

- Wenn ein VI erneut geöffnet wird, entweder manuell oder automatisch, geschieht Folgendes:
  - Der VI-Status ändert sich in „Offen“. Der ursprüngliche Status der Korrekturaufgabe wird nicht aktualisiert.
  - Die VI wird neu ausgewertet und in eine neue oder vorhandene Korrekturaufgabe eingefügt, die auf den aktiven Regeln für Korrekturaufgaben basiert.

  Dadurch bleibt der Verlauf erhalten, während weitere Fehlerkorrekturen möglich sind.
- Wenn Sie eine Korrekturaufgabe automatisch oder manuell erstellen, eine Korrekturaufgabe aufteilen oder eine VI aktualisieren, werden die **Felder**Status, **Grund**und **Bis** für neue und alte Korrekturaufgaben ausgewertet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn alle VIs in einer Korrekturaufgabe zurückgestellt werden und denselben Grund haben, wird der Status der Korrekturaufgabe in „Zurückgestellt“ geändert, und der Grund für die VIs wird einer Korrekturaufgabe zugewiesen. Wenn sich die AEs im Grund unterscheiden, wird der Grund der Korrekturaufgabe in **Keine**geändert.
- Das nächste **Bis** -Datum aller AEs wird im Feld **Bis** der Korrekturaufgabe aktualisiert.
- Wenn Sie eine VI erneut öffnen, ändert sich der Status der Korrekturaufgabe in „ **Offen**“.

Diese Auswertung erfolgt durch die geplante Aufgabe *`Rollup vulnerability item values to vulnerability and group`*, die alle 15 Minuten ausgeführt wird.

### Erkennungen, Korrekturaufgaben und Status angreifbarer Elemente

Drittanbieterintegrationen rufen die Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, die von den Scannern gemeldet werden.

Erkennungsdaten werden mit angreifbaren Elementen (VIs, VITs) kombiniert, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn keine VI gefunden wird, wird eine neue erstellt. Erkennungen werden nur durch die Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden wurden.

Wenn alle Erkennungen für ein angreifbares Element geschlossen sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz lautet der Status Geschlossen/ Korrigiert. Wenn alle AEs für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen. Ansonsten bleibt der Statusfluss derselbe.

Geschlossene AEs mit dem Substatus „Korrigiert“ oder „Veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die AEs mit der neuen Schwachstelle abgeglichen werden können.

Wenn ab Version 20.0 von Vulnerability Responsedie Erkennung „Veraltet“ ist und sich der zugeordnete AE im Status „Geschlossen“ befindet, wechselt der Status des AE nicht in „Geschlossen – Veraltet“. Dadurch wird verhindert, dass der VI erneut geöffnet wird, wenn eine neue Erkennung erkannt wird, sodass Sie nicht den gesamten falsch positiven Anforderungs- und Genehmigungsprozess durchlaufen müssen. Um dieses Verhalten umzukehren, deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren** im Formular „Konfiguration für automatisches Schließen“. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Gemäß Skripteinbindung *`DetectionBase`*, Methode *`_shouldReOpenVI()`*wird die VI, die zuvor mit dem Substatus „Fest“, „Veraltet“ oder „CI außer Betrieb genommen“ geschlossen wurde, erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Angenommen, das Abschlussdatum einer AEs liegt nach dem Datum des letzten Funds einer Erkennung. Sie würden erwarten, dass diese VI-Datensätze geschlossen bleiben. Wenn Sie jedoch sehen, dass eine zuvor geschlossene VI erneut geöffnet wurde, bedeutet dies, dass die VI durch eine frühere Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die der geschlossenen VIT entspricht, die dieselbe Schwachstelle im Konfigurationselement der VI aufweist, wird die VI erneut geöffnet.

### Status von Korrekturaufgaben und angreifbaren Elementen

Die Status von Korrekturaufgaben und angreifbaren Elementen können sich gegenseitig beeinflussen. Meistens wird durch den Status einer Korrekturaufgabe der Status des



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbaren Elements aktualisiert, wobei der Aufgabenstatus mit der höchsten Priorität zum Aktualisieren der angreifbaren Elemente in der Gruppe verwendet wird.

Die Statusrangfolge lautet wie folgt.

**Zurückgestellt** > **Gelöst** > **Warten auf Implementierung** > **Wird untersucht** > **Offen**

- Wenn sich eine Gruppe angreifbarer Elemente in einer Korrekturaufgabe befindet und nicht auf individueller Ebene geändert wird, haben sie denselben Status wie ihre Korrekturaufgabe.
- Wenn die Korrekturaufgabe vom Status „Offen“ in den Status „Warten auf Implementierung“ wechselt, werden alle AEs in der Korrekturaufgabe in den Status „Warten auf Implementierung“ versetzt.
- Wenn die Korrekturaufgabe zurückgestellt wird, wird auch der VI zurückgestellt.
  Ab Version 16.5 können Sie nachverfolgen, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Containerelement oder eine Korrekturaufgabe zurückgestellt wurde. Die regelmäßige Aufgabe `set deferral counts` wird täglich ausgeführt, um Anzahlen für die Datensätze zu veröffentlichen, die in der Spalte Zurückstellungsanzahl in den Modulen für mehrere Zurückstellungen für VR, AVR und CVR mehrmals zurückgestellt wurden. Alle Anzahlen für AEs, die einer Korrekturaufgabe zugeordnet sind, werden erfasst und veröffentlicht, wenn eine Korrekturaufgabe mehr als einmal zurückgestellt wird.

**Angreifbare Elemente werden nur durch Korrekturaufgaben aktualisiert**

Elemente stimmen mit den folgenden Ausnahmen mit dem Status der Korrekturaufgabe überein, wenn sie nicht einzeln aktualisiert wurden:

- Wenn sich der Status der Korrekturaufgabe in Geschlossen und ihre Auflösung in Abgebrochen oder Mit Ausnahme korrigiert ändert, ist das Element nicht betroffen und nimmt den Status einer anderen Korrekturaufgabe an, die es enthält. Wenn sich das angreifbare Element in keiner anderen Korrekturaufgabe befindet, wird es in den Status „Offen“ zurückgesetzt.
- Wenn der Status des angreifbaren Elements Geschlossen/Korrigiert ist (aktualisiert durch einen Scan oder Import), bleibt das angreifbare Element im Status Geschlossen/Korrigiert, wenn die Korrekturaufgabe ihren Status ändert. Diese Bedingung ist unabhängig vom Status der Korrekturaufgabe erfüllt.

**Angreifbare Elemente in Status werden einzeln festgelegt**

Angreifbare Elemente in einem für das Element aktualisierten Status, z. B. Elemente, die einzeln geschlossen oder zurückgestellt wurden, stimmen nicht automatisch mit dem Status der Korrekturaufgabe überein. Stattdessen wird sein Status mit allen zugeordneten Gruppen verglichen, um den Status mit der höchsten anzuwendenden Rangfolge zu ermitteln.

**Hinweis:**
Der Status Geschlossen/Repariert ist ein Sonderfall. Wenn bei den angreifbaren Elementen, die auf den Status Geschlossen/Korrigiert gesetzt sind, alle angreifbaren Elemente innerhalb einer Korrekturaufgabe auf Geschlossen/Korrigiert festgelegt sind – z. B. wenn ein Scanner feststellt, dass alle Schwachstellen behoben wurden, wird die Korrekturaufgabe automatisch als markiert Geschlossen/Korrigiert.

**Korrekturaufgaben enthalten leere Zuweisungsfelder**

Wenn sich der Status der AEs in einer Korrekturaufgabe von „Gelöst“ in „Offen“ ändert, wird auch der Status der Korrekturaufgabe von „Gelöst“ in „Wird untersucht“ aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn jedoch beide Felder **Zugewiesen an** und **Zuweisungsgruppe** in der Korrekturaufgabe leer sind, bleibt die Korrekturaufgabe im Status Gelöst und wird nicht in den Status Wird untersucht verschoben.

**Zuweisungsgruppen für angreifbare Elemente werden nicht immer aktualisiert, wenn ihre Korrekturaufgabe aktualisiert wird**

Wenn die Zuweisungsgruppe für eine VI im Status „Offen“ manuell aktualisiert wird, wird sie nicht erneut aktualisiert, wenn die Zuweisungsgruppe für ihre Korrekturaufgabe aktualisiert wird. Diese Informationen werden nicht überschrieben, da die Zuweisungsgruppe für den VI absichtlich aktualisiert wurde und möglicherweise Teil einer anderen Korrekturaufgabe ist.

### Status der Korrekturaufgabe für angreifbare Elemente (AEs) in mehreren Gruppen

Wenn sich eine VI in mehreren Korrekturaufgaben befindet (Gruppe in den folgenden Tabellen) und ihr eigener Status nicht festgelegt wurde, bestimmt der Gruppenstatus mit höherer Priorität den Status dieser VI, wie in der folgenden Tabelle gezeigt.

#### Beispiele für Status von angreifbaren Elementen

| Status der Korrekturaufgabe | Status des angreifbaren Elements |
|---|---|
| Gruppe A: **Offen** > **Wird untersucht**<br><br>Gruppe B: **Offen** | **Wird untersucht**<br><br>Wenn Gruppe A den Status „Wird untersucht“ und Gruppe B den Status „Offen“ hat, ändert sich der VI in „Wird untersucht“. Nach der Suche hat Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität. |
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Offen** > **Wird untersucht** | **Wird untersucht**<br><br>Wenn Gruppe B „Wird untersucht“ und Gruppe A „Wird untersucht“ ist, bleibt der VI „Wird untersucht“. Nach der Suche haben sie zwischen Gruppe A und Gruppe B den Status mit derselben Rangfolge. |
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Wird untersucht** > **Warten auf Implementierung** | **Warten auf Implementierung**<br><br>Wenn Gruppe B „Warten auf Implementierung“ und Gruppe A „Untersuchung“ lautet, ändert sich der VI in „Warten auf Implementierung“. Nach der Suche hat Gruppe B zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität. |
| Gruppe A: **Wird untersucht** > **Zurückgestellt**<br><br>Gruppe B: **Warten auf Implementierung** | **Zurückgestellt**<br><br>Wenn Gruppe A „Zurückgestellt“ und Gruppe B „Warten auf Implementierung“ ist, ändert sich der VI in „Zurückgestellt“. Nach der Suche hat Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Angreifbares Element in Sonderfällen mit mehreren Gruppen

| Status der Korrekturaufgabe | Status des angreifbaren Elements |
|---|---|
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Warten auf Implementierung** > **Geschlossen (repariert oder storniert)** | **Wird untersucht**<br><br>Wenn Gruppe B den Status „Geschlossen/behoben“ oder „Geschlossen/abgebrochen“ hat und Gruppe A den Status „Wird untersucht“ hat, ändert sich der VI von „Warten auf Implementierung“ (bisher die höchste Rangfolge) zu „Wird untersucht“ (derzeit die höchste Rangfolge). |
| Gruppe A: beliebiger Status<br><br>Gruppe B: beliebiger Status | Wenn der Quellstatus des angreifbaren Elements Repariert ist (aktualisiert durch einen Scan oder Import), ändert sich der Status des angreifbaren Elements in Geschlossen/Repariert, wenn die Gruppe ihren Status ändert. Diese Bedingung ist unabhängig vom Status der anderen zugeordneten Gruppen erfüllt. Die Suche nach angreifbaren Elementen für den Gruppenstatus erfolgt nicht. |

Wenn ein VI-Status einzeln festgelegt wird, wird sein Status wie bei jeder anderen Korrekturaufgabe bei der Bewertung der Rangfolge berücksichtigt. Wenn eine VI zu mehr als einer Korrekturaufgabe gehört, werden in der folgenden Tabelle die vorgenommenen Aktualisierungen aufgelistet.

### Status des angreifbaren Elements individuell festgelegt Sonderfälle

| Status des angreifbaren Elements innerhalb einer Gruppe | Endstatus des angreifbaren Elements |
|---|---|
| Status der Gruppe A: **Wird untersucht**<br><br>Status der Gruppe B: **Wird untersucht** > **Warten auf Implementierung**<br><br>Ursprünglicher VI-Status: **Wird untersucht** > **(am VI festgelegt)** | **Warten auf Implementierung**<br><br>Wenn Gruppe B zu „Warten auf Implementierung“ verschoben wurde und Gruppe A weiterhin „Untersuchung“ bleibt, ändert sich der VI in „Warten auf Implementierung“ (höchste Rangfolge). |
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Wird untersucht** > **Warten auf Implementierung**<br><br>Ursprünglicher VI-Status: **Zurückgestellt** > **(am VI festgelegt)** | **Zurückgestellt**<br><br>Wenn Gruppe B in den Status „Warten auf Implementierung“ verschoben wurde und Gruppe A weiterhin „Untersuchung“ bleibt, verbleibt der VI im Status „Zurückgestellt“ (höchste Priorität). |

Die folgende Tabelle zeigt, dass der Status zurückgestellt wird, wenn zwei Korrekturaufgaben mit gemeinsamen angreifbaren Elementen zurückgestellt werden, bis das letzte Datum erreicht ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Sonderfälle im Status „Zurückgestellter Status“ für angreifbare Elemente**

| Status des angreifbaren Elements innerhalb einer Gruppe | Endstatus des angreifbaren Elements |
|---|---|
| Status der Gruppe A: **Wird überprüft (bis 10. April)**<br><br>Status der Gruppe B: **Wird untersucht** > **Wird überprüft (bis 30. April)**<br><br>Ursprünglicher VI-Status: **Wird überprüft (bis 10. April)** > **(am VI festgelegt)** | **Zurückgestellt (bis 30. April)**<br><br>Wenn Gruppe B in den Status „Zurückgestellt“ verschoben wurde (bis 30. April) und Gruppe A in „Zurückgestellt“ bleibt (bis 10. April), ändert sich der VI von „Zurückgestellt“ (bis 5. April) in den Status „Zurückgestellt“ (bis 30. April). |
| Gruppe A: **Wird überprüft (bis 15. Juli)**<br><br>Gruppe B: **Wird untersucht** > **Wird überprüft (bis 10. Juli).**<br><br>Ursprünglicher VI-Status: **Zurückgestellt** > **(bis 15. Juli)** | **Zurückgestellt (bis 15. Juli)**<br><br>Wenn Gruppe B in den Status „Zurückgestellt“ verschoben wurde (bis 10. Juli) und Gruppe A in „Zurückgestellt“ bleibt (15. Juli), bleibt der VI in „Zurückgestellt“ (bis 15. Juli). |

## Zusätzliche Einstellungen für die Domänentrennung

Für eine genaue Ausführung und genaue Ergebnisse sind die folgenden Vorsichtsmaßnahmen und Einstellungen für die Domänentrennung in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Responseund Configuration Complianceerforderlich.

Ändern Sie nicht die Geschäftslogiken und Prozesse in der globalen Domäne, um Probleme zu vermeiden, sodass bei jedem Upgrade die neuesten Änderungen aktualisiert werden. Duplizieren Sie alle Geschäftslogiken und Prozesse in jeder Domäne separat, und stellen Sie sicher, dass sie in der globalen Domäne inaktiv sind. Andernfalls haben die Geschäftslogiken und Prozesse in der globalen Domäne Vorrang vor der untergeordneten Domäne. Angenommen, Sie haben eine Risikoregel in einer untergeordneten Domäne erstellt, und die globale Domäne verfügt ebenfalls über eine ähnliche Risikoregel. Dann hat die Regel der globalen Domäne Vorrang gegenüber der Regel der untergeordneten Domäne.

## Erneute Auswertung von Rechnern und Regeln

Wenn Sie vor v20.0 Rechner oder Regeln erneut anwenden, wird die Kennzeichnung für die erneute Ausführung auf „wahr“ gesetzt, und eine Geschäftsregel wird ausgelöst, um eine geplante Aufgabe auszuführen, die die Rechner und Regeln erneut anwendet. Ab v20.0 sind Sie nicht mehr von der Kennzeichnung für die erneute Ausführung abhängig. Wenn Sie auf die **Schaltfläche Rechner erneut anwenden** klicken, wird ein Hintergrundauftrag ausgelöst, der die Rechner und Regeln erneut anwendet. Auf diese Weise können Sie Rechner und Regeln für alle Domänen erstellen.

## Einstellungen für Rollup-Rechner

In einer Domäne darf nur ein Rollup-Rechner für eine Tabelle aktiv sein. Betrachten Sie beispielsweise die Korrekturaufgabentabelle `sn_vul_vulnerability` mit dem Rollup-Rechner Korrekturaufgaben- **Rollup** in der globalen Domäne. Wenn Sie diesen Rollup-Rechner duplizieren, indem Sie die Gewichtungen für dieselbe Tabelle in derselben Domäne ändern, kommt es zu Diskrepanzen bei den Rollup-Berechnungen. Stellen Sie daher sicher, dass Sie nur einen Rollup-Rechner aktivieren, wenn zwei oder mehr Rollup-Rechner für eine Tabelle in derselben Domäne vorhanden sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Felder des Formulars „Erkannte Elemente“.

Assets werden automatisch mit Konfigurationselementen (CIs) in Configuration Management Database (CMDB) abgeglichen, wenn sie mit den CI-Suchregeln importiert werden. Datensätze für nicht abgeglichene CIs werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt und in erkannte Elemente aufgenommen. Für Cloud-Assets, die in CMDB CI nicht vorhanden sind, wird der Datensatz jedoch in der Cloud-Ressourcenklasse erstellt.

## Felder „Erkannte Elemente“

Die Informationen in diesen Datensätzen werden aus den Datensätzen der Drittpartei erfasst und während des Imports klassifiziert.

| Feld | Beschreibung |
|---|---|
| Nummer | Bezeichner, der dem Datensatz zugewiesen ist. |
| Konfigurationselement | Konfigurationselement, das aus der Drittanbieterquellenintegration importiert wird.<br>Ab v12.0 ist Configuration Item das neueste CI aus der Liste der CIs, nachdem die außer Betrieb genommenen gefiltert wurden. |
| Klasse | Klasse, die dem CI während des Imports von Vulnerability Responsezugewiesen wurde. |
| Quelle | Quelle, die aus der Drittanbieterquellen-Integration importiert wird. |
| CI-Übereinstimmungsregel | Die CI-Übereinstimmungsregel, die zum Erstellen des Elements verwendet wurde. |
| V18.0: Übereinstimmungstyp für den DI | Zum Erstellen des erkannten Elements verwendeter Übereinstimmungstyp. Die Optionen sind:<br>• Erstellt von VR<br>• Erstellt von IRE<br>• Mit CI-Suche abgeglichen<br>• Abgeglichen mit IRE<br>Diese Informationen sind nur für Daten verfügbar, die für Vulnerability Response v18.0 und höher ausgefüllt wurden. Bei vorhandenen Daten enthält diese Spalte keinen Wert.<br>**Hinweis:**<br>Wenn Sie die CI-Suchregeln erneut anwenden, werden möglicherweise einige CIs in DIs aktualisiert, was dazu führt, dass diese Spalte ausgefüllt wird. |
| Andere übereinstimmende CIs | Liste der anderen Konfigurationselemente, die der CI-Suchregel entsprechen. |
| Status | Status des CI, der während des Imports bestimmt wird. Die Auswahlmöglichkeiten lauten wie folgt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | • **Abgestimmt**: In der CMDB wurde ein übereinstimmendes Konfigurationselement gefunden.<br>• Nicht**abgeglichen**: In der CMDB wurde keine Übereinstimmung gefunden. Ein Platzhalterdatensatz wird erstellt. |
| Erstellt | Datum, an dem der Datensatz „Erkanntes Element“ erstellt wurde. |
| Aktualisiert | Datum, an dem der Datensatz „Erkanntes Element“ aktualisiert wurde. |
| Aktualisiert von | Benutzer, der die Daten aktualisiert hat. |
| Host-Tag | Host-Tags, die diesem erkannten Element während des Imports zugewiesen wurden. Sie können bis zu 31 Host-Tags pro erkanntem Element haben. |
| Vollqualifizierter Domänenname | Daten, die diesem CI zugeordnet sind und in der CMDB gefunden wurden. |
| MAC-Adresse | Daten, die diesem CI zugeordnet sind und in der CMDB gefunden wurden. |
| Betriebssystem | Betriebssystem, das diesem CI zugeordnet ist |
| NetBIOS | NetBIOS, das aus der Quellintegration einer Drittpartei importiert wurde. |
| IP-Adresse | Daten, die diesem CI zugeordnet sind und in der CMDB gefunden wurden. |
| Quelldaten | Aktuelle Daten, die diesem CI aus der Quelle zugeordnet sind |
| V16: Anfängliche Quelldaten | Anfängliche Daten, die diesem CI aus der Quelle zugeordnet sind. |
| V16: CI neu auswerten | Empfängt Daten vom Scanner. Wenn aktualisierte Daten vorhanden sind, wird der Wert auf „true“ festgelegt.<br>**Hinweis:**<br>Die Quelldatenwerte werden gemäß den neuesten Quelldaten neu berechnet. Wenn aktualisierte Daten vom Scanner abgerufen werden, werden die Quelldaten aktualisiert. Der vorhandene Quelldatenwert wird in das ursprüngliche Quelldatenfeld verschoben. Um die erkannten Elemente erneut auszuwerten, aktivieren Sie die CI-Suchregeln erneut anwenden für die regelmäßige Aufgabe „Erkannte Elemente geändert“. |
| Agent ist vorhanden | Gibt „ true“ an, wenn der Agent auf dem Asset installiert ist. Wenn die Werte hostUID und UUID in der Spalte Quelldaten leer sind, wird dieser Wert als trueausgefüllt.<br>**Hinweis:**<br>Dieses Feld wird ab Version 19.0 von Vulnerability Responseangezeigt. |

Ab Version 18.0 von Vulnerability Responsekönnen die Scanner Qualys, Tenable for Vulnerability Response und Rapid7 die folgenden zusätzlichen Metadaten für Cloud-Assets empfangen.

| Feld | Beschreibung |
|---|---|
| Cloud-Service-Provider | Name des Cloud-Service-Providers, der Cloud-Computing-Services anbietet. Zum Beispiel Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP). |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Cloud-Region | Standort, an dem die Ressource gehostet wurde |
| Cloud-Account | Konto, das von Cloud-Service-Providern wie AWS, GCPusw. bereitgestellt wird, um auf Cloud-Computing-Services zuzugreifen. |
| Cloud-Ressourcentyp | Arten von Assets, die in der Cloud vorhanden sind, z. B. Amazon EC2-Computer (Elastic Compute Cloud), AWS S3-Buckets usw. |
| Ressourcen-ID | Eindeutiger Bezeichner, der einer Ressource in einer Cloud-Computing-Umgebung zugewiesen ist. Diese ID wird zum Identifizieren und Verwalten der Ressource verwendet. |
| Ressourcenname | Benutzerdefinierter Name zum Identifizieren und Verwalten einer Ressource in einer Cloud-Computing-Umgebung. |
| Bild | Das Image eines virtuellen Computers oder Server-Image ist ein vorkonfigurierter virtueller Computer, der ein Betriebssystem, Anwendungen und andere Software enthält. Beispiel: Amazon Machine Image. |

Eine neue CI-Suchregel, „Cloud-Ressourcen-ID“, wurde eingeführt, um die Cloud-CIs basierend auf den Cloud-Metadaten abzugleichen.

## Vulnerability Response Felder des Formulars „Schwachstelle“.

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) oder Drittanbieterintegrationen heruntergeladen und unter **Bibliotheken** in Vulnerability Responsegespeichert werden.

## NVD-Eintragsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt. Angreifbare Elemente (AEs), angreifbare Software und Schwachstellenreferenzen werden automatisch zugeordnet, und Einträge können manuell hinzugefügt werden.

| Feld | Beschreibung |
|---|---|
| ID | Bezeichner für diesen Schwachstelleneintrag. |
| Risikobewertung | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Quantifizierte **Risikopunktzahl**, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikobewertungen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.<br>**Hinweis:** Diese **Basisrisikobewertung** ist nicht mit der Risikobewertung des Lösungsdatensatzes identisch . |
| Risikopunktzahl | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Berechneter Betrag des Risikos, das das angreifbare Element für Ihre Umgebung darstellt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:**<br>Diese Basis- **Risikopunktzahl** ist nicht mit der Risikopunktzahl des Lösungsdatensatzes identisch .<br><br>Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow Drittanbieterintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung. |
| Exploit vorhanden | Ja, wenn mindestens ein Exploit mit dieser Schwachstelle verknüpft ist. |
| Exploit-Kompetenzniveau | Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist. |
| Exploit-Angriffsvektor | Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle.<br><br>Verfügbar, wenn SAM-NVD aktiviert ist. |
| Aktive AEs | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Anzahl der mit dieser Schwachstelle verknüpften angreifbaren Elemente, die sich nicht im Status „Geschlossen“ befinden. Wenn für diese Schwachstelle keine aktiven AEs vorhanden sind, werden **Risikobewertung** und **Risikopunktzahl** nicht angezeigt. |
| CWE-Eintrag | Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt. |
| Veröffentlichungsdatum | Datum, an dem die Schwachstelle veröffentlicht wurde. |
| Zuletzt geändert | Datum, an dem die Schwachstelle zuletzt geändert wurde. |
| Zusammenfassung | Beschreibung der Schwachstelle. |
| Threat Intelligence (ab Vulnerability Response Version 20.0) | Von Qualysbereitgestellte Threat Intelligence. Mit diesen Daten können Sie die Motive, Ziele und Angriffsverhalten eines Bedrohungsakteurs verstehen. |
| **Schwachstellendetails** | |
| CVSS v2 | Importierte CVSS v2-Daten |
| CVSS v3 | Importierte CVSS v3-Daten, vor 2015 nicht verfügbar. |
| Bevorzugte Lösung | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br><br>Lösung mit der höchsten Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersetzung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen. |
| **CISA-Exploit** | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| (Diese Registerkarte ist nur verfügbar, wenn die CISA-Anwendung installiert ist.) | |
| CISA-Fälligkeitsdatum | Frist für die Behebung der Schwachstelle. |
| Hinzugefügt am | Datum, an dem die Schwachstelle dem CISA-Katalog hinzugefügt wurde. |
| Produkt | Produkt, in dem die Schwachstelle identifiziert wurde. |
| Lieferant/Projekt | Lieferant, der der identifizierten Schwachstelle zugeordnet ist. |
| Bekannte Ransomware<br><br>Ab Version 21.0 von Vulnerability Response. | Ausgewählt, wenn das Feld, das **bekanntermaßen in Ransomware-Kampagnen verwendet** wird, aus dem KEV-Katalog (CISA Known Exploited Vulnerabilities) erfasst wird. Die Kennzeichnung wird auf der Ebene von Common Vulnerabilities and Exposures (CVE) festgelegt und per Rollup zum Drittparteieintrag (TPE) zusammengefasst. |
| **Nachbesserungsstatus**<br><br>(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) | |
| **Zurückgestellte sind ausgeschlossen** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| **Beinhaltet Zurückgestellte** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. |
| **Zugehörige Links** | |
| Vor v13.0: Import von Softwareschwachstellen erzwingen<br><br>**Hinweis:**<br>In v13.0 entfernt | (Veraltet) Berechnet die Produktzuordnung mit ITSM Software Asset Management basierend auf Informationen aus NVD neu. Aktualisiert die Bibliothek für angreifbare Software. |
| Zustand aktualisieren | Zeigt Datum und Uhrzeit der letzten Aktualisierung an.<br><br>Aktualisiert Folgendes: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | • Status der Korrekturaufgabe<br>• Risikopunktzahl und -bewertung<br>• Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“. |
| **Zugehörige Listen** | |
| Angreifbare Elemente | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind. |
| Verwundbarkeitsreferenzen | Informationen über die Schwachstelle aus externen Quellen, angegeben von NVD. |
| Exploits | Exploits, die dieser Schwachstelle zugeordnet sind |
| Lösungen | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Alle Vulnerability Solution Management Integrationslösungen, die dieser Schwachstelle zugeordnet sind. |
| Schwachstellen | **Importierte** Schwachstellendaten, die einer gemeinsamen Schwachstelle und Gefährdung (CVE) zugeordnet sind |
| Software mit Schwachstellen | (Ausgeblendet, wenn Software mit dem CVE verknüpft ist)<br>Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind |
| Schwachstellen-Malware-Kits | Malware, die aus verschiedenen Scanner-Quellen für eine Schwachstelle importiert wurde |

## CWE-Schwachstelleneintragsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

| Feld | Beschreibung |
|---|---|
| CWE-ID | Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird sowohl für Kategorien als auch für Schwachstellen verwendet und ist zwischen den beiden Datensätzen eindeutig. |
| Name | Beschreibender Name, der dieser CWE-ID zugewiesen ist. |
| Wahrscheinlichkeit der Ausnutzung | Wie wahrscheinlich es ist, dass die Schwachstelle auf einer qualitativen Skala ausgenutzt wird. Einer der folgenden:<br>• Niedrig<br>• Mittel<br>• Hoch |
| Position in OWASP Top 10 | Numerische Position dieser Schwachstelle in der OWASP Top 10-Liste. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| SANS an Position 25 | Numerische Position dieser Schwachstelle in der SAN-Top-25-Liste. |
| Klasse | Typ der Schwachstelle |
| Status | Einer der folgenden:<br>• Unvollständig<br>• Entwurf<br>• Stabil<br>• Überholt<br>• Veraltet<br>• Unstabil |
| Zusammenfassung | Einer der folgenden:<br>• Variante<br>• Klasse<br>• Basis<br>• Verbindung |
| Aktualisiert | Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz. |
| Funktionsbereiche | Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung**. Wird nur für 24/862 Schwachstellen ausgefüllt. |
| Betroffene Ressourcen | Liste der betroffenen Ressourcen. Beispiel: **Datei** oder **Verzeichnis**. Wird nur für 51/863 Schwachstellen ausgefüllt. |
| URL | Knowledge Base-Artikel, der dieser Schwachstelle zugeordnet ist. |
| Beschreibung | Beschreibung der Schwachstelle. |
| Integrationsausführung | Die Integrationsausführung, in der diese CWE importiert wurde. |
| Abschnitte | |
| Zusätzliche Details | Beschreibungen des Softwarekonzepts, die die Schwachstelle weiter erläutern. Beinhaltet:<br>• Erweiterte Beschreibung<br>• Hintergrunddetails<br>• Notizen |
| Erkennungsmethoden | Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können. |
| Einführungsmodi | Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **„Implementierung“**, „ **Architektur und Design“**usw. |
| Demo-Beispiele | Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen. |
| Potenzielle Minderungen | Details darüber, wie die Schwachstelle verhindert werden kann, einschließlich der Phase des Anwendungslebenszyklus, in der sie auftritt, und Effektivität der Verringerung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| **Zugehörige Listen** | |
| Beziehungen | CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnet/untergeordnet, folgt/vorangehend, erforderlich von/erfordert (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, MemberOf enthalten. |
| Beispiele für Beobachtung | Einige CVEs, die für diese Schwachstelle repräsentativ sind. |
| Häufige Konsequenzen | Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Beispiel:<br>Bereich: Vertraulichkeit<br>Auswirkung: Anwendungsdaten lesen |
| Mitgliedschaften | CWE-Mitgliedschaften mit dieser Schwachstelle. |
| Anwendbare Plattformen | Plattformen, die dieser Schwachstelle zugeordnet sind |
| Anwendungsschwachstelleneinträge | Anwendungsschwachstelleneinträge, die einem zugeordnet sind. |
| Externe Referenzen | Informationen zur Schwachstelle aus externen Quellen. |

## Eingabefelder für Drittpartei-Schwachstellen

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

| Feld | Beschreibung |
|---|---|
| ID | Bezeichner für diesen Schwachstelleneintrag. |
| Version 16.0: CVEs | Mehrere gemeinsame Schwachstellen und Gefährdungen (CVEs), die mit dieser Drittpartei-Schwachstelle verbunden sind. |
| Quelle | Ursprung der Schwachstelle – ob ein Scanner oder physischer Test. |
| Risikobewertung | Quantifizierte **Risikopunktzahl**, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikobewertungen finden Sie unter, Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.<br>**Hinweis:**<br>Diese **Basisrisikobewertung** ist nicht mit der **Risikobewertung**des Lösungsdatensatzes identisch |
| Risikopunktzahl | Berechneter Betrag des Risikos, das das angreifbare Element für Ihre Umgebung darstellt, basierend auf der Risikopunktzahl.<br>**Hinweis:**<br>Diese Basis- **Risikopunktzahl** ist nicht mit der Risikopunktzahl des Lösungsdatensatzes identisch . |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow Drittanbieterintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung. |
| Exploit vorhanden | Ja, wenn mindestens ein Exploit mit dieser Schwachstelle verknüpft ist. |
| Exploit-Kompetenzniveau | Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist. |
| Exploit-Angriffsvektor | Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle. |
| Aktive AEs | Anzahl der mit dieser Schwachstelle verknüpften angreifbaren Elemente, die sich nicht im Status „Geschlossen“ befinden. |
| Kategorie | Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung. |
| Fehlerkorrekturtyp | Typen von Korrekturaktionen.<br>• Patch<br>• Konfigurationsänderung<br>• Patch und Konfigurationsänderung<br>• Gegenmaßnahme |
| CWE-Eintrag | Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt. |
| PCI | Wenn das Kontrollkästchen aktiviert ist, wird die Schwachstelle als erhebliches Risiko für die Offenlegung von Zahlungsinformationen gekennzeichnet. |
| PCI-Schweregrad | Risikoniveau für die Offenlegung von Zahlungsinformationen. [Nur Qualys] |
| Veröffentlichungsdatum | Datum, an dem die Schwachstelle veröffentlicht wurde. |
| Zuletzt geändert | Datum, an dem die Schwachstelle zuletzt geändert wurde. |
| Zusammenfassung | Beschreibung der Schwachstelle. |
| **Schwachstellendetails** | |
| CVSS v2 | Importierte CVSS v2-Daten |
| CVSS v3 | Importierte CVSS v3-Daten, vor 2015 nicht verfügbar. |
| Bedrohung | Beschreibung der Bedrohung durch diese Schwachstelle. |
| Bevorzugte Lösung | Lösung mit der höchsten Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersetzung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen. |
| Nachbesserungshinweise | Beschreibung der vom Lieferanten abgerufenen Korrekturlösung. |
| **Nachbesserungsstatus** | |
| **Zurückgestellte sind ausgeschlossen** | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| **Beinhaltet Zurückgestellte** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. |
| **Zugehörige Links** | |
| Zustand aktualisieren | Zeigt Datum und Uhrzeit der letzten Aktualisierung an.<br>Aktualisiert Folgendes:<br>• Status der Korrekturaufgabe<br>• Risikopunktzahl und -bewertung<br>• Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“. |
| **Zugehörige Listen** | |
| Angreifbare Elemente | Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind. |
| Verwundbarkeitsreferenzen | Informationen über die Schwachstelle aus externen Quellen, angegeben von NVD. |
| CVEs | CVE-Datensatz (Common Vulnerability Enumeration), der dieser Schwachstelle zugeordnet ist. |
| Kategorien | Kategorien, die dieser Schwachstelle zugeordnet sind. |
| Exploits | Exploits, die dieser Schwachstelle zugeordnet sind |
| Schwachstellen-Malware-Kits | Malware-Kits, die dieser Schwachstelle zugeordnet sind. |
| Lösungen (Rapid7) | Lösungsinformationen aus den Rapid7-Lösungsintegrationen. Wird angezeigt, wenn verfügbar. |
| Exploit-Frameworks | Exploit-Frameworks, die dieser Schwachstelle zugeordnet sind |
| Lösungen | Vulnerability Solution Management -Lösungen, die dieser Schwachstelle zugeordnet sind. |
| **CISA-Exploit** | |
| CISA vorhanden | CISA-Exploit für die Tabelle „Drittpartei-Schwachstelleneintrag“ vorhanden. |
| CISA-Fälligkeitsdatum | Frist für die Behebung der Schwachstelle. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Felder des Formulars „Korrekturaufgabe“.

Mithilfe von Korrekturaufgaben kann der Analyst den Fortschritt überwachen und den Mediationsprozess effizienter gestalten.

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

### Felder für Korrekturaufgaben

| Feld | Beschreibung |
|---|---|
| Nummer | Die automatisch generierte Nummer des angreifbaren Elements (AE) für diesen Datensatz. |
| Risikobewertung | Rollup der Risikopunktzahlen angreifbarer Elemente, die in Bereiche unterteilt sind: „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“. Weitere Informationen zu Risikobewertungen finden Sie unter, Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.<br>**Hinweis:**<br>Diese **Basisrisikobewertung** ist nicht mit der Risikobewertung des Lösungsdatensatzes identisch . |
| Risikopunktzahl | Rollup der Risikopunktzahlen aller angreifbaren Elemente, die dieser Korrekturaufgabe zugeordnet sind. Ausmaß des Risikos, das die angreifbaren Elemente zusammen für Ihre Umgebung darstellen.<br>**Hinweis:**<br>Diese Basis- **Risikopunktzahl** ist nicht mit der Risikopunktzahl des Lösungsdatensatzes identisch . |
| Korrekturziel | Datum, bis zu dem die angreifbaren Elemente korrigiert werden sollen, seit sie zuerst identifiziert wurden.<br>Weitere Informationen zu Korrekturzielen finden Sie unter Vulnerability Response Korrekturzielregeln. |
| Korrekturstatus | Status der Korrektur für die Aufgabe. Sie wird durch das angreifbare Element mit dem nächsten Fälligkeitsdatum bestimmt.<br>Zu den offenen Gruppenstatus gehören:<br>• In Ausführung<br>• Ziel rückt näher<br>• Ziel fehlt<br>Zu den Status geschlossener Gruppen gehören:<br>• Kein Ziel<br>• Ziel erfüllt<br>• Ziel fehlt<br>Wenn die Aufgabe für berechnete Korrekturzieldaten geschlossen wird, wird der allgemeine Korrekturstatus aller geschlossenen angreifbaren Elemente in der Aufgabe angezeigt. Diese bestimmen, |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

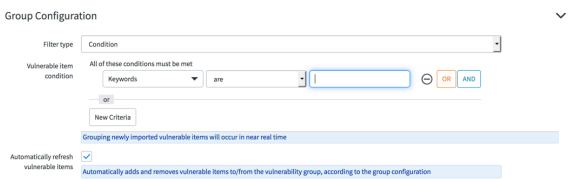
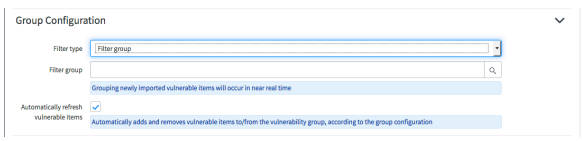
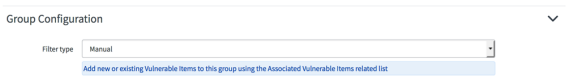
**Felder für Korrekturaufgaben (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | ob die Aufgabe ihr Datum erreicht hat oder nicht. Der Korrekturstatus einer geschlossenen Aufgabe lautet „ **Kein Ziel** “, wenn keines der geschlossenen Elemente ein Korrekturzieldatum hatte. Er lautet **„Ziel verfehlt“**, wenn eines der geschlossenen Elemente sein Zieldatum verfehlt hat. Es ist **Ziel** erfüllt, wenn mindestens ein geschlossener VI sein Ziel erreicht hat und keiner der anderen es verfehlt hat. |
| Status | Fortschrittsstatus der Aufgabe.<br>Zu den Status gehören:<br>• Offen<br>• Wird untersucht<br>• Warten auf Implementierung<br>• Zurückgestellt<br>• Wird überprüft<br>• Gelöst<br>• Geschlossen<br>Weitere Informationen zu den Status finden Sie unter Vulnerability Response Status von Korrekturaufgaben und angreifbaren Elementen. |
| Bis-Datum für Risikominderung | Datum, an dem die auf die Korrekturaufgabe angewendeten Ausgleichskontrollen ablaufen.<br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn der Wert verfügbar ist. |
| Zuweisungsgruppe | Gruppe, die für die Arbeit an dieser Korrekturaufgabe ausgewählt wurde. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet. |
| Erstellt | Datum, an dem diese Korrekturaufgabe erstellt wurde. |
| Aktualisiert | Datum, an dem diese Korrekturaufgabe zuletzt aktualisiert wurde. |
| Schwachstelle | Schwachstelle, die für die Aufgabe gilt. (Sichtbar, wenn die Gruppe basierend auf einer einzelnen Schwachstelle gebildet wird.) |
| Kurzbeschreibung | Kurze Beschreibung dieser Korrekturaufgabe. |
| **Wird überprüft** (sichtbar, wenn sich die RT im Status „Wird überprüft“ befindet) | |
| Angefordert von | Person, die die Zurückstellung angefordert hat. |
| Gewünschter Grund | Grund für Zurückstellung. |
| Gewünschter Zustand | Der vom Genehmiger angeforderte Status. |
| Gewünschter Substatus | Der vom Genehmiger angeforderte Grund. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Felder für Korrekturaufgaben (Fortsetzung)

| Feld | Beschreibung |
|---|---|
| **Zurückstellung**(sichtbar, wenn sich die Aufgabe im Status „Zurückgestellt“ befindet) | |
| Zurückgestellt um | Einzelperson, die die Aufgabe zurückgestellt hat. |
| Ablauf zurückstellen | Datum, an dem die Zurückstellung abläuft. |
| Grund für Zurückstellung | Grund für die Zurückstellung. |
| **Auflösung** (sichtbar, wenn sich die RT im Status „Gelöst“ befindet) | |
| Gelöst von | Einzelperson, die die Korrekturaufgabe gelöst hat. |
| Datum der Lösung | Datum, an dem die Korrekturaufgabe gelöst wurde. |
| Details | Zusätzliche Informationen. |
| **Schließen** (sichtbar, wenn sich die RT im Status „Geschlossen“ befindet) | |
| Geschlossen von | Einzelperson, die die Korrekturaufgabe gelöst hat. |
| Geschlossen | Datum, an dem die Korrekturaufgabe geschlossen wurde |
| Abschlussnotizen | Zusätzliche Informationen. |
| **Gruppenkonfiguration** (in allen Status sichtbar) | |
| Filtertyp | Typ der Filterung, die zum Auswählen von Schwachstellen für die Gruppe verwendet wird:<br>**Bedingung**<br>  <br>**Hinweis:**<br>Wird einmal pro Stunde aktualisiert.<br>**Filtergruppe**<br>  <br>**Hinweis:**<br>Wird einmal pro Stunde aktualisiert.<br>**Manuell**<br>  |
| **Nachbesserungsstatus** | |
| **Zurückgestellte sind ausgeschlossen** | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Felder für Korrekturaufgaben (Fortsetzung)

| Feld | Beschreibung |
|---|---|
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| VIs insgesamt | Gesamtzahl der angreifbaren Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| **Beinhaltet Zurückgestellte** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe. |
| VIs insgesamt | Gesamtzahl der angreifbaren Elemente in dieser Aufgabe. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe. |
| **Notizen** (in allen Status sichtbar) | |
| Beschreibung | Beschreibung der Gruppen- oder Korrekturaktionen. |
| Zusätzliche Anmerkungen | Zusätzliche Informationen. |
| Aktivitäten | Systemhinweise |
| **Zugehörige Links** | |
| Angreifbare Elemente erneut scannen | Löst einen erneuten Scan der angreifbaren Elemente aus, um festzustellen, ob sie behoben sind. |
| Aktualisierungsstatus | Zeigt Datum und Uhrzeit der letzten Aktualisierung an.<br>Fasst Folgendes aus den AEs in der Aufgabe zusammen:<br>• Status der Korrekturaufgabe<br>• Risikopunktzahlen und Risikobewertungen<br>• Korrekturzieldatum und -status (falls zutreffend)<br>• Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“. |
| **Zugehörige Listen** | |
| Angreifbare Elemente | Angreifbare Elemente in dieser Aufgabe. |
| Aufgaben-SLAs | Plattform-SLAs, die dieser Aufgabe zugeordnet sind. |
| Bevorzugte Lösungen | Bevorzugte Lösungen der angreifbaren Elemente in dieser Aufgabe. |
| Change-Anforderungen | Change-Anforderungen, die dieser Aufgabe zugeordnet sind. |
| Angeforderte Genehmigungen | (Sichtbar, wenn sich die Aufgabe im Status Wird überprüft befindet.) Liste der Genehmiger. Sobald die Zurückstellung genehmigt wurde, wird die Korrekturaufgabe in den Status „Zurückgestellt“ verschoben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Felder des Formulars „Fragebogenkonfiguration“.

Sie können einen eindeutigen Fragebogen für eine eindeutige Sammlung von Schwachstellen oder Korrekturaufgaben definieren, indem Sie die Schwachstellen oder Korrekturaufgaben im Abschnitt „VR-Fragebogenkonfiguration“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ filtern.

Das Formular „Fragebogenkonfiguration“ wird angezeigt, wenn Sie im Abschnitt „VR-Fragebogenkonfiguration“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“ auf die Schaltfläche **Neu** klicken.

### Felder des Formulars „Fragebogenkonfiguration“.

| Feld | Beschreibung |
|---|---|
| Name | Name des Fragebogens. |
| Freigaberegel | Genehmigungsregel, für die der Fragebogen gilt.<br>• **Ausnahmeanforderung für Schwachstellengruppen**<br>• **Ausnahmeanforderung für angreifbare Elemente**<br>• **Falsch positiv für Schwachstellengruppen**<br>• **Falsch positiv für angreifbare Elemente**<br>• **Fragebogen für Ausgleichskontrollen für angreifbare Gruppen** für Risikominderungsanforderungen der Korrekturaufgabe.<br>• **Fragebogen für Ausgleichskontrollen für angreifbare Elemente** für Risikominderungsanforderungen angreifbarer Elemente. |
| Beschreibung | Kurzbeschreibung für die Fragebogenkonfiguration. |
| Bestellung | Fragebogen mit der niedrigsten Reihenfolge wird während der Anforderungen angezeigt. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass der Fragebogen verwendet wird. |
| Tabelle | Tabelle, für die die Genehmigungsregel gilt.<br>• Angreifbares Element [sn_vul_vulnerable_item] für die Genehmigungsregeln im Zusammenhang mit angreifbaren Elementen.<br>• Korrekturaufgabe [sn_vul_vulnerability] für die Genehmigungsregeln im Zusammenhang mit Korrekturaufgaben. |
| Bedingung | Bedingung für die Datensätze, für die der Fragebogen angezeigt werden muss. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Felder des Formulars „Fragebogenkonfiguration“. (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | Sie können die Bedingung auf alle Felder eines angreifbaren Elements und einer Korrekturaufgabe mit Ausnahme von **Grund**anwenden. |
| Fragebogen | Fragebogen, der angezeigt werden muss, wenn der Korrekturbesitzer eine Ausnahme, falsch positive Meldungen oder Risikominderung anfordert. |

**Zugehörige Informationen**

Konfigurieren Sie Exception Management für Vulnerability Response

Konfigurieren Sie einen Fragebogen für die Risikominderung

## Vulnerability Response Formularfelder für angreifbare Elemente

Angreifbare Elemente werden beim Import von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

## Felder für angreifbare Elemente

Wenn Sie das SAM-NVD-Schwachstellen-Scanning aktiviert haben, werden die Datensätze mit der Software in Ihrem Configuration Management Database (CMDB) verglichen, und es werden Übereinstimmungen mit angreifbarer Software oder Konfigurationselementen (Configuration Items, CIs) gefunden.

| Feld | Beschreibung |
|---|---|
| Sicherheits-Tag auswählen | Sicherheits-Tag, um dem Datensatz Metadaten hinzuzufügen oder zu identifizieren, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird nur angezeigt, nachdem das angreifbare Element gespeichert wurde. |
| Nummer | Automatisch generierte Nummer des angreifbaren Elements für diesen Datensatz. |
| Quelle | Scanner, der dieses angreifbare Element gefunden hat. |
| Risikobewertung | Quantifizierte **Risikopunktzahl**, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikobewertungen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.<br>**Hinweis:**<br>Diese **Basisrisikobewertung** ist nicht mit der Risikobewertung des Lösungsdatensatzes identisch . |
| Risikopunktzahl | Berechneter Betrag des Risikos, das das angreifbare Element für Ihre Umgebung darstellt.<br>**Hinweis:**<br>Diese Basis- **Risikopunktzahl** ist nicht mit der Risikopunktzahl des Lösungsdatensatzes identisch . |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln. |
| Schwachstelle | ID der Schwachstelle, die diesem angreifbaren Element zugeordnet ist. |
| Konfigurationselement | Betroffenes Asset. |
| Status | Dieses Feld ist standardmäßig auf **Offen**gesetzt, Sie können es jedoch in **Untersuchung** wird überprüft ändern, wenn die Schwachstelle zur sofortigen Korrektur bereit ist. |
| Bis-Datum für Risikominderung | Datum, an dem die auf das angreifbare Element angewendeten Ausgleichskontrollen ablaufen.<br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn der Wert Ursprüngliche Risikopunktzahl verfügbar ist. |
| Zuweisungsgruppe | Gruppe, die für die Arbeit an dieser Korrekturaufgabe ausgewählt wurde. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet. |
| Erstellt | Datum, an dem dieses angreifbare Element in Ihrer Instanz erstellt wurde. |
| Zuletzt geöffnet | Datum, an dem das angreifbare Element zuletzt in Ihrer Instanz geöffnet wurde. Anfänglich ist dies mit dem Erstellungsdatum des angreifbaren Elements identisch. Wenn es jedoch geschlossen und dann erneut geöffnet wurde, enthält Zuletzt geöffnet Datum das Datum und die Uhrzeit der erneuten Öffnung. |
| Aktualisiert | Datum des letzten Scans. |
| **Schwachstelle** | |
| Zusammenfassung | Beschreibung der Schwachstelle. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow Drittanbieterintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie eine Vulnerability Response -Schweregradzuordnung. |
| Schwachstellenpunktzahl (v3) | CVSS v3-Punktzahl. |
| Schwachstellenpunktzahl (v2) | CVSS v2-Punktzahl. |
| Exploit vorhanden | Ja, wenn mindestens ein Exploit mit den mit diesem angreifbaren Element verknüpften Schwachstellen verknüpft ist. |
| Exploit-Angriffsvektor | Am angreifbarster Angriffsvektor der Exploits für die mit diesem angreifbaren Element verknüpften Schwachstellen. |
| Exploit-Kompetenzniveau | Niedrigste Kompetenzstufe, die zum Ausnutzen der mit diesem angreifbaren Element verbundenen Schwachstellen erforderlich ist. |
| Veröffentlichungsdatum | Datum, an dem die Schwachstelle veröffentlicht wurde. |
| Zuletzt geändert | Datum, an dem die Schwachstelle zuletzt geändert wurde. |
| Bedrohung | Relevante Informationen zur Bedrohung. Aus dem Datensatz des angreifbaren Eintrags abgerufen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags. |
| Nachbesserungshinweise | Relevante Lösung für die Bedrohung, abgerufen aus dem Datensatz des angreifbaren Eintrags. |
| **Nachbesserungsschritte**<br>Nur verfügbar mit Vulnerability Solution Management. | |
| Bevorzugte Lösung | Bevorzugte Lösung, die aus dem Schwachstellendatensatz importiert wurde.<br>**Hinweis:** Alle hier vorgenommenen manuellen Änderungen ändern nicht den Schwachstellendatensatz und bleiben bei nachfolgenden Importen unverändert. |
| Zusammenfassung | Zusammenfassung aus dem Lösungsdatensatz importiert. |
| **Erstmalige Erkennung** | |
| DNS-Name | Name des Domänennamenservice. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| NetBIOS-Name | Name des NetBIOS Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| IP-Adresse | IPv4- oder IPv6-Adresse Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| Port | Adresse des Ports |
| Protokoll | Name des Protokolls. |
| SSL | Gibt an, ob SSL-Verschlüsselung verwendet wird oder nicht. |
| **Erkennungen** | |
| Status | Status der Erkennung. |
| Erste ermittelte | Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset erstmals gefunden hat. |
| Zuletzt gefunden | Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset zuletzt gefunden hat. |
| DNS-Name | Name des Domänennamenservice. Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| NetBIOS-Name | Name des NetBIOS Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| IP-Adresse | IPv4- oder IPv6-Adresse Wenn kein CI angegeben ist, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls eines vorhanden ist. |
| Port | Adresse des Ports |
| Protokoll | Name des Protokolls. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| SSL | Gibt an, ob SSL-Verschlüsselung verwendet wird oder nicht. |
| Anzahl Ermittlungen | Anzahl, die angibt, wie oft diese Schwachstelle für dieses Asset von der Drittparteiquelle erkannt wurde. |
| Integrationsausführung | Integrationsausführung, die die Erkennung importiert hat. |
| **Schließen**<br>Verfügbar, sobald das angreifbare Element korrigiert und geschlossen wurde. Elemente in diesem Abschnitt sind schreibgeschützt. | |
| Geschlossen von | Wer das angreifbare Element geschlossen hat. |
| Geschlossen | Datum, an dem das angreifbare Element geschlossen wurde. |
| Abschlussnotizen | Informationen, die im Abschluss enthalten sind. |
| Geschlossen mit Alter | Zeitraum, nach dem der VI geschlossen wurde. Wenn die AE erneut geöffnet wird, wird der Wert des Felds „Alter der Schließung“ auf 0 gesetzt. |
| **Notizen** | |
| Zusätzliche Kommentare/ Arbeitsnotizen | Alle relevanten Informationen. Aktivieren Sie die Checkbox, um Zusätzliche Anmerkungen hinzuzufügen.<br>Ab Vulnerability Response v20.0 können Sie Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Element hinzufügen. |
| Aktivität | Wird nur angezeigt, wenn eine Arbeitsnotiz erstellt wurde. |
| **Zugehörige Links** | |
| Risikopunktzahl berechnen | Wenn entweder der **Schwachstellenschweregrad** oder der **Risikopunktzahl** -Rechner aktiviert ist, wird das Feld **„Risikopunktzahl“** aktualisiert. |

Im Folgenden finden Sie die zugehörigen Listen für angreifbare Elemente.

| Zugehörige Liste | Beschreibung |
|---|---|
| Korrekturaufgaben | Aufgaben, die diesem angreifbaren Element zugeordnet sind. |
| Betreffende Aufgaben | Aufgaben, die diesem angreifbaren Element zugeordnet sind. |
| Zugeordnete IP-Adressen | Verfügbar, wenn die Anwendung Qualys Vulnerability Integration Vulnerability Integration installiert ist.<br>IP-Adressen, die während der Deduplizierung gefunden werden |
| Betroffene Services | Geschäftsservices, die von diesem angreifbaren Element betroffen sind. Wird angezeigt, wenn diese Informationen im CMDB -Datensatz verfügbar sind. Diese Informationen können manuell oder mit der Anwendung ServiceNow® Service-Mapping eingegeben werden. Weitere Informationen finden Sie unter Service Mapping .<br>Wenn ein betroffenes CI, das dem angreifbaren Element zugeordnet ist, hinzugefügt oder aktualisiert wird, werden die Informationen in |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Liste | Beschreibung |
|---|---|
| | dieser zugehörigen Liste beim Speichern des Datensatzes automatisch aktualisiert. |
| Qualys-Tickets | Qualys Informationen zur Ticket-Integration, die diesem angreifbaren Element zugeordnet sind. |

## Felder des Lösungsformulars

Lösungen werden automatisch erstellt, wenn Datensätze aus Lösungsintegrationen von Drittanbietern heruntergeladen und unter **Lösungen** in Vulnerability Responsegespeichert werden.

## Eingabefelder der Lösungsintegration

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

| Feld | Beschreibung |
|---|---|
| Nummer | Bezeichner, der der Lösung zugewiesen ist. |
| Quelle | Ursprung der Lösung. |
| Quellen ID | Quellbezeichner für diese Lösung. |
| Risikobewertung | Unterteilt die Risikopunktzahl des **Lösungsdatensatzes** in Bereiche von „Kritisch“ bis „Keine“. Weitere Informationen zur **Risikobewertung**der Lösung finden Sie unter Vulnerability Solution Management.<br>**Hinweis:**<br>**Die Risikobewertung** der Lösung ist nicht identisch mit der **Risikobewertung**der Datensätze **„AngreifbaresElement** “, „ **Drittpartei-Schwachstelleneintrag**“ und „Korrekturaufgabe“. |
| Risikopunktzahl | Gewichtete Berechnung basierend auf der **Risikopunktzahl** und der Anzahl der angreifbaren Elemente mit dieser Lösung als **bevorzugte Lösung**. Weitere Informationen zur Lösungsrisikopunktzahl finden Sie unter Vulnerability Solution Management.<br>**Hinweis:**<br>Die Risikopunktzahl des **Lösungsdatensatzes** ist nicht mit der **Risikopunktzahl**der Datensätze **„AngreifbaresElement“**, „ **Drittpartei-Schwachstelleneintrag“**und „Korrekturaufgaben“ identisch.<br>Verfügbar, wenn SAM-NVD aktiviert ist, aber wenn einer Schwachstelle keine aktiven angreifbaren Elemente (AE) zugeordnet sind, wird die Risikopunktzahl der Lösung auf **0** festgelegt. |
| Höchste Ersatzlösung | Gibt an, dass sie durch keine Lösung ersetzt wird. |
| Lösungstyp | Um welche Art von Lösung handelt es sich? Die Auswahlmöglichkeiten lauten wie folgt:<br>• Workaround<br>• Mitigation |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | • Lieferantenkorrektur<br>• Patch<br>• Rollup<br>• Berechtigung<br>• Wird nicht korrigiert<br>• Keine verfügbar |
| Neustart erforderlich | Neustart erforderlich. Die Auswahlmöglichkeiten lauten wie folgt:<br>• Ja<br>• Nein<br>• Vielleicht |
| Veröffentlichungsdatum | Datum, an dem die Schwachstelle nach Quelle veröffentlicht wurde. |
| Zuletzt geändert | Datum, an dem die Schwachstelle zuletzt nach Quelle geändert wurde. |
| Zusammenfassung | Zusammenfassung der Fehlerkorrektur der Lösung. |
| Bulletin | Sicherheitsbulletin, das der Lösung zugeordnet ist. |
| Produktkategorien | Produktkategorien, für die die Lösung gilt. |
| Produkte | Produkte, für die die Lösung gilt. |
| **Lösungsdetails** | |
| Beschreibung | Wenn in der Lösungsquelle kein Inhalt verfügbar ist, werden Sie zu einem anderen relevanten Abschnitt oder einer anderen Lösung weitergeleitet, um weitere Informationen zu erhalten. |
| Links | Importierte Internetressourcen, die der Lösung zugeordnet sind. |
| **Schwachstellendetails** | |
| Hinweise zu Schwachstellen | Zusammenfassung der von der Lösung behobenen Schwachstellen. |
| **Nachbesserungsstatus** | |
| **Bevorzugte Lösungsziele**<br><br>Korrekturstatus für angreifbare Elemente und ihre eindeutigen Konfigurationselemente (CIs), für die dies die bevorzugte Lösung ist.<br><br>**Hinweis:**<br>Ein eindeutiges CI wird nur einmal gezählt, unabhängig davon, wie vielen VIs es zugeordnet ist. | |
| Angreifbare Elemente | Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| VIs insgesamt | Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| Behobene VIs in Prozent | Abschluss in Prozent für die Korrektur angreifbarer Elemente (AEs). Gilt für AEs, für die diese Lösung bevorzugt wird. Diese Anzahl enthält nicht die zurückgestellten AEs. |
| Verbleibende CIs | Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus. |
| CIs insgesamt | Anzahl der eindeutigen CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus. |
| Behobene CIs in Prozent | Abschluss in Prozent der korrigierten eindeutigen CIs (d. h. alle VIs für dieses CI und diese Lösung werden korrigiert). Bestimmt durch die Anzahl der korrigierten CIs im Verhältnis zur Gesamtzahl der eindeutigen CIs, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus. |
| **Bevorzugte Lösungsziele (beinhaltet zurückgestellte)**<br><br>Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs, einschließlich zurückgestellt, für die dies die bevorzugte Lösung ist. | |
| Angreifbare Elemente | Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. |
| VIs insgesamt | Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. |
| Behobene VIs in Prozent | Abschluss in Prozent für die Korrektur angreifbarer Elemente (AEs). Gilt für AEs, für die diese Lösung bevorzugt wird. |
| Verbleibende CIs | Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. |
| CIs insgesamt | Anzahl der eindeutigen CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. |
| Behobene CIs in Prozent | Abschluss in Prozent der korrigierten eindeutigen CIs (d. h. alle VIs für dieses CI und diese Lösung werden korrigiert). Bestimmt durch die Anzahl der korrigierten CIs im Verhältnis zur Gesamtzahl der eindeutigen CIs, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus. |
| **Potenzielle Lösungsziele**<br><br>Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs mit einer mit dieser Lösung verbundenen Schwachstelle. | |
| Angreifbare Elemente | Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Verbleibende CIs | Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| **Potenzielle Lösungsziele (enthält zurückgestellte)**<br><br>Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs, einschließlich zurückgestellter, mit einer Schwachstelle, die von dieser Lösung behoben werden kann, einschließlich Anzahl der bevorzugten Lösungen. | |
| Angreifbare Elemente | Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. |
| Verbleibende CIs | Anzahl der eindeutigen CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. |
| **Notizen** | |
| Interne Hinweise | Bearbeitbares Feld, das für den Korrekturspezialisten bereitgestellt wird. |
| **Zugehörige Links** | |
| Zustand aktualisieren | Datum und Uhrzeit der letzten Aktualisierung des Korrekturstatus.<br><br>Aktualisiert Folgendes:<br>• Status der Korrekturaufgabe<br>• Risikopunktzahl und -bewertung<br>• Metriken aus dem Abschnitt „Korrekturstatus“. |
| **Zugehörige Listen** | |
| Angreifbare Elemente | Angreifbare Elemente, die dieser Lösung als bevorzugte Lösung für die Korrektur zugeordnet sind. |
| Schwachstellen von Drittparteien | Mit dieser Lösung verknüpfte Schwachstellen von Drittparteien. |
| CVEs | Häufige CVE-Schwachstellen (Vulnerability and Exposure), die mit dieser Lösung verbunden sind. |
| Korrekturaufgaben | Korrekturaufgaben, die zugehörige angreifbare Elemente enthalten, wobei diese Lösung für die Korrektur bevorzugt wird. |
| Vorhergehende Lösungen | Frühere Lösungen, die eine oder mehrere der Schwachstellen dieser Lösung beheben. |
| Ersatzlösungen | Spätere Lösungen, die alle Schwachstellen dieser Lösung beheben. Diese Liste ist leer, wenn das Kontrollkästchen für die **höchste Ersetzung** aktiviert ist. |

## Genehmigungsworkflow-Konfigurationen für Anforderung zum Aufheben der Zuweisung

Sie können den Genehmigungs-Workflow für die Entfernung von Zuweisungen von angreifbaren Elementen (VIs, VITs), Korrekturaufgaben, angreifbaren



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungselementen (AVITs) und angreifbaren Containerelementen (CVITs) für sich und Ihre Gruppe entwerfen.

VIT, Korrekturaufgabe, AVIT und CVIT haben jeweils eine Standardgenehmigungsregel. Jede Genehmigungsregel verfügt über eine standardmäßige Genehmigungskonfiguration. Jede Genehmigungskonfiguration hat eine Standardgenehmigerebene. Die Genehmigungsregeln für VITs, Korrekturaufgaben, AVIT und CVIT sind standardmäßig aktiviert. Als Administrator können Sie die folgenden Aktionen ausführen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Meine Freigaben** > **Genehmigungsregeln** und Auswahl der entsprechenden Genehmigungsregel.

- Aktivieren oder deaktivieren Sie eine Genehmigungsregel.
- Erstellen und aktualisieren Sie eine Genehmigungskonfiguration.
- Bedingungen für angreifbare Elemente und Korrekturaufgaben definieren, für die die Genehmigungsregeln gelten.
- Mehrere Genehmigerebenen erstellen und aktualisieren.

Die folgende Tabelle zeigt die standardmäßigen Genehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen für VIT, Korrekturaufgabe, AVIT und CVIT, die im Lieferumfang des Basissystems enthalten sind.

**Standardmäßige Genehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen**

| Typ | Genehmigungsregel | Genehmigungskonfigura | Genehmiger-Ebenen |
|---|---|---|---|
| VIT oder VI | Change-Anforderung für Feld zu angreifbarem Element | Change-Anforderung für Feld zu angreifbarem Element | Anforderung zum Aufheben der Zuweisung der Ebene 1 für VI |
| Korrekturaufgabe | Schwachstellegruppenfeld Change-Anforderung | Change-Anforderung für Schwachstellenfeld | Ebene 1 – Anforderung der Zuweisungsaufhebung für SG |
| AVIT | Change-Anforderung für Feld zu angreifbaren Elementen der Anwendung | Change-Anforderung für Anwendungsschwachstellenfeld | Heben Sie die Zuweisung des angreifbaren App-Elements auf |
| CVIT | Genehmigung für Container-Verwaltung | Standardkonfiguration – CVIT-Zuweisung aufheben | CVIT-Zuweisung aufheben – Genehmigungsebene 1 |

Weitere Informationen zum Genehmigen von Anforderungen zum Aufheben der Zuweisung finden Sie unter Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Vulnerability Response.

## Vulnerability Response Beispiele für Korrekturaufgabenregeln

Beispiele für Korrekturaufgabenregeln mit Schwachstelle und Risiko oder Auswirkung oder Konfigurationselement (CI).

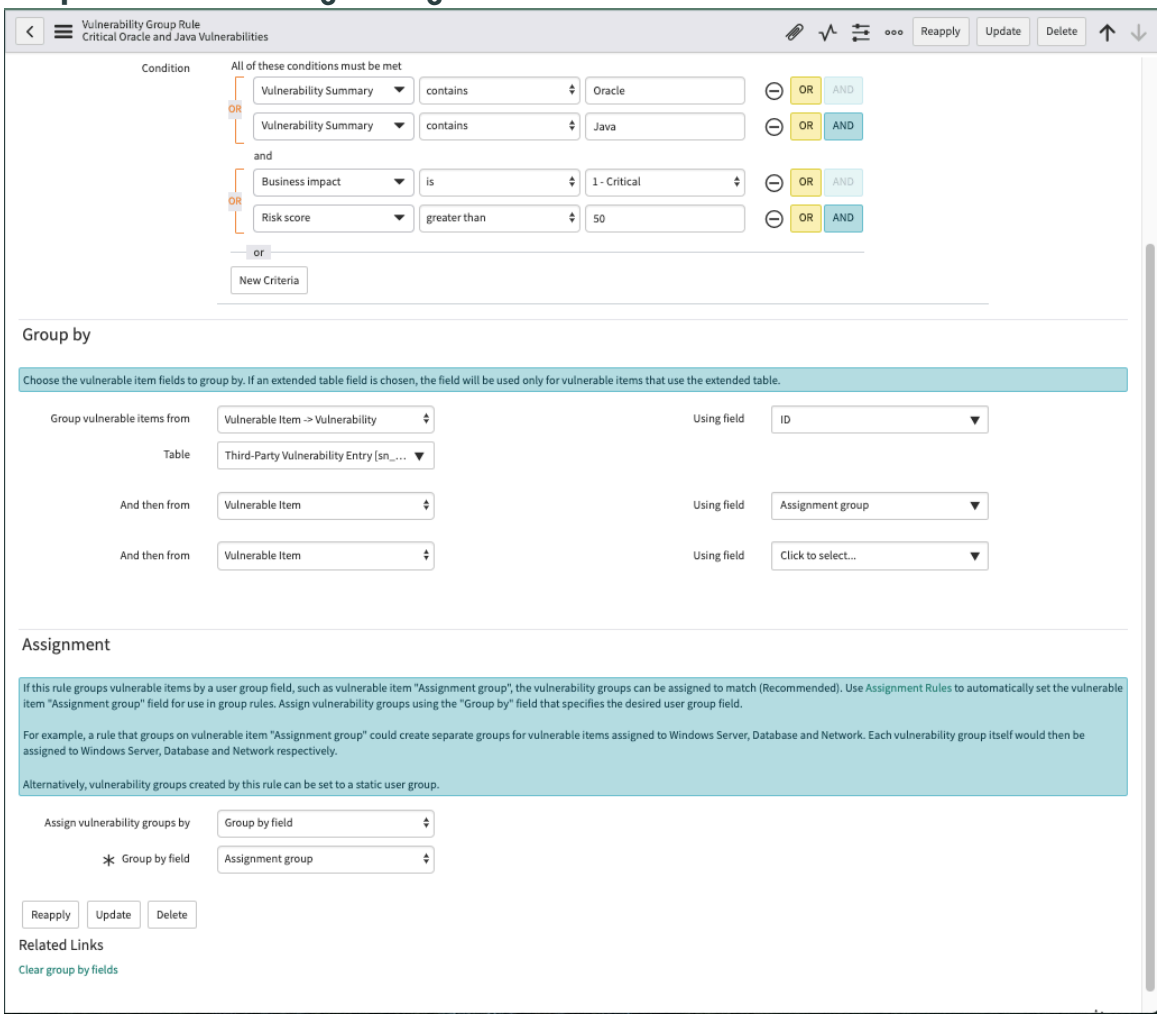


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Regel für Korrekturaufgaben zum Gruppieren von angreifbaren Java- und Oracle-Elementen mit hohem Risiko

Dieses Beispiel zeigt eine Vorstellung der Regel, die angreifbare Java- und Oracle-Elemente nach Schwachstelle gruppiert und ihren jeweiligen Supportgruppen zuweist.

### Beispiel für Korrekturaufgabenregel



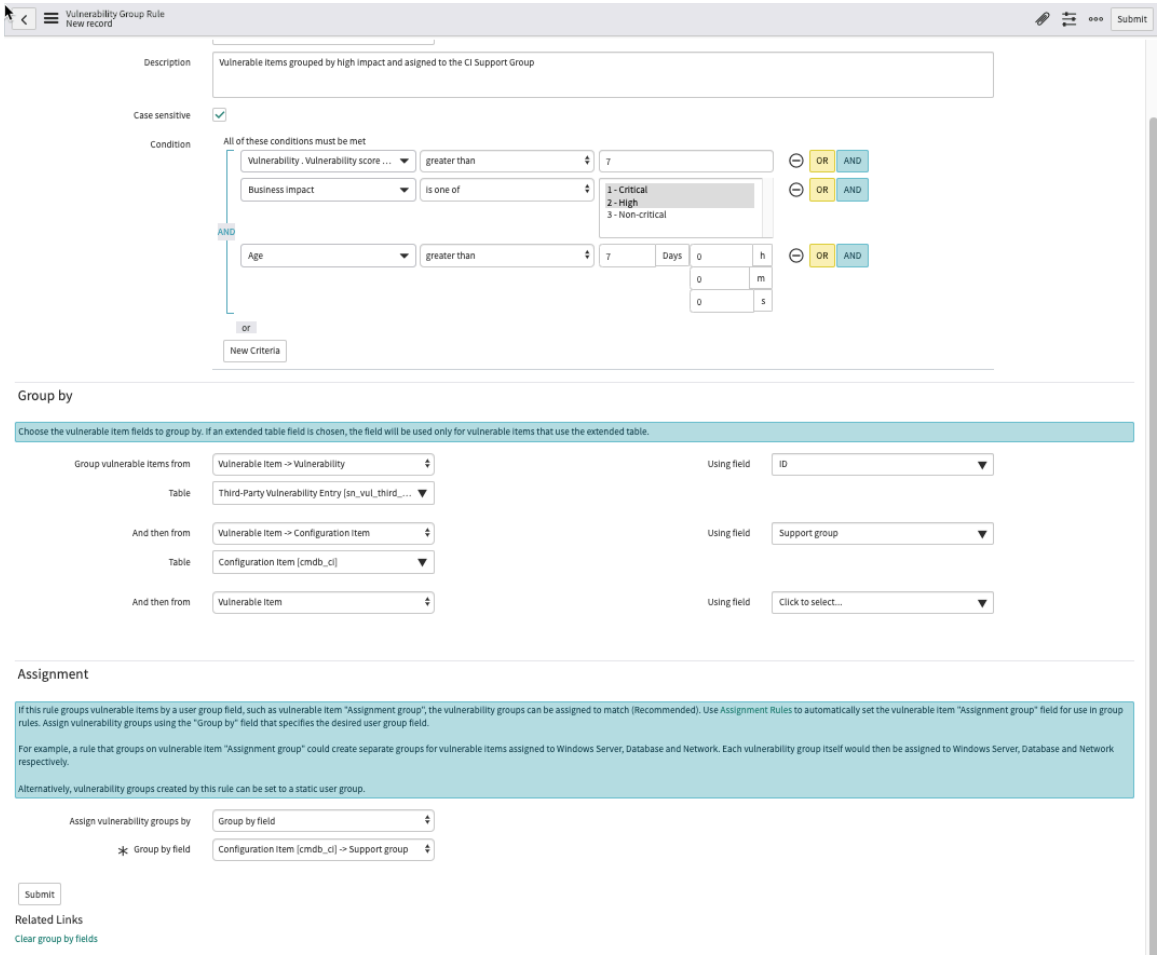

Klicken Sie mit der rechten Maustaste auf den Header, um **Speichern**.

## Korrekturaufgabenregel zum Gruppieren aller angreifbaren Elemente mit hoher Auswirkung nach Schwachstelle und CI-Supportgruppe

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für angreifbare Elemente mit hoher Auswirkung, die sie der CI-Supportgruppe zuweist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

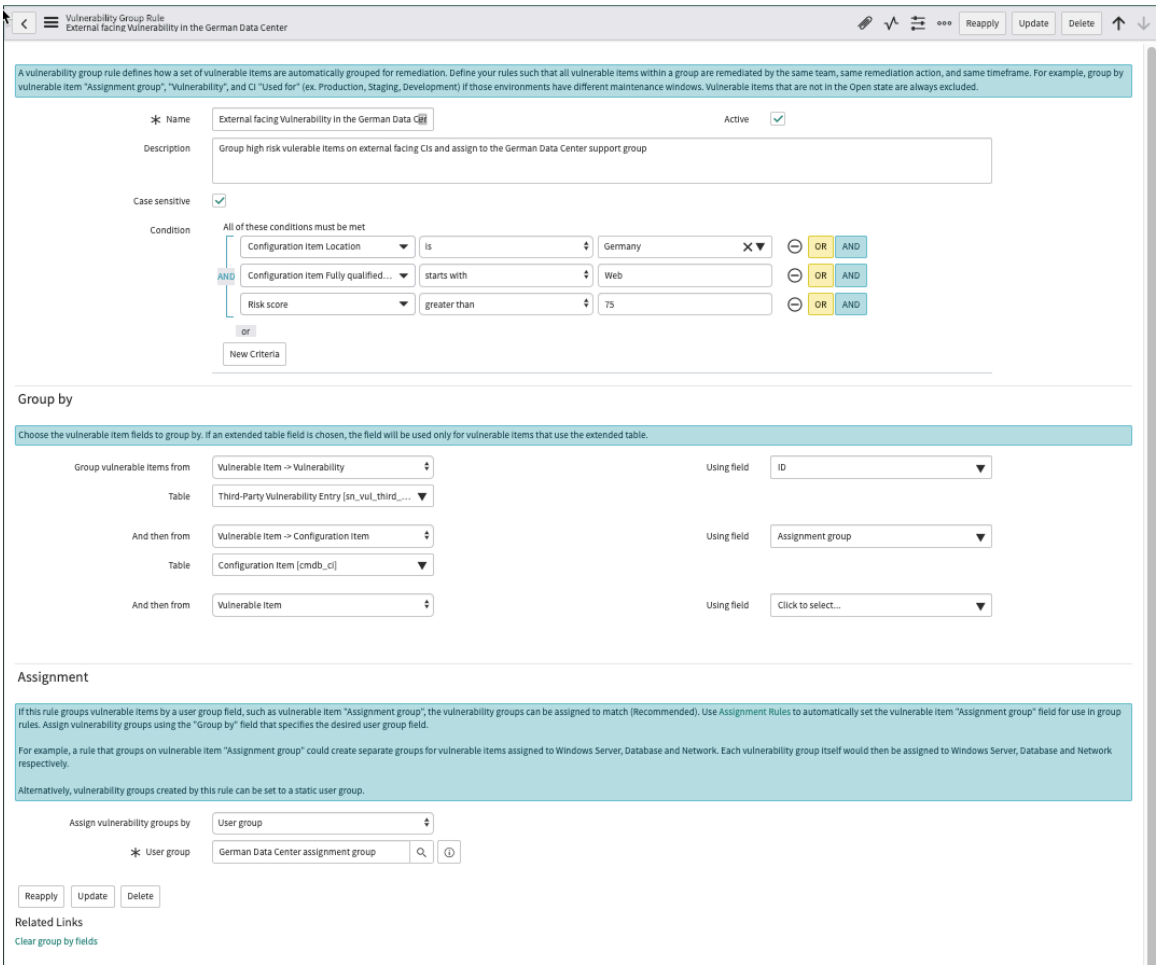



## Korrekturaufgabenregel zum Gruppieren aller Schwachstellen mit hohem Risiko auf einem nach außen gerichteten CI in einem Rechenzentrum in Deutschland

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für Schwachstellen mit hohem Risiko für nach außen gerichtete CIs in einem Rechenzentrum in Deutschland. Sie werden der Zuweisungsgruppe „Rechenzentrum Deutschland“ zugewiesen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Beispiel für die Berechnung der Risikopunktzahl für Vulnerability Response

Sie können die Risikopunktzahl-Rechner festlegen, um Risikopunktzahlen zu generieren, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten verwenden.

## Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregelrechner bestimmt werden.

Angenommen, ein Risikoregelrechner ist mit den Feldern in der folgenden Tabelle konfiguriert:

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| Schwachstelle.Schweregrad | 50 | Standard: 20<br>1 – Kritisch: 100<br>2 – Hoch: 80<br>3 - Mittel: 60<br>4 – Niedrig: 40<br>5 – Keine: 20 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| Schwachstelle.Exploit vorhanden | 50 | Standard: 50<br>Ja: 100<br>Nein: 0 |

Nehmen Sie außerdem an, dass die in dieser Tabelle angezeigten angreifbaren Elemente im System vorhanden sind:

| ID | Schwachstellenschweregrad | Schwachstellen-Exploit ist vorhanden |
|---|---|---|
| VIT00001 | 1 – Kritisch | 1: Ja |
| VIT00002 | 2 – Hoch | 1: Ja |
| VIT00003 | 3 – Mittel | 2: Nein |
| VIT00004 | 4 – Niedrig | 2: Nein |
| VIT00005 | 5 – Keine | 2: Nein |

Die Risikopunktzahlberechnung für die angreifbaren Elemente wird basierend auf der Formel berechnet:

`Risikopunktzahl = (W(Schweregrad) * FV (Schweregrad). + W(Exploitexistiert) * FV(Exploit vorhanden)) / 100`

wobei **W** die Gewichtung und **FV** der Gewichtungsprozentsatz des Feldwerts ist.

Die resultierende Risikopunktzahl für diese angreifbaren Elemente wird in der folgenden Tabelle beschrieben:

| ID | Schwachstellenschwereg (50 %) | Schwachstellen-Exploit vorhanden (50 %) | Resultierende Risikopunktzahl |
|---|---|---|---|
| VIT00001 | 1 – Kritisch (50 % x 100) | 1 – Ja (50 % x 100) | 100 |
| VIT00002 | 2 – Hoch (50 % x 80) | 1 – Ja (50 % x 100) | 90.0 |
| VIT00003 | 3 – Mittel (50 % x 60) | 2 – Nein (50 % x 0) | 30 |
| VIT00004 | 4 – Niedrig (50 % x 40) | 2 – Nein (50 % x 0) | 20 |
| VIT00005 | 5 – Keine (50 % x 20) | 2 – Nein (50 % x 0) | 10 |

**Hinweis:**
Für VIT00005 wird die Standardgewichtung angewendet, da der Wert des Schweregrads leer ist.

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie in dieser Tabelle die Ergebnisse:

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| Schwachstelle.Schweregrad | 50 | • Standard: 20<br>• 1 – Kritisch: 100 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| | | • **2 – Hoch: 70**<br>*überarbeiteter Wert<br>• 3 - Mittel: 60<br>• 4 – Niedrig: 40 |
| Schwachstelle.Exploit vorhanden | 50 | • Standard: 50<br>• Ja: 100<br>• Nein: 0 |

Die Risikopunktzahl für die angreifbaren Elemente nach erneuter Anwendung des Rechners wird in der folgenden Tabelle angezeigt:

| ID | Schwachstellenschwereg (50 %) | Schwachstellen-Exploit vorhanden (50 %) | Resultierende Risikopunktzahl |
|---|---|---|---|
| VIT00001 | 1 – Kritisch (50 % x 100) | 1 – Ja (50 % x 100) | 100 |
| VIT00002 | **2 – Hoch (50 % x 70)**<br>*überarbeiteter Wert | 1 – Ja (50 % x 100) | **85**<br>*überarbeiteter Wert |
| VIT00003 | 3 – Mittel (50 % x 60) | 2 – Nein (50 % x 0) | 30 |
| VIT00004 | 4 – Niedrig (50 % x 40) | 2 – Nein (50 % x 0) | 20 |
| VIT00005 | 5 – Keine (50 % x 20) | 2 – Nein (50 % x 0) | 10 |

### Fehlerbehandlung für Erkennungen

Fehler werden beim Erstellen von Erkennungen oder beim Erstellen und Aktualisieren angreifbarer Elemente während der Verarbeitung der Anhänge protokolliert. Wenn ein Schwachstellenintegrationsprozess fehlschlägt, werden Fehler auf der Registerkarte „Protokoll für Schwachstellenintegrationen“ protokolliert.

Diese Fehler werden mit einer der folgenden Kategorien protokolliert.

| Feld | Beschreibung |
|---|---|
| VI-Erstellung | Fehler beim Erstellen oder Aktualisieren der Erkennung. |
| Erkennung | Fehler beim Erstellen einer Erkennung. |

## Mobile Experience für Vulnerability Response

Wenn Sie für die Korrektur von Schwachstellen zuständig sind, können Sie mit Ihrem Android- oder iOS-Mobilgerät auf die Anwendung Vulnerability Response (VR) in Ihrer Now Platform®-Instanz zugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## Vulnerability Response

Informationen dazu, wie Sie sich mit den Konzepten von Vulnerability Response vertraut machen und erfahren, wie dieses Produkt Ihrem Unternehmen helfen kann, finden Sie unter Vulnerability Response verstehen.

**Hinweis:**
Machen Sie sich mit der vertraut, bevor Sie Vulnerability Response Mobile-App Mobileinstallieren Mobile Agent .

## Übersicht

Als Benutzer mit der Rolle „Korrekturbesitzer“ (sn_vul.remediation_owner) können Sie mit Vulnerability Response Mobile-App die Schwachstellen, Korrekturaufgaben und Zuweisungen in Ihrer Instanz von [ Now Platform direkt von Ihrem Mobilgerät Android oder iOS anzeigen und durchsuchen.

Sie werden benachrichtigt, wenn Ihnen oder Ihrer Zuweisungsgruppe Korrekturaufgaben (RTs) oder VIs zugewiesen wurden. Diese App bietet einem Korrekturbesitzer die Flexibilität, neu zuzuweisen, Felder zu bearbeiten und mit der Korrektur zu beginnen, ohne an den Desktop gebunden zu sein.

Sie haben Zugriff auf Schwachstellen, angreifbare Elemente, Module und alle Lösungen. Sie können die folgenden Aufgaben auf Ihrem Mobilgerät ausführen:

- Korrekturaufgaben anzeigen und aktualisieren
- Change-Anforderungen anzeigen.
- Weisen Sie eine Korrekturaufgabe oder ein angreifbares Element einem anderen Mitglied einer Zuweisungsgruppe neu zu.
- Zeigen Sie Benachrichtigungen an, wenn Ihnen oder einer Ihrer Zuweisungsgruppen eine kritische Korrekturaufgabe zugewiesen wird.
- Bearbeiten Sie eine Teilmenge von Feldern in Datensätzen für Korrekturaufgaben.
- Suchen Sie nach Korrekturaufgaben, die bestimmten Suchkriterien entsprechen.

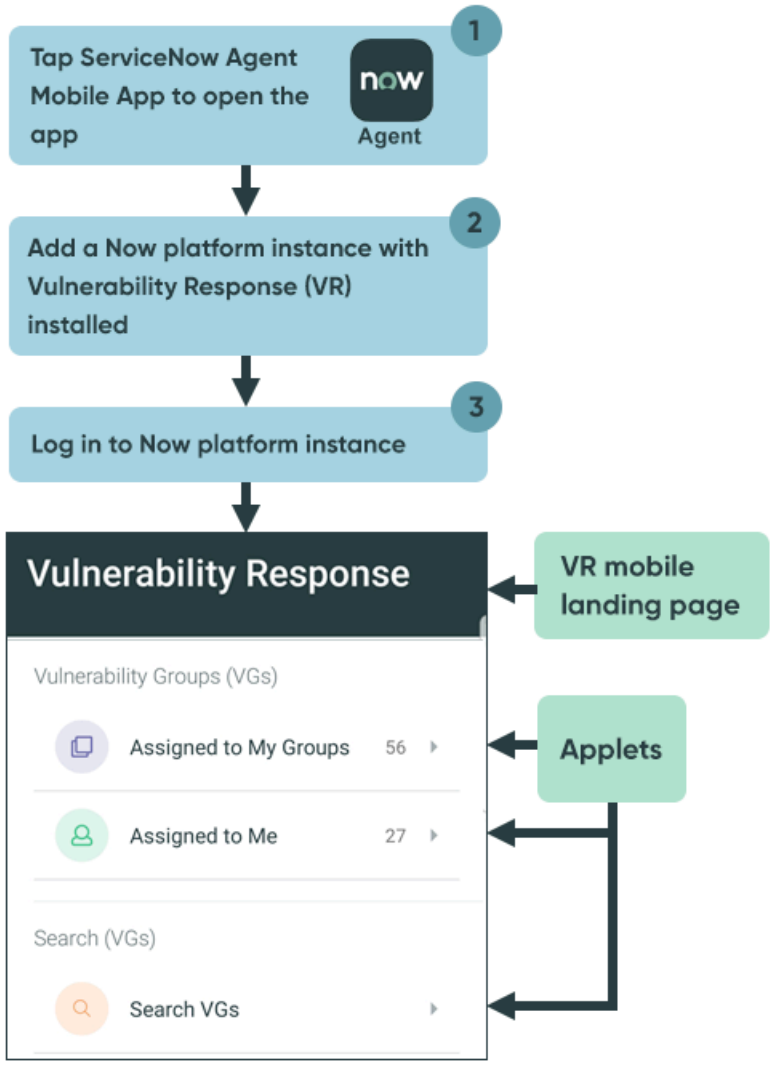
Die folgende Abbildung zeigt, wie Sie sich von Ihrem Mobilgerät aus bei Ihrer Now Platform -Instanz anmelden und wie der Zielbildschirm von Vulnerability Response Mobile-App nach der Anmeldung angezeigt wird.

Eine Schritt-für-Schritt-Anleitung zum Einrichten der Instanz Now Platform und zur Installation von Vulnerability Response Mobile-Appfinden Sie unter Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich beim an Vulnerability Response Mobile-App.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vulnerability Response Mobile-App**






### Anwendungen

Anwendungen sind die ServiceNow -Softwarekomponenten wie Security Incident Response (SIR), Vulnerability Response (VR), Governance, Risk und Compliance (GRC) und andere ServiceNow -Produkte, die bestimmte Features und Funktionalitäten in Ihrer Now Platform -Instanz bereitstellen. Nachdem Sie Kernanwendungen mit Mobile-Apps in Ihrer Instanz Now Platform installiert haben, werden diese Anwendungen als Symbole am unteren Rand Ihres Mobilgeräts angezeigt.

**Vulnerability Response-Symbol auf Mobilgerät**



### Ordner

Jede ServiceNow® Mobile Anwendung enthält Ordner, die die Applets nach Kategorien trennen. In der vorherigen Abbildung sind Korrekturaufgaben und Suche (VGs) die Ordner für Vulnerability Response Mobile-App.

### Applets

Applets sind die verschiedenen Optionen in der Anwendung. In der vorherigen Abbildung sind die Symbole unter Korrekturaufgaben und Suche (VGs) die verfügbaren Applets für Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In den folgenden Themen finden Sie weitere Informationen zu den Applets von Vulnerability Response Mobile-App.

## Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-App

Die folgende Prüfliste enthält die Setupaufgaben, die Sie in Ihrer Instanz Now Platform® und auf Ihrem Mobilgerät ausführen müssen, bevor Sie Vulnerability Response Mobile-Appverwenden können.

### Vorbereitungen

Weitere Informationen folgen jedem Schritt in der rechten Spalte. Geschätzte Zeit bis zum Abschluss dieser Aufgabe: 15 bis 20 Minuten.

Erforderliche Rolle: admin, sn_vul.remediation_owner

Sie haben Ihr Mobilgerät erfolgreich für Vulnerability Response Mobile-Appeingerichtet. Der nächste Schritt besteht darin, sich bei Vulnerability Response Mobile-App anzumelden und Ihrem Mobilgerät eine Now Platform -Instanz hinzuzufügen.

### Prozedur

1. Alternativ können Sie diese Prüfliste drucken und sie durch die Aufgaben führen, die für die Installation von Vulnerability Response Mobile-Apperforderlich sind.
2. Stellen Sie sicher, dass jedes Element in der Liste abgeschlossen ist, damit Sie sich bei Vulnerability Response Mobile-App anmelden und eine Now Platform -Instanz hinzufügen können.

#### Prüfliste für Mobilgeräte

| Element | Beschreibung |
|---|---|
| ☐ | Stellen Sie als Benutzer mit der Administratorrolle sicher, dass Sie die Kernanwendung Vulnerability ResponseNow Platform in einer Instanz von [] installiert haben. Dies ist die Instanz Now Platform, die Sie auf Ihrem Mobilgerät anzeigen.<br><br>**Hinweis:**<br>Die Kernanwendung Vulnerability Response und die Instanz Now Platform müssen aus demselben Familien-Release stammen.<br><br>**a.** Um sicherzustellen, dass die Kernanwendung in Ihrer Instanz installiert ist, navigieren Sie zu **Plugins**, und suchen Sie nach Vulnerability Response.<br><br>**b.** Wenn die Kernanwendung Vulnerability Response noch nicht installiert ist, klicken Sie auf **Installieren**, um sie zu installieren.<br><br>Weitere Informationen zur Installation der Kernanwendung Vulnerability Response finden Sie unter Vulnerability Response installieren.<br><br>Weitere Informationen zum Abrufen der Kernanwendung Vulnerability Response auf dem ServiceNow Store, zum Abrufen von -Berechtigungen, zum Installieren von Kernanwendungen und zum Aktivieren von Abhängigkeiten finden Sie unter Security Operations und ServiceNow Store. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
| --- | --- |
| ☐ | Stellen Sie als Benutzer mit der Administratorrolle sicher, dass [ Now Platform in der Instanz von Vulnerability Response Mobile-App installiert ist, die Sie auf Ihrem Mobilgerät anzeigen möchten.<br><br>**Hinweis:**<br>Die Instanzen Vulnerability Response Mobile-App und Now Platform müssen aus demselben Familien-Release stammen. Die Anwendungen Vulnerability Response Mobile-App und Vulnerability Response sollten kompatibel sein. Weitere Informationen zur Kompatibilität der Vulnerability Response-Anwendung finden Sie unter Vulnerability Response und Configuration Compliance Compatibility Matrix .<br><br>Laden Sie Vulnerability Response Mobile-App aus dem ServiceNow Store in Ihrer Now Platform -Instanz herunter, und installieren Sie sie.<br><br>Wenn Sie Vulnerability Response Mobile-Appinstallieren, werden die zugehörigen Abhängigkeiten com.glide.sg und com.glide.sg.agent_native_client ebenfalls installiert.<br><br>So überprüfen Sie, ob diese Abhängigkeiten installiert sind:<br>**a.** Navigieren zu **Alle** > **Plugins**.<br>**b.** Suchen Sie nach den Plugin-IDs (com.glide.sg und com.glide.sg.agent_native_client).<br>**c.** Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für Vulnerability Response Mobile-Apperforderlich.<br><br>Weitere Informationen zum Abrufen der Anwendung Vulnerability Response Mobile-App auf dem ServiceNow Store, zum Abrufen von Berechtigungen, zum Installieren von Anwendungen und zum Aktivieren von Abhängigkeiten finden Sie unter Security Operations und ServiceNow Store. |
| ☐ | Vergewissern Sie sich als Benutzer mit der Administratorrolle in Ihrer Instanz Now Platform, dass Sie Mobile-Benutzern die erforderlichen Now Platform Rollen zugewiesen haben.<br>**a.** Um die einem Benutzer zugewiesenen Rollen anzuzeigen, navigieren Sie zu **Alle** > **Administration** > **Anwender**.<br>**b.** Wählen Sie den Benutzernamen gefolgt von der zugehörigen Liste der Rollen aus. Alle diesem Benutzer zugewiesenen Rollen werden angezeigt.<br>**c.** Vergewissern Sie sich, dass ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der IT Infrastructure Library-Rolle (itil) zu. Benutzer mit der Rolle „itil“ können Change-Anforderungen und Korrekturaufgaben erstellen, öffnen, aktualisieren und schließen. Nur Benutzern mit der Rolle „itil“ können Aufgaben zugewiesen werden.<br>**d.** Vergewissern Sie sich, dass ein Benutzer zugewiesen ist, oder weisen Sie einen Benutzer mit der Rolle „Korrekturbesitzer“ (sn_vul.remediation_owner) zu. Benutzer mit der Rolle „sn_vul.remediation_owner“ können Schwachstellen- und |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
| --- | --- |
| | Lösungsdatensätze lesen. Diese Rolle wird automatisch hinzugefügt, wenn Sie die itil-Rolle zuweisen.<br>**e.** Vergewissern Sie sich, dass Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Benutzer zugewiesen haben.<br>**Hinweis:**<br>Wenn Sie eine große Anzahl von Benutzern für die mobile Anwendung haben, können Sie die Rolle sn_vul.remediation_owner alternativ einer Gruppe zuweisen. Jeder Benutzer, den Sie der Gruppe hinzufügen, erbt diese Rolle.<br>Weitere Informationen zu Zuweisungsregeln und -gruppen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.<br>Weitere Informationen zu Benutzern und zum Zuweisen von Rollen zu Benutzern und Gruppen finden Sie unter Benutzeradministration . |
| ☐ | Laden Sie als Benutzer mit der Rolle „Korrekturbesitzer“ (sn_vul.remediation_owner) die aktuelle ServiceNow® Agent-App auf Ihr Mobilgerät herunter.<br> <br>Die aktuelle App „Service Desk-Mitarbeiter“ ist im Apple App Store GoogleiOS und im Play Store [] verfügbar. |
| ☐ | Vergewissern Sie sich als Benutzer mit der Rolle „sn_vul.remediation_owner“, dass -Benachrichtigungen auf Ihrem Mobilgerät und in Ihrer Now Platform -Instanz aktiviert sind.<br>Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Korrekturaufgaben zugewiesen werden. Um Sie bei der rechtzeitigen Korrektur zu unterstützen, klicken Sie nach dem Aktivieren von Benachrichtigungen auf eine Benachrichtigung in Vulnerability Response Mobile-App, und navigieren Sie direkt zum Datensatz. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Element | Beschreibung |
| --- | --- |
| | Führen Sie die folgenden Schritte aus, um Benachrichtigungen in Ihrer Now Platform -Instanz zu aktivieren, damit sie auf Ihrem Mobilgerät angezeigt werden.<br>**a.** Vergewissern Sie sich, dass Sie [] heruntergeladen und in Ihrer Instanz von Now PlatformVulnerability Response Mobile-App installiert haben.<br>**b.** Überprüfen Sie in den Systemeinstellungen in Ihrer Instanz Now Platform unter Benachrichtigungen, ob die **ServiceNow Mobile-Anwendung**aktiviert ist.<br>Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Notification preferences .<br>Now Platform -Benachrichtigungen werden auch auf dem Nachrichtenbildschirm Ihres Mobilgeräts angezeigt. Stellen Sie sicher, dass Benachrichtigungen auch in den Einstellungen Ihres Mobilgeräts aktiviert sind. |

## Melden Sie sich beim an Vulnerability Response Mobile-App

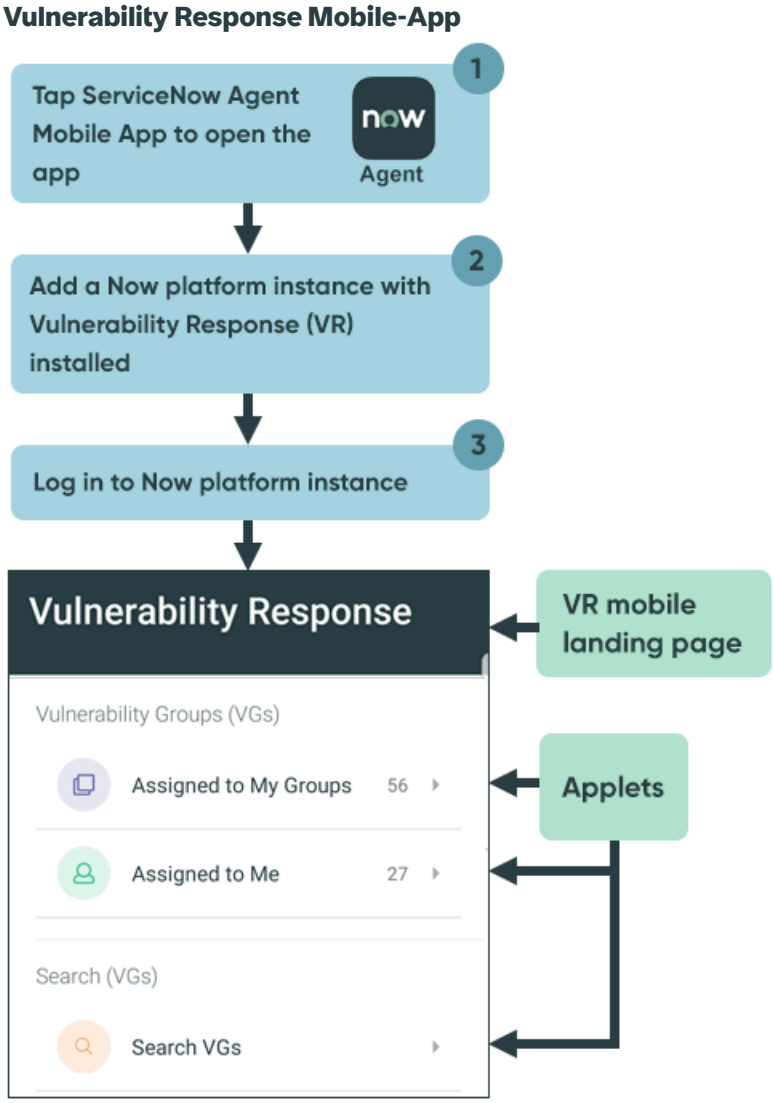
Öffnen Sie die Vulnerability Response Mobile-App, und fügen Sie Ihrem Mobilgerät eine Now Platform-Instanz mit Vulnerability Response hinzu.

### Vorbereitungen

Vergewissern Sie sich, dass Sie die in Richten Sie eine Prüfliste für ein Vulnerability Response Mobile-Appbeschriebenen Setup-Schritte abgeschlossen haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

### Warum und wann dieser Vorgang ausgeführt wird

Zeit bis zum Abschluss dieser Aufgabe: 5 bis 7 Minuten.

### Prozedur

1. Tippen Sie auf Ihrem Mobilgerät auf die **ServiceNow Agent** -App.

   Wenn Sie noch nicht bei einer Now Platform -Instanz angemeldet sind, wird der Bildschirm „Instanzen“ angezeigt.

2. Wenn die Instanz Now Platform mit der Kernanwendung Vulnerability Response noch nicht zu Ihrem Mobilgerät hinzugefügt wurde, führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Tippen Sie im angezeigten Bildschirm „Instanzen“ auf das Plus-Symbol ( ).
Ein Bildschirm wird angezeigt, in dem Sie aufgefordert werden, eine Adresse einer Now Platform -Instanz einzugeben und zu speichern.

b. Füllen Sie die Felder aus.

c. Tippen Sie auf **Speichern und anmelden**

3. Geben Sie auf dem angezeigten Anmeldebildschirm ServiceNow den Benutzernamen und das Passwort für die Instanz Now Platform ein, die Sie hinzufügen möchten, und tippen Sie auf **Anmelden**.
Der Zielbildschirm von Vulnerability Response wird angezeigt. Sie haben sich erfolgreich bei Vulnerability Response Mobile-App angemeldet!
4. Überprüfen Sie nach der Anmeldung, ob Benachrichtigungen in Vulnerability Response Mobile-Appaktiviert sind.

a. Tippen Sie unten im Zielbildschirm auf **Benachrichtigung**.

b. Tippen Sie im Bildschirm „Benachrichtigungen“ auf **Benachrichtigungen** aktivieren, wenn diese Option nicht aktiviert ist.
Benachrichtigungen von Now Platform werden auf dem Bildschirm „Benachrichtigungen“ in Vulnerability Response Mobile-App] angezeigt.

5. Nachdem Sie sich bei einer Instanz auf Ihrem Mobilgerät angemeldet haben, ist dies die Standardinstanz Now Platform auf dem Gerät.
Wenn Sie eine andere Now Platform auf dem Gerät anzeigen möchten, müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

a. Tippen Sie auf das Symbol „ **Einstellungen** “.

b. Tippen **Sie auf Abmelden**.
Der Bildschirm „Instanzen“ wird mit allen Now Platform Instanzen angezeigt, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich anzumelden, oder führen Sie alternativ die vorherigen Schritte aus, um eine weitere Instanz hinzuzufügen.

## Ergebnisse

Wenn der Instanzbildschirm für Vulnerability Response Mobile-App nicht angezeigt wird, nachdem Sie auf Ihrem Gerät auf die **ServiceNow Agent** -App getippt haben, stellen Sie sicher, dass **ServiceNow Agent** als vertrauenswürdige App auf Ihrem Gerät zugelassen ist. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und der allgemeinen Geräteverwaltung, und tippen Sie auf die Option (App vertrauen usw.), um den Zugriff zu gewähren.

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie Ihre Anmeldeinformationen auf dem Anmeldebildschirm eingegeben haben, überprüfen Sie, ob Ihr Benutzername und Ihr Passwort für die Instanz Now Platform korrekt sind.

Wenn Sie Probleme beim Anzeigen des Zielbildschirms haben, überprüfen Sie Ihre Netzwerkverbindung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie den Bildschirm „Instanzen“ nicht anzeigen können, nachdem Sie auf die **ServiceNow Agent** -App getippt haben, versuchen Sie, sie von Ihrem Gerät zu deinstallieren. Vergewissern Sie sich, dass Sie die aktuelle Version der App aus dem Apple iOS App Store oder dem Google Play Store haben, und versuchen Sie, sie erneut zu installieren.

## Mit können Sie Korrekturaufgaben anzeigen, zuweisen und bearbeiten Vulnerability Response Mobile-App

Sie können die Felder in Korrekturaufgabendatensätzen, die Ihrer Gruppe zugewiesen sind, anzeigen, zuweisen oder bearbeiten. Navigieren Sie durch Schwachstellen, angreifbare Elemente und Lösungsdatensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

### Vorbereitungen

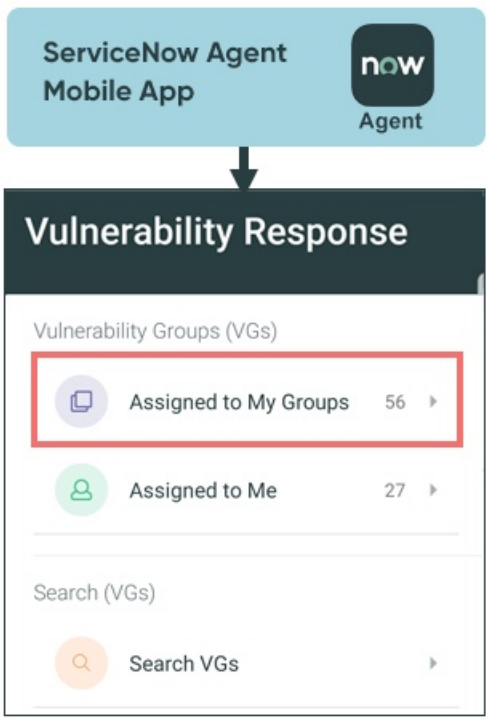
Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

### Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie sich selbst RT (VUL)-Datensätze zu, oder weisen Sie sie einem anderen Mitglied Ihrer Gruppe zu. Alternativ können Sie die Details aktiver Korrekturaufgabendatensätze, angreifbarer Elemente (VI), NVD-Schwachstellen und Lösungen anzeigen, bevor Sie sie bearbeiten, zuweisen oder korrigieren. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

### Prozedur

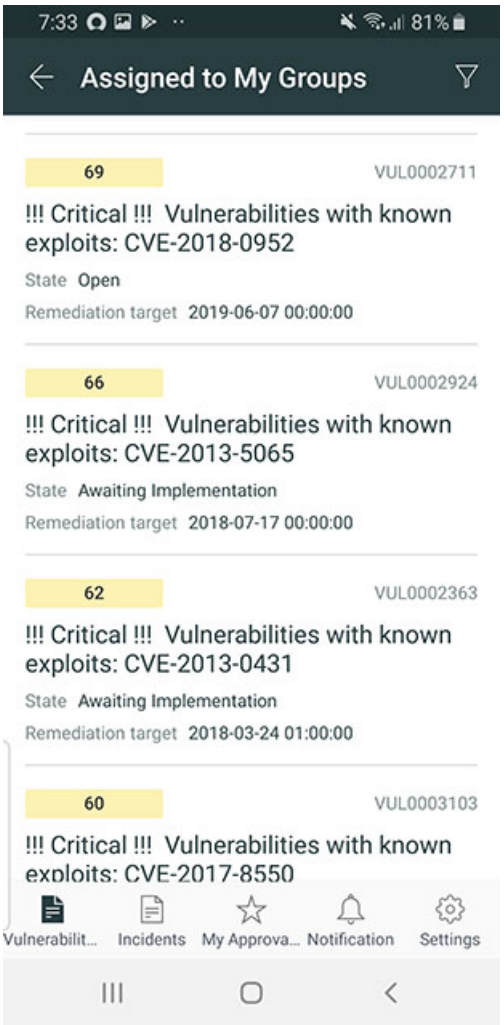
1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Vulnerability Response Mobile-App.
2. Wenn der Zielbildschirm von Vulnerability Response angezeigt wird, tippen **Sie auf Zugewiesen zu Meinen Gruppen**.
   Wenn Sie Vulnerability Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Die Liste der offenen Datensätze, die Ihrer Gruppe zugewiesen sind, wird angezeigt.

Automatische Übersetzung

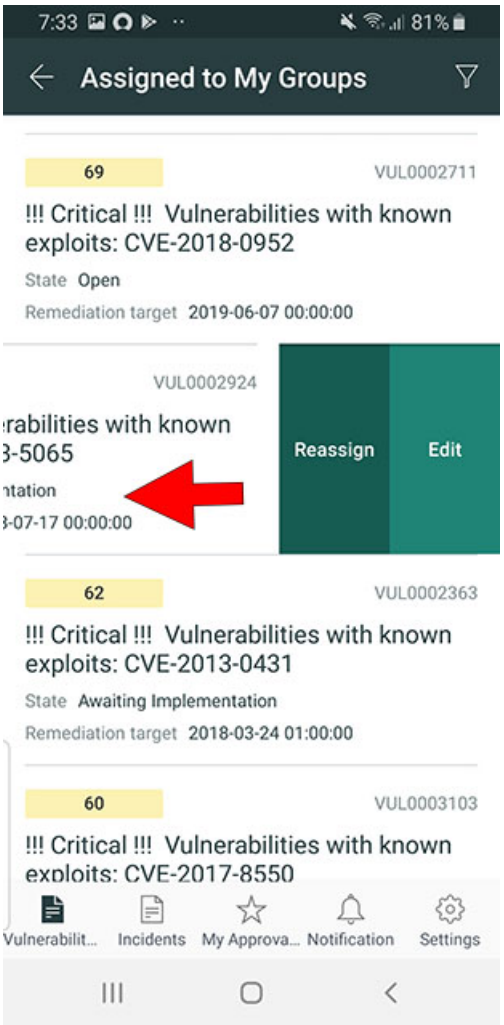
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. **Wahlweise:** Informationen zur Suche nach Datensätzen, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App.
4. Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen.
   Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im Now Platform.
5. Um einen Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wischen Sie in der Liste der offenen Datensätze auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



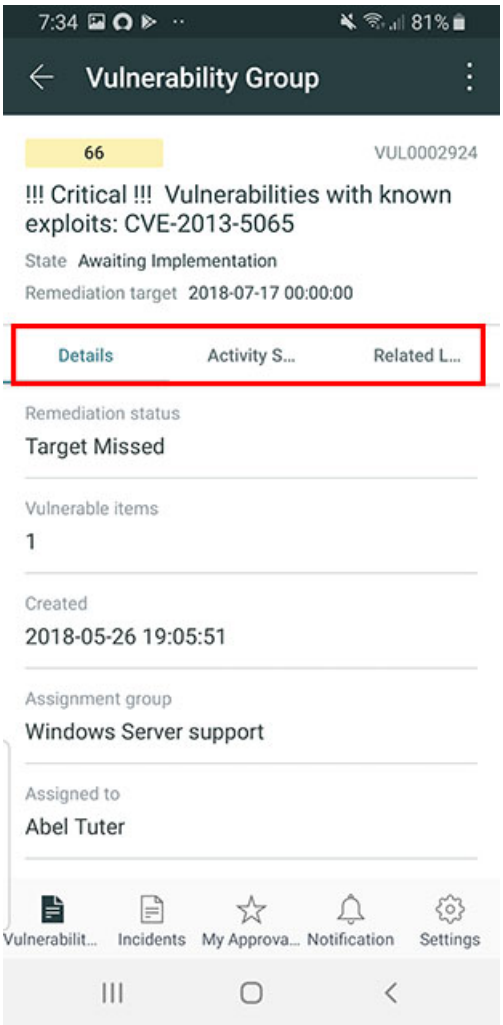

6. Wählen Sie eine Option aus dem angezeigten Menü aus, um fortzufahren.

7. Um die Details eines offenen Schwachstellendatensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, tippen Sie im angezeigten Bildschirm Meinen Gruppen zugewiesen auf einen Datensatz in der Liste.

8. Wählen Sie im angezeigten Datensatz der offenen Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder die zugehörigen Listen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die folgende Abbildung zeigt den Navigationspfad vom Datensatz der Korrekturaufgabe zum Datensatz der bevorzugten Lösung für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Navigationspfad von der Korrekturaufgabe durch einen Lösungsdatensatz**

**9.** Wählen Sie nach dem Überprüfen, Bearbeiten oder Remediieren eines aus, um fortzufahren.

## Ihnen zugewiesene Korrekturaufgaben mit dem anzeigen, neu zuweisen und bearbeiten Vulnerability Response Mobile-App

Sie können die Ihnen zugewiesenen Felder in Korrekturaufgabendatensätzen anzeigen, zuweisen oder bearbeiten. Navigieren Sie durch Datensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.

### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

### Warum und wann dieser Vorgang ausgeführt wird

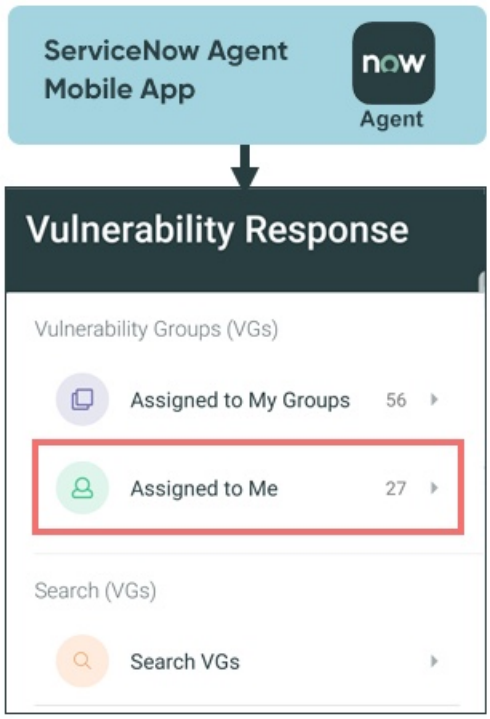
Ihnen zugewiesene Datensätze neu zuweisen oder bearbeiten Zeigen Sie die Details von aktiven Korrekturaufgabendatensätzen, Datensätzen für angreifbare Elemente (AE), Schwachstellen und Lösungen an, bevor Sie sie bearbeiten, zuweisen oder korrigieren. Zeit bis zum Abschluss dieser Aufgabe: 5–10 Minuten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

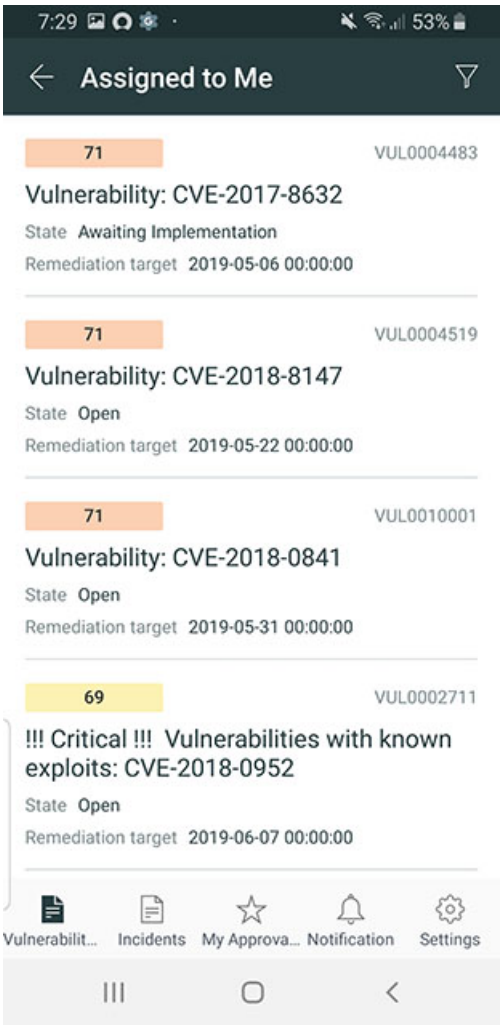
1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Vulnerability Response Mobile-App.
2. Wenn der **Vulnerability Response** -Zielbildschirm angezeigt wird, tippen **Sie auf Mir zugewiesen**. Wenn Sie Vulnerability Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




Die Liste der Korrekturaufgaben-Datensätze, die Ihnen zugewiesen sind, wird angezeigt.

Automatische Übersetzung

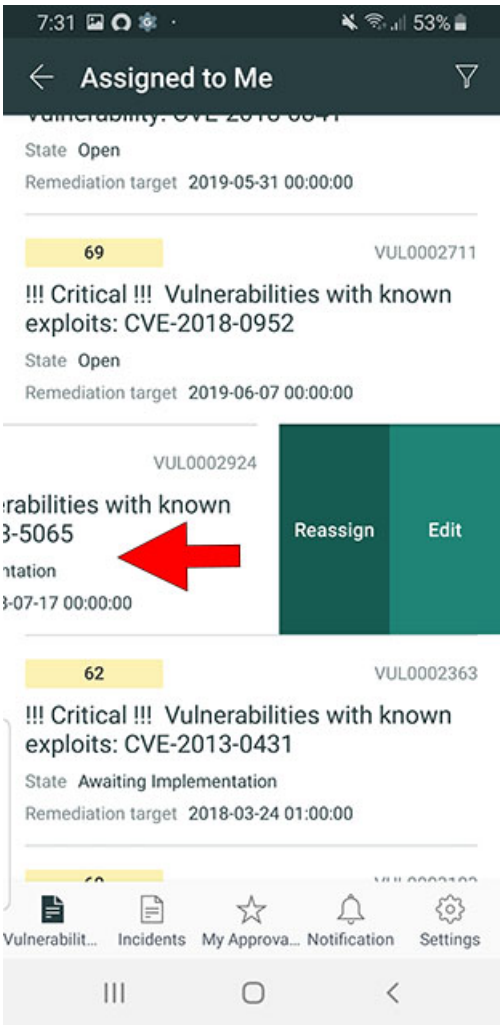
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. **Wahlweise:** Informationen zur Suche nach Datensätzen, die bestimmten Kriterien entsprechen, finden Sie unter Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App.
4. Alternativ können Sie bei angezeigtem Filtersymbol ( ) Filter festlegen, um die Anzahl der Datensätze in der Liste zu begrenzen.
   Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im Now Platform.
5. Um den Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wischen Sie bei angezeigtem Bildschirm „Mir zugewiesen“ auf einem Datensatz nach links, um das Menü zu öffnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

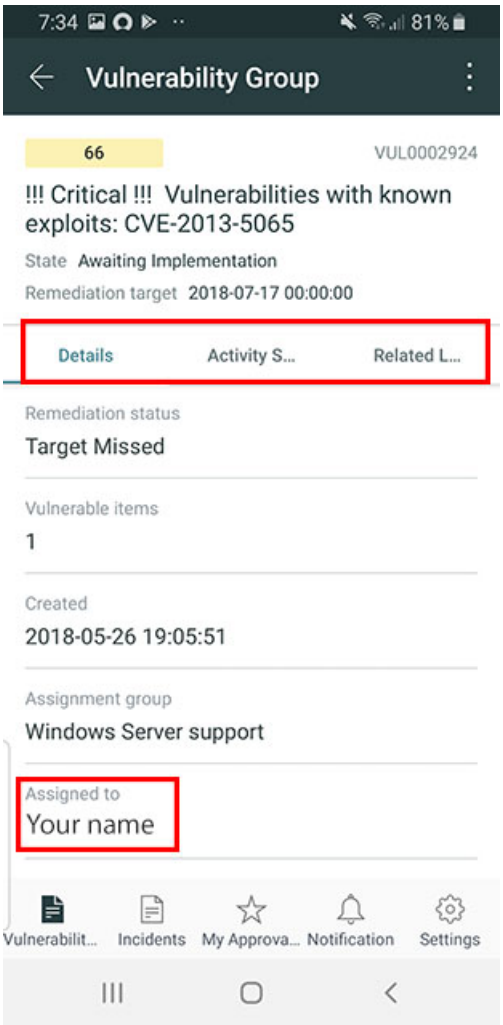



6. Wählen Sie eine, um fortzufahren.

7. Alternativ können Sie im angezeigten Bildschirm „Mir zugewiesen“ auf einen Datensatz in der Liste tippen, um die Details eines geöffneten Datensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen.
8. Wählen Sie im angezeigten Datensatz der offenen Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder die zugehörigen Listen anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die folgende Abbildung zeigt den Navigationspfad vom Datensatz der Korrekturaufgabe zum Datensatz der bevorzugten Lösung für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behebende Elemente anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Navigationspfad von RT durch einen Lösungsdatensatz**

**9.** Wählen Sie eine, um fortzufahren.

## Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

Suchen Sie nach Korrekturaufgaben, die den von Ihnen ausgewählten Suchkriterien entsprechen.

### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

### Warum und wann dieser Vorgang ausgeführt wird

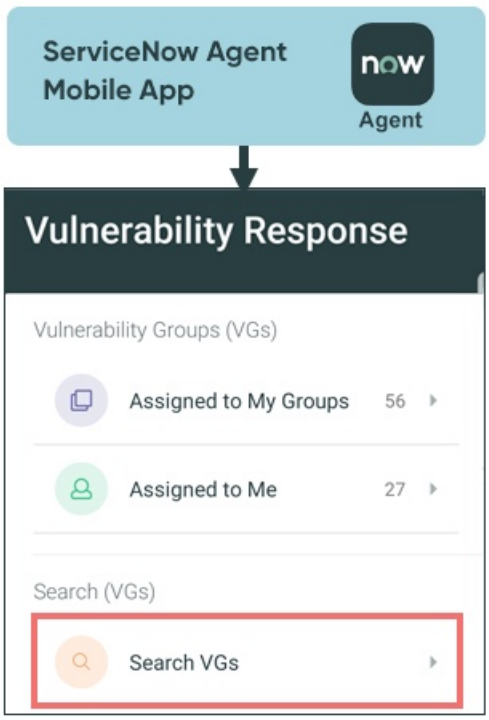
Zeit bis zum Abschluss dieser Aufgabe: 5 bis 7 Minuten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Wenn Sie auf Ihrem Mobilgerät nicht bei Ihrer Instanz Now Platform angemeldet sind, finden Sie weitere Informationen unter Melden Sie sich beim an Vulnerability Response Mobile-App.
2. Wenn der **Vulnerability Response** -Zielbildschirm angezeigt wird, tippen **Sie auf Search RTs**(RTs durchsuchen).
   Wenn Sie Vulnerability Response Mobile-App verlassen, nachdem Sie sich angemeldet haben, können Sie jederzeit auf die Now Agent-App tippen, um zum zuletzt angezeigten Bildschirm zurückzukehren.




3. Tippen Sie im angezeigten Suchbildschirm auf die Felder, und füllen Sie das Formular mit den gewünschten Suchkriterien aus.

   Befolgen Sie die Anweisungen nach der Tabelle, um Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu übermitteln.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | So fügen Sie einen Eintrag auf iOS Geräten hinzu |
|---|---|---|
| Nummer | Tippen Sie auf den Bildschirm, und geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Nummer wird rechts oben im RT-Datensatz angezeigt. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie auf das Symbol zum Schließen (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs (RTs durchsuchen) zurückzukehren. | Geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Nummer wird oben rechts im RT-Datensatz angezeigt. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | So fügen Sie einen Eintrag auf iOS Geräten hinzu |
|---|---|---|
| Risikobewertung | Tippen Sie auf ein oder mehrere Elemente und anschließend auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie auf das Symbol zum Schließen (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs (RTs durchsuchen) zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |
| Korrekturstatus | Tippen Sie auf ein oder mehrere Elemente und anschließend auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie auf das Symbol zum Schließen (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs (RTs durchsuchen) zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |
| Status | Tippen Sie auf ein oder mehrere Elemente und anschließend auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie auf das Symbol zum Schließen (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs (RTs durchsuchen) zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |
| Grund | Tippen Sie auf ein oder mehrere Elemente und anschließend auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie auf das Symbol zum Schließen (X), um Ihre Eingabe abzubrechen und zum Feld Search RTs (RTs durchsuchen) zurückzukehren. | Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |
| Zuweisungsgruppe | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tippen Sie auf dieses Feld | So fügen Sie einen Eintrag auf Android Geräten hinzu | So fügen Sie einen Eintrag auf iOS Geräten hinzu |
|---|---|---|
| | geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. | geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. |
| Zugewiesen an | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. | Wählen Sie eine Option aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.<br><br>Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie **Keine**aus, wenn kein Eintrag vorhanden ist. |
| Kurzbeschreibung | Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalterzeichen (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. | Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalterzeichen (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. |
| Beschreibung | Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalterzeichen (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm „RTs durchsuchen“ zurückzukehren. | Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalterzeichen (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf **Fertig**, um zum Bildschirm „RTs durchsuchen“ zurückzukehren.<br><br>Tippen Sie im erweiterten Feld auf **Abbrechen**, um den Eintrag zu löschen und zum Bildschirm SearchRTs zurückzukehren. |

Wählen Sie für Android -Geräte bei angezeigtem Bildschirm „RTs durchsuchen“ und allen eingegebenen Kriterien eines aus, um fortzufahren.

4. Wählen Sie für iOS -Geräte bei angezeigtem Bildschirm „RTs durchsuchen“ eines aus, um fortzufahren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie Filtern Sie Datensätze mit Vulnerability Response Mobile-App, um die Suchergebnisse einzugrenzen.

## Filtern Sie Datensätze mit Vulnerability Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der Now Platform.

### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.remediation_owner)

### Warum und wann dieser Vorgang ausgeführt wird

Zeit bis zum Abschluss dieser Aufgabe: 5 Minuten.

### Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien für eine beliebige Liste von Datensätzen einzugeben, tippen Sie auf das Filtersymbol ( ).
2. Wenn der Bildschirm „Filter“ angezeigt wird, tippen Sie auf ein Feld, um es zu erweitern.
   Ein häufiges Feld zur Eingabe von Suchkriterien für Datensätze von Korrekturaufgaben ist das Feld Status.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf das Zurück-Symbol ( Back) oder auf **FERTIG**, um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden auf dem Filter-Bildschirm angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird auch oben auf dem Bildschirm angezeigt. Tippen Sie auf **ZURÜCKSETZEN**, um alle Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 bei angezeigtem Filter-Bildschirm, um mit dem Festlegen Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Schnittmenge-Symbol ( ), um UND-Bedingungen zu erstellen.
7. Alternativ können Sie auf das Schnittmengensymbol ( ) tippen, um ODER-Bedingungen zu erstellen.
8. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, tippen Sie im angezeigten Bildschirm „Filter“ auf **FERTIG**.
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

#### Zugehörige Informationen

Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

# Orchestration für Vulnerability Response

Mit Vulnerability Response Orchestration Workflows und Aktivitäten können Sie mithilfe der Workflow-Orchestrierung mit Windows- oder UNIX-basierten Systemen und Umgebungen interagieren und Daten aus diesen abrufen. Durch die Anreicherung von Daten können Sie den Lebenszyklus der Fehlerkorrektur verkürzen.

Weitere Informationen zum Bearbeiten von Workflows oder Erstellen benutzerdefinierter Workflows finden Sie unter Exploring Flow Designer .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vulnerability Response Orchestration Workflows und Aktivitäten

Vulnerability Response Orchestrationenthält mehrere Workflows. Workflows und Aktivitäten automatisieren und beschleunigen Ihre Prozesse. Verwenden Sie Workflows und Aktivitäten, um Scan-Datensätze zu erstellen, angreifbare Elemente zu scannen, Scan-Datensätze zu erstellen und vieles mehr.

### Vulnerability Response Workflow zum Scannen auf Schwachstellen

Automatisieren Sie Schwachstellenprüfungen für einzelne oder mehrere angreifbare Elemente mit dem Workflow „ **Vulnerability Response – Scan Vulnerability** “, der im Basissystem enthalten ist.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow „ **Vulnerability Response – Scan Vulnerability** “ erstellt einen Scan-Datensatz für die Schwachstelle oder Gruppe von Schwachstellen, von der aus er aufgerufen wurde.

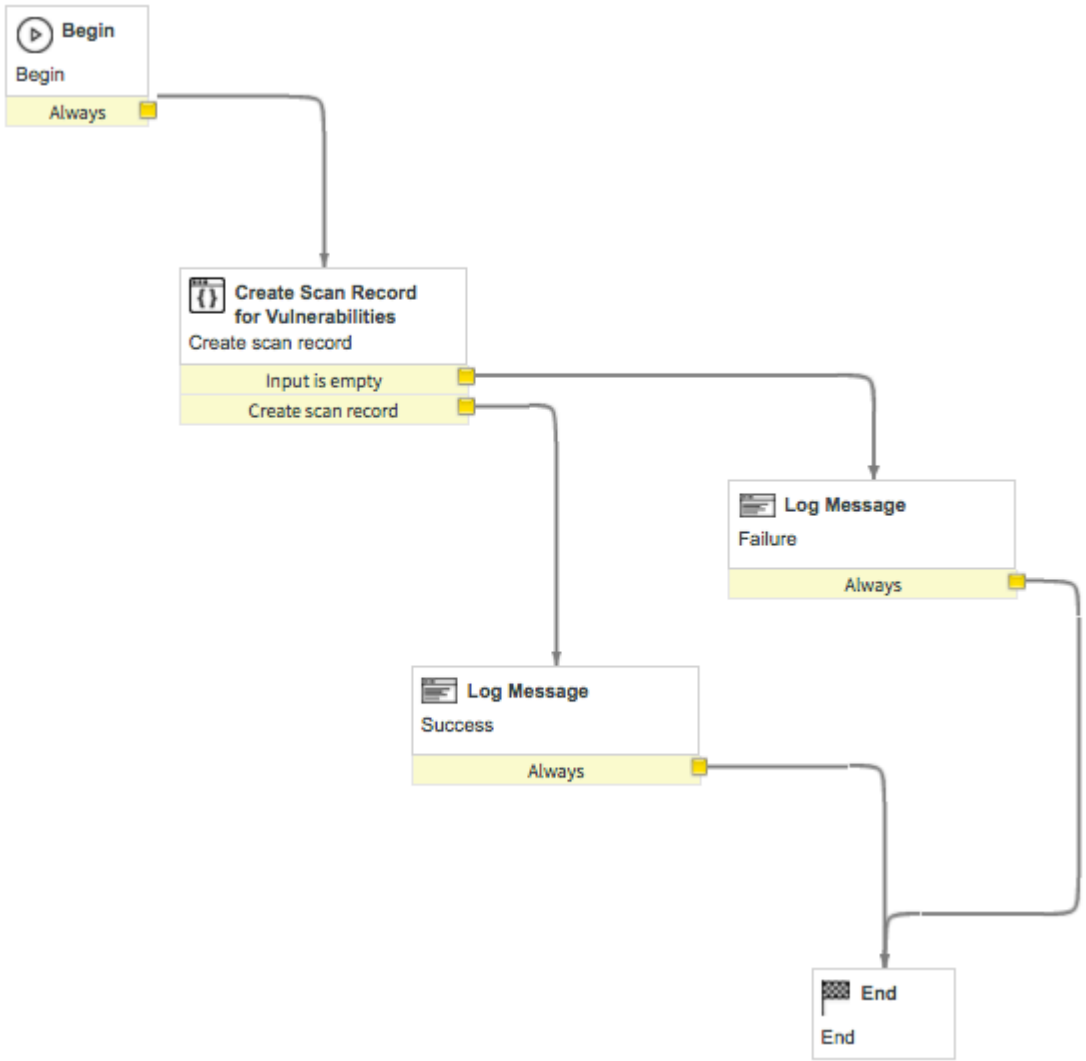
**Hinweis:**
Es wird empfohlen, Schwachstellen oder angreifbare Elemente nach der Korrektur erneut zu scannen, wenn ein Schwachstellen-Patch auf die betroffenen Datensätze angewendet wird. Sie können den erneuten Scan mit der beschriebenen Methode durchführen oder die erneuten Scans automatisieren.

Zu den Workflow-Aktivitäten gehören Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow „Vulnerability Response – Scan Vulnerability“**




### Scan-Schwachstellen-Workflow

Die zugehörigen Listen namens **Vulnerability Response** > **Scan-Schwachstelle** Der Workflow scannt eine Korrekturaufgabe erneut.

### Vorbereitungen

Erforderliche Rolle: keine

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird durch **„Angreifbare Gruppe erneut scannen“** während einer Aktion „ **Schließen/Ignorieren** “ ausgelöst.

Workflow-Prozessaktivitäten umfassen:

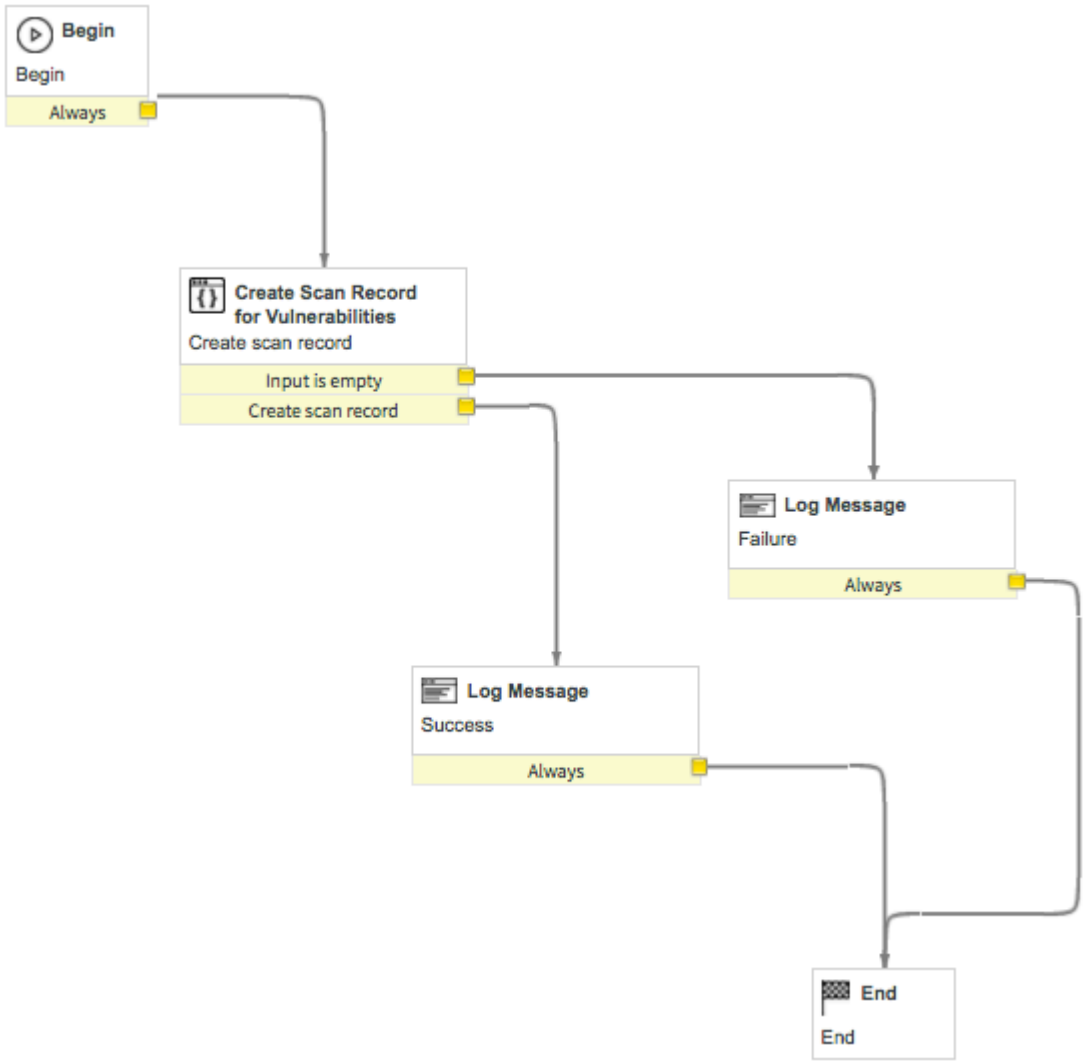
Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Protokollnachricht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Scan-Schwachstellen-Workflow






## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen Aufgabendatensatz (VUL).
3. Klicken Sie auf **Schließen**.
4. Wählen Sie **Geschlossen** für **Gewünschter Zustand**.
5. Wählen Sie **Fest** für den **Substatus**.
6. Wählen Sie **Warten auf Bestätigung beim nächsten Scan** für **Jetzt schließen?**
   Für die Korrekturaufgabe und angreifbaren Elemente ändert sich der **Status** in „ **Bestätigung ausstehend**“, der **Substatus** ändert sich in „ **Festgelegt**“, und ein erneuter Scan wird ausgeführt.

### Vulnerability Response Workflow zum Scannen angreifbarer Elemente

Automatisieren Sie Schwachstellenprüfungen für einzelne oder mehrere angreifbare Elemente mit dem Workflow „ **Vulnerability Response –** Angreifbare Elemente scannen“, der im Basissystem enthalten ist.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

### Warum und wann dieser Vorgang ausgeführt wird

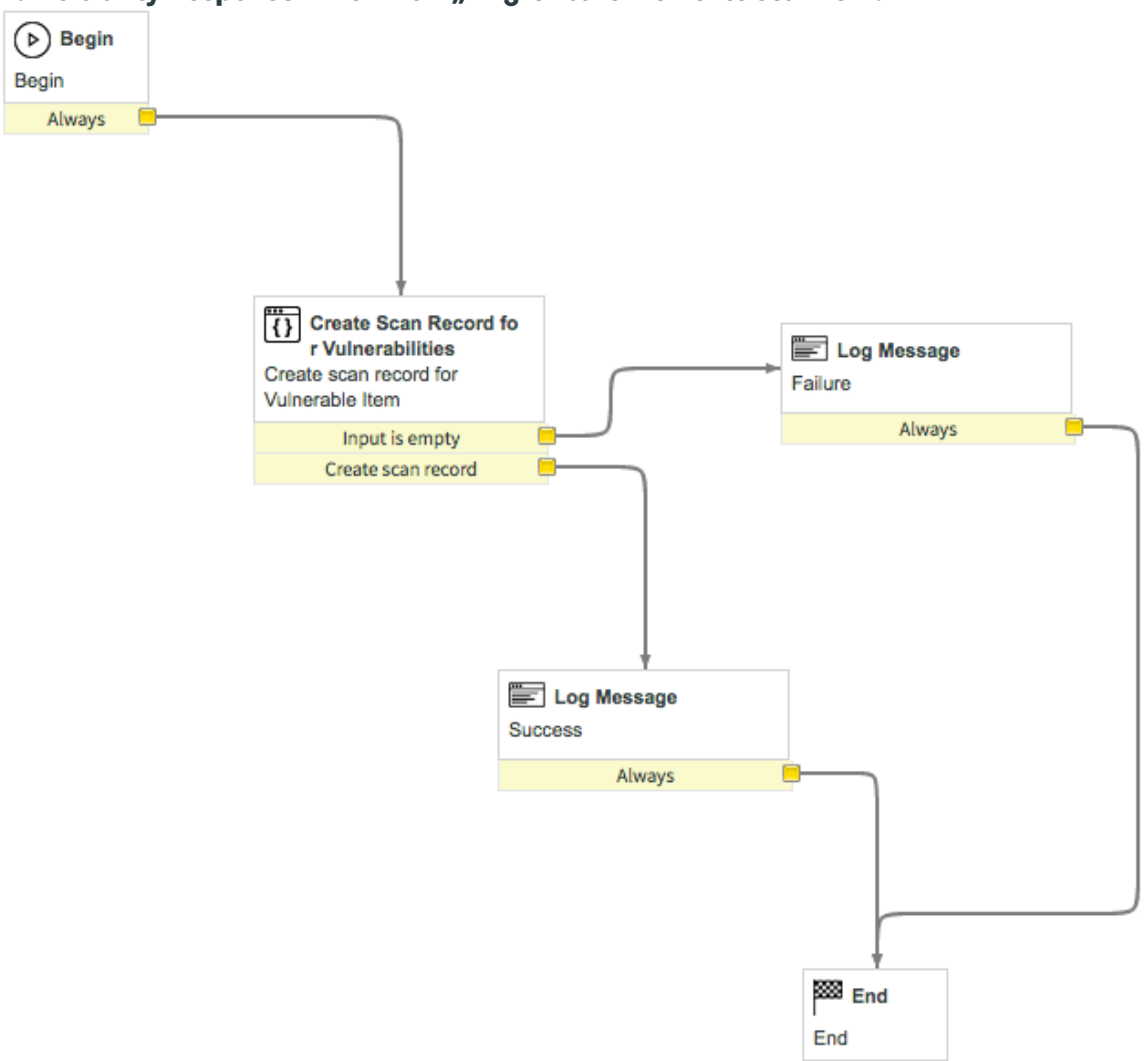
Der Workflow „ **Vulnerability Response –** Angreifbare Elemente scannen“ erstellt einen Scan-Datensatz für das angreifbare Element oder die Gruppe von Elementen, aus der er aufgerufen wurde.

**Hinweis:**

Es wird empfohlen, Schwachstellen oder angreifbare Elemente nach der Korrektur erneut zu scannen, wenn ein Schwachstellen-Patch auf die betroffenen Datensätze angewendet wird. Sie können den erneuten Scan mit der beschriebenen Methode durchführen oder den erneuten Scan automatisieren.

Workflow-Prozessaktivitäten umfassen: Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

**Vulnerability Response – Workflow „Angreifbare Elemente scannen“.**






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Workflow zum Scannen angreifbarer Elemente

Die zugehörigen Listen namens**Vulnerable Response** > **Angreifbares Element scannen** Der Workflow scannt ein angreifbares Element erneut.

### Vorbereitungen

Erforderliche Rolle: keine

### Warum und wann dieser Vorgang ausgeführt wird

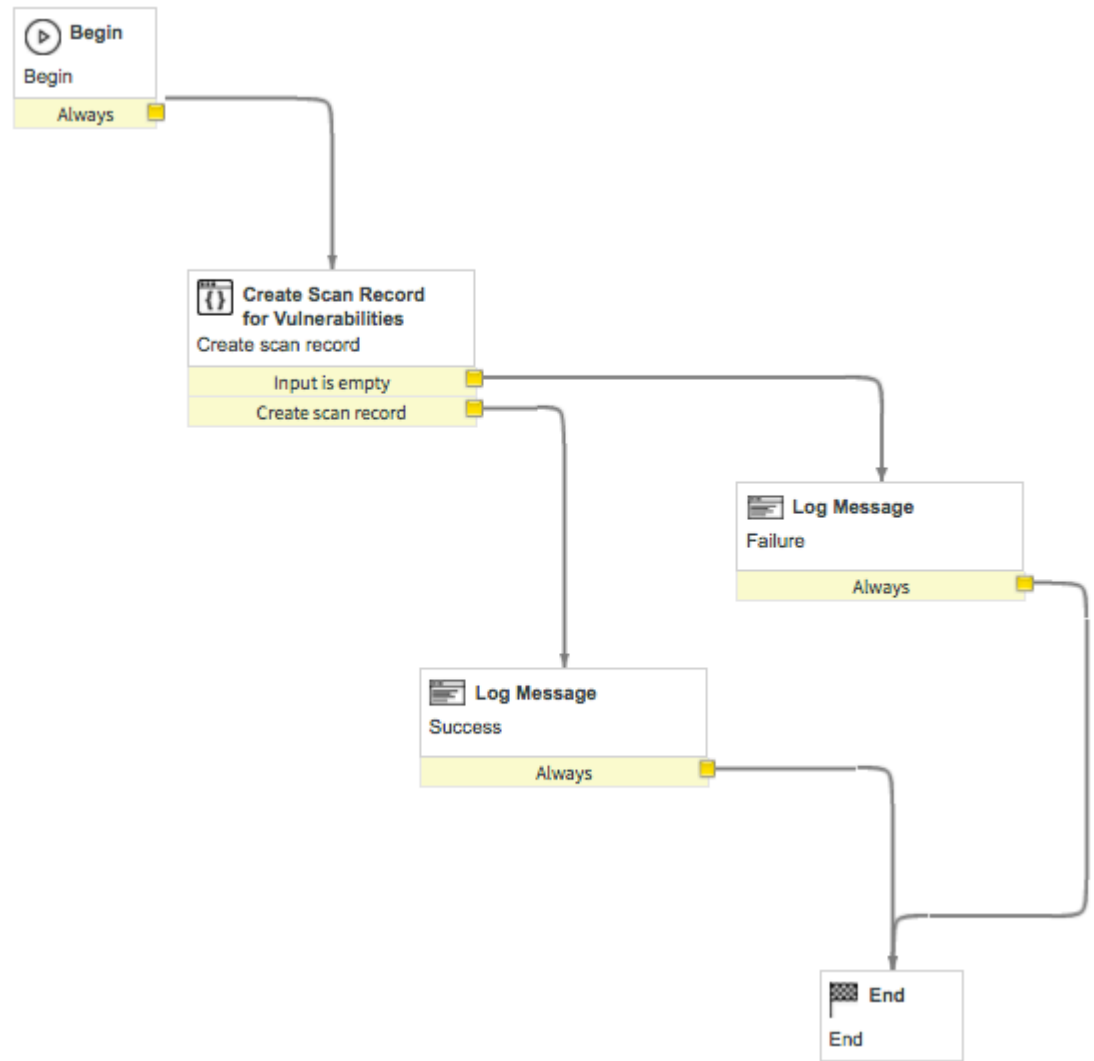
Dieser Workflow wird durch **Rescan Schwachstelle**(Rescan Schwachstelle) während einer Aktion **Schließen/Ignorieren** ausgelöst.

Workflow-Prozessaktivitäten umfassen:

Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Protokollnachricht

**Scan-Schwachstellen-Workflow**




### Prozedur

1. Navigieren zu **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie auf **Schließen/Ignorieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Geschlossen**für **Gewünschter Zustand**.
5. Wählen Sie **Fest** für den **Substatus**.
   Der **Status** der Gruppe ändert sich in **Bestätigung ausstehend**, der **Substatus** ändert sich in **Festgelegt**, und ein erneuter Scan wird ausgeführt.

## Vulnerability Response Orchestration Workflow-Aktivitäten

Vulnerability Response Orchestration Mit -Aktivitäten können Benutzer mithilfe der Workflow-Orchestrierung feststellen, ob eine Schwachstelle bereits in anderen Security Incidents oder auf anderen Systemen erkannt wurde.

### Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Schwachstellenprüfungen für einzelne oder mehrere angreifbare Elemente können mit der Workflow-Aktivität **Scan-Datensatz für Schwachstellen erstellen** ausgeführt werden, die im Basissystem enthalten ist. Wenn die Eingabe an die Aktivität übergeben wird, wird ein Scan-Datensatz erstellt.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| Aufgaben-IDs [Zeichenfolge] | Eine Zeichenfolge von durch Kommas getrennten sysIds, die die erwarteten Eingaben definieren. Dieses Feld ist ein Pflichtfeld. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| scanResult [Boolesch] | Gibt „True“ zurück, wenn die Eingabe nicht leer ist. Für die taskIds wird ein Scan-Datensatz erstellt. |

# Application Vulnerability Response

Die Funktion Application Vulnerability Response (AVR) der Anwendung ServiceNow® Vulnerability Response importiert angreifbare Elemente (AVIs) und ermöglicht gemäß den Regeln die Behebung von Anwendungsschwachstellen. Vulnerability Response ist über ein separates Abonnement verfügbar.

Ab AVR v19.0 wurden einige wichtige Tabellen- und Spaltennamen aktualisiert. Daher werden in der Dokumentation sowohl Verweise auf die älteren als auch auf die neueren Namen angezeigt. Die vollständige Liste der aktualisierten Begriffe finden Sie unter Application Vulnerability Response -Produktansicht.

Ab v19.0 von Vulnerability Responsekönnen Sie Schwachstellendaten für Software Composition Analysis (SCA) und Software Bill of Material (SBOM) erfassen, um

Automatische Übersetzung

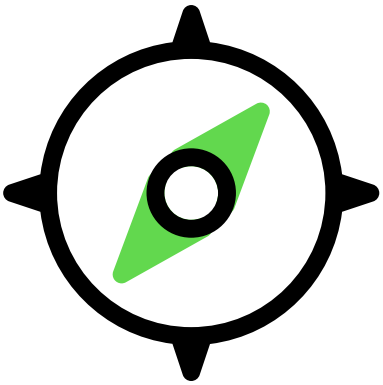
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden und Veracode Vulnerability Integration.

Ab Version 18.0 von Vulnerability Responsekönnen Sie AVIs in Vulnerability Manager Workspace bzw. IT Remediation Workspace überwachen und beheben. Weitere Informationen finden Sie unter Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

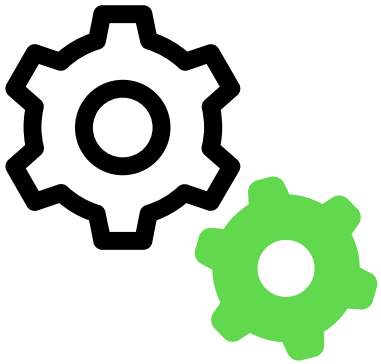
## Application Vulnerability Response

### Erkunden



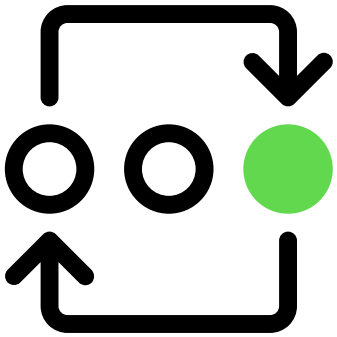
Erfahren Sie mehr über die Konzepte und Funktionen von Application Vulnerability Response.

### Konfigurieren



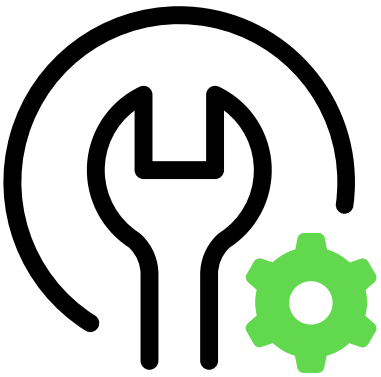
Konfigurieren Sie Application Vulnerability Response.

### integrieren



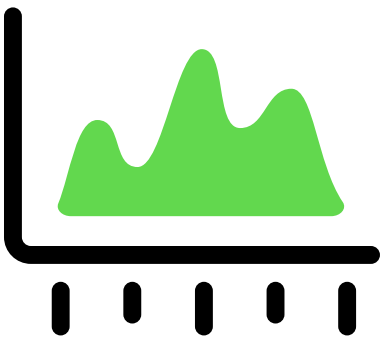
Erweitern Sie Application Vulnerability Response durch die Integration mit anderen Anwendungen.

### Beheben



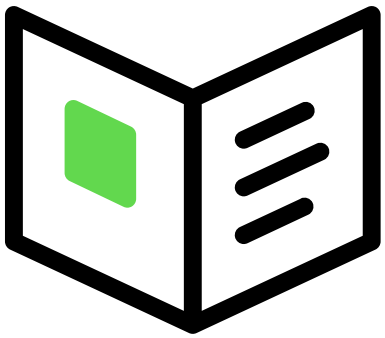
Erfahren Sie, wie Sie Anwendungsschwachstellen beheben können.

### Analytik und Berichterstellung



Zeigen Sie Application Vulnerability Response-Analysen an

### Referenz



Rufen Sie Details zu Komponenten von Application Vulnerability Response wie Feldern, Tabellen und Eigenschaften ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Application Vulnerability Response erkunden

Anwendungsschwachstellen sind Schwachstellen in Ihren benutzerdefinierten Softwareanwendungen, die während des gesamten Entwicklungslebenszyklus der Anwendung gescannt werden.

## Übersicht über Application Vulnerability Response und verfügbare Versionen

Application Vulnerability Response (AVR) ist der Teil der Anwendung Vulnerability Response, die Anwendungsschwachstellen verarbeitet.

### Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Vulnerability Response v21.0<br>Vulnerability Response v20.0<br>Vulnerability Response v19.0<br>Vulnerability Response v18.2<br>Vulnerability Response v18.0 | Application Vulnerability Response release notes<br><br>Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Funktionsweise

Schwachstellendaten werden aus internen und externen Quellen importiert, z. B. Common Weakness Enumeration (CWE) oder Integrationen von Drittanbietern. Nachdem die Daten importiert wurden, werden sie mit Anwendungsdaten in Configuration Management Database (CMDB) verglichen und in der Anwendung Application Vulnerability Response ] verarbeitet. Wenn eine Übereinstimmung zwischen importierten Anwendungsschwachstellendaten und Daten in Ihrer CMDB besteht, wird ein angreifbares Anwendungselement (AVI) erstellt.

Application Vulnerability Response umfasst die folgenden Hauptfunktionen:

- Integrieren Sie unterstützte Scanner von Drittparteien, um Schwachstellendaten zu importieren.
- Vergleichen Sie Daten im Zusammenhang mit Anwendungsschwachstellen, und bestimmen Sie, ob Anwendungsschwachstellen in einer Anwendung gefunden werden.
- Priorisieren, korrigieren und verwalten Sie angreifbare Elemente in Anwendungen (AVI). Jede Anwendungsschwachstelle stellt einen Schwachstelleneintrag in den Bibliotheken von CWE oder Drittanbietern dar.
- Ab Version 18.0 von Vulnerability Responsekönnen Sie AVIs im Vulnerability Manager Workspace bzw. IT Remediation Workspace überwachen und korrigieren. Weitere Informationen finden Sie unter Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.
- Korrelieren Sie Application Vulnerability Response Daten mithilfe von Rechnern und Bibliotheken, um die folgenden Aufgaben auszuführen.

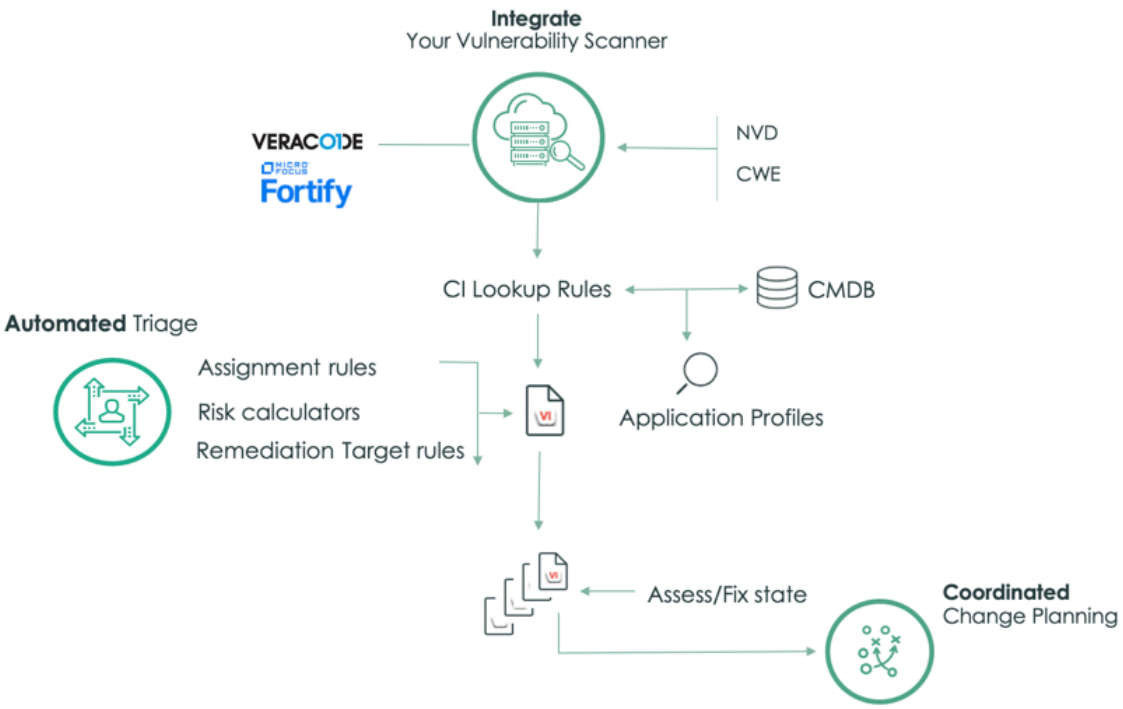
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie mithilfe von **CI-Suchregeln**automatisch angreifbare Anwendungselemente. Während des Imports werden Schwachstellen von Drittparteien einer CWE zugeordnet, um eine AVI zu erstellen.
- Erstellen Sie Zuweisungsregeln, um die Zuweisungen von angreifbaren Anwendungselementen zu automatisieren.
- Verwenden Sie Rechnergruppen, um die geschäftlichen Auswirkungen zu bestimmen, unterschiedliche Bedingungen mithilfe von Filtern anzugeben, einfache Berechnungen anzuwenden oder ein Skript zu verwenden.
- Erstellen Sie Korrekturzielregeln, die den erwarteten Zeitrahmen für die Korrektur angreifbarer Anwendungselemente definieren, damit Sie bevorstehende Korrekturaktivitäten überwachen können.

- Verknüpfen Sie eine einzelne Drittpartei-Schwachstelle mit mehreren CWE-Einträgen, und suchen Sie die primäre CWE für eine Schwachstelle, um das Risiko zu bestimmen. Weitere Informationen zur **primären CWE**finden Sie unter Anwendungsschwachstellen-Felder.
- Verwenden Sie CWE-Datensätze, die aus der CWE-Datenbank heruntergeladen oder aus Integrationen von Drittanbietern importiert werden, als Referenz, um zu entscheiden, ob Sie eine Schwachstelle eskalieren müssen. Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt.

Verwenden Sie Application Vulnerability Response, um den Informationsfluss zu verfolgen, von der Integration über die Untersuchung bis hin zur Lösung.




## Typen der importierten Schwachstellendaten

Application Vulnerability Response unterstützt die folgenden Arten von importierten Anwendungsschwachstellendaten.

**Hinweis:**
Vor v19.0 wurden SAST-, SCA-, IAST- und Penetrationstestdaten nicht erfasst, was zu Unterschieden zwischen der Darstellung in Veracode, Fortify und Invicti und der Darstellung in Application Vulnerability Responseführen kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Dynamische Anwendungssicherheitstests (DAST)**

DAST-Scans finden Schwachstellen in Anwendungen, indem sie Eingaben an Ihre Anwendungen senden und deren Antworten überwachen, während sie ausgeführt werden. Dieser Ansatz kann einen Angriff von außen imitieren. Während des dynamischen Scans wird ein ausgeführter Service (URL) auf Schwachstellen gescannt. Schwachstellenergebnisse enthalten einen URL-Speicherort einer erkannten Schwachstelle.

**Statische Anwendungssicherheitstests (SAST)**

SAST-Scans überprüfen den Quellcode von Anwendungen im Ruhezustand und helfen Ihnen, Schwachstellen in der Art und Weise zu finden, wie Sie Ihren Code geschrieben haben. Der SAST-Scan erfolgt für nicht kompilierten Quellcode und ist daher unabhängig von Anwendungsservices vorhanden. Die zurückgegebenen Ergebnisse umfassen eine Datei und eine Zeilennummer des Speicherorts einer erkannten Schwachstelle.

**Interaktive Anwendungssicherheitstests (IAST)**

IAST-Scans erkennen Softwareschwachstellen durch Interaktion mit dem Programm, während es ausgeführt wird. Beobachtung durch Menschen, automatisierte Tests und Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren und Schwachstellen zu lokalisieren.

**Software Composition Analysis (SCA)**

Ab v19.0 von Vulnerability Responsekönnen Sie SCA-Schwachstellen (Software Composition Analysis) erfassen. SCA-Schwachstellendaten in helfen Ihnen, Schwachstellen in der Open Source-Software zu identifizieren, die in Ihren Softwareanwendungen verwendet wird.

**Penetrationstests**

Sie konfigurieren Penetrationstest-Bewertungsanforderungen in Application Vulnerability Response, um nachzuvollziehen, wo Ihre Anwendungsschwachstellen liegen und was Sie tun können, um sie zu beheben.

**Software-Stückliste**

Laden Sie Software Bill of Materials (SBOM) Daten hoch, um Schwachstellen in Ihren Open Source-Komponenten zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

## Anwendungsfälle

Einige der folgenden DAST-Anwendungsfälle werden unterstützt:

- Verknüpfen Sie jede Schwachstelle aus Scan-Ergebnissen mit einer Art cmdb_ci (untergeordnete Klasse).
- Verknüpfen Sie DAST-Scan-Ergebnisse mit einer vorhandenen Anwendung, wenn ein Datensatz in CMDB von Discovery oder einer Drittanbieterintegration vorhanden ist.
- Verknüpfen Sie das DAST-Scan-Ergebnis mit einer neu eingefügten gescannten Anwendung, wenn eine neue Anwendung zuvor nicht identifiziert und/oder in der CMDB gespeichert wurde.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie Ihre Anwendungen in einem anderen Produkt als ServiceNow®verwalten.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie sie zuvor für einen anderen Zweck angepasst haben.
- Erstellen Sie eine Anwendung für das Quellcode-Repository manuell.

Einige der unterstützten SAST-Anwendungsfälle werden unterstützt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verknüpfen Sie jede Schwachstelle aus Scan-Ergebnissen mit einer Art cmdb_ci (untergeordnete Klasse).
- Erstellen Sie manuell ein CI für das Quellcode-Repository.
- Speichert SAST-Scan-Ergebnisse ohne zugehörigen Anwendungsservice.

[store-future: BEGIN review]Einige der folgenden IAST-Anwendungsfälle werden unterstützt:[End]

[store-future: BEGIN review]Einige der unterstützten SCA-Anwendungen werden unterstützt:[End]

## Integrationen von Drittparteien

Die von Application Vulnerability Response unterstützten Drittanbieterintegrationen sind als separate Anwendungen in der ServiceNow Storeverfügbar. Weitere Informationen finden Sie unter Integration von Application Vulnerability Response mit anderen Anwendungen.

## Schlüsselfunktionen

- Eine gemeinsam genutzte API importiert DAST-, SAST-, IAST-und SCA-Daten sowie manuelle Pen-Testergebnisse. Weitere Informationen finden Sie unter Penetrationstests.
- Eine separate API wird zum Importieren von SBOM-Daten verwendet. Weitere Informationen finden Sie unter Software Bill of Materials erkunden und Veracode Vulnerability Integration.

**CI-Suchregeln**

Anwendungsdaten automatisch nach Übereinstimmungen in Configuration Management Database (CMDB)durchsuchen.

**Zuweisungsregeln**

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Benutzergruppen, Benutzergruppenfeldern und Skripts zu.

**Risikorechner**

Priorisieren und bewerten Sie die Auswirkung von AVIs automatisch mithilfe von Rechnern basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern.

**Schweregradzuordnung**

Anfangswerte für Felder in angreifbaren Anwendungselementen automatisch berechnen. Schwachstelleneinträge haben sowohl einen Quellschweregrad als auch einen normalisierten Schweregrad (basierend auf der Schweregradzuordnung). Der Schweregrad ist an die Common Weakness Enumeration (CWE) gebunden.

**Korrekturzielregeln**

Definieren Sie den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Anwendungselements.

**Reporting**

Erhalten Sie schnell Einblick in Ihre Sicherheitslage, Fehlerkorrekturtrends und die 10 wichtigsten Anwendungen oder Geschäftsbereiche mit den wichtigsten AVIs.

Der gemeinsame Punkt für beide Arten von Scans ist das Anwendungs-Release. Ein Anwendungs-Release, das eine **Namenszeichenfolge** definiert, ist der Verbindungspunkt, um die gescannten Schwachstellenergebnisse auf der Scanner-Seite zu gruppieren. Auf



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Weise weiß AVR, zu welchem Anwendungs-Release die Ergebnisse gehören, wenn Scan-Ergebnisse über die Integration importiert werden.

Die untergeordnete Configuration Item-Tabelle [cmdb_ci], Gescannte Anwendungen [sn_vul_app_scanned_application], wurde in der Anwendung und im Bereich Vulnerability Response erstellt. Diese Tabelle speichert die Abstraktion des Anwendungs-Release und bietet Servicegrafiken über ihre CMDB-Beziehungen. Sie können im angezeigt werden **Alle** > **Application Vulnerability Response** > **Administration** > **Anwendungen** -Modul. Die Listenansicht für gescannte Anwendungen enthält die **Abteilung** und die **Supportgruppe**, die während des Setups hinzugefügt wurden.

### Angreifbare Anwendungselemente (AVIs)

Bei Anwendungsschwachstellen verknüpft AVR eine Schwachstelle mit einer Anwendung, um den Datensatz des angreifbaren Elements (AVI) der Anwendung zu erstellen. Aufgrund der mehreren Definitionen dessen, was eine Anwendung in der CMDB ausmacht, beschränkt Application Vulnerability Response Anwendungen auf gescannte Anwendungen. Gescannte Anwendungen sind die in Ihrer Umgebung gescannten Anwendungen, die von AVR als **Name** und **ID**identifiziert werden. **AVIs** basieren auf der letzten Scan-Zusammenfassung, bis sie vom Scanner bestätigt wird. Wenn eine AVI nicht mehr gefunden wird, bleibt sie an die Scan-Zusammenfassung gebunden, in der sie zuletzt angezeigt wurde.

Angreifbare Anwendungselemente können im angezeigt werden **Alle** > **Application Vulnerability Response** > **Schwachstellen** > **Angreifbare Elemente** -Modul.

Wenn eine Anwendung aus der CMDB entfernt wird, werden alle zugehörigen AVIs geschlossen.

Weitere Informationen zu AVI-Formularfeldern finden Sie unter Felder für angreifbares Anwendungselement.

### Benutzergruppen und Rollen in Application Vulnerability Response

Häufig arbeitet ein Team zusammen, um Anwendungsschwachstellen zu erstellen, zu verwalten und zu überwachen. Unter den Teammitgliedern gibt es strategische Rollen sowie operative Rollen. In den meisten Organisationen nehmen Sie an mehr als einer Rolle teil und teilen sich häufig Rollen mit anderen. Application Vulnerability Response verwendet drei Benutzergruppen mit granularen Rollen: App-Sec-Manager, Application Security Champion und Developer. Weitere Informationen zu diesen Gruppen und Rollen finden Sie unter Application Vulnerability Response -Benutzergruppen und -Rollen.

### Application Vulnerability Response Status

Application Vulnerability Response bietet ein Statusmodell für den Status Ihrer angreifbaren Elemente (AVIs) und hilft Ihnen zu bestimmen, wann und wie Ihre AVIs korrigiert werden müssen.

Ein angreifbares Anwendungselement hat mehrere mögliche Status. Weitere Informationen finden Sie unter Status des angreifbaren Elements in der Anwendung (AVI)..

## Application Vulnerability Response konfigurieren

Bevor Sie Application Vulnerability Response in Ihrer Instanz von Now Platform ] ausführen, müssen Sie sie konfigurieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Application Vulnerability Response konfigurieren

Führen Sie vor der Konfiguration die folgende Setup-Prüfliste aus.

### Vorbereitungen

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Performance Analytics for Vulnerability Response installiert und aktiviert ist, um Application Vulnerability Response -Berichte anzuzeigen. | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren und konfigurieren Sie die Anwendung Performance Analytics for Vulnerability Response [PA].. |
| Vergewissern Sie sich, dass Veracode Vulnerability Integration installiert, aktiviert und konfiguriert ist. [Führen Sie die Integrationen zu diesem Zeitpunkt noch nicht aus.] | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter ServiceNow Vulnerability Response Integration with Veracodeinstallieren. |
| Version 14.0: Vergewissern Sie sich, dass Fortify Vulnerability Integration installiert, aktiviert und konfiguriert ist. [Führen Sie die Integrationen zu diesem Zeitpunkt noch nicht aus.] | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| | Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter ServiceNow Vulnerability Response Integration with Fortifyinstallieren und Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration. |
| Stellen Sie sicher, dass die CWE 2000-Integration in Vulnerability Responseausgeführt wird. | Informationen zur Überprüfung finden Sie unter Vergewissern Sie sich, dass die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird. |
| [Optional] Stellen Sie sicher, dass die NVD-Integration in Vulnerability Responseausgeführt wird. | Informationen zur Überprüfung finden Sie unter Vergewissern Sie sich, dass die regelmäßige Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer den folgenden Benutzergruppen zu: App-Sec Manager, Security Champion und Developer. Weitere Informationen zu Gruppenrollen finden Sie unter, Application Vulnerability Response -Benutzergruppen und -Rollen.<br>• Die App-Sec-Manager-Gruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.<br>**Hinweis:** Die KonfigurationApplication Vulnerability Response ist nicht über die Funktion „Setup-Assistent“ in Vulnerability Responseverfügbar. |



Erforderliche Rolle: Benutzergruppe „App-Sec-Manager“.

### Prozedur

1. Navigieren zu **Security Operations** > **CMDB** > **Suchregeln**.
   Informationen zum Erstellen oder Ändern von CI-Suchregeln für Ihre Umgebung finden Sie unter Erstellen Sie eine CI-Suchregel.
2. Navigieren zu **Application Vulnerability Response** > **Administration**.
3. Wählen Sie **Zuweisungsregeln aus**.
   Informationen zum Erstellen oder Ändern von Anwendungszuweisungsregeln für Ihre Umgebung finden Sie unter Erstellen oder bearbeiten Sie Application Vulnerability Response Zuweisungsregeln.
4. Wählen Sie **Schwachstellenrechner aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erstellen oder Ändern von Anwendungsschwachstellen-Rechnern für Ihre Umgebung finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen.

5. Wählen Sie **Korrekturzielregeln aus**.
   Informationen zum Erstellen oder Ändern von Anwendungskorrekturzielen für Ihre Umgebung finden Sie unter Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur.
6. Wählen Sie **Normalisierte Schweregradzuordnungen aus**.
   Unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu erfahren Sie, wie Sie Schweregradzuordnungen für Ihre Umgebung erstellen oder ändern.
7. Navigieren Sie zu einem der beiden **Veracode Vulnerability Integration** > **Integrationen** oder **Fortify Vulnerability Integration** > **Integrationen**.
8. Öffnen Sie die Veracode-Anwendungslistenintegration oder die Fortify On Demand-Anwendungslistenintegration.
9. Wenn er noch nicht ausgeführt wurde, klicken Sie auf **Jetzt**ausführen.

   **Hinweis:**
   Die anderen Veracode - oder Fortify -Integrationen sind standardmäßig inaktiv.

   Informationen zum Status der Integrationsausführung finden Sie unter, Zeigen Sie den Importausführungsstatus von Veracode Application Vulnerability Integration (Integration von Anwendungsschwachstellen) an oder Zeigen Sie den Importausführungsstatus Fortify Vulnerability Integration an.
10. Sobald die Ausführung von Veracode oder Fortify on Demand abgeschlossen ist, navigieren Sie zu **Application Vulnerability Response** > **Administration** > **Anwendungen**.
11. Geben Sie für jede Anwendung einen Wert für **Supportgruppe** (von Zuweisungsregeln verwendet) und für **Abteilung** (in Berichterstellung verwendet) ein.
    Informationen zum Aktualisieren mehrerer Einträge finden Sie unter Mehrere Datensätze in einer Liste mit dem Listeneditor bearbeiten , um die Aufgabe in einem Massenvorgang abzuschließen.

    **Hinweis:**
    Um den automatisch aktualisierten **Geschäftsbereich anzuzeigen**, aktualisieren Sie die Seite.
    Informationen zu den Feldern des gescannten Anwendungsformulars finden Sie unter, Gescannte Anwendungsfelder.
12. Kehren Sie zur Liste „Integrationen“ zurück, und aktivieren Sie die anderen Veracode - oder Fortify -Integrationen.
    Informationen zum Festlegen der Delta-Datenintegrationsimporte finden Sie unter Aktivieren Sie Application Vulnerability Response Integrations.

    Die Integrationen Veracode und Fortify sind verkettet und werden nacheinander ausgeführt, wenn sie aktiviert werden.
13. **Wahlweise:** Navigieren zu **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**.

    a. **Wahlweise:** Wenn Sie beim Erstellen oder Bearbeiten Ihrer Zuweisungsregeln zuvor **Konfigurationselement: Supportgruppe** für das **Feld Benutzergruppe** ausgewählt haben, können die Werte, die Sie der Listenansicht „Gescannte Anwendungen“ hinzugefügt haben, jetzt verwendet werden.
    Bearbeiten Sie Ihre Zuweisungsregeln entsprechend.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**b.** Klicken Sie auf **Aktualisieren**.

**c.** Klicken Sie in der Listenansicht „Schwachstellen-Zuweisungsregeln“ auf **Änderungen** übernehmen, um die Zuweisungsregeln erneut auf Ihre AVIs anzuwenden.

**14.** Ihre Application Vulnerability Response Konfiguration ist jetzt abgeschlossen.

### Nächste Maßnahme

Navigieren zu **Application Vulnerability Response** > **Übersicht** und im Dashboard von Application Vulnerability Management [PA] finden Sie Informationen zur allgemeinen Sicherheitslage.

### Vergewissern Sie sich, dass die regelmäßige Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird

Verwenden Sie CWE-Datensätze (Common Weakness Enumeration), die aus der CWE-Datenbank heruntergeladen wurden, als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Aktualisieren Sie allgemeine Schwachstellendatensätze aus der Common Weakness Enumeration-Datenbank regelmäßig. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die geplante Aufgabe **CWE Comprehensive 2000 Integration** (CWE Comprehensive 2000-Integration) aus.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

   **Hinweis:**
   Die Einstellungen in diesem Formular werden von Vulnerability Response und Application Vulnerability Responsegemeinsam verwendet. Das Ändern der Integrationseinstellungen erfordert eine Koordination mit und Kenntnisse in Vulnerability Response und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

   **Hinweis:**
   Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in Vulnerability Responsekonfiguriert werden. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

   Wenden Sie sich bei Bedarf an Schwachstellenbibliotheken anzeigen, um die importierten Einträge anzuzeigen.

   Das Feld **Primäre CWE** enthält den CWE-Eintrag. Wenn einer Schwachstelle mehr als eine CWE zugeordnet ist, finden Sie unter Anwendungsschwachstellen-Felder Informationen dazu, wie die primäre CWE bestimmt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vergewissern Sie sich, dass die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird

Identifizieren Sie die Repositorys, die regelmäßig aktualisiert werden sollen. Sie können eine regelmäßige Aufgabe ausführen, um die Datensätze der National Vulnerability Database (NVD) jede Nacht oder wöchentlich zu aktualisieren. Wenn er noch nicht ausgeführt wird, können Sie den Auftrag aktivieren

#### Vorbereitungen

Erforderliche Rollen: App-Sec-Manager-Gruppe

Die NVD-Integration wird standardmäßig täglich montags um 00:00:00 Uhr als regelmäßige Aufgabe ausgeführt.

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen Sie die regelmäßige Aufgabe **NIST National Vulnerability Database** aus.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

   **Hinweis:**
   Die Einstellungen in diesem Formular werden von Vulnerability Response und Application Vulnerability Responsegemeinsam verwendet. Das Ändern der Integrationseinstellungen erfordert eine Koordination mit und Kenntnisse in Vulnerability Response und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

   **Hinweis:**
   Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in Vulnerability Responsekonfiguriert werden. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

   Wenden Sie sich bei Bedarf an Schwachstellenbibliotheken anzeigen, um die importierten Einträge anzuzeigen.

### Aktivieren Sie Application Vulnerability Response Integrations

Aktivieren Sie Application Vulnerability Response Integrationen, um regelmäßige Updates durchzuführen.

#### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Wiederholen Sie diese Schritte nach Bedarf für jede Integration.
   Nach der ersten Ausführung werden die Integrationen verkettet, um Delta-Importe für nachfolgende Ausführungen durchzuführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Exception Management in Application Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Anwendungselement (AVI), das gemäß der Richtlinie nicht behoben werden kann.

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen der Nichtbehebung der Schwachstelle anerkennen und akzeptieren.

**Hinweis:**

Ab v21.0 von Application Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Anwendungselement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

## Lebenszyklus einer Ausnahme

**Definition einer Ausnahme**

Eine Ausnahme ist eine Anforderung, die Korrektur einer AVI für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

**Eine Ausnahme wird angefordert**

Als Entwickler können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine AVI beantragen. Nachdem der Anwendungssicherheitsanalyst diese Anforderung genehmigt hat, wird die AVI in den Status „Zurückgestellt“ **verschoben**.

**Ausnahmeregeln**

Ab v20 können Sie Ausnahmeregeln erstellen, um vorhandene und neue angreifbare Elemente (AVIs) automatisch für einen bestimmten Zeitraum zurückzustellen, wenn sie den Bedingungen der Regel entsprechen. Durch die Verwendung von Ausnahmeregeln zum automatischen Zurückstellen von AVIs wird das Risiko von fehlenden Servicelevel-Vereinbarungen minimiert. Die Regeln können Ihnen bei der Verwaltung mehrerer Elemente helfen, da Sie manuelle Eingriffe vermeiden. Weitere Informationen finden Sie unter Ausnahmeregeln erstellen.

**Fordern Sie eine Verlängerung für eine Ausnahmeregel an**

Ab v20 können Sie eine Verlängerung des Datums „Zurückgestellt **bis** “ einer Ausnahmeregel anfordern. Sie können eine Erweiterung einer Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von Datensätzen, die von der Regel erstellt wurden, nicht **bis** zum Datum „Zurückgestellt bis“ aufgelöst wird, dem Datum, an dem die Korrekturaufgabe keine neuen AVIs mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum Ihrer vorhandenen Regel automatisch verlängert wird. Sie können Daten bis zu einem Jahr nach dem aktuellen Datum eingeben und müssen einen Grund für die Verlängerung angeben. Eine Verlängerungsanforderung erfordert eine zweistufige Genehmigung durch separate Genehmigungsgruppen.

**Eine Ausnahmeanforderung wird genehmigt**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AVIs, die nicht sofort korrigiert werden können, werden von Anwendungssicherheitsanalysten überprüft, auf Risiko bewertet und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Die Genehmigung einer Ausnahmeanforderung kann ein zweistufiger Flow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response.

**Hinweis:**

Nachdem eine Ausnahmeanforderung für eine AVI genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Rufen Sie weitere Details ab

**Nachverfolgung einer Ausnahmeanforderung**

Nach dem Auslösen der Ausnahme können Sie ihren Status mithilfe der Registerkarte „ **Statusänderungsgenehmigungen** “ der AVI nachverfolgen.

**Ablauf einer Ausnahmeanforderung und Anforderung einer Verlängerung einer Ausnahmeregel**

Wenn eine Ausnahmeanforderung für eine bestimmte AVI abläuft, wird die betroffene AVI in den Status „ **Offen** “ zurückgesetzt.

Ab v20 können Sie jedoch eine Anforderung zum Verlängern des Datums für „Zurückgestellt **bis** “ für die Ausnahmeregel senden.

### Konfigurieren Sie Exception Management für Application Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme und fügen Sie der Ausnahme oder falsch positiven Anforderung mithilfe des -Moduls einen Fragebogen hinzu . Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Application Vulnerability Response angefordert. Sie können eine Ausnahme auch mit der GRC: Policy and Compliance Management -Integration anfordern.

**Vorbereitungen**

Erforderliche Rolle: sn_vul.app_manage_exception_configuration

**Warum und wann dieser Vorgang ausgeführt wird**

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Policy and Compliance Management installiert ist, GRC: Policy and Compliance Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Policy and Control-Ziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird dieser an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen Fragebogen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste Ausnahmen verwalten mit auswählen.

   **Hinweis:**
   Ab Vulnerability Response Version 17.1 können Sie entweder Vulnerability Response oder GRC: Policy and Compliance Managementauswählen. Sie müssen das Plugin [ GRC aktivieren, um GRC: Policy and Compliance Management zum Anfordern einer Ausnahme zu verwenden. Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.

3. Füllen Sie die Felder im Formular basierend auf der von Ihnen ausgewählten Option aus.
   - Wenn Sie die Option Vulnerability Response ausgewählt haben, füllen Sie die Felder im Formular aus.

     **Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

     | Feld | Beschreibung |
     |---|---|
     | Dauer | Zeitraum, für den eine Ausnahme angefordert werden kann. |
     | Einheit | Zeiteinheit für den angegebenen Zeitraum. |
     | Fragebogen aktivieren, um Ausnahme anzufordern | Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung. |
     | Fragebogen, um Ausnahme anzufordern | Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Anfordern einer Ausnahme. Der Ausnahmefragebogen wird standardmäßig angezeigt. |
     | Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |
     | Fragebogen, um falsch positive Meldung zu markieren | Option zum Anzeigen des von Ihnen ausgewählten Fragebogens, um ihn als falsch positiv zu kennzeichnen. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt. |

   - Wenn Sie die Option GRC: Policy and Compliance Management ausgewählt haben, füllen Sie die Felder im Formular aus.

     **Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

     | Feld | Beschreibung |
     |---|---|
     | Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Fragebogen, um falsch positive Meldung zu markieren | Option zum Anzeigen des von Ihnen ausgewählten Fragebogens, um ihn als falsch positiv zu kennzeichnen. Der Fragebogen für falsch positive Anforderungen wird standardmäßig angezeigt. |

4. Wählen Sie **Speichern**.

### Konfigurieren Sie Genehmigungsregeln für Exception Management

Verwenden Sie ab Application Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Meldungen zu genehmigen. Wenn Sie Application Vulnerability Response (AVR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie bereits VR-Benutzer sind, lautet die Standardoption workflow.
Wenn Sie Application Vulnerability Response v15.0 oder höher bereitgestellt haben, wird der Wert der Systemeigenschaft *sn_vul.flow_designer_activation* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Application Vulnerability Response bereits vor v15.0 verwenden, wird der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

**Hinweis:**
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Anwendungselemente
- Ausnahmeregel
- Falsch positive Werte für Korrekturaufgaben
- Falsch positiv für angreifbare Anwendungselemente

**Hinweis:**
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

#### Formular „Genehmigungsregel“

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Tabelle | Tabelle, auf die die Regel angewendet wird. |
| Anwendung | Der Standardwert ist Vulnerability Response. |
| Regeltyp | Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, Falschmeldungen oder Ausnahmeregel. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungsregeln. |
| Ablaufdatum der Genehmigung (Tage)<br><br>Ab v21.0 von Application Vulnerability Response | Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann. |
| Genehmiger benachrichtigen (Tage)<br><br>Ab v21.0 von Application Vulnerability Response | Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen. |

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren.

**Hinweis:**
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen.

**Example:**
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden wurden.

#### Korrektur in wird zurückgestellt Application Vulnerability Response

Ab v20.0 können Sie die Fehlerkorrektur mit dem Status „ **Warten auf Implementierung** “ zurückstellen, der für angreifbare Anwendungselemente (AVI) und Korrekturaufgaben verfügbar ist, während sie ihre Lebenszyklen durchlaufen. Sie können Datensätze nur manuell in diesen Status überführen, indem Sie **„Warten auf Implementierung“** aus AVI und Korrekturaufgabendatensätzen im Status „Wird **untersucht** “ auswählen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Anwendungsfall

Als Fehlerkorrekturspezialist können Sie einen Datensatz in „ **Warten auf Implementierung** “ verschieben, um Ihrem Team mitzuteilen, dass Ihre Recherche und Arbeit an einer Aufgabe abgeschlossen ist. Sie können dieses Update auswählen, wenn Sie feststellen, dass ein Fix zur Implementierung bereit, aber nicht verfügbar ist. Ein Beispiel für eine nicht verfügbare Korrektur ist ein Software-Patch. Wenn das Wartungsfenster für einen Patch nach Abschluss Ihrer Recherche nicht verfügbar ist, können Sie die Aufgabe in den Status „ **Warten auf Implementierung** “ verschieben, bis der Patch bereitgestellt werden kann.

## Pflichtfelder

Es gibt zwei erforderliche, bearbeitbare Felder in den AVI- und Korrekturaufgaben-Datensätzen, die sich im Status „Warten auf Implementierung“ befinden:

**Datum der Korrekturzusage**

Das geplante Korrekturdatum.

**Korrekturplan**

Die Beschreibung des Korrekturplans für die Korrektur. Dieser Text wird in den Notizen im Datensatz angezeigt.

## Felder und Systemeigenschaften

Es gibt zwei Systemeigenschaften, die standardmäßig auf „ `true` “ für das Dialogfeld festgelegt sind, das angezeigt wird, wenn Sie einen Datensatz in den Status „ **Warten auf Implementierung**“ überführen. Wenn sie in den Standardeinstellungen belassen werden:

**sn_vul.remediation_fields**

Legt **das Datum** der Korrekturzusage und den **Korrekturplan** als Pflichtfelder fest. Bei „ `false`“ sind diese Felder optional.

**sn_vul.waiting_implementation**

**Zeigt**das **Modal** mit den Feldern Korrekturzusagedatum und Korrekturplan an, nachdem Sie **Warten auf Implementierung** für einen Datensatz ausgewählt haben. Bei `false`können Sie den Status einer AVI in „Warten auf Implementierung“ ändern, ohne zur Eingabe eines Zusagendatums oder eines Plans aufgefordert zu werden.

## Modul „Datum der Korrekturzusage versäumt“.

Zeigen Sie im Modul „ **Datum** der Korrekturzusage“ alle AVIs an, die ihre Daten der Korrekturzusage verpasst haben. Navigieren **Application Vulnerability Response** > **Angreifbare Elemente** > **Datum der Korrekturzusage vergangen** , um die Liste anzuzeigen.

## Status-Rolldown von Korrekturaufgaben zu AVIs

Die UI-Aktionsschaltfläche zum Überführen eines Datensatzes in **„Warten auf Implementierung“** ist nur für Datensätze für angreifbare Anwendungselemente und Korrekturaufgaben im Status „Wird **untersucht** “ sichtbar. Für den Status-Rolldown gibt es im modalen Fenster, das angezeigt wird, wenn Sie „ **Warten auf Implementierung** “ für eine Korrekturaufgabe auswählen, die Option **Vorhandene AVIs überschreiben**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| Wählen Sie **Vorhandene AVIs überschreiben aus**. | Wählen Sie diese Option aus, um die Daten der Korrekturzusage zu überschreiben und alle vorhandenen AVIs in der Aufgabe zu überschreiben, die sich bereits im Status „ **Warten auf Implementierung** “ befinden.<br><br>Wenn diese Option ausgewählt ist, werden die Datums- und Plandaten der Korrekturaufgabe per Rolldown in die AVIs übertragen. |
| Lassen Sie **Vorhandene AVIs überschreiben** deaktiviert. | Lassen Sie die Option deaktiviert, um die Datums- und Planwerte für vorhandene AVIs für die Aufgabe zu erhalten, die sich bereits im Status „ **Warten auf Implementierung** “ befinden.<br><br>Wenn diese Option deaktiviert ist, behalten AVIs, die sich bereits im Status „ **Warten auf Implementierung** “ befinden, ihre vorhandenen Datums- und Plandaten bei und sind nicht vom Status-Rolldown betroffen. |

## Rolldown-Beispiele

Angenommen, Sie möchten eine Korrekturaufgabe von **Offen** zu **Warten auf Implementierung umstellen**, damit Sie das Zusagedatum und die Planinformationen der Aufgabe für ein Softwarepatch-Wartungsfenster aktualisieren können. Angenommen, in dieser Aufgabe ist eine AVI mit dem Status „ **Warten auf Implementierung** “ vorhanden, und Sie möchten das Zusagedatum und die Planinformationen entsprechend der Korrekturaufgabe aktualisieren.

Um die Datums- und Plandaten der AVIs zu überschreiben, damit sie der Korrekturaufgabe entsprechen, aktivieren Sie das Kontrollkästchen **Vorhandene AVIs überschreiben**, wenn Sie dazu aufgefordert werden. Die Datums- und Planwerte der AVI werden zu den Plan- und Datumswerten, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie **Awaiting Implementation**(Warten auf Implementierung) auswählen.

Wenn Sie in diesem Fall die Überschreibungsoption nicht auswählen und eine AVI in **Warten auf Implementierung**vorhanden ist, bleiben die ursprünglichen Datums- und Plandaten in der AVI unverändert. Die Plan- und Datumswerte, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie „ **Warten auf Implementierung** “ auswählen, werden nicht für AVIs verwendet, die sich bereits im Status „ **Warten auf Implementierung** “ in der Aufgabe befinden.

Wenn sich eine AVI für eine Aufgabe im Status „ **Gelöst** “ oder „ **Geschlossen – behoben** “ befindet und Sie die Aufgabe in den Status „ **Warten auf Implementierung**“ überführen, werden durch Auswahl von **Vorhandene AVIs überschreiben die AVIs aufgrund einer höheren Statusrangfolge** nicht von „ **Geschlossen – behoben** “ und „ **Gelöst** “ zu „ **Warten** auf Implementierung“ geändert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Überschreiben beim Verschieben der Aufgabe in „ **Warten auf Implementierung** “ nicht ausgewählt ist und bereits eine AVI in „ **Warten auf Implementierung** “ vorhanden ist und Sie die Aufgabe zurück in den Status „ **Offen** “ oder „Wird **untersucht**“ verschieben, bleibt die AVI in **„Warten auf Implementierung“**.

### Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response

Fügen Sie den Genehmigergruppen Benutzer hinzu, damit Sie eine Ausnahme anfordern können.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.app_exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

Eine Ausnahmeanforderung für ein angreifbares Anwendungselement wird mit dem standardmäßigen zweistufigen Genehmigungs-Flow genehmigt. Die Anforderung kann von zwei Genehmigerebenen genehmigt werden. Das Hinzufügen von Benutzern zur Gruppe der ersten Ebene ist obligatorisch. Wenn sich keine Benutzer auf der zweiten Ebene befinden, wird die Anforderung nach der Genehmigung auf der ersten Ebene genehmigt.

#### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.
2. Suchen Sie in der Spalte Name nach **Exception**(Ausnahme) und klicken Sie auf Ausnahmegenehmiger für **Anwendungen – Ebene 1**.

   **Hinweis:**
   Ab Application Vulnerability Response v12.8.1 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie `sn_vul.app_exception_approver_L1`, `sn_vul.app_exception_approver_L2`oder `sn_vul.app_false_positive_approver_group`, um den Eigenschaftswert zu ändern.
3. Klicken Sie im Formular „Gruppenanwendungsausnahmegenehmiger – Ebene 1“ auf die zugehörige Liste Gruppenmitglieder.
4. Klicken Sie auf **Neu**, um eine Liste zu erstellen.
5. Füllen Sie die Felder des Formulars aus.

**Benutzerformular**

| Feld | Beschreibung |
|---|---|
| Anwender-ID | Eindeutiger Bezeichner für den Benutzer |
| Vorname | Vorname des Benutzers. |
| Nachname | Nachname des Benutzers. |
| Titel | Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus. |
| Abteilung | Abteilung des Benutzers. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Passwort | Dem Benutzer zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder temporär sein. |
| Passwort muss zurückgesetzt werden | Option, mit der Benutzer das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten. |
| Gesperrt | Option, um den Benutzer für die Instanz zu sperren und alle aktiven Sitzungen des Benutzers zu beenden. Das System verhindert, dass Benutzer mit der Administratorrolle sich selbst aussperren. |
| Aktiv | Option zum Aktivieren dieses Anwenders. Nur Sie können einen inaktiven Benutzer in diesen Bereichen sehen:<br>○ Listen der Benutzer<br>○ Auswahlliste für Referenzfelder (Lupensymbol)<br>○ Autovervollständigen-Liste, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben |
| Nur Webservice-Zugang | Option, um diesen Benutzer als nicht interaktiven Benutzer festzulegen. |
| Interner Integrationsbenutzer | Option zum Festlegen dieses Benutzers als internen Integrationsbenutzer. |
| E-Mail | E-Mail-Adresse des Benutzers. |
| Sprache | Bevorzugte Sprache des Benutzers. |
| Kalenderintegration | Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook. |
| Zeitzone | Zeitzone für den Standort dieses Benutzers. |
| Datumsformat | Bevorzugtes Datumsformat des Anwenders. |
| Telefon (geschäftlich) | Geschäftliche Telefonnummer des Benutzers. |
| Mobiltelefon | Mobiltelefon des Benutzers. |
| Foto | Foto, das Sie hochladen können, indem Sie **auf Hinzufügen klicken... klicken**. |



6. Klicken Sie auf **Absenden**.
7. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 5, um eine Anwendungsausnahme zu erstellen – Ebene 2. Der Genehmiger muss zu **Application Vulnerability Response** > **Meine Genehmigungen** navigieren und Anforderungen genehmigen.

### Ausnahmen in anfordern und genehmigen Application Vulnerability Response

Sie können anfordern, dass die Korrektur eines angreifbaren Anwendungselements und einer Korrekturaufgabe für einen bestimmten Zeitraum zurückgestellt wird.

Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen von anderen Benutzern genehmigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auch Ausnahmeregeln erstellen und eine Ausnahmeverlängerung für eine Ausnahmeregel anfordern. Standardmäßig sind für Zurückstellungen, Ausnahmeregeln und Ausnahmeverlängerungsanforderungen zwei Genehmigungsebenen erforderlich.

Informationen zum Anfordern oder Genehmigen einer Ausnahme finden Sie unter:

- Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an
- Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Policy and Compliance Management
- Genehmigen Sie Ausnahmeregeln und Erweiterungsanforderungen für Ausnahmeregeln in Application Vulnerability Response
- Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Application Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Anwendungselement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an

Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

#### Vorbereitungen

Erforderliche Rolle: Entwicklergruppe

#### Prozedur

1. Navigieren zu **Application Vulnerability Response** > **Angreifbare Anwendungselemente** > **Alle** und wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „Wird untersucht“ befinden.

   **Hinweis:**

   Ab Version 21.0 von Application Vulnerability Responsewird der vorherige Status eines angreifbaren Anwendungselements im Feld **„backup_state“** gespeichert.

2. Klicken Sie im Formular „Angreifbares Anwendungselement“ auf **Ausnahme anfordern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Abhängig davon, ob Vulnerability Response oder GRC: Policy and Compliance Management in ausgewählt ist **Application Vulnerability Response** > **Ausnahmenverwaltung** Im Bildschirm „“ ändert sich das Formular „Ausnahme anfordern“. Wenn GRC: Policy and Compliance Management, siehe Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Policy and Compliance Management.

3. Wenn Vulnerability Response im Bildschirm „Exception Management“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der im ausgewählten Zeitraum liegen **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** -Bildschirm.<br><br>Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „ **Offen** “ zurück.<br><br>**Hinweis:**<br>Ab Version 18.0 von Application Vulnerability Response (AVR) kann ein zurückgestelltes angreifbares Anwendungselement von einem Scanner geschlossen und erneut geöffnet werden. Wenn das Element vor Ablauf des Ausnahmefensters erneut geöffnet wird, wird der Status der AVIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ zurückgesetzt. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_avit_in_active_exception_window auf true fest. Außerdem bleibt das zurückgestellte Bis-Datum bestehen, auch nachdem die AVIT geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle ist sn_vul.app_manage_exception_configuration für Lese- und Schreibvorgänge. |
| Grund | Wählen Sie den **Grund aus**. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Behebung nicht verfügbar<br>○ Ausgleichende Steuerung vorhanden<br>○ Sonstige |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Informationen zum Hinzufügen neuer Gründe finden Sie unter Definieren Sie die Ursachenzuordnung für Richtlinien. |
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer aktualisiert werden. |

4. Klicken Sie auf **Genehmigung anfordern**, um die Ausnahmeanforderung zu übermitteln.
   Der Status des angreifbaren Anwendungselements ändert sich in Wird überprüft. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

### Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Policy and Compliance Management

Fordern Sie Richtlinienausnahmen mit der Funktion GRC zur Verwaltung von Richtlinienausnahmen in der Anwendung Policy and Compliance Management aus Application Vulnerability Responsean.

## Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Policy and Compliance Management aus dem ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_Besitzer

Sie können Ausnahmen auch in der klassischen Benutzeroberfläche anfordern:

## Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (oder **Korrekturaufgaben**)>**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme anfordern**.
3. Wenn GRC: Policy and Compliance Management im Bildschirm „Exception Management“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

### Formular „Ausnahme anfordern“.

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |
| Kontrollziel | Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und sich der Status des angreifbaren Elements oder |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ ändert.<br><br>**Hinweis:**<br>Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in Policy and Compliance festgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen . |
| Grund | Grund für die Anforderung einer Ausnahme. |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden. |

**a.** Klicken Sie auf **Genehmigung anfordern**, um die Ausnahmeanforderung zu übermitteln. Der Status der angreifbaren Elemente ändert sich in Wird überprüft, und eine Richtlinienausnahme wird erstellt. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

**b.** Klicken Sie auf die zugehörige Liste Richtlinienausnahmen, um die Richtlinienausnahme anzuzeigen.

**c.** Klicken Sie auf die Nummer der Richtlinienausnahme.

**d. Wählen Sie** im Feld Genehmiger den Namen des Genehmigers aus.

**e.** Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

**f.** Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie im Feld Risikobewertung die **Risikobewertung** aus.

**g.** Speichern Sie das Formular.

**h.** Klicken Sie auf die Registerkarte Betroffene Steuerungen, und klicken Sie auf Hinzufügen, um die Steuerungen hinzuzufügen.

**i.** Speichern Sie das Formular.

**Hinweis:**
Sie können eine Compliance-Überprüfung durchführen, indem Sie auf **Compliance-Überprüfung anfordern**klicken.

**j.** Das Genehmigungsformular wird an den Genehmiger gesendet.

**k.** Als Genehmiger können Sie entweder die Anforderung genehmigen, indem Sie auf **Genehmigen klicken**, oder eine zusätzliche Genehmigung anfordern, indem Sie auf **Zusätzliche Genehmigung**anfordern klicken.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datensatzstatus ändert sich in „Zurückgestellt“. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte Zurückstellung enthält zusätzliche Hinweise zum Datensatz.

**Hinweis:**
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

4. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management .

### Fordern Sie eine Ausnahme für eine Anwendungskorrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Anwendungskorrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

#### Vorbereitungen

Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Erforderliche Rollen: sn_vul.remediation_owner, sn_vul.app_security_changion oder sn_vul_container.remediation_owner.

Sie können auch Ausnahmen für Anwendungskorrekturaufgaben in der klassischen Umgebung anfordern.

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Wählen Sie im Datensatz der Anwendungskorrekturaufgabe die **Option Ausnahme anfordern**aus.
4. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist. |
| Grund | Begründung für die Anforderung einer Ausnahme. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden. |

5. Klicken Sie auf **Genehmigungs-Engine**.

### Genehmigen Sie Ausnahmeregeln und Erweiterungsanforderungen für Ausnahmeregeln in Application Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Anwendungselemente, die nicht sofort korrigiert werden können. Sie müssen diese Anforderungen auf Risiken bewerten und sie dann zur Zurückstellung genehmigen, bis sie korrigiert werden können.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.app_exception_approver

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

### Definieren Sie die Ursachenzuordnung für Richtlinien

Sie können die Grundoptionen so definieren, dass sie jedem Benutzer zur Verfügung stehen, der eine Ausnahme anfordert.

#### Vorbereitungen

Die Anwendung GRC: Policy and Compliance Management muss installiert sein. Diese Anwendung ist über den ServiceNow® Store mit einem separaten Abonnement verfügbar.

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

Erforderliche Rolle: sn_vul.compliance.manager und sn_vul.vulnerability_admin

#### Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

   **Hinweis:**
   Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung für Ihre Anwendung, z. B. **Application Vulnerability Response**, **Vulnerability Response**usw.
3. Führen Sie die folgenden Schritte aus, um eine vorhandene Grundauswahl hinzuzufügen:
   a. Klicken Sie in der Liste Grundauswahl auf **Neu**.
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Führen Sie die folgenden Schritte aus, um der Tabelle „Grundauswahlmöglichkeiten“ neue Gründe hinzuzufügen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie in der Liste Grundauswahl auf **Neu**.

**b.** Klicken Sie auf das Lupensymbol.

**c.** Klicken Sie auf **Neu**.

**d.** Füllen Sie die Felder des Formulars aus.

**Formular „Grundauswahlliste“**

| Feld | Beschreibung |
|---|---|
| Bezeichnung | Eindeutige Bezeichnung für diese Auswahl. |
| Wert | Eindeutiger Wert für diese Auswahl.<br><br>Dieser Wert wird in der Tabelle „Richtlinienausnahme – Grundzuordnungen“ für die entsprechenden Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_vul_policy_reason_mapping.LIST ein. |
| Bestellung | Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert. |
| Standard | Option, um anzugeben, dass diese Grundauswahl immer dann verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, sind alle Grundoptionen verfügbar, für die das Feld **Standard** ausgewählt ist. |
| Aktiv | Option zum Anzeigen der Auswahl in der Liste der Grundoptionen. |

**5.** Klicken Sie auf **Absenden**.

### Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie ihr Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen
Erforderliche Rollen: App-Sec Manager sn_vul.app_sec_manager, Security Champion sn_vul.app_security_change.

#### Warum und wann dieser Vorgang ausgeführt wird
In einem Verlängerungsregel-Datensatz können Sie nur dann eine Verlängerung für das Datum „ **Zurückgestellt bis** “ anfordern, wenn sich die Regel im Status „ **Genehmigt** “ befindet. Sie können diese Erweiterung einer Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von Datensätzen, die von der Regel erstellt wurden, nicht **bis** zum Datum „Zurückgestellt bis“ aufgelöst wird, dem Datum, an dem die Korrekturaufgabe keine neuen AVIs mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum Ihrer vorhandenen Regel automatisch verlängert wird.

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein.<br>Zur Auswahl stehen:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder „Zurückgestellt bis“, „Grund“ und „Zusätzliche Informationen“ für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Anwendungselemente aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

## Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie ihr zurückgestelltes Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Anwendungselemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Anwendungselemente sollten sich jedoch im Status „Zurückgestellt“ befinden und ihre aktuellen „Bis“-Daten vor dem „Aktualisiert bis“-Datum liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement in an Application Vulnerability Response

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement an, bevor das Fälligkeitsdatum erreicht ist. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

### Prozedur
1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Anwendungselement.
3. Wählen Sie **Verlängerung anfordern aus**.

   **Hinweis:**
   Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Anwendungselements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Anwendungselements erweitert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Nach der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   **Hinweis:**
   - Die Anforderung durchläuft zwei Genehmigungsstufen.
   - Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Notizen für Bis, Grund und Zurückstellung aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen, löschen und stornieren Sie eine Ausnahmeregel für Application Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für angreifbare Anwendungselemente (AVI) anzufordern, die bestimmte Bedingungen erfüllen.

#### Vorbereitungen

Sie können beispielsweise eine Regel mit einer Bedingung erstellen, die auf einer bestimmten bekannten oder kritischen Schwachstelle basiert, von der Sie wissen, dass Sie sie nicht sofort beheben kann. Mit dieser Regel können Sie neue und vorhandene AVIs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

- Die Ausnahmeregel wird ab dem Datum **Gültig ab** bis zum Datum **Gültig bis** angewendet, das Sie im Regeldatensatz eingegeben haben.
- Die Korrekturaufgabe (AVUL) wird erstellt, nachdem die Regel für übereinstimmende **AVIs** im Status „Zurückgestellt“ genehmigt wurde.
- Die Gruppierungsmethode für diese AVUL wird als Ausnahmeregeln bezeichnet.
- Sie können diese AVUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete AVIs werden zurückgestellt und dieser AVUL ab dem **Gültig-ab** -Datum hinzugefügt, bis die Gruppe am **Gültig-bis** -Datum abläuft.

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann zur Genehmigung erneut übermitteln.

Erforderliche Rollen: App SEC Manager sn_vul.app_sec_manager und Security Champion sn_vul.app_security_change.

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Wählen Sie auf der Seite „Ausnahmeregel für neuen Datensatz“ die Option **Neu**aus.
3. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Ausnahmeregel. |
| Status | Schreibgeschützt: Entwurf |
| Gültig ab | Datum, ab dem diese Regel zum Zurückstellen von AVIs aktiv ist. |
| Ausführungsbefehl | Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert hat Vorrang vor einem höheren. |
| Gültig bis | Datum, an dem die Korrekturaufgabe die Annahme neuer AVIs beendet. |
| Zurückgestellt bis | Datum, bis zu dem die Korrekturaufgaben und AVIs zurückgestellt werden. An diesem Datum werden |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | die AVULs geschlossen, und alle AVIs werden aus den Aufgaben entfernt und erneut geöffnet. Gruppenregeln werden erneut auf diese AVIs angewendet. |
| Grund | Grund für die Erstellung dieser Ausnahmeregel. |
| Zuweisungsgruppe | Gruppe, der die Korrekturaufgabe für die Nachverfolgung der zurückgestellten AVIs zugewiesen ist. |
| Zusätzliche Informationen | Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen. |
| Bedingung | Filterbedingungen, um anzugeben, welche AVIs dieser Regel entsprechen. |
| Für vorhandene Daten ausführen | Option, mit der Sie diese Regel für vorhandene Daten ausführen können, wenn sie zum ersten Mal ausgeführt wird.<br><br>Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der regelmäßigen Aufgabe *Associate existing AVIs with Auto Exception Rule* ausgeführt, beginnend mit neuen Daten.<br><br>Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten am **Gültig ab** -Datum ausgeführt. |

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Wählen Sie einen aus.

   Nachdem die Regel genehmigt wurde, wird sie in den Status **„Genehmigt“** versetzt. Ihre Regel wertet AVIs mit dem Auftrag *Associate existing AVIs with Auto Exception Rule scheduled* aus. Wenn Sie Für **vorhandene Daten**ausführen ausgewählt haben, werden vorhandene AVIs ausgewertet. Für die Regel wird automatisch eine Korrekturaufgabe erstellt, und alle übereinstimmenden AVIs, die ihre Bedingungen erfüllen, werden der Aufgabe zugeordnet.

   Die regelmäßige Aufgabe führt die Ausnahmeregel einmal für vorhandene Daten aus. Die Regel wird für vorhandene Daten nicht erneut ausgeführt, auch wenn keine AVIs gefunden werden. Es werden nur neue Daten ausgewertet, da die vorhandenen AVIs, die der Regel entsprechen, bereits zurückgestellt wurden.

6. Um eine Regel zu löschen, wählen Sie im Datensatz der Ausnahmeregel die Option **Löschen** aus. Die folgende Meldung wird angezeigt: Wenn Sie die Regel löschen, wird die zugeordnete Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen AVIs angewendet, und die Ausnahmeregel wird gelöscht.

7. Wählen**Sie Regel** beibehalten, um anzuhalten, oder **Regel löschen**, um fortzufahren.
8. Um eine Regel zu deaktivieren, sie jedoch in der Liste der Ausnahmeregeln zu belassen, wählen Sie **Abbrechen**.
   Die folgende Meldung wird angezeigt: Wenn Sie diese Regel abbrechen, wird die zugeordnete Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen angreifbaren Elemente angewendet, und die Ausnahmeregel wird in den Status „Entwurf“ verschoben.
9. Wählen**Sie Regel** beibehalten, um anzuhalten, oder **Abbrechen**, um die Regel in den **Entwurfsstatus** zu verschieben und zu deaktivieren.

### Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln

Konfigurieren Sie Korrekturaufgaben (AVULs), um Analysten und Korrekturspezialisten bei der Organisation und Massenanalyse von angreifbaren Elementen in Anwendungen (AVI) zu unterstützen. Die Kriterien, nach denen Korrekturaufgaben gebildet werden, sind so konfiguriert, dass AVIs automatisch Korrekturaufgaben zugewiesen werden. Mithilfe von Korrekturaufgaben können Sie den Fortschritt überwachen und den Korrekturprozess effizienter gestalten.

## Nachverfolgung der Zurückstellungsanzahl für angreifbare Anwendungselemente und Korrekturaufgaben

Verfolgen Sie nach, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Containerelement oder eine Korrekturaufgabe zurückgestellt wurde. Die geplante Aufgabe `set deferral counts` wird täglich ausgeführt, um Anzahlen für die Datensätze zu veröffentlichen, die mehr als einmal in der Spalte Zurückstellungsanzahl zurückgestellt wurden. Datensätze werden in den Modulen für mehrere Zurückstellungen für VR, AVR und CVR angezeigt.

## Grundlegendes zu Regeln für Korrekturaufgaben

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Anwendungselemente automatisch gruppiert und zugewiesen werden. Eine Standardregel **Schwachstelle** ist im Basissystem enthalten, das AVIs basierend auf ihren Schwachstellen erfasst. Sie können jedoch nach anderen Wertesätzen in Spalten gruppieren, auf die über die AVI zugegriffen werden kann. Diese Werte können Konfigurationselement (CI), Schwachstelleneintrag und Ähnliches umfassen.

Es gibt Aufgabenregeln für Application Vulnerability Response, die in der Anwendung Vulnerability Response enthalten sind, die verfügbar ist, wenn Sie sie aktivieren.

Sie können mit dem Bedingungsgenerator mehrere Bedingungen erstellen. Nachdem Sie ein Feldpaar festgelegt haben, wird im Abschnitt Gruppieren nach eine weitere Zeile angezeigt. Sie können bis zu sechs **Gruppieren nach-** Auswahlen haben. Sie können die Gruppenzuweisung auch automatisieren. Weitere Informationen finden Sie unter Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu und Filtern innerhalb Vulnerability Response.

Sie können beispielsweise angreifbare Anwendungselemente nach dem Konfigurationselement oder nach dem Produktmodell gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit geringem Schweregrad oder CIs mit geringem Risiko haben. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen haben, die das Unternehmen einem höheren Risiko aussetzen. Unter Erstellen, bearbeiten



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und löschen Sie Application Vulnerability Response Regeln für Korrekturaufgaben finden Sie weitere Informationen zu den Optionen, die Ihnen zur Verfügung stehen.

Ein anderer Satz von Regeln kann für angreifbare Anwendungselemente verwendet werden, die das Unternehmen einem höheren Risiko aussetzen. Der Name der Korrekturaufgabe wird an die Korrekturaufgabenregel Gruppieren **nach** Werten angehängt, um die Kurzbeschreibung des neuen Datensatzes zu erstellen.

Wenn ein neues angreifbares Anwendungselement erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln dafür ausgewertet. Eine AVI wird nur einmal automatisch ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jede neue oder erneut geöffnete AVI verwendet:

- Für jede Regel für Korrekturaufgaben wird die AVI mit dem Regelfilter für Korrekturaufgaben verglichen.
- Für jede Regel, mit der die Regelbedingung für Korrekturaufgaben übereinstimmt, ruft die Regel die Daten aus der **Auswahl** Gruppieren nach im AVI ab. Es werden ein Gruppenname und ein Feld erstellt. In diesem Fall, **Hohes Risiko: QID-32342:***Zusammenfassung von QID-3242* (Name: Schwachstellen-ID: Zusammenfassung der Schwachstelle).

  **Hinweis:**
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel überprüft, ob eine **offene** Korrekturaufgabe vorhanden ist, die derselben Zuweisungsgruppe wie die AVI zugewiesen ist.
  - Wenn die Aufgabe gefunden wird, wird die AVI der vorhandenen Aufgabe im Status „ **Offen** “ hinzugefügt.
  - Wenn keine Aufgabe im Status „ **Offen** “ gefunden wird, erstellt die Regel eine Aufgabe mit **hohem Risiko: QID-32342**, weist sie derselben Zuweisungsgruppe wie die AVI zu und platziert die AVI in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Regelbedingungen der Korrekturaufgabe verglichen wird, bevor sie in eine Korrekturaufgabe eingefügt wird, können zu viele Regeln die Leistung beeinträchtigen. Richten Sie Ihre Aufgabenregeln so ein, dass die Bedingungen Ihnen helfen, die Erstellung doppelter Korrekturaufgaben zu vermeiden.

Standardmäßig verwenden Korrekturaufgabenregeln beim Gruppieren der Elemente die Zuweisungsgruppe, die durch die **Zuweisungsregeln** in der AVI festgelegt wurde, und weisen die Korrekturaufgabe entsprechend den AVIs zu.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln im Modul **„Zuweisungsregeln“** gesteuert. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel aus dem Formular oder der Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle von dieser Regel erstellten **offenen** Aufgaben zu löschen. Aufgaben, die sich nicht im Status „ **Offen** “ befinden, werden ausgeschlossen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Regel für Korrekturaufgaben ändern möchten, verwenden Sie die **Schaltfläche Erneut anwenden** auf der Seite für Korrekturaufgaben, um die geänderte Regel für alle aktiven **offenen** Korrekturaufgaben erneut auszuführen, die von dieser Regel erstellt wurden. Sie löscht und erstellt Korrekturaufgaben basierend auf der geänderten Regel automatisch neu.

**Erneut anwenden** überprüft nur vorhandene Korrekturaufgaben.

Nachdem Sie Erneut anwenden ausgewählt **haben**, wird die folgende Meldung angezeigt: Durch die erneute Anwendung dieser Regel für Korrekturaufgaben werden die Korrekturaufgaben für diese Regel gelöscht und neu erstellt. Korrekturaufgaben, die sich nicht im Status „Offen“ befinden, werden nicht gelöscht.

## Korrekturaufgaben erstellen und AVIs manuell hinzufügen

Sie erstellen eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Anwendungskorrekturaufgaben-Datensatz und fügen angreifbare Anwendungselemente (AVITs) manuell hinzu. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response.

## Regeln für Korrekturaufgaben und Erstellung und Aktualisierung von AVIs

Wenn ein CI oder Produktmodell aus einem Scan einer bekannten Schwachstelle zugeordnet ist, wird eine AVI erstellt. Nach der Erstellung wird die AVI anhand der Bedingungen der Korrekturaufgabenregeln für eine Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für die AVI erstellt.

Wenn eine Eigenschaft, die in den Filterbedingungen für Korrekturaufgaben erfasst wird, in einer AVI aktualisiert oder geändert wird, wird die aktualisierte AVI auch anhand der Regeln für Korrekturaufgaben auf eine Übereinstimmung ausgewertet. Wenn es eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe gibt, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für die AVI erstellt.

## Status-Rollup und -Rolldown

Wenn Sie eine Korrekturaufgabe auf „Offen“ oder von „Offen“ auf „Wird untersucht“ aktualisieren, wird der neue Status auf alle zugeordneten AVIs übertragen. Das Status-Rolldown erfolgt unmittelbar nach dem Ändern des Status.

Status-Rollup von AVIs zur Korrekturaufgabe erfolgt nur, wenn sich alle **AVIs** für die Aufgabe im Status „Zurückgestellt“ oder **„Geschlossen – behoben“** befinden. Das Rollup erfolgt mit der regelmäßigen Aufgabe *`Rollup application vulnerable item values to vulnerability and group`*, die alle 15 Minuten ausgeführt wird. Für den Status wird erst ein Rollup durchgeführt, wenn die Aufgabe ausgeführt wird. Damit ein Rollup für einen Status von den AVIs zur Korrekturaufgabe durchgeführt werden kann, müssen sich alle AVIs im selben Status befinden.

### Erstellen, bearbeiten und löschen Sie Application Vulnerability Response Regeln für Korrekturaufgaben

Sie können Regeln erstellen, um basierend auf Filterbedingungen automatisch angreifbare Anwendungselemente (AVI) in Korrekturaufgaben (AVUL) zu gruppieren. Diese Regeln gruppieren AVIs automatisch, wenn sie importiert oder manuell erstellt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Wenn Sie eine neue Regel erstellen, gilt sie nicht für vorhandene Daten. Nachdem Sie sie übermittelt haben, wird sie für neue Importe ausgeführt.

Erforderliche Rolle: App-Sec-Manager

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**.
2. Öffnen Sie die Regel, oder wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie.

#### Regel für Korrekturaufgaben

| Feld | Beschreibung |
|---|---|
| Name | Name der Aufgabenregel. |
| Aktiv | Gibt an, ob die Aufgabe aktiv ist. |
| Beschreibung | Eine Beschreibung der Regel. |
| Groß-/ Kleinschreibung beachten | Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht.<br>**Hinweis:**<br>Beim Standardwert wird die Groß-/Kleinschreibung beachtet. |
| Bedingung | Optionale Filterbedingungen für die Regel.<br>Standardmäßig wird beim**Suchtext**, den Sie im Bedingungsgenerator für Datensätze und Formulare für Aufgabenregeln eingeben, nicht zwischen Groß- und Kleinschreibung unterschieden. Sie haben die Möglichkeit, die Suche nach Groß-/Kleinschreibung in Aufgabendatensätzen und Formularen zu aktivieren.<br>Eine Beispielbedingung ist **Schwachstelle** > **ist** > **Schwachstelle123451** (eine bekannte importierte Schwachstelle). Alle AVIs mit dieser Schwachstelle entsprechen dieser Bedingung. |
| **Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)** | |
| Gruppieren Sie angreifbare Anwendungselemente aus | Die Tabelle, die die Regel zum Gruppieren von AVIs verwendet.<br>Wählen Sie die Elemente aus der Struktur aus:<br>○ Angreifbares Anwendungselement [sn_vuln_vulnerable_item]<br>○ Angreifbares Anwendungselement – Konfigurationselement [cmdb_ci]<br>○ Angreifbares Anwendungselement Anwendungsschwachstelle [sn_vul_thritte_partei_entry]<br>○ Angreifbares Anwendungselement – Produktmodell |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:**<br>Wenn Sie eine erweiterte Tabelle auswählen, wird das **Feld Verwenden** nur für angreifbare Anwendungselemente angewendet, die diese erweiterte Tabelle verwenden. |
| Mit Feld | Feld in der Tabelle, das die Regel zum Gruppieren von AVIs verwendet. Wählen Sie Bedingungen aus der Struktur aus.<br>**Hinweis:**<br>Sie können Gruppieren nach Bedingungen erstellen, damit nicht alle AVIs, die Daten freigeben, derselben Korrekturaufgabe zugewiesen werden. Wenn Sie beispielsweise Zuweisungsgruppe und IP-Adresse als Verwenden von Feldern auswählen und mehrere AVIs die anfängliche Filterbedingung **Schwachstelle**erfüllen, können diese AVIs mithilfe der vielen im Abschnitt Gruppieren nach verfügbaren Optionen verschiedenen Zuweisungsgruppen zur Korrektur zugewiesen werden. Die Bedingungen für Gruppieren nach geben Ihnen die Flexibilität, unterschiedliche Korrekturaufgaben zu erstellen, die verschiedenen Gruppen zugewiesen werden können, auch wenn sie einige Daten gemeinsam nutzen. |
| **Zuweisung** | |
| Korrekturaufgaben zuweisen nach | Bei der automatischen Zuweisung **von** Korrekturaufgaben wird die Auswahl Zuweisung zusätzlich zu den Auswahlmöglichkeiten Gruppieren nach verwendet, um die angreifbaren Elemente zu gruppieren. Bei Bedarf werden neue Aufgaben erstellt, sodass jede AVI in eine Aufgabe mit einem übereinstimmenden Zuweisungsgruppensatz eingefügt wird.<br>Um die Zuweisung von Aufgaben zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.<br>○ Feld Gruppieren nach: Wenn Sie ein Benutzergruppenfeld aus **Feldwerte** verwenden **im**Abschnitt Gruppieren nach ausgewählt haben, werden diese im Dropdown-Menü angezeigt.<br>○ Benutzergruppe: Verwenden Sie die Nachschlageliste, um eine statische Benutzergruppe auszuwählen. |

Wenn Sie eine Regel aus der Formular- oder Listenansicht löschen, haben Sie die Möglichkeit, alle von dieser Regel erstellten **offenen** Korrekturaufgaben zu löschen. Gruppen, die sich nicht im Status „ **Offen** “ befinden, werden ausgeschlossen.

4. Wählen Sie **Absenden** für neue Regeln aus.
   Nachdem Sie Absenden ausgewählt haben, wird Ihre Regel in der Liste „Korrekturaufgabenregeln“ [**sn_vul_grouping_rule**] angezeigt. In den folgenden Situationen wird Ihre Regel initiiert.
   - Wenn neue AVIs erstellt werden.
   - Wenn Sie **Erneut anwenden**wählen. Sie wählen **Erneut anwenden**, um Aufgabenregeln nur für vorhandene Korrekturaufgaben auszuwerten.
   - Wenn AVIs aktualisiert werden, entweder von Ihnen oder vom System.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine AVI aktualisiert wird, werden Aufgabenregeln auf Übereinstimmungen mit vorhandenen Korrekturaufgaben ausgewertet. Einige häufige Updates, die eine Regelprüfung initiieren, sind:

- Wenn sich der Status von „Geschlossen“ in „Offen“ oder von „Geschlossen“ in „Wird untersucht“ ändert.
- Das Konfigurationselement (CI) wurde geändert.
- Die Schwachstelle wurde geändert.

Das System überprüft alle Aufgabenregeln auf Übereinstimmungen mit der aktualisierten AVI. Wenn die Bedingungen einer Regel mit den Bedingungen einer Korrekturaufgabe übereinstimmen, werden ihr übereinstimmende AVIs zugewiesen.

Wenn keine Übereinstimmung gefunden wird, wird eine neue Korrekturaufgabe erstellt.

Weitere Informationen zum Status-Rollup von AVIs zu Korrekturaufgaben und zum Status-Rolldown von Korrekturaufgaben zu AVIs finden Sie unter Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.

Ein Beispiel für eine Regel für Korrekturaufgaben finden Sie unter Application Vulnerability Response Beispiele für Korrekturaufgabenregeln.

5. Um eine Aufgabenregel zu löschen, wählen Sie die Regel aus der Liste „Korrekturaufgabenregeln“ aus, und wählen Sie **Löschen**.
Die folgende Meldung wird angezeigt: Die ausgewählte Regel für Korrekturaufgaben hat n Korrekturaufgaben erstellt. Von den Korrekturaufgaben befinden sich n im Status „Offen“.

| Option | Beschreibung |
|---|---|
| Kontrollkästchen deaktiviert (Standard). | Löschen Sie nur die Regel. Aufgaben, die sich nicht im Status „ **Offen** “ befinden, werden ausgeschlossen. |
| Kontrollkästchen aktiviert. | Schließen Sie die Korrekturaufgaben in den Status „ **Offen** “ ein, wenn Sie die Regel für Korrekturaufgaben löschen. Löschen Sie die Regel und alle Korrekturaufgaben im Status „ **Offen** “. |

6. Wählen Sie eine Option und dann **Löschen**aus.

### Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response

Erstellen Sie eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Anwendungskorrekturaufgaben-Datensatz, und fügen Sie angreifbare Anwendungselemente (AVITs) manuell hinzu.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.app_sec_manager

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie rechts oben auf der Seite **Neu**aus.
3. Wählen Sie auf der Registerkarte Gruppenkonfiguration für Gruppierungsmethode die Option **Manuell**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Absenden**.
5. Suchen Sie Ihren neuen Aufgabendatensatz (AVUL) in der Tabelle „Anwendungskorrekturaufgaben“ [sn_vul_app_vulnerability].
   Der Datensatz wird im Status „ **Offen** “ erstellt.
6. Öffnen Sie den Datensatz, und fügen Sie dieser Gruppe mithilfe der zugehörigen Liste „Angreifbare Anwendungselemente“ (**Bearbeiten** oder **Hinzufügen**) neue oder vorhandene angreifbare Anwendungselemente hinzu.
7. Wählen Sie **Aktualisieren** aus, um den Datensatz zu speichern, oder andere UI-Aktionen, um den Datensatz in einen anderen Status zu überführen.

## Konfigurieren Sie Penetrationstests

Sie können die Sprint-Dauer und den geschätzten Aufwand für Penetrationstest-Bewertungstypen konfigurieren. Dies bietet die Planungsfunktion für Anwendungsbesitzer, mit der sie einen vorläufigen Zeitrahmen für ihre Penetrationstest-Bewertungsanforderungen bestimmen können.

### Vorbereitungen

Erforderliche Rolle: Ethical Hacker

### Warum und wann dieser Vorgang ausgeführt wird

Die Konfiguration der Penetrationstest-Bewertungseinstellungen für das Ethical Hacking-Team hilft auch bei der Bestimmung der Gruppe und des Kontaktpunkts, die die Penetrationstest-Bewertungsanforderung erhalten.

Ab Version 19.0 von Vulnerability ResponseVeracode Vulnerability Integrationsind die Penetrationsbewertungstests in Veracode Vulnerability Integration bei Verwendung von [] manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstest-Bewertungsanforderungen verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstest-Bewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Verwenden Sie den ersten Abschnitt, um die Zuweisungsgruppe zu konfigurieren.
3. Füllen Sie die Felder des Formulars aus.

#### Formular Penetrationstestkonfiguration

| Feld | Beschreibung |
|---|---|
| Anwendergruppe des Penetrationstestteams | Gruppe, der die Penetrationstest-Bewertungsanforderung zugewiesen ist. |
| Standard-Beauftragter für Bewertungsanforderungen für Penetrationstests | Ansprechpartner für die Penetrationstest-Bewertungsanforderung. |

4. Wählen Sie **Aktualisieren**.
5. Verwenden Sie den zweiten Abschnitt, um Sprints zu konfigurieren.
   Details finden Sie unter Konfigurieren Sie Sprints für Penetrationstests.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verwenden Sie den dritten Abschnitt, um Bewertungstypen zu konfigurieren.
   Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.

### Konfigurieren Sie Sprints für Penetrationstests

Konfigurieren Sie die Sprint-Dauer und -Kapazität für das Team für ethisches Hacken, damit es die Sprint-Kapazität für Penetrationstest-Bewertungen verwalten kann.

#### Vorbereitungen
Erforderliche Rolle: Ethical Hacking

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Wählen Sie die Option **Konfigurieren** für Sprints konfigurieren aus.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Sprint-Konfiguration“.**

| Feld | Beschreibung |
|---|---|
| Sprint-Dauer (Tage) | Anzahl der Tage in einem Sprint. |
| Startdatum | Startdatum für die Sprintdauer. |
| Anzahl der Sprints | Anzahl der Sprints, die basierend auf dem Start- und Enddatum für den Sprintbereich generiert werden können. |
| Enddatum | Enddatum für die Sprintdauer. |
| Sprint-Kapazität | |
| Sprint-Kapazität (Stunden) | Kapazität eines Sprints in Stunden. |

4. Wählen **Sie Sprints generieren aus**.
   Um die erstellten Sprints anzuzeigen, wählen Sie **Sprints**anzeigen aus.

**Hinweis:**
Nachdem die Sprints generiert und ausgeführt wurden und Sie **Sprints generieren** für dieselbe Dauer auswählen, wird der aktuelle Sprint wie gewohnt abgeschlossen. Die verbleibenden Sprints werden basierend auf der aktualisierten Sprintkonfiguration neu berechnet.

### Konfigurieren Sie Bewertungstypen für Penetrationstests

Konfigurieren Sie den geschätzten Aufwand für jede Art von Penetrationstestbewertung. Auf diese Weise können Sie die Kapazität jedes Sprints verwalten, indem Sie den für jeden Bewertungstyp erforderlichen Aufwand schätzen.

#### Vorbereitungen
Erforderliche Rolle: Ethical Hacking

#### Warum und wann dieser Vorgang ausgeführt wird
Jeder Sprint ist einer Penetrationstestanforderung zugewiesen. Basierend auf dem geschätzten Aufwand für den Bewertungstyp werden die Stunden so angepasst, dass sie die verbleibenden Stunden für den Sprint widerspiegeln.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**.
2. Ab v19.0 von Vulnerability Responsewählen Sie **Konfigurieren**, um Bewertungstypen, Anwendungsgröße und Geschätzter Aufwand anzuzeigen.
3. **Wahlweise:** Wählen Sie einen Bewertungstyp-Datensatz aus, um die Felder nach Bedarf zu aktualisieren, oder erstellen Sie neue Datensätze.

   (Optional) Die Werte der Anwendungsgröße bieten Ihnen weitere Optionen, um Testzeit und -aufwand genauer einzuschätzen. Sie können die Stunden für diese Datensätze bearbeiten oder **Neu** wählen, um eigene Kombinationen zu erstellen.

   Sie können Bewertungstyp und Anwendungsgröße für Werte in vorhandenen Penetrationstest-Anforderungsdatensätzen ändern, damit Sie Tests entsprechend der Sprint-Kapazität planen können. Wenn Sie beispielsweise eine Testanforderung ausfüllen, wird die Anzahl der von Ihnen konfigurierten Sprints möglicherweise nicht angezeigt, da einige Sprints bereits zum Testen verwendet wurden. Wenn die geschätzten Aufwandsstunden eines Sprints mit der für Typ und Größe eines Tests erforderlichen Kombination übereinstimmen, sind sie für neue Anforderungen nicht verfügbar.

   Sie können die Sprints anzeigen, die Testanforderungen in Datensätzen in der Liste Penetrationstest-Sprints unter zugewiesen sind **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration** > **Sprints konfigurieren**. Weitere Informationen zum Konfigurieren von Sprints finden Sie unter Konfigurieren Sie Sprints für Penetrationstests.

   Die Basiswerte für Bewertungstyp, Anwendungsgröße und Geschätzter Aufwand sind:

   **Formular zur Konfiguration des Bewertungstyps für Penetrationstests**

| Bewertungstyp | Anwendungsgröße | Geschätzter Aufwand (Stunden) |
|---|---|---|
| Fokussierter Test | Klein | 20 |
| Fokussierter Test | Mittel | 30 |
| Fokussierter Test | Groß | 40 |
| Fokussierter Test | Standard | 40 |
| Erneut testen | Klein | 10 |
| Erneut testen | Mittel | 15 |
| Erneut testen | Groß | 20 |
| Erneut testen | Standard | 20 |
| Vollständiger Penetrationstest | Klein | 60 |
| Vollständiger Penetrationstest | Mittel | 70 |
| Vollständiger Penetrationstest | Groß | 80 |
| Vollständiger Penetrationstest | Standard | 80 |

4. Wählen Sie Aktualisieren, um Ihre Änderungen zu speichern, oder Absenden, um einen neuen Datensatz zu erstellen.
5. Wählen Sie vor v19.0 die Option **Konfigurieren** für Bewertungstypen konfigurieren aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Aktualisieren Sie die Werte für die Bewertungstypen nach Bedarf.
   Basiswerte:

**Formular zur Konfiguration des Bewertungstyps für Penetrationstests**

| Bewertungstyp | Geschätzter Aufwand (Stunden) |
|---|---|
| Fokussierter Test | 40 |
| Erneut testen | 20 |
| Vollständiger Penetrationstest | 80 |

7. Speichern Sie die Änderungen.

## Integration von Application Vulnerability Response mit anderen Anwendungen

Vulnerability Response bietet Unterstützung für Integrationen von Drittparteien.

### Integrationen von Drittparteien

Anwendungsschwachstellenintegrationen helfen, die Anwendungsschwachstellendaten in Ihrer Instanz zu bereichern, indem Daten von externen Systemen und Lieferanten abgerufen werden. In den folgenden Übersichtsthemen finden Sie weitere Informationen zu unterstützten Integrationen:

- Fortify Vulnerability Integration
- GitHub Application Vulnerability Integration
- Invicti Vulnerability Integration
- Veracode Vulnerability Integration

**Hinweis:**

Integrationen mit mehreren Quellen werden in Application Vulnerability Responsenicht unterstützt. Drittanbieterintegrationen werden separat behandelt. Wenn in Ihrer Umgebung mehr als eine Integrationsanwendung einer Drittpartei verwendet wird, erfolgt keine Deduplizierung angreifbarer Elemente (AVI) über Integrationen hinweg.

### Zusätzliche Hinweise für -Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

## Fortify Vulnerability Integration

Fortify Vulnerability Integration verwendet Daten, die aus dem Produkt Fortify ] importiert wurden, um die Auswirkung und Priorität von Fehlern in Ihrem Code zu bestimmen.

## Fortify Vulnerability Integration

Das Produkt Fortify erfasst Scannerdaten und stellt diese Daten Now Platform®zur Verfügung. Sie lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittparteien zuzuordnen, die die Daten in Ihrer Instanz ergänzen.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Jeden Tag rufen regelmäßige Aufgaben die Integrationen automatisch auf. Sobald alle Integrationen aktiviert sind, werden sie verkettet, um der Reihe nach ausgeführt zu werden. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

## Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Vulnerability Response integration with<br><br>Fortify v2.2<br><br>Fortify v2.1<br><br>Fortify v2.0 | Application Vulnerability Response release notes<br><br>Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Fortify Vulnerability Integration

Um Fortify Vulnerability Integrationanzuzeigen, navigieren Sie zu **Fortify-Schwachstellenintegration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

**Fortify Schwachstellenintegrationen**

| Integration | Beschreibung |
|---|---|
| Fortify bei Bedarf Anwendungslistenintegration | Ruft Fortify Anwendungsscanner-Daten (Schwachstellen, Metadaten) ab und erweitert Ihre Drittpartei-Anwendungsdaten. Diese Integration wird täglich um 00:00:00 Uhr ausgeführt. Sie ist standardmäßig aktiviert. |
| Fortify Zusammenfassungsintegration von On-Demand-Scans | Ruft Scan-Datensätze von Fortifyab. Diese Integration ist so verkettet, dass sie bei Aktivierung nach Fortify on Demand Application List Integration ausgeführt wird. Sie ist standardmäßig inaktiv. |
| Fortify bei Bedarf Integration von angreifbaren Anwendungselementen | Ruft Scan-Ergebnisse von Fortifyab, fügt AVIs ein und erweitert Ihre Schwachstellendaten von Drittparteien. Wenn sich der Scanner-Datensatz im Status **Geschlossen** befindet, werden keine AVIs erstellt. Vorhandene AVIs werden weiterhin aktualisiert.<br><br>Diese Integration ist so verkettet, dass sie bei Aktivierung nach Fortify on Demand Scan Summary Integration ausgeführt wird. Sie ist standardmäßig inaktiv. |

Informationen zu Integrationsausführungsstatus finden Sie unter, Zeigen Sie den Importausführungsstatus Fortify Vulnerability Integration an.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

### wird vorbereitet Fortify Vulnerability Integration

Eine erfolgreiche Fortify Vulnerability Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Fortify Vulnerability Integration setzt voraus, dass Sie mit dem Produkt und der API von Fortify vertraut sind.

### Vorbereitungen

Die CWE-Integration (Common Weakness Enumeration) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration von Fortify Vulnerability Integrationausgeführt werden.

**Hinweis:**
NVD-Daten (NIST Vulnerability Database) sind für die Installation von Fortify Vulnerability Integrationnicht erforderlich. Sie stellen jedoch eine Ergänzung dar und sind nützlich.

Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie voraussichtlich importieren. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Fortify Vulnerability Integration erfordert einen API-Schlüssel, ein API-Geheimnis und eine API-Stamm-URL, die über Ihren Fortify on Demand-Account verfügbar sind.

### Prozedur

So erstellen Sie einen geheimen API-Schlüssel:

**a.** Melden Sie sich bei Ihrem Fortify im Demand-Portal an.

**b.** Navigieren zu **Alle** > **Administration** > **Einstellung** > **API**.

**c.** Fügen Sie ServiceNow als Anwendung hinzu.

**d.** Klicken Sie auf **Neues Geheimnis**, um ein API-Geheimnis zu generieren.

**e.** Notieren Sie Ihr API-Geheimnis zur späteren Verwendung.

## ServiceNow® Vulnerability Response Integration with Fortifyinstallieren

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Fortify ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer der App-Sec Manager-Gruppe zu. Weitere Informationen zu Gruppenrollen finden Sie unter, Application Vulnerability Response -Benutzergruppen und -Rollen.<br>• Die App-Sec-Manager-Gruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rolle: App-Sec-Manager

### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie Fortify Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Store] nach der Anwendung Vulnerability Response Integration with Fortify.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Nächste Maßnahme

Konfigurieren Sie Fortify Vulnerability Integration für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration.

#### Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Fortify ordnungsgemäß in die Funktion Application Vulnerability Response von Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Erforderliche Rolle: App-Sec Manager

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response Integration with Fortify installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter ServiceNow Vulnerability Response Integration with Fortifyinstallieren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die App und weist Benutzer der App-Sec Manager-Gruppe zu.<br>• Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |
| Halten Sie für Fortify Vulnerability Integrationlhre **API-ID** und Ihren **API-Schlüssel** bereit. | Wenden Sie sich an Fortify, um die **API-ID** und den **API-Schlüssel**zu erhalten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie die Schwachstellenintegrationen der Anwendung Fortify installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in [ ServiceNow Storenach der Anwendung Vulnerability Response integration with Fortify.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.
11. Navigieren Sie nach Abschluss der Installation zu **Fortify-Schwachstellenintegration** > **FoD-Konfiguration**.
12. Füllen Sie die Felder des Formulars aus.

### Fortify on Demand-Konfigurationsformular

| Feld | Beschreibung |
|---|---|
| API-Stamm-URL | Fortify-Instanz-URL des Anwenders. |
| API Key | Eindeutiger Bezeichner, der an die Fortify -API gesendet wird. |
| Geheimer API-Schlüssel | Von Fortifybereitgestellter geheimer Clientschlüssel. |
| DAST einbeziehen | Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans identifizieren Schwachstellen im Verhalten der gesamten Anwendung. |
| SAST einbeziehen | Option zum Einbeziehen von Schwachstellen aus SAST-Scans. SAST-Scans identifizieren Schwachstellen im Code. |
| Selektierung von Ausnahmen und falsch positiven Meldungen in ServiceNow (ab v20.0 von Vulnerability Response) | Wählen Sie Optionen aus, um die Workflows für Ausnahmenverwaltung und Falschmeldungen für AVIs mit ServiceNow automatisch beim Import zu verwalten. Diese Optionen sind standardmäßig aktiviert. Ein Beispiel für einen Anwendungsfall finden Sie unter Statuszuordnung für Zurückstellungen und Falschmeldungen in verwalten Application Vulnerability Response. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Verwalten Sie Ausnahmen in ServiceNow**<br>Lassen Sie diese Option aktiviert, wenn Sie importierte **AVIs** selektieren möchten, die für den Status „Zurückgestellt“ markiert sind.<br>**AVIs** mit **Quellstatus**, die in Ihrer Instanz normalerweise einem Status „Zurückgestellt“ zugeordnet sind, werden stattdessen „ **Offen**“ zugeordnet.<br>Sie **fordern eine Ausnahme** aus dem AVI-Datensatz an.<br>**Verwalten Sie Falschmeldungen in ServiceNow**<br>Lassen Sie diese Option aktiviert, wenn Sie importierte AVIs mit **Quellstatus** selektieren möchten, die als **Falsch positiv** oder **Potenziell falsch positiv**markiert sind.<br>AVIs mit diesen **Quellstatus**, die in Ihrer Instanz normalerweise dem Status **Geschlossen** zugeordnet sind, werden **Offen**zugeordnet.<br>Sie fordern ein **falsch positives** Ergebnis aus dem AVI-Datensatz an.<br>○ Deaktivieren Sie eine oder beide Checkboxen, wenn Sie die von Ihrem Scanner importierten **Quellstatus** beibehalten möchten.<br>○ Diese AVIs werden beim Import den Zielstatus und Zielgrundstatus zugeordnet, aber nicht von den Ausnahme- und falsch positiven Workflows selektiert. Die Aktionen „ **Anforderungsausnahme** “ und „ **Falsch positiv** “ sind in AVIs nicht sichtbar. |
| Selektierung in ServiceNow (vor v20.0 von Vulnerability Response) | Verwalten Sie die Selektierung von Anwendungsschwachstellen in der Instanz ServiceNow.<br>○ Aktivieren Sie die Checkbox, um die AVIs in ServiceNowzu selektieren. Wenn diese Option ausgewählt ist, werden AVIs im Status „Offen“ importiert. Sie können dann eine Ausnahme anfordern oder die AVI als falsch positiv markieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Um den Quellstatus beizubehalten, d. h. den vom Scanner importierten Status, stellen Sie sicher, dass das Kontrollkästchen nicht aktiviert ist.<br><br>**Hinweis:**<br>Die Optionen **Als falsch positiv** markieren und **Ausnahme anfordern** sind nur für AVIs verfügbar, die innerhalb von ServiceNowselektiert werden. |

13. Klicken **Sie auf Anmeldeinformationen speichern und testen**.

### Nächste Maßnahme

Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

Bei der Erstinstallation finden Sie weitere Anweisungen unter Application Vulnerability Response konfigurieren.

Informationen zu Änderungen nach der Erstinstallation finden Sie unter Fortify Vulnerability Integration Änderung und Aktivitäten.

## Zeigen Sie den Importausführungsstatus Fortify Vulnerability Integration an

Verwenden Sie die zugehörige Liste „Ausführungen von **Schwachstellenintegrationen“**, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Korrekturentscheidungen zu treffen.

### Vorbereitungen

So zeigen Sie den Importausführungsstatus Fortify an:

- Die Anwendungen Vulnerability Response und Fortify Vulnerability Integration müssen installiert und konfiguriert sein.
- Die Importe Fortify Vulnerability Integration müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

### Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste Ausführungen der **Schwachstellenintegration**.
4. Vergewissern Sie sich, dass alle Importe erfolgreich waren.

## Fortify Vulnerability Integration Änderung und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Fortify Vulnerability Integration.

**Hinweis:**
Das Ändern anderer Fortify Vulnerability Integration -Einstellungen als der hier aufgeführten erfordert fortgeschrittene ServiceNow - und Application Vulnerability Response -Kenntnisse und geht über den Umfang der Produktdokumentation hinaus.

## Führen Sie einen manuellen Fortify -Anwendungsschwachstellenimport durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie einen vollständigen Datenimport unabhängig von der täglichen geplanten Aufgabe durchführen.

### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

### Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus, z. B. Fortify Application List Integration.
3. Wählen Sie **Jetzt ausführen**.

**Hinweis:**
Führen Sie für einen vollständigen Datenabruf die Schwachstellenintegrationen der Fortify-Anwendung nacheinander aus.

## Importieren Sie Daten mit Fortify Vulnerability Integration

Importieren Sie Daten aus dem Fortify-Scanner, um angreifbare Anwendungselemente (AVIs) zuzuordnen und so die Daten in Ihrer Instanz anzureichern.

### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Nach dem ersten Import führen Fortify Schwachstellenintegrationen bei jeder Ausführung einen Delta-Import durch, um die neuesten Daten abzurufen. Weitere Informationen zu vollständigen Importen finden Sie unter Führen Sie einen manuellen Fortify -Anwendungsschwachstellenimport durch.

### Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Integrationsausführung. |
| Aktiv | Option zum Aktivieren einer Integration. |
| Run-Kosten | Häufigkeit der Integrationsausführung. |
| Zeit | |
| Anwendung | Anwendung, die diesen Datensatz enthält. |
| Quellenintegration | Quellintegration für diese Integration. |
| Quellinstanz | Quellinstanz für diese Integration. |
| Nächste Integration | Nächste Integration in der Sequenz, die nach der aktuellen Integration ausgeführt werden soll. |
| Startzeit | Startdatum und -uhrzeit der letzten erfolgreichen Integrationsausführung. Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für die erste Ausführung ist 00:00:00. |
| Integrationsdetails | |
| Integrationsskript | Skripteinbindung, die die `VulnerabilityIntegrationBase` erweitert, die ausgeführt werden soll, wenn die Integration ausgeführt wird. Dieses Skript definiert, wie Daten aus einem Drittanbietersystem abgerufen werden. |
| Integrationswerksskript | Skript, das definiert, wie die für das Integrationsskript ausgewählte Skripteinbindung erstellt wird. |
| Berichtsprozessorstrategie | Strategie, die Sie für die Verarbeitung der vom Integrationsskript zurückgegebenen Daten verwenden möchten, wenn die Integration ausgeführt wird. |

4. Wählen Sie **Jetzt** ausführen aus, um die Integration auszuführen.

### Schließen Sie angreifbare Elemente der Anwendung „Geschlossene Fortify on Demand“ ein

Standardmäßig werden während der Integration von Fortify angreifbaren Elemente keine **geschlossenen** angreifbaren Elemente (AVIs) erstellt. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Fortify Vulnerability Integration muss installiert sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

### Prozedur

1. Geben Sie im Textfeld Filternavigator der linken Navigation sys_properties.list ein.
2. Geben Sie im Suchfeld **Name** für die Liste sn_vul.create_closedein.
3. Doppelklicken Sie auf das Feld **Wert**, und legen Sie es auf **True**fest
4. Klicken Sie zum Speichern auf das grüne Häkchensymbol .
   Datensätze im Status „ **Geschlossen** “ werden beim nächsten Import von Fortify als AVIs in Application Vulnerability Responseerstellt.

## GitHub Application Vulnerability Integration

GitHub Application Vulnerability Integration importiert Daten aus statischen Anwendungssicherheitstests (SAST) und Software Composition Analysis (SCA), um Sie beim Anzeigen von Schwachstellenwarnungen in den Repositorys in Ihrer GitHub-Umgebung zu unterstützen.

## GitHub-Schwachstellenintegration

Der GitHub Application Vulnerability Integration erfasst Scannerdaten und stellt diese Daten dem Now Platform®zur Verfügung. Sie lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittanbietern und GitHub-Warnungen in Ihrer Instanz zuzuordnen.

Die GitHub-Umgebung unterstützt mehrere Organisationen. Diese Organisationen, sowohl lokal als auch Enterprise, können verschiedene Abteilungen enthalten, z. B. Engineering, Qualität, Dokumentation usw. Jede Organisation kann wiederum mehrere Repositorys unterstützen. Diese Integration importiert Schwachstellenwarnungsdaten aus diesen Repositorys. Importierte Daten werden wie eine Anwendung in der Anwendung Application Vulnerability Response verarbeitet. Wenn Scanner Schwachstellen erkennen und Warnungen für die Repositorys generieren, werden Schwachstellen in Application Vulnerability Response erstellt.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Der für das Abrufen von Daten erforderliche Bereich ist **repo**.

## Verfügbare Versionen

## GitHub-Integrationen

| Integration | Beschreibung |
|---|---|
| GitHub-CodeScan-Integration | Ruft Schwachstellenwarnungen zum Code-Scannen aus GitHub-Repositorys für Sicherheitsschwachstellen und Codierungsfehler ab. Importierte Daten werden SAST-Ergebnissen in Ihrer Instanz zugeordnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integration | Beschreibung |
|---|---|
| GitHub Dependabot-Integration | Ruft Dependabot-Warnungen für Abhängigkeiten mit bekannten Schwachstellen aus Repositorys ab. Importierte Daten werden SCA-Ergebnissen in Ihrer Instanz zugeordnet. |

## Importierte Daten anzeigen

Importierte Daten (Ergebnisse) aus der GitHub Dependabot-Integration werden in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_app_release].
- Zusammenfassungen des Anwendungsschwachstellen-Scans [sn_vul_app_vul_scan_summary].
- Angreifbare Anwendungselemente [sn_vul_app_vulnerable_item].
- Pakete [sn_vul_app_package].

Importierte Daten aus der GitHub CodeScan-Integration werden in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_app_release].
- Zusammenfassungen des Anwendungsschwachstellen-Scans [sn_vul_app_vul_scan_summary].
- Anwendungsschwachstelleneinträge [sn_vul_app_vul_entry].
- Angreifbare Anwendungselemente [sn_vul_app_vulnerable_item].

### wird vorbereitet GitHub Application Vulnerability Integration

Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. GitHub Application Vulnerability Integration setzt voraus, dass Sie mit dem GitHub-Produkt und der GitHub-API vertraut sind.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rollen:

- Administrator, um Anwendungen herunterzuladen, zu installieren und zu aktivieren und Rollen zuzuweisen.
- GitHub-Administrator, um Anmeldeinformationen abzurufen und Token in der GitHub-Konsole zu generieren.
- -Administrator, um Verbindungen und Aliasdatensätze in Ihrer Instanz einzurichten.

#### Setupaufgaben

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Setupaufgaben (Fortsetzung)**

| Setupaufgaben | Beschreibung |
| --- | --- |
| | Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass GitHub Application Vulnerability Integration installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren Sie ServiceNow GitHub Application Vulnerability Integration. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die App und weist Benutzer der App-Sec Manager-Benutzergruppe zu.<br>• Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.<br>• sn_vul_github_config_integration wird von der App-Sec Manager-Benutzergruppe geerbt. Diese Rolle enthält die Rollen connection_admin und oauth_admin. |
| Rufen Sie Ihre GitHub-Anmeldeinformationen und Kontoinformationen ab. | Account-Informationen sind in Datensätzen erforderlich, die Sie für die Authentifizierung erstellen. Weitere Informationen zum Einrichten der erforderlichen Datensätze für die OAuth-Authentifizierung finden Sie unter Erstellen Sie die erforderlichen Datensätze für die OAuth-Authentifizierung für GitHub Application Vulnerability Integration. |
| Stellen Sie sicher, dass Sie CWE-Daten (Common Weakness Enumeration) importieren. | Die CWE-Integration (Common Weakness Enumeration) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration der GitHub-Schwachstellenintegration ausgeführt werden. Er wird standardmäßig mit Vulnerability Responseinstalliert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Setupaufgaben (Fortsetzung)**

| Setupaufgaben | Beschreibung |
| --- | --- |
| | **Hinweis:** NVD-Daten (NIST Vulnerability Database) sind für die Installation der GitHub-Schwachstellenintegration nicht erforderlich. Sie stellen jedoch eine Ergänzung dar und sind nützlich. Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern. |

### Erstellen Sie die erforderlichen Datensätze für die OAuth-Authentifizierung für GitHub Application Vulnerability Integration

Wenn Sie keine OAuth-Anmeldeinformationen haben, richten Sie Ihre Anmeldeinformationen und Verbindungsinformationen für die OAuth-Authentifizierung ein, wenn Sie diese Methode für Verbindung und Authentifizierung verwenden möchten.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**.
2. Wählen Sie in der Liste „Anwendungsregistrierungen“ die Option **Neu**aus.
3. Wählen Sie auf der OAuth-Anwendungsseite **Verbindung mit OAuth-Drittpartei herstellen aus**.
4. Füllen Sie das Formular im Datensatz „Anwendungsregistrierungen“ aus.
5. Wählen Sie **Absenden**.
   Ihr neuer Anwendungsregistrierungsdatensatz (OAuth-Provider) wird in der Anwendungsregistrierungsliste angezeigt.
6. Wählen Sie Ihren neuen Datensatz aus, um ihn zu öffnen.

   Auf der zugehörigen Listenregisterkarte **OAuth-Entitätsprofile** in Ihrem neuen Datensatz wurde ein OAuth-Entitätsprofil-Datensatz erstellt, als Sie den Datensatz übermittelt haben.
7. Wählen Sie diesen Profildatensatz aus, um ihn zu öffnen, damit Sie einen Bereich zum Abrufen von Repositorys erstellen können.
8. Doppelklicken Sie **im Abschnitt „Anwendungsbereiche OAuth-Entitätsprofil“ auf Neue Zeile einfügen**.
9. Wählen Sie im Feld das Suchsymbol aus.
10. Wählen Sie im angezeigten modalen Fenster **Neu**, und füllen Sie die Felder aus.
11. Wählen Sie **Absenden**, klicken Sie auf das grüne Häkchen, und wählen Sie **Aktualisieren**.
    Ihr Anwendungsregistrierungen-Datensatz wird angezeigt. Dieser Datensatz ist abgeschlossen.
12. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Berechtigungen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Wählen Sie **Neu**.
14. Wählen Sie **OAuth 2.0-Anmeldeinformationen** aus, und füllen Sie die Felder aus.
15. Wählen Sie **Absenden**.
    Die Liste der Anmeldeinformationen wird angezeigt.
16. Öffnen Sie den von Ihnen erstellten Datensatz, und wählen Sie den zugehörigen Link **OAuth-Token** abrufen aus.
    Die GitHub-Anmeldeseite wird angezeigt. Sie erhalten die Berechtigungen und generieren das Token über Ihre GitHub-Konsole.
17. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Aliasse für Verbindungen und Berechtigungen**.
18. Wählen Sie **Neu**, und füllen Sie die Felder aus.
19. Wählen Sie **Absenden**.
    Die Liste der Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt.
20. Öffnen Sie Ihren Datensatz, und wählen Sie auf der Registerkarte „Verbindungen“ die Option **Neu** aus, und füllen Sie die Felder im HTTP-Verbindungsdatensatz aus.
21. Wählen Sie **Absenden**.
    Die Liste der Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt. Sie sind jetzt bereit, die Schritte bis Konfigurieren Sie die Eigenschaften GitHub Application Vulnerability Integrationauszuführen . Im Feld Verbindung geben Sie die Anmeldeinformationen ein, die Sie in den vorherigen Schritten erstellt haben.

### Installieren Sie ServiceNow® GitHub Application Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit GitHub Application Vulnerability Integration ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie GitHub Application Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow StoreGitHub Application Vulnerability Integration nach der Anwendung [].
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Wählen Sie **App anfordern aus**, und geben Sie Ihre Anmeldeinformationen Now Support ein.
6. Wählen **Sie Abrufen aus**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance**(Instanz validieren) aus.
8. Wählen Sie **Anforderung aus**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen **Sie Installieren**aus.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Konfigurieren Sie die Eigenschaften GitHub Application Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das GitHub-Produkt ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen

Der für das Abrufen von Daten erforderliche Bereich ist **repo**. Sie legen diesen Parameter in Erstellen Sie die erforderlichen Datensätze für die OAuth-Authentifizierung für GitHub Application Vulnerability Integrationfest.

Erforderliche Rollen:

- Benutzergruppe des App-Sec-Managers
- Administrator für OAuth-Setup erforderlich

#### Prozedur

1. Navigieren zu **Alle** > **GitHub-Schwachstellenintegration** > **Konfiguration**.
2. Füllen Sie die Felder aus.
3. Wählen **Sie Anmeldeinformationen speichern und testen aus**.

### Zeigen Sie den Importausführungsstatus GitHub Application Vulnerability Integration an

Verwenden Sie die zugehörige Liste „Ausführungen von **Schwachstellenintegrationen“**, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Korrekturentscheidungen zu treffen.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **GitHub-Schwachstellenintegration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Wählen Sie die zugehörige Liste „ **Schwachstellenintegrationsausführungen“** aus.
4. Vergewissern Sie sich, dass alle Importe erfolgreich waren.

**Trouble?**

Zu den häufigsten Ursachen für eine fehlgeschlagene Ausführung gehören:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

Wenn eine dieser Bedingungen auftritt, wählen Sie **Jetzt ausführen**aus, und führen Sie die Integration erneut aus.

### Zeigen Sie GitHub Application Vulnerability Integration Importsätze an

Zeigen Sie Details für Importinformationen für GitHub Application Vulnerability Integrationan.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren Sie zu **GitHub-Schwachstellenintegration** > **Importsatztabellen**.
2. Wählen Sie einen Datensatz für eine Integration aus.
3. Wählen Sie einen zugehörigen Link aus, um die folgenden Informationen anzuzeigen:
   - Importsätze
   - Transformationszuordnungen
   - Verlauf umwandeln

## Invicti Vulnerability Integration

Invicti Vulnerability Integration verwendet Anwendungsdaten, die aus dem Invicti-Produkt importiert wurden, um die Auswirkung und Priorität von Fehlern in Ihrem Code zu bestimmen.

## Invicti Vulnerability Integration

Der Invicti Vulnerability Integration erfasst Scannerdaten und stellt diese Daten dem Now Platform®zur Verfügung. Sie lässt sich problemlos in die Funktion ServiceNow® Application Vulnerability Response von Vulnerability Response integrieren, um importierte Informationen zu Anwendungsschwachstellen von Drittparteien in Ihrer Instanz zuzuordnen.

Die Integration importiert die folgenden Arten von gescannten Daten.

- Dynamische Anwendungssicherheitstests (DAST)
- Interaktive Anwendungssicherheitstests (IAST)

Weitere Informationen zu DAST und IAST finden Sie unter Application Vulnerability Response erkunden.

## Verfügbare Versionen

| Release-Version | Versionsinformationen |
|---|---|
| Vulnerability Response integration with Invicti<br><br>Erstveröffentlichung | Application Vulnerability Response release notes<br><br>Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Release-Version | Versionsinformationen |
| --- | --- |
| | Compatibility Matrix and Release Schema Changes |

## Integrationen

Die folgenden Integrationen sind im Basissystem enthalten. Die Integrationen sind verkettet, sodass nach dem erfolgreichen Abschluss einer Integration die nächste Integration initiiert wird. Die Integrationen werden in der in der folgenden Tabelle aufgeführten Reihenfolge ausgeführt.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um diese Integrationen automatisch der Reihe nach auszuführen. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

### Invicti-Anwendungsschwachstellenintegrationen

| Integration | Beschreibung |
| --- | --- |
| Invicti-Anwendung Listenanwendung | Importiert von Invicti gescannte Anwendungen in die Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] oder die Tabelle „Gescannte Anwendung“ [sn_vul_app_scanned_application], je nachdem, wie die Systemeigenschaft `sn_vul.use_product_model` für die CI-Suchregeldatensätze festgelegt ist.<br>• Wenn die Produktmodelleigenschaft auf „true“ festgelegt ist, wird eine Anwendung in die Release-Tabelle „Erkannte Anwendungen“ eingefügt.<br>• Wenn die Produktmodelleigenschaft auf „false“ festgelegt ist, wird eine Anwendung in die Tabelle „Gescannte Anwendung“ eingefügt.<br><br>Sie können Suchregeln mit Konfigurationselementen (CIs) als Suchziele aktivieren, indem Sie die Systemeigenschaft ändern. Wenn Sie sie ändern, sollten Sie auch CI-Suchregeln aktivieren, damit sie dem Suchziel entsprechen. Weitere Informationen finden Sie unter:<br>• Konfigurieren Sie die Eigenschaften Invicti Vulnerability Integration<br>• Erstellen Sie eine CI-Suchregel<br>• CI-Suchregeln in werden erneut angewendet Application Vulnerability Response |
| Invicti-Scan-Listenintegration | Diese Integration wird initiiert, nachdem die Integration der Anwendungsliste erfolgreich |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Invicti-Anwendungsschwachstellenintegrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | abgeschlossen wurde. Diese Integration importiert Daten über das Datum und die Uhrzeit, zu der ein Scan ausgeführt wurde. |
| Integration von angreifbaren Elementen der Invicti-Anwendung | Diese Integration wird initiiert, nachdem die Scan List Integration erfolgreich abgeschlossen wurde.<br><br>Jede Schwachstelle in Invicti hat einen Typ, z. B.**DirectoryListing**. Dieser Typ wird als eindeutige ID in Ihrer Instanz zugeordnet und als Teil des Werts im Feld Schwachstelle im AVI-Datensatz (Application Vulnerability Item) angezeigt: **Invicti-DirectoryListing**.<br><br>Weitere Informationen zur Zuordnung finden Sie unter Invicti Vulnerability Integration Statuszuordnung. |

Die Obergrenze für Elemente pro Seite für alle drei Integrationen beträgt 200.

### Bereiten Sie sich auf die vor Invicti Vulnerability Integration

Eine erfolgreiche Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Invicti Vulnerability Integration setzt voraus, dass Sie mit dem Invicti-Produkt und der API vertraut sind.

Die CWE-Integration (Common Weakness Enumeration) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration der Invicti Vulnerability-Integration ausgeführt werden.

**Hinweis:**
NVD-Daten (NIST Vulnerability Database) sind für die Installation der Integration nicht erforderlich, bieten jedoch eine Ergänzung zu Schwachstellen und sind nützlich.

Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

**Hinweis:**
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie voraussichtlich importieren. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support. Die Administratorrolle ist erforderlich, um Anwendungen in Ihrer Now Platform-Instanz zu installieren und zu konfigurieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rufen Sie Ihre API-Anmeldeinformationen und Ihr API-Token über Ihre Invicti-Konsole ab. Überprüfen Sie die Informationen, die auf der Invicti-Produktwebsite unter API-Übersicht verfügbar sind.

### Installieren Sie ServiceNow® Vulnerability Response Integration with Invicti

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit die Anwendung Invicti Vulnerability Integration ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie Invicti Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in [ ServiceNow Storenach der Anwendung Invicti Vulnerability Integration.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Wählen Sie **App anfordern aus**, und geben Sie Ihre Anmeldeinformationen Now Support ein.
6. Wählen **Sie Abrufen aus**.
7. Geben Sie den **Instanznamen** und **den Grund für die Instanz**ein, und wählen Sie **Validate Instance**(Instanz validieren) aus.
8. Wählen Sie **Anforderung aus**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen **Sie Installieren**, um sie zu aktivieren.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Konfigurieren Sie die Eigenschaften Invicti Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit Invicti Vulnerability Integration ordnungsgemäß mit der Funktion Application Vulnerability Response von Vulnerability Response] funktioniert.

#### Vorbereitungen
Erforderliche Rollen:

- -Administrator zum Installieren und Aktivieren von Anwendungen
- App-Sec-Manager-Benutzergruppe zum Konfigurieren der Integration

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Invicti Vulnerability Integration installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren Sie ServiceNow Vulnerability Response Integration with Invicti. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die App und weist Benutzer der App-Sec Manager-Gruppe zu.<br>• Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |
| Halten Sie für die Inviciti Vulnerability-Integration Ihre **Benutzer-ID** und Ihr **API-Token** bereit. | Wenden Sie sich an Ihren Invicti-Administrator, um die **Benutzer-ID** und das **API-Token** zu erhalten, wenn Sie sie nicht kennen.<br><br>Weitere Informationen finden Sie auf der Invicti-Produktwebsite unter API-Übersicht . |

### Prozedur

1. Navigieren zu **Alle** > **Invicti** > **Invicti-Konfiguration**.
2. Füllen Sie die Felder aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| API-URL | Invicti-Instanz-URL des Anwenders. Dies sind die Informationen, die Sie von Bereiten Sie sich auf die vor Invicti Vulnerability Integrationerhalten haben. |
| Anwender-ID | Eindeutige Anwender-ID. |
| API-Token | API-Token, das Sie über Ihre Invicti-Konsole generiert haben. Dies sind die Informationen, die Sie von Bereiten Sie sich auf die vor Invicti Vulnerability Integrationerhalten haben. |
| Wählen Sie den Scan-Typ aus. Sie müssen mindestens einen auswählen. | |
| Importieren Sie DAST | Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans finden dynamisch Schwachstellen für eine Anwendung, während sie ausgeführt wird. Dieser Ansatz kann einen Angriff von außen imitieren. |
| Importieren Sie IAST | Option zum Einbeziehen von Schwachstellen aus IAST-Scans. IAST-Scans erkennen Softwareschwachstellen durch Interaktion mit dem Programm, während es ausgeführt wird. Beobachtung durch Menschen, automatisierte Tests und Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren und Schwachstellen zu lokalisieren. |
| Datumsformat | Parameter, der die Startzeit in das Format konvertiert, das von der Invicti-API unterstützt wird, die von der Invicti-Anwendungsintegration für angreifbare Elemente verwendet wird.<br><br>Dieser Parameter muss dem Format entsprechen, das Sie in Ihrem Invicti-Konto definiert oder ausgewählt haben, z. B. **tt/MM/jjjj**. Stellen Sie sicher, dass die Datums- und Uhrzeitformate in Ihrer Invicti-Konsole mit denen übereinstimmen, die Sie für das Datumsformat in Ihrer Now Platform -Instanz eingegeben haben.<br><br>So ändern Sie dieses Format in Ihrer Invicti-Konsole:<br><br>**a.** Melden Sie sich bei Invicti Sign In an.<br>**b.** Wählen Sie oben rechts **Benutzername** aus.<br>**c.** Navigieren zu **Benutzereinstellungen** > **Datums-/Uhrzeitformat**. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Fehlgeschlagene Importe können auftreten, wenn Sie in Ihrer Now Platform -Instanz ein ungültiges Datumsformat eingeben.<br><br>Wenn Sie in Ihrer Instanz ein gültiges Format eingeben, das sich vom Datumsformat in Ihrer Invicti-Konsole unterscheidet, gibt Invicti eine leere Nutzlast zurück. |
| Ausnahmen in ServiceNow verwalten | Wählen Sie eines aus:<br>**Aktiviert (ausgewählt)**<br>Angreifbare Anwendungselemente ( **AVIT** ) von Invicti mit Status wie „Vorhanden“ und „ **AkzeptiertesRisiko** “, die in Ihrer Instanz möglicherweise zurückgestellt werden, werden stattdessen automatisch „ **Offen** “ zugeordnet.<br>**Deaktiviert (nicht ausgewählt)**<br>Quellstatus für aus Invicti importierte angreifbare Elemente (AVITs) werden beibehalten. Sie müssen Ausnahmen für diese AVITs aus AVIT-Datensätzen verwalten (zurückstellen).<br><br>Weitere Informationen zu Invicti-Quellstatus und -Zielfeldern finden Sie unter Invicti Vulnerability Integration Statuszuordnung. |
| Falsch positive Ergebnisse in ServiceNow verwalten | Wählen Sie eines aus:<br>**Aktiviert (ausgewählt)**<br>**AVITs** mit Status aus Invicti wie „Vorhanden“ und „ **Falsch positiv** “, die in Ihrer Instanz in „ **Geschlossen** “ übergehen können, werden stattdessen automatisch „ **Offen** “ zugeordnet.<br>**Deaktiviert (nicht ausgewählt)**<br>Aus Invicti importierte AVIT-Status werden beibehalten. Sie müssen Falschmeldungen oder potenzielle Falschmeldungen für diese AVITs aus AVIT-Datensätzen verwalten. |

3. Klicken **Sie auf Anmeldeinformationen speichern und testen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Wahlweise:** Ändern Sie Ihre Suchregeln so, dass sie auf Konfigurationselementen basieren.

   (Optional) Standardmäßig ist die **Systemeigenschaft sn_vul.use_product_model** für Ihre Suchregeln in der Tabelle [sn_sec_cmn_ci_lookup_rule] basierend auf dem Produktmodell aktiviert (auf „ true“ festgelegt). Wenn diese Regel aktiviert ist:

   - Diese Regel identifiziert Übereinstimmungen zwischen importierten Daten und den Daten in Configuration Management Database (CMDB) basierend auf dem Produktmodell.
   - Datensätze werden in der Tabelle „Erkannte Anwendungen“ [sn_vul_app_release] erstellt oder aktualisiert.
   - Wenn Sie Suchregeln für Invicti erstellen oder bearbeiten, wird das **Produktmodell** im Feld **Suchziel** des Regelformulars angezeigt.

   Um Ihre Regeln so zu ändern, dass sie auf Konfigurationselementen basieren, müssen Sie die **Systemeigenschaft sn_vul.use_product_model**manuell deaktivieren (auf false setzen).

   a. Navigieren zu **Alle** > **Systemeigenschaften** und suchen Sie den Datensatz **sn_vul.use_product_model**, und legen Sie den Wert auf falsefest.

   b. Wählen Sie **Aktualisieren**.

   c. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln**.

   d. Suchen Sie die Regeln Anwendungsname und Quellanwendungs-ID, die das Suchziel als **Konfigurationselement**haben.

   e. Aktivieren Sie für diese Regeln das Kontrollkästchen Aktiv.

   f. Wählen Sie **Aktualisieren**.
   Wenn Sie Suchregeln für Invicti erstellen oder bearbeiten, beachten Sie, dass **Configuration Item** im Feld **Suchziel** des Regelformulars angezeigt wird. Datensätze werden in der Tabelle „Gescannte Anwendungen“ [sn_vul_app_scanned_application] erstellt oder aktualisiert.

### Anzeigen des Importausführungsstatus Invicti Vulnerability Integration und der Datensätze

Verwenden Sie die zugehörige Liste „Ausführungen von **Schwachstellenintegrationen“**, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Korrekturentscheidungen zu treffen.

## Importstatus, Importsätze und Datensätze anzeigen

Um den Status Ihrer Importe anzuzeigen, navigieren Sie als Benutzer in der App-Sec Manager-Benutzergruppe zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** und wählen Sie einen Integrationsdatensatz aus. Wählen Sie die zugehörige Liste „ **Schwachstellenintegrationsausführungen“** aus.

Um die Importsätze anzuzeigen, navigieren Sie zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** > **Importsatztabellen** und wählen Sie eine Integration aus.

Die Anwendungslisten-Integration erstellt oder aktualisiert Datensätze basierend auf dem Suchziel:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Produktmodell: Tabelle „Erkannte Anwendungen“ [sn_vul_app_release].
- Konfigurationselement: Tabelle „Gescannte Anwendungen“ [sn_vul_app_scanned_application].

Die Integration „Scan List“ erstellt oder aktualisiert Datensätze in der Tabelle „Gescannte Anwendungen“ [sn_vul_app_scan_summary].

Die Integration von angreifbaren Anwendungselementen erstellt oder aktualisiert Datensätze in den Tabellen „Angreifbare Anwendungselemente“ [sn_vul_app_vulnerable_item] und „CWEs“ [sn_vul_cwe].

**Hinweis:**
Jede Schwachstelle in Invicti hat einen „Typ“, z. B. „ProductDirectoryListing“. Dieser Typ wird importiert, als eindeutige ID in Ihre Instanz zugeordnet und als Teil des Werts im Feld Schwachstelle im Datensatz des angreifbaren Elements (AVIT) der Anwendung angezeigt. In diesem Beispiel lautet der Wert Invicti-ProductDirectoryListing, und dieser Wert wird auch als eindeutige ID im Datensatz „Anwendungsschwachstelleneintrag“ angezeigt. Invicti-AVITs unterstützen mehrere CWE-Einträge (Common Weakness Enumeration), daher werden CWEs nicht als eindeutige IDs verwendet. CWEs werden auch im AVIT-Datensatz angezeigt.

Wenn bei Invicti-AVITs in Invicti doppelte Typen für eine Schwachstelle vorhanden sind, wird das Wort „benutzerdefiniert“ in den Wert eingefügt, z. B. Invicti-custom-ProductDirectoryListing. Wenn Sie einen benutzerdefinierten Typ für Schwachstellen erstellen, lautet die Schwachstellen-ID möglicherweise Invicti-Custom-<title of vulnerability>.

Neue Felder: Für Scan-Typ = Invictikönnen die Felder Betroffene Parameter und Benutzerdefinierte Felder Daten enthalten, die Ihnen helfen können, die Schwachstelle zu verstehen und zu beheben. Wenn keine Daten vorhanden sind, werden diese Felder nicht in der AVIT angezeigt.

### Invicti Vulnerability Integration Statuszuordnung

Die folgenden Quellstatus aus Invicti Vulnerability Integration und ihre Zielstatus in Ihrer Instanz sind in der folgenden Tabelle aufgelistet.

**Invicti-Quellstatus und die entsprechenden Now Platform-Status**

| Invicti-Quellstatus | Beschreibung der Quellstatus | Zielstatus in Now Platform |
|---|---|---|
| Anwesend | Das Problem wurde identifiziert. | Offen |
| Vorhanden, akzeptiertes Risiko, wiederbelebend | Das Problem wurde berücksichtigt und ist als Schwachstelle mit geringem Risiko gekennzeichnet. | Zurückgestellt |
| Vorhanden, falsch positiv | Das Problem wurde berücksichtigt und ist als keine echte Schwachstelle gekennzeichnet. | Geschlossen |
| „FixedUnconfirmed“, „Fixed Unconfirmed“. | Das Problem wurde behoben, aber nicht von Invicti Enterprise bestätigt. | Gelöst |
| Behoben (Bestätigt), Bestätigt, Bestätigt, Bestätigt, AkzeptiertRisiko, Bestätigt, Falsch positiv | Das Problem wurde von Invicti Enterprise behoben und bestätigt, und es ist keine weitere Aktion erforderlich. | Geschlossen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Invicti-Quellstatus und die entsprechenden Now Platform-Status (Fortsetzung)**

| Invicti-Quellstatus | Beschreibung der Quellstatus | Zielstatus in Now Platform |
|---|---|---|
| Repariert (erneuter Test nicht möglich) | Das Problem wurde identifiziert, aber Invicti kann nicht erneut testen, um zu bestätigen, ob das Problem behoben wurde oder nicht. | Gelöst |
| Wiederbelebend | Das Problem wurde in vorherigen Scans behoben, wurde jedoch erneut gefunden. | Offen |
| Zurückgestellt, ignoriert | Das Problem wurde vom Anwender ignoriert. Um in Invicti Enterprise ein Problem zu ignorieren, aktualisiert ein Benutzer dessen Status auf „Risiko akzeptiert“. | Risiko akzeptiert |

## Anwendungs-Release-Zuordnung

| Quellfeld | Zielfeld in Now Platform |
|---|---|
| ID | source_app_id |
| CreatedAt | app_creation_date |
| Aktualisiert um | app_updation_date |
| Name | app_name |
| Stamm-URL | Source_zusätzliche_info |
| Beschreibung | Beschreibung |
| Tags | Tags |

## Schwachstellenzuordnung

| Quellfeld | Zielfeld in Now Platform |
|---|---|
| Typ | Kategoriename |
| Schwachstellendetail | Zusammenfassung |
| Impact | Bedrohung |
| Quellreferenzen | Webreferenzen |
| Quellempfehlung | Lösung |
| Typ | source_entry_id/ID |
| Schweregrad | source_severity |
| Klassifizierung[“Cwe”] | CWE-Liste |
| CvssVectorString | CVVS v3-Felder |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Scan-Zusammenfassungszuordnung

| Quellenfeld | Zielfeld |
|---|---|
| Quelle | Quelle |
| TotalVulnerabilityCount | Detected_flaw_count |
| Initiierungsdatum | Dynamisches Scan-Datum |
| id | source_scan_id |

### Zuordnung des angreifbaren Elements (AVIT).

| Quellfeld | Zielfeld in Now Platform |
|---|---|
| Typ | Überprüfungstyp |
| Website-ID | Quell-App-ID |
| ID | AVIT-ID der Quelle |
| Datum der letzten Anzeige | Zuletzt gefunden |
| Datum der ersten Sichtung | Erste ermittelte |
| Datum der letzten Aktualisierung | Datum des letzten Scans |
| parameters | Betroffener Parameter |
| URL | Betroffene URL |
| Schweregrad | Quellenschweregrad |
| URL | Quell-Link |
| Schwachstellendetail | Zusammenfassung der Quellschwachstelle |
| Externe Referenzen | Quellreferenzen |
| Remedy + Remedy-Referenzen | Quellempfehlung |
| Status | Quellenkorrekturstatus |
| Impact | Erklärung der Quellschwachstelle |



## Veracode Vulnerability Integration

Die Anwendung Vulnerability Response Integration with Veracode verwendet Daten, die aus dem Produkt Veracode importiert wurden, um die Auswirkungen und Priorität von Fehlern in Ihrem Code zu bestimmen.

## Veracode Vulnerability Integration

Das Produkt Veracode erfasst dynamische Anwendungssicherheitstests (DAST), statische Anwendungssicherheitstests (SAST) und manuelle Scannerdaten und stellt diese Daten Now Platform® zur Verfügung. Sie lässt sich problemlos in die Funktion Application Vulnerability Response von Vulnerability Response integrieren, um Schwachstellen von Drittparteien zuzuordnen, die die Daten in Ihrer Instanz ergänzen.

Ab v19.0 von Vulnerability Responsekönnen Sie SCA-Schwachstellen (Software Composition Analysis) und Schwachstellendaten von Software Bill of Materials (SBOM) importieren, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Eine gemeinsam genutzte API erfasst DAST-, SAST-, SCA-Daten und Ergebnisse manueller Penetrationstests.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Regelmäßige Aufgaben rufen die Integrationen jeden Tag automatisch in der Reihenfolge auf, in der sie aufgelistet sind. Sie können einzelne regelmäßige Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenkorrektur, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

## Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Veracode 4.1<br><br>Veracode 4.0 | Application Vulnerability Response release notes<br><br>Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Benutzergruppe und Rollen

Veracode Vulnerability Integration wird von einem Systemadministrator [admin] installiert und von einem Mitglied der App-Sec-Manager-Gruppe konfiguriert. Weitere Informationen finden Sie unter Application Vulnerability Response -Benutzergruppen und -Rollen.

## Veracode Vulnerability Integration

Um die Veracode Schwachstellenintegrationen anzuzeigen, navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

### Veracode Vulnerability Integration

| Integration | Beschreibung |
|---|---|
| Ab v4.1: Veracode Integration von Projekten verknüpfen | Diese Integration ist standardmäßig aktiviert. Ruft alle zugeordneten Projekte für jede Anwendung aus Veracodeab.<br><br>Anwendungen können mehrere Projekte in der Anwendung Veracode haben. Importierte Daten aus dieser Integration werden in den folgenden Datensätzen angezeigt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Veracode Vulnerability Integration (Fortsetzung)

| Integration | Beschreibung |
|---|---|
| | • **Das Datum des letzten SCA-Scans**, das **App-Erstellungsdatum**und das **App-Aktualisierungsdatum** werden in Datensätzen unter **Erkannte Anwendungen**aufgelistet.<br>• In den Zusammenfassungsdatensätzen des Anwendungsschwachstellen-Scans und der angreifbaren Elemente (AVIs) wird der **Quell-SDLC-Status** (Software Development Life Cycle) angezeigt.<br>• **Die Ausnutzbarkeit der Quelle** wird in AVI-Datensätzen (Application Vulnerable Item) angezeigt. |
| Ab v4.0: Veracode Application List Integration (JSON) | Diese Integration ist standardmäßig inaktiv. Ruft Veracode Anwendungsscanner-Daten (Schwachstellen, Metadaten) ab und erweitert Ihre Anwendungsdaten.<br>Ruft Scan-Datensätze von Veracode über eine JSON-basierte API ab. |
| Ab v4.0: Veracode Application List Integration (XML) | Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Veracode Anwendungsscanner-Daten (Schwachstellen, Metadaten) ab und erweitert Ihre Anwendungsdaten. Diese Integration wird täglich um 00:00:00 Uhr ausgeführt.<br>**Hinweis:**<br>Eine JSON-basierte API von Veracode wird verwendet, um die Liste der Anwendungen abzurufen. Diese API importiert das Datum der letzten Complianceprüfung der Richtlinie für diese Anwendungen und gibt an, wann diese Anwendungen zuletzt von Veracodegescannt wurden. |
| Ab v4.0: Veracode Software Bill of Materials (SBOM) Integration | Diese Integration ist standardmäßig aktiviert. Importiert Software Bill of Materials -Dateien im von Veracode generierten CycleneDX-Format und stellt sie zur Analyse in Ihrer Instanz in die Warteschlange. Sie müssen die Anwendungen Software-Stückliste installiert haben, um diese Daten zu importieren und anzuzeigen. |
| Ab v4.0: Veracode Scan Summary Integration (JSON) | Diese Integration ist standardmäßig inaktiv. Ruft Scan-Datensätze von Veracode über eine JSON-basierte API ab. Diese Integration ersetzt die XML-basierte API-Integration. Sie ist verkettet und folgt der Anwendungslistenintegration Veracode, wenn sie aktiviert wird. |
| Ab v4.0: Veracode Scan-Zusammenfassung (XML) | Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Scan-Datensätze von Veracodeab. Diese Integration ist verkettet und folgt der Anwendungslistenintegration Veracode, wenn sie aktiviert wird.<br>**Hinweis:**<br>Verfolgt automatisch die Integration der Anwendungsliste Veracode, wenn sie aktiviert wird. Mit „Letzte Complianceprüfung der Richtlinie“ für die Anwendungen von Veracoderuft diese Integration nur Daten für die Anwendungen ab, die nach „delta_start_time“ dieser Integration gescannt wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Veracode Vulnerability Integration (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| Ab v4.0: Veracode JSON-Integration von angreifbaren Anwendungselementen | Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse mit mehr Schwachstellendaten als die XML-basierte Integration von Veracodeab. Es fügt AVIs ein und erweitert Ihre Schwachstellendaten von Drittparteien. |
| Ab v4.0: Veracode Integration von angreifbaren Elementen in Anwendungen (XML) | Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse von Veracodeab, fügt AVIs ein und erweitert Ihre Schwachstellendaten von Drittparteien. Wenn sich der Scanner-Datensatz im Status **Geschlossen** befindet, werden standardmäßig keine AVIs erstellt. Vorhandene AVIs werden weiterhin aktualisiert.<br><br>Diese Integration ist verkettet und folgt der Integration der Veracode Scan-Zusammenfassung, wenn sie aktiviert wird. Die XML-basierte API ist für die JSON-Integration der Veracode Scan-Zusammenfassung veraltet.<br><br>**Hinweis:**<br>Verfolgt automatisch die Integration der Veracode Scan-Zusammenfassung. Mit „Letzte Compliancеprüfung der Richtlinie“ für die Anwendungen von Veracoderuft diese Integration nur Daten für die Anwendungen ab, die nach „delta_start_time“ dieser Integration gescannt wurden. |
| Ab v4.0: Integration von Veracode Kategorien | Diese Integration ist standardmäßig inaktiv. Ruft erweiterte Kategoriedaten aus Veracodeab. |
| Ab v4.0: Veracode CWE-Integration | Diese Integration ist standardmäßig aktiviert. Ruft Veracode spezifische CWE-Daten (Common Weakness Enumeration) für Bedrohungsinformationen und Korrekturempfehlungen ab. Diese Daten werden in Datensätzen zu Anwendungsschwachstelleneinträgen ausgefüllt und aktualisiert.<br><br>Diese CWE-Integration funktioniert unabhängig von der geplanten Aufgabe für die CWE Comprehensive 2000-Integration, die Sie für die Anwendung Vulnerability Response aktivieren.<br><br>Ihre Daten werden nicht dupliziert, wenn Sie die Veracode CWE-Integration und die CWE Comprehensive 2000-Integration aktiviert haben. |
| Ab v4.0: Veracode DevOps-Integration | Diese Integration ist standardmäßig inaktiv. Die Integration kann in der Liste „Integrationen von Anwendungsschwachstellen“ in Application Vulnerability Responseangezeigt werden. Wenn Sie eine DevOps Change Velocity-Lizenz haben, ist diese Funktion so strukturiert, dass DevOps-Benutzer keine SecOps-Lizenz benötigen, um Zusammenfassungsdetails für Schwachstellenprüfungen von Drittanbietern anzuzeigen. Es gibt keine Auswirkungen oder Änderungen an Application Vulnerability Response. |

Informationen zu Integrationsausführungsstatus finden Sie unter, Zeigen Sie den Importausführungsstatus von Veracode Application Vulnerability Integration (Integration von Anwendungsschwachstellen) an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

### wird vorbereitet Veracode Vulnerability Integration

Eine erfolgreiche Veracode Vulnerability Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Veracode Vulnerability Integration setzt voraus, dass Sie mit dem Produkt und der API von Veracode vertraut sind.

### Vorbereitungen

Die CWE-Integration (Common Weakness Enumeration) wird auch von Application Vulnerability Response verwendet und sollte vor der Installation und Konfiguration von Veracode Vulnerability Integrationausgeführt werden. Er wird standardmäßig mit Vulnerability Responseinstalliert.

**Hinweis:**
NVD-Daten (NIST Vulnerability Database) sind für die Installation von Veracode Application Vulnerability Integration nicht erforderlich. Sie stellen jedoch eine Ergänzung dar und sind nützlich. Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

Für jeden Integrationsdatensatz ist ein „Ausführen als“-Benutzer konfiguriert. Der Standardwert für diesen Benutzer ist **VR.System**. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager-Gruppe

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie voraussichtlich importieren. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Veracode Vulnerability Integration erfordert eine API-ID und einen API-Schlüssel.

### Prozedur

So erstellen Sie die API-ID und die Schlüsselanmeldeinformationen:

**a.** Melden Sie sich bei der Veracode -Plattform an.

**b.** Wechseln Sie zum Menü „Benutzerkonto“, und wählen Sie **API-Anmeldeinformationen**aus.

**c.** Klicken **Sie auf API-Anmeldeinformationen generieren**.

**d.** Notieren Sie Ihre Anmeldeinformationen zur späteren Verwendung.

### ServiceNow® Vulnerability Response Integration with Veracodeinstallieren

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Veracode ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Benutzer der App-Sec Manager-Gruppe zu. Weitere Informationen zu Gruppenrollen finden Sie unter, Application Vulnerability Response -Benutzergruppen und -Rollen.<br>• Die App-Sec-Manager-Gruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rolle: admin

## Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie Veracode Vulnerability Integration installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow Store] nach der Anwendung Vulnerability Response Integration with Veracode.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   **Hinweis:**
   Ziehen Sie in Betracht, die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten** zu lesen.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Nächste Maßnahme

Konfigurieren Sie Veracode Vulnerability Integration für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration.

## Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen sein, damit das Produkt Veracode ordnungsgemäß in Application Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass die Anwendung Vulnerability Response Integration with Veracode installiert und aktiviert ist. | Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
|---|---|
| | Informationen unter ServiceNow Vulnerability Response Integration with Veracodeinstallieren. |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die App und weist Benutzer der App-Sec Manager-Benutzergruppe zu.<br>• Der App-Sec-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |
| Halten Sie für die Integration von Veracode Application Vulnerability Ihre **API-ID** und Ihren **API-Schlüssel** bereit. | Wenden Sie sich an Veracode, um die**API-ID** und den **API-Schlüssel**zu erhalten. Weitere Informationen finden Sie unter wird vorbereitet Veracode Vulnerability Integration.<br><br>Wenn Sie ab Version 4.0 Veracode Vulnerability Integrationverwenden, sind die Penetrationsbewertungstests in Veracode Vulnerability Integration manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Penetrationstest-Bewertungsanforderungen verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstestanforderungen in Application Vulnerability Responsefinden Sie unter Konfigurieren Sie Penetrationstests. |

Erforderliche Rolle: Benutzergruppe „App-Sec-Manager“.

### Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Konfiguration**.
2. Füllen Sie die Felder **API-ID** und **API-Schlüssel** aus.
3. Wählen Sie Ihre Testergebnisse aus.

| Option | Bezeichnung |
|---|---|
| **Version 4.0:** | **a.** Wählen Sie die Datentypen **DAST** oder **SAST** aus, die in den Import einbezogen werden sollen.<br><br>**Hinweis:**<br>Sie können das eine oder das andere oder beide auswählen, Sie müssen jedoch mindestens eines auswählen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | **b.** Wählen Sie **SCA** aus, um SCA-Schwachstellen (Software Composition Analysis) zu importieren.<br>**c.** Wählen Sie **Manuelle einbeziehen** aus, um die Ergebnisse manueller Penetrationstests aus Veracodezu importieren. Für diese Ergebnisse werden AVIs erstellt. |
| **Version 3.0** | Wählen Sie die Datentypen **DAST** oder **SAST** aus, die in den Import einbezogen werden sollen.<br>**Hinweis:**<br>Sie können das eine oder das andere oder beide auswählen, Sie müssen jedoch mindestens eines auswählen. |
| **Version 1.0:** | Die Ergebnisse des dynamischen Anwendungssicherheitstests sind standardmäßig ausgewählt. |

4. Fügen Sie den Veracode- **Schweregrad** hinzu, um Ihre importierten Daten zu filtern.
   Dieser Wert wird aus Veracode importiert. Sie können dem Feld mehrere Werte hinzufügen. Wenn ausgefüllt, erfasst der Import nur Daten, die den von Ihnen hinzugefügten Schweregradstufen entsprechen.
5. Speichern und validieren Sie Ihre Auswahl.

| Option | Bezeichnung |
| --- | --- |
| **Version 3.0:** | Klicken **Sie auf Anmeldeinformationen speichern und testen**.<br>**Hinweis:**<br>Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein. |
| **Version 1.0:** | Klicken Sie auf **Speichern**.<br>Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf **Anmeldeinformationen testen**klicken.<br>**Hinweis:**<br>Die Konfiguration ist erfolgreich abgeschlossen, sofern keine Fehlermeldung angezeigt wird. Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie aus, wie Sie Ausnahmen und falsch positive Meldungen für AVIs beim Import verwalten möchten.
   Optionen zum Verwalten von AVIs beim Import mit den ServiceNow Ausnahmeverwaltungs- und Falsch positiven Workflows sind standardmäßig aktiviert. Die Workflows werden basierend darauf ausgelöst, wie die **Quellstatus** in den AVIs in Ihrer Instanz zugeordnet werden. Ein Beispiel für einen Anwendungsfall finden Sie unter Statuszuordnung für Zurückstellungen und Falschmeldungen in verwalten Application Vulnerability Response.

7. Klicken **Sie auf Anmeldeinformationen speichern und testen**.

### Nächste Maßnahme
Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

Weitere Anweisungen zur Erstinstallation finden Sie unter Application Vulnerability Response konfigurieren.

Informationen zu Änderungen nach der Erstinstallation finden Sie unter Veracode Vulnerability Integration Änderungen und Aktivitäten.

## Zeigen Sie den Importausführungsstatus von Veracode Application Vulnerability Integration (Integration von Anwendungsschwachstellen) an

Verwenden Sie die zugehörige Liste „Ausführungen von **Schwachstellenintegrationen“**, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Korrekturentscheidungen zu treffen.

### Vorbereitungen
So zeigen Sie den Importausführungsstatus Veracode Vulnerability Integration an:

- Application Vulnerability Response und Veracode Vulnerability Integration müssen installiert und konfiguriert sein.
- Die Importe Veracode Vulnerability Integration müssen geplant sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager-Gruppe

### Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Application Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. [store-future: BEGIN review]Wenn Sie nicht das Integrationsausführungsstatusdiagramm Veracode ] verwenden, benötigt [End] Navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf die zugehörige Liste Ausführungen der **Schwachstellenintegration**.
4. Vergewissern Sie sich, dass alle Importe erfolgreich waren.

**Trouble?**

Zu den häufigsten Ursachen für eine fehlgeschlagene Ausführung gehören:

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

Wenn eine dieser Bedingungen auftritt, klicken Sie auf **Jetzt ausführen**, und führen Sie die Integration erneut aus.

## Zeigen Sie Veracode Scan-Zusammenfassungen an

Zeigen Sie Details für Scan-Zusammenfassungsinformationen für die Veracode Vulnerability-Integration an.

### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

### Prozedur

1. Navigieren Sie zur Tabelle „Zusammenfassungen von Application Vulnerability Scan“ [sn_vul_app_vul_scan_summary_list].
2. Wählen Sie einen Datensatz für einen Veracode -Scan aus.
3. Verwenden Sie ab Version 19.0 von Vulnerability Response und Version 4.0 von Veracode Vulnerability Integration das Symbol zum Personalisieren von Listen (Zahnradsymbol), um die folgenden Spalten anzuzeigen.
   - Größe des statischen Scans
   - Anzahl Bibliotheken von Drittparteien
   - Anzahl anfälliger Drittparteibibliotheken
   - Gesamtanzahl der Drittanbieterfehler nach Schweregrad
   - Anzahl Probleme von Drittparteibibliotheken
   - Anzahl Probleme von Drittparteilizenzen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anzahl gemischter Fehler
- Anzahl verringerter Fehler
- Anzahl der nicht verringerten Fehler
- Anzahl statischer Fehler nach Schweregrad
- Anzahl neuer Fehler nach Schweregrad
- Anzahl nicht verringerter Fehler nach Schweregrad
- Gesamtanzahl der Fehler nach Schweregrad
- Bewertung des letzten SCA-Scans
- Datum des letzten SCA-Scans
- Veröffentlichungsdatum des Scans
- Tags

### Datentransformation für die Veracode Vulnerability-Integration

Nachdem Sie die Daten identifiziert haben, die Sie importieren möchten, werden die Daten aus der Anwendung Veracode abgerufen, über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz transformiert.

## Veracode Integration von angreifbaren Anwendungselementen

Die Daten aus der API werden zuerst in die Tabelle [ Veracode AppVul-Elementimport [sn_vul_veracode_appvul_item_import] geladen, und die Veracode AppVul-Elementtransformation wird verwendet, um die importierten Informationen zu transformieren.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu *System Import Sets > Transform Maps*, und suchen Sie nach Veracode AppVul-Elementtransformation. In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### Veracode AppVul-Elementtransformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| app_id | source_app_id | Anwendungs-ID |
| Ausgabe-ID | source_avit_id | AVIT-ID |
| app_name | app_name | Anwendungsname. |
| version | app_version | Anwendungsversion. |
| build_id | source_scan_id | Build-ID der Anwendung. |
| account_id | account_id | Account-ID. |
| Sandbox-ID | Sandbox-ID | Sandbox-ID |
| last_update_time | last_scan_date | Zeit der letzten Aktualisierung. |
| app_name + last_scan_date | scan_summary_name | Scan-Zusammenfassung. |
| „life_cycle_stage“ | source_sdlc_status | SDLC-Quellstatus |
| level | source_severity | Quellschweregrad |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Veracode AppVul-Elementtransformationszuordnungsfelder (Fortsetzung)

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| category_name | Kategorie | Kategorie |
| source_severity | source_severity | Quellschweregrad |
| category_id + "CWE-" + cweId | source_entry_id | Quelleintrags-ID |
| source_vulnerability_summary | source_vulnerability_summary | Zusammenfassung der Quellschwachstelle. |
| source_recommendation | source_recommendation | Quellempfehlung. |
| Beschreibung | Beschreibung | Beschreibung aus der Quelle. |
| Beschreibung | source_vulnerability_explanation | Erklärung der Quellschwachstelle. |
| mitigation_status_desc | source_mitigation_status | Quellminderungsstatus. |
| remediation_status | source_remediation_status | Quellkorrekturstatus. |
| Zeile | line_number | Zeile, in der der Fehler gefunden wurde. |
| -Modul | application_module | Anwendungsmodul. |
| Quelldatei | source_notes | Quellnotizen. |
| wirkt sich auf_policy_compliance aus | entspricht_mit_Richtlinie | Die Werte können „Ja“ oder „Nein“ sein, je nachdem, ob die Quellinformationen „true“ oder „false“ sind. |
| Quelldateipfad + Quelldatei | location | Standortzuordnung im Falle eines `static` -Fehlers. |
| URL | location | Standortzuordnung im Falle eines `dynamic` -Fehlers. |
| Umfang, Typ, ExploitLevel | source_zusätzliche_info | Namenswertfeld, das bei statischen Fehlern mit den Werten aus der Quelle ausgefüllt wird. |

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

## Veracode Timing und Zweck des Transformationszuordnungsskripts

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist) | Skript, das verwendet wird, um die Datenquelle zu verarbeiten und die Anzahl der erstellten, aktualisierten oder unveränderten AVITs und der im Rahmen dieser Integration aus Veracodeimportierten AVITs zu aktualisieren. Dieses Skript ist für den internen Gebrauch bestimmt und darf nicht geändert oder gelöscht werden. |

### Veracode Vulnerability Integration Änderungen und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Veracode Vulnerability Integration.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Das Ändern anderer Veracode Vulnerability Integration -Einstellungen als der hier aufgeführten erfordert fortgeschrittene ServiceNow - und Application Vulnerability Response -Kenntnisse und geht über den Umfang der Produktdokumentation hinaus.

### Ändern Sie die Parameter der Integrationsinstanz Veracode .

Nach der Erstinstallation können Sie Parameter für die Veracode -Integrationen in der Veracode ]-Integrationsinstanz ändern.

### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

### Warum und wann dieser Vorgang ausgeführt wird
Sie können die Parameter für eine Integration in ihrer Instanz ändern, um zu bestimmen, welche Art von Daten Sie erfassen. Für einige dieser Einstellungen können Sie diese Parameter auch auf der Konfigurationsseite der Integration ändern.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**.
2. Wählen **Sie Veracode-Anwendungsschwachstelle** in der Spalte Quellinstanz für die Veracode -Integration aus, die Sie ändern möchten.
3. Wechseln Sie zur Registerkarte „ **Integrationsinstanzparameter** “, und doppelklicken Sie auf ein Feld in der Spalte „Wert“, um die Werte zu ändern.

   Ab Version 19.0 von Vulnerability Response und Version 4.0 von Veracode Vulnerability Integrationkönnen Sie die folgenden Parameter für die Integrationen von Veracode ] konfigurieren.

   **Importhandbuch**

   Geben Sie true ein, um die Ergebnisse manueller Penetrationstests aus Veracodezu importieren. Sie können diesen Wert auch auf der Integrationskonfigurationsseite ändern.

   Die Penetrationsbewertungstests in Veracode Vulnerability Integration sind manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Penetrationstest-Bewertungsanforderungen verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstestanforderungen in Application Vulnerability Responsefinden Sie unter Konfigurieren Sie Penetrationstests.

   **import_sca**

   Geben Sie true ein, um SCA-Schwachstellen (Software Composition Analysis) zu importieren. Sie können diesen Wert auch auf der Integrationskonfigurationsseite ändern.

   **Status**

   Geben Sie Offen oder Geschlossen ein, um Ergebnisse für die gewünschten Status zu importieren. Wenn Sie dieses Feld leer lassen, werden von der Integration Ergebnisse für die Status „Offen“ und „Geschlossen“ importiert.

   **policy_sandbox**

   Geben Sie eine Richtlinie oder Sandbox ein, um Datensätze zu importieren, die einer Richtlinie oder einer Sandbox entsprechen. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

   **policy_rule_passed**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie `true` oder `false` ein, um Datensätze zu importieren, die eine Richtlinienregel übergeben haben. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

4. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

### Führen Sie einen manuellen Veracode -Anwendungsschwachstellenimport durch

Wenn der erste Import fehlgeschlagen ist oder Sie nicht auf den geplanten ersten Import warten möchten, können Sie einen vollständigen Datenimport unabhängig von der täglichen geplanten Aufgabe durchführen.

#### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

#### Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie und Integration aus, z. B. Veracode Application List Integration.
3. Klicken Sie auf **Jetzt ausführen**.

**Hinweis:**
Jede der Veracode Anwendungsschwachstellenintegrationen soll einen möglichst vollständigen Datenabruf ermöglichen. Wenn sie in falscher Reihenfolge ausgeführt werden, sind Kenntnisse von ServiceNow und Application Vulnerability Response erforderlich, was zu unvollständigen Daten führen kann.

Sobald der Import abgeschlossen ist, werden die geplanten Importe fortgesetzt.

4. Informationen zu Integrationsausführungsstatus finden Sie unter, Zeigen Sie den Importausführungsstatus von Veracode Application Vulnerability Integration (Integration von Anwendungsschwachstellen) an.
5. Wenn Sie andere Integrationsparameter ändern möchten, müssen Sie zur Integrationsinstanz navigieren.

### Legen Sie Veracode Vulnerability Integration Importzeiten fest

Sie können die Startzeit für die Veracode Vulnerability Integration s zurücksetzen.

#### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

#### Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import führen die Veracode Schwachstellenintegrationen bei jeder Ausführung einen vollständigen Import durch. Weitere Informationen zum Ausführen von Importen finden Sie unter Führen Sie einen manuellen Veracode -Anwendungsschwachstellenimport durch.

#### Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**.
2. Wählen Sie eine Integration aus.
3. Legen Sie die neue **Startzeit fest**.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für die Importe von Veracode Application List Integration ist 00:00:00. Die anderen Integrationen sind **On-Demand** -Integrationen und werden so verkettet, dass sie nach der Veracode Application List-Integration ausgeführt werden. Das Ändern der **Startzeit** für eine dieser Optionen erfordert fortgeschrittene Kenntnisse von ServiceNow und Application Vulnerability Management.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

### Schließt geschlossene angreifbare Veracode-Anwendungselemente ein

Standardmäßig werden während der Integration von Veracode angreifbaren Elemente keine **geschlossenen** angreifbaren Elemente (AVIs) erstellt. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

#### Vorbereitungen

Veracode Vulnerability Integration muss installiert sein und ausgeführt werden.

Erforderliche Rolle: admin

#### Prozedur

1. Geben Sie im Textfeld Filternavigator der linken Navigation sys_properties.list ein**.**
2. Geben Sie im Suchfeld **Name** für die Liste sn_vul.create_closedein.
3. Doppelklicken Sie auf das Feld **Wert**, und legen Sie es auf **True**fest
4. Klicken Sie zum Speichern auf das grüne Häkchensymbol .
   Datensätze im Status „ **Geschlossen** “ werden beim nächsten Import von Veracode als AVIs in Application Vulnerability Responseerstellt.

## Application Vulnerability Response Schwachstellen werden korrigiert

Die Überwachung der Fehlerkorrektur ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen von angreifbaren Elementen in Anwendungen (AVIs) endet. Application Vulnerability Response bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

### Application Vulnerability Response Korrekturprozess

Die Korrektur angreifbarer Anwendungselemente erfolgt manuell.

Übersicht über den Prozess:

- Melden Sie sich bei der Application Vulnerability Response-Instanz an.
- Überprüfen Sie, ob Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Anwendungselemente wie erwartet funktionieren. Weitere Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter Identifizieren Sie Anwendungen in Application Vulnerability Response automatisch. Weitere Informationen zu Zuweisungsregeln finden Sie unter Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu.
- Validieren Sie, ob Ihre Korrekturziele korrekt sind. Unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response finden Sie Informationen dazu, wie Korrekturzielregeln funktionieren und wie sie überarbeitet werden können. Zeigen Sie den Status des Korrekturziels eines angreifbaren Anwendungselements an

  **Hinweis:**
  Korrekturzielregeln gehören zu AVIs. Diese Regeln werden ausgeführt, wenn die AVI importiert wird.

- Überprüfen Sie die Dashboards oder Berichte. Zeigen Sie beispielsweise Dashboards an, in denen die Alterung der AVIs nach Status angezeigt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Wenn die Anwendung Performance Analytics for Vulnerability Response (com.snc.vulnerability.analytics) aktiviert ist, können Benutzer mit bestimmten Rollen Daten anzeigen, die für die Mitglieder der Gruppen „App-Sec-Manager“ und „Security Champion“ von Interesse sind.

Für App-Sec-Manager enthält Performance Analytics for Vulnerability ResponseApplication Vulnerability Response die Übersicht [], die Ihnen bei der Überwachung von Problembereichen helfen kann. Weitere Informationen finden Sie unter Analytics and Reporting-Lösungen für dasDashboard „Application Vulnerability Response“ und „Application Vulnerability Management“ [PA].

Ab Version 13.0 der Anwendung Vulnerability Response : Für Security Champions enthält Performance Analytics for Vulnerability Response das Dashboard „Meine Anwendungsschwachstellen“, mit dem Sie Ihre Problembereiche überwachen können. Siehe Dashboard „Meine Anwendungsschwachstellen“.

Ab Version 13.0 der Anwendung Vulnerability Response : Informationen zum Begrenzen der für Berichte oder zugehörigen Listen erfassten Datenmenge finden Sie unter Definieren Sie Serviceklassifizierungen für die Berichterstellung Vulnerability Response und zugehörige Listen.

- Überprüfen Sie den Status der AVIs in der Reihenfolge ihrer Priorität nach Änderungen.
- Überarbeiten Sie das Risiko für die AVIs nach Bedarf. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsschwachstellen-Rechner.
- Weisen Sie die AVI bei Bedarf einer Zuweisungsgruppe zur Korrektur zu.
- Erneute Scans werden automatisch durch den Importzeitplan der Drittpartei ausgelöst.
- Wenn der Status nach dem erneuten Scannen **Fest**ist, werden AVIs während des Imports automatisch geschlossen.
- Wenn der Status nach dem Scan nicht **„Fixed**“ lautet, wird die AVI erneut geöffnet.

## Schwachstellenbibliotheken anzeigen

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) oder von Drittparteien importiert wurden, um zu entscheiden, ob eine Schwachstellengruppe eskaliert werden soll.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > für **Bibliotheken**.

Die folgenden Bibliotheken sind verfügbar:

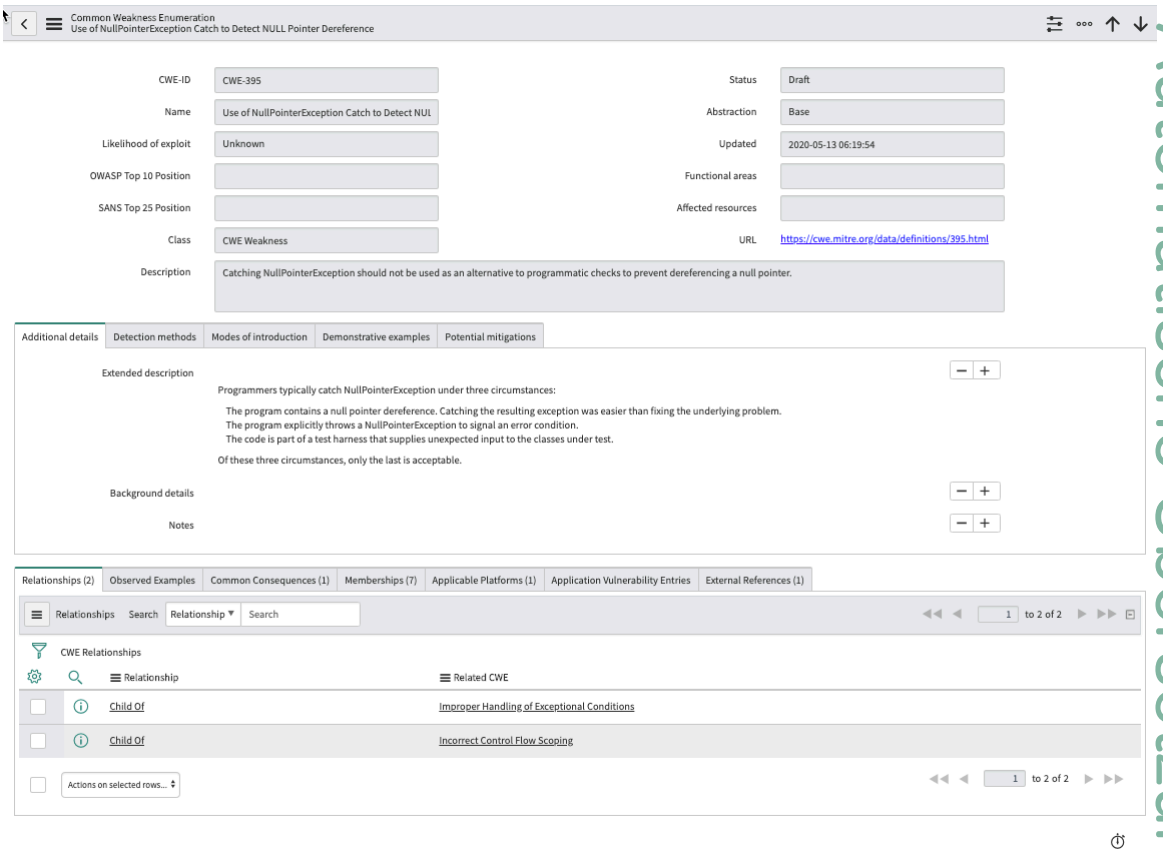
| Bibliotheken | Beschreibung |
|---|---|
| NVD | Liste der von NVD gefundenen Schwachstellen, einschließlich Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken, einschließlich Exploits. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Bibliotheken | Beschreibung |
|---|---|
| CWE | Liste der von der Community entwickelten Softwareschwachstellentypen.<br><br>Jeder CWE-Datensatz enthält auch einen zugehörigen Wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Common Weakness Enumerations“ eskalieren, er dient nur als Referenz. |
| Drittpartei | Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits, CWEs und CVEs |

2. Wählen Sie eine Bibliothek aus, um Schwachstellen anzuzeigen.




Automatische Übersetzung

Weitere Informationen zu bestimmten Feldern finden Sie unter Anwendungsschwachstellen-Felder.

### Anwendungsschwachstellen-Felder

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) oder Integrationen von Drittanbietern heruntergeladen werden. NVD und CWE werden unter **Bibliotheken** in Vulnerability Response oder unter **Schwachstellen** in Application Vulnerability Responsegespeichert.

## CWE-Schwachstelleneintragsfelder

Die Felder in dieser Tabelle sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| CWE-ID | Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird sowohl für Kategorien als auch für Schwachstellen verwendet und ist zwischen den beiden Datensätzen eindeutig. |
| Name | Beschreibender Name, der dieser CWE-ID zugewiesen ist. |
| Wahrscheinlichkeit der Ausnutzung | Wie wahrscheinlich es ist, dass die Schwachstelle auf einer qualitativen Skala ausgenutzt wird. Einer der folgenden:<br>• Niedrig<br>• Mittel<br>• Hoch |
| Position in OWASP Top 10 | Numerische Position dieser Schwachstelle in der OWASP Top 10-Liste. |
| SANS an Position 25 | Numerische Position dieser Schwachstelle in der SAN-Top-25-Liste. |
| Klasse | Typ der Schwachstelle |
| Status | Einer der folgenden:<br>• Unvollständig<br>• Entwurf<br>• Stabil<br>• Überholt<br>• Veraltet<br>• Unstabil |
| Zusammenfassung | Einer der folgenden:<br>• Variante<br>• Klasse<br>• Basis<br>• Verbindung |
| Aktualisiert | Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz. |
| Funktionsbereiche | Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung**. Wird nur für 24/862 Schwachstellen ausgefüllt. |
| Betroffene Ressourcen | Liste der betroffenen Ressourcen. Beispiel: **Datei** oder **Verzeichnis**. Wird nur für 51/863 Schwachstellen ausgefüllt. |
| URL | Knowledge Base-Artikel, der dieser Schwachstelle zugeordnet ist. |
| Beschreibung | Beschreibung der Schwachstelle. |
| Integrationsausführung | Die Integrationsausführung, in der diese CWE importiert wurde. |
| Abschnitte | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zusätzliche Details | Beschreibungen des Softwarekonzepts, die die Schwachstelle weiter erläutern. Beinhaltet:<br>• Erweiterte Beschreibung<br>• Hintergrunddetails<br>• Notizen |
| Erkennungsmethoden | Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können. |
| Einführungsmodi | Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **„Implementierung“**, „ **Architektur und Design“**usw. |
| Demo-Beispiele | Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen. |
| Potenzielle Minderungen | Details darüber, wie die Schwachstelle verhindert werden kann, einschließlich der Phase des Anwendungslebenszyklus, in der sie auftritt, und der Effektivität der Verringerung. |
| **Zugehörige Listen** | |
| Beziehungen | CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnet/untergeordnet, folgt/vorangehend, erforderlich von/erfordert (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, MemberOf enthalten. |
| Beispiele für Beobachtung | Einige CVEs, die für diese Schwachstelle repräsentativ sind. |
| Häufige Konsequenzen | Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Beispiel:<br>Bereich: Vertraulichkeit<br>Auswirkung: Anwendungsdaten lesen |
| Mitgliedschaften | CWE-Mitgliedschaften mit dieser Schwachstelle. |
| Anwendbare Plattformen | Plattformen, die dieser Schwachstelle zugeordnet sind |
| Anwendungsschwachstelleneinträge | Anwendungsschwachstelleneinträge, die einem zugeordnet sind. |
| Externe Referenzen | Informationen zur Schwachstelle aus externen Quellen. |

## Anwendungsschwachstellen-Eintragsfelder

Die Felder in dieser Tabelle sind schreibgeschützt.

| Feld | Beschreibung |
|---|---|
| ID | Bezeichner für diesen Schwachstelleneintrag. |
| Quelle | Ursprung der Schwachstelle – ob ein Scanner oder physischer Test. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow Drittanbieterintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu. |
| Version 13.0: Primäre CWE<br><br>Version 12.1: CWE-Eintrag | Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt.<br><br>Wenn der Schwachstelle mehr als eine CWE zugeordnet ist, wird die primäre CWE wie folgt bestimmt:<br>• Ist das CWE den OWASP Top 10 zugeordnet? Wenn dies der Fall ist, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort.<br>• Wird CWE den SANs Top 25 zugeordnet? Wenn dies der Fall ist, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort.<br>• Hat die CWE den höchsten Schweregrad? Wenn dies der Fall ist, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort.<br>• Wählen Sie die neueste aller CWEs aus. Die neueste CWE ist die mit dem letzten **aktualisierten** Feldwert im CWE-Datensatz. |
| Kategoriename | Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung. |
| **Schwachstellendetails** | |
| Bedrohung | Beschreibung der Bedrohung durch diese Schwachstelle. |
| Beschreibung der Verringerung | Beschreibung der Schritte, die zur Minderung der Schwachstelle durchgeführt werden können. |
| **Zugehörige Liste** | |
| Version 13.0:<br><br>CWEs | Liste der mit dieser Schwachstelle verknüpften CWEs Gilt nicht für Veracode Vulnerability Integration. |

## NVD-Eintragsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

### Hinweis:

NVD-Daten werden in Application Vulnerability Response nicht verwendet, und Einträge stellen nur Daten von Vulnerability Response dar.

CWEs, die in Application Vulnerability Responseverwendet werden, können auf NVD-Einträge als Beispiele für eine Schwachstelle verweisen und werden hier nur zu Informationszwecken bereitgestellt.

| Feld | Beschreibung |
|---|---|
| ID | Bezeichner für diesen Schwachstelleneintrag. |
| Risikobewertung | (Ausgeblendet, wenn der Schwachstelle keine Vulnerability Response angreifbaren Elemente (AEs) zugeordnet sind) |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Quantifizierte **Risikopunktzahl**, die VIs in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. |
| Risikopunktzahl | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Berechneter Betrag des Risikos, das das angreifbare Element für Ihre Umgebung darstellt. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle in Vulnerability Response. Schweregradzuordnungen werden für NVD und mit ServiceNow Drittanbieterintegrationen bereitgestellt. Application Vulnerability Response **Schweregrad** wird vom importierten **Quellschweregrad** und nicht von NVD abgeleitet. Weitere Informationen zur Schweregradzuordnung Application Vulnerability Response finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu. |
| Exploit vorhanden | Ja, wenn mindestens ein Exploit mit dieser Schwachstelle verknüpft ist. |
| Exploit-Kompetenzniveau | Niedrigste Kompetenzstufe, die zum Ausnutzen dieser Schwachstelle erforderlich ist. |
| Exploit-Angriffsvektor | Angreifbarster Angriffsvektor der Exploits für diese Schwachstelle. |
| Aktive AEs | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Anzahl der mit dieser Schwachstelle verknüpften angreifbaren Elemente, die sich nicht im Status „Geschlossen“ befinden. Wenn keine aktiven **AVIs** für diese Schwachstelle vorhanden sind, werden **Risikobewertung** und Risikopunktzahl nicht angezeigt. |
| CWE-Eintrag | Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle gemäß NVD am besten passt. |
| Veröffentlichungsdatum | Datum, an dem die Schwachstelle veröffentlicht wurde. |
| Zuletzt geändert | Datum, an dem die Schwachstelle zuletzt geändert wurde. |
| Zusammenfassung | Beschreibung der Schwachstelle. |
| **Schwachstellendetails** | |
| CVSS v2 | Importierte CVSS v2-Daten |
| CVSS v3 | Importierte CVSS v3-Daten, vor 2015 nicht verfügbar. |
| Bevorzugte Lösung | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Lösung mit der höchsten Ersatzlösung in der Kette, abgeleitet von den Lösungen, auf die in der Schwachstelle verwiesen wird. Wenn in der Kette mehr als eine höchste Ersetzung vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen. |
| **Nachbesserungsstatus**<br>(Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind) | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| **Zurückgestellte sind ausgeschlossen** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Anwendungselemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl enthält nicht die zurückgestellten angreifbaren Elemente. |
| **Beinhaltet Zurückgestellte** | |
| Angreifbare Elemente | Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. |
| VIs insgesamt | Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. |
| Behobene AEs in % | Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. |
| **Zugehörige Links** | |
| Vor v13.0: Import von Softwareschwachstellen erzwingen<br>**Hinweis:** In v13.0 entfernt | (Veraltet) Berechnet die Produktzuordnung mit ITSM Software Asset Management basierend auf Informationen aus NVD neu. Aktualisiert die Bibliothek für angreifbare Software. |
| Zustand aktualisieren | Zeigt Datum und Uhrzeit der letzten Aktualisierung an.<br>Aktualisiert Folgendes:<br>• Status der Schwachstellengruppe<br>• Risikopunktzahl und -bewertung<br>• Metriken wie Aktive AEs, AEs insgesamt aus dem Abschnitt „Korrekturstatus“. |
| **Zugehörige Listen** | |
| Angreifbare Elemente | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind. |
| Verwundbarkeitsreferenzen | Informationen über die Schwachstelle aus externen Quellen, angegeben von NVD. |
| Exploits | Exploits, die dieser Schwachstelle zugeordnet sind |
| Lösungen | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br>Alle Vulnerability Solution Management Integrationslösungen, die dieser Schwachstelle zugeordnet sind. |
| Version 13.0:<br>Schwachstellen | Importierte CWE-Schwachstellendaten, die einer gemeinsamen Schwachstelle und Gefährdung (CVE) zugeordnet sind |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Version 13.0:<br><br>Software mit Schwachstellen | (Ausgeblendet, wenn der Schwachstelle keine AEs zugeordnet sind)<br><br>Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind |

## Identifizieren Sie Anwendungen in Application Vulnerability Response automatisch

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Application Vulnerability Response automatisch Anwendungsdaten, um nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln identifizieren Anwendungen für den Datensatz des angreifbaren Elements (AVI), um die Korrektur zu unterstützen.

Beim Importieren von Anwendungen wird eine Suche in der gescannten Anwendung [sn_vul_app_scanned _application] tdurchgeführt, wobei „source_app_id“ und „app_name“ verwendet werden, um Übereinstimmungen mit Anwendungen aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Anwendungs-ID gefunden wird, werden ihre Werte in den Feldern **Anwendung** und **App-Release** im Datensatz des angreifbaren Anwendungselements verwendet.

Wenn keine Übereinstimmung gefunden wird oder das Feld „Anwendungs-ID“ leer ist, verwenden die Regeln die anderen Anwendungsinformationen, um zu versuchen, die Anwendung korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-Datensatz der gescannten Anwendung nur mit den Feldern **Anwendungsname** und **Anwendungs-ID** erstellt.

Die **Suchregeln für Quellanwendungs-ID** und **Anwendungsname** werden standardmäßig mit Veracode Vulnerability Integrationgeliefert.

**Hinweis:**
Standardmäßige CI-Suchregeln für Application Vulnerability Response sind nur für die Schwachstellenintegration Veracode ] verfügbar.

Beim Versuch einer Übereinstimmung werden die Suchregeln zuerst nach dem niedrigsten Wert für die **Reihenfolge** ausgewertet. Sie werden angehalten, wenn eine Regel ein einzelnes CI als Übereinstimmung zurückgibt.

**Hinweis:**
Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

Um die Suche nach Übereinstimmungsproblemen zu erleichtern, wird die CI-Suchregel, anhand derer eine Übereinstimmung gefunden wird, dem Feld **CI** -Übereinstimmungsregel für gescannte Anwendungen hinzugefügt, wenn eine Übereinstimmung gefunden wird. Klicken Sie oben in der Listenansicht der gescannten Anwendung auf das „Personalisierte Liste aktualisieren“, um sie der Ansicht hinzuzufügen.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie, wenn Sie neue Regeln erstellen.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Wenn unterstützt, kann jede Quelle mehrere Bereitstellungen haben. Beispielsweise kann Veracode Vulnerability



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration mehrere Bereitstellungen von Veracode Vulnerability Integration aufweisen. Jede Bereitstellung verfügt über eigene CI-Suchregeln.

**Hinweis:**
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenintegration gemeinsam verwendet. Wenn eine Regel gelöscht oder geändert wird, wirkt sich die Löschung oder Änderung auf alle Bereitstellungen der Schwachstellenintegration aus.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Abgleichen innerhalb von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie benutzerdefinierte CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Verhindern Sie doppelte oder verwaiste Datensätze nach der Ausführung von Application Vulnerability Response-CI-Suchregeln finden Sie weitere Informationen zum Verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

**Zugehörige Informationen**

Konfigurationsverwaltung und die CMDB

### Erstellen Sie eine CI-Suchregel

Das Modul **„CI-Suchregeln“** enthält Regeln, die definieren, welche Felder übereinstimmende Daten in der Configuration Management Database (CMDB)enthalten. Diese Regeln werden verwendet, um Anwendungen und Anwendungsveröffentlichungen zu identifizieren und dem AVI-Datensatz (Anwendung angreifbare Elemente) hinzuzufügen, um die Korrektur zu unterstützen.

### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

### Warum und wann dieser Vorgang ausgeführt wird
Das Erstellen von CI-Suchregeln erfordert fortgeschrittene Kenntnisse von ServiceNow und Application Vulnerability Management. Anstatt eine der vorhandenen Suchregeln zu ändern, sollten Sie sie kopieren und die Kopie ändern. Wenn Sie zufrieden sind, dass die neue Regel das tut, was Sie wollen, deaktivieren Sie die ursprüngliche.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie, wenn Sie neue Regeln erstellen.

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „CI-Suchregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel. |
| Suchmethode | Für den Abgleich verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

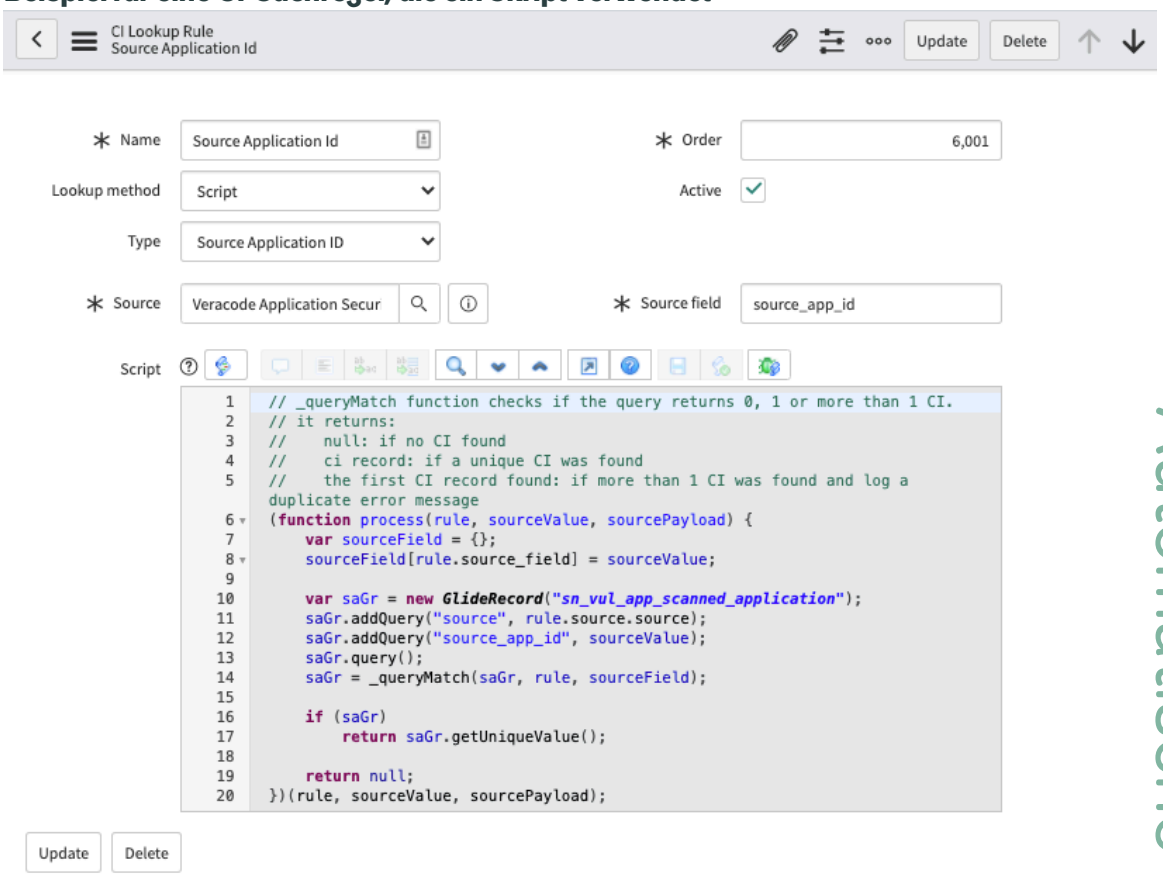
| Feld | Beschreibung |
|---|---|
| | ○ **Skript**: Vorgefertigtes oder benutzerdefiniertes Skript.<br>○ **Feldabgleich**: Durchsuchen Sie die Tabelle oder das Feld in der CMDB. |
| Typ | Mit der **Skriptsuchmethode**verwendeter Typ. |
| Bestellung | Rangfolge für die Regel. Übereinstimmungen mit der niedrigsten Reihenfolge werden zuerst ausgewertet. |
| Aktiv | Checkbox, ob die Regel aktiv oder deaktiviert ist. |
| Quelle | Quelle, die als Eingabe für diese Regel verwendet wird. Nach der Auswahl werden Bedingungsfilter angezeigt. |
| Quellenfeld | Quellfeld, das als Eingabe für diese Regel verwendet wird. Felder müssen eine Zeichenfolge oder Zahl sein. |
| Beschreibung | Text, der die Regel beschreibt. |
| V19.0: Suchziel | Suchansatz, den Sie verfolgen möchten. Wählen Sie aus:<br>○ Konfigurationselement<br>○ Produktmodell |
| Skript | Bearbeitbares Beispielskript, basierend auf dem **Typ**, wird angezeigt. Implementieren Sie das benutzerdefinierte Skript nach den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind.<br>**Hinweis:**<br>Die Prozessfunktion hat drei Parameter: *`rule`*, *`sourceValue`*und *`sourcePayload`*. |
| Durchsuchen Sie die Tabelle CI . | Tabelle, die in der CMDB durchsucht werden soll. Wird mit dem Feld verwendet, das der **Suchmethode**entspricht. |
| V19.0: Suche in Produkttabelle | Wenn Sie das **Suchziel**Produktmodell auswählen, lautet der Standardwert Anwendungsmodell. |
| Suchen Sie im Feld CI . | Feld, das Informationen enthält, die zum Suchen eines CI verwendet werden können. Wird mit der **Suchmethode**verwendet, die dem Feld entspricht. Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz befinden, z. B. ein Netzwerkadapter. |
| V19.0: Suche im Produktmodellfeld | Wenn Sie das **Suchziel**Produktmodell auswählen, lautet der Standardwert Name. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

**Beispiel für eine CI-Suchregel, die ein Skript verwendet**




**Zugehörige Informationen**

Felder für angreifbares Anwendungselement

### CI-Suchregeln in werden erneut angewendet Application Vulnerability Response

Sie können die Suchregeln für Configuration Items (CIs) erneut anwenden, um vorhandene CIs (gescannte Anwendungen und Produktmodelle) in erkannten Anwendungsdatensätzen zu aktualisieren.

## Erneutes Anwenden einer Suchregel

Durch erneutes Anwenden der CI-Suchregeln werden alle aktivierten Regeln auf vorhandene erkannte Anwendungen angewendet. Das Aktualisieren der erkannten Anwendungsdatensätze kann einige Zeit in Anspruch nehmen.

Um die Regeln erneut auf vorhandene erkannte Anwendungen anzuwenden, navigieren Sie zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln** und wählen **Sie Änderungen übernehmen**aus.

## Suchziel wird festgelegt

Standardmäßig ist die Systemeigenschaft *sn_vul.use_product_model* aktiviert (auf **true**festgelegt). Abhängig davon, wie die Systemeigenschaft für die CI-Suchregeldatensätze festgelegt ist, werden erkannte Anwendungsdatensätze auf folgende Weise aktualisiert:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn das Feld Wert auf **true**festgelegt ist, ist das Produktmodell das Suchziel für CI-Suchregeln, und erkannte Anwendungen werden mit den Produktmodellen aktualisiert.
- Wenn das Feld Wert auf **false**festgelegt ist, ist das Konfigurationselement (gescannte Apps) das Suchziel, und erkannte Anwendungen werden mit den Konfigurationselementen (gescannte Anwendungen) aktualisiert.

So ändern Sie die Systemeigenschaft *sn_vul.use_product_model*, sodass Konfigurationselemente als Ziel verwendet werden:

1. Navigieren Sie als Benutzer mit der Rolle sn_vul.app_sec_manager zu **Alle** > **Systemeigenschaften** > **Alle**
2. Suchen Sie *sn_vul.use_product_model*.
3. Öffnen Sie den Datensatz.
4. Legen Sie das Feld Typ auf **false fest**.
5. Wählen Sie **Aktualisieren**.

Wenn Sie diese Systemeigenschaft zurücksetzen, müssen Sie Ihre Regeln so ändern, dass die Suchziele mit der Einstellung der Systemeigenschaft übereinstimmen. Wenn Sie beispielsweise die Systemeigenschaft zurücksetzen, sodass Sie das Konfigurationselement als Ziel verwenden, suchen Sie die Regeln, die das Suchziel als Konfigurationselement enthalten.

1. Aktivieren Sie für diese Regeln das Kontrollkästchen Aktiv, und wählen Sie **Aktualisieren**.
2. Suchen Sie die Regeln, die das Produktmodell als Ziel verwenden, und deaktivieren Sie sie, indem Sie das Kontrollkästchen Aktiv deaktivieren und **Aktualisieren**auswählen.

Wenn Sie eine neue Suchregel erstellen, legen Sie das Suchziel für die Regel im Regelformular fest. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

#### Verhindern Sie doppelte oder verwaiste Datensätze nach der Ausführung von Application Vulnerability Response-CI-Suchregeln

Ergreifen Sie Maßnahmen, um doppelte oder verwaiste Datensätze zu verhindern, die aus dem Abgleich von (Konfigurationselementen (CIs)) innerhalb der CMDBresultieren.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Durchlaufen und Abgleichen in der CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Gründliches Testen und Debuggen von Verarbeitungsskripts in den Regeln trägt dazu bei, das Risiko später im Prozess auftretender Probleme zu verringern.

### Doppelte oder verwaiste Datensätze werden verhindert

- Verwenden Sie kleine Teilmengen von Daten, die für die getestete CI-Suchregel spezifisch sind.
  - Legen Sie alle **CI-Suchregeln**außer der getesteten auf **Inaktiv fest**.
  - Analysieren Sie die importierten Anwendungen und Konfigurationselemente (CIs), um sicherzustellen, dass Sie das erwartete Verhalten beobachten und die Übereinstimmung ordnungsgemäß erfolgt.
- Überprüfen Sie CI-Status wie **Deaktiviert**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Entfernen Sie die Testdaten. Sobald Sie das richtige oder erwartete Verhalten bei der CI-Übereinstimmung beobachten, beginnen Sie von vorne. Dies kann wie folgt erfolgen:
  - Löschen der zum Testen verwendeten Daten: (siehe Abschnitt **Daten aus Tabellen** löschen)
    - Gescannte Anwendungen
    - Angreifbare Anwendungselemente (AVIs)
  - Führen Sie die Integrationen manuell erneut aus.

.

### Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und feststellen, dass etwas nicht stimmt. Wenn dies in einer Entwicklungs- oder Leistungsumgebung geschieht, können Sie aus einer besseren Umgebung erneut klonen. Dies ist jedoch nicht immer eine Option.

**Hinweis:**
Das Ausführen dieser Aktionen erfordert fortgeschrittene ServiceNow.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

- Verwenden von **„Alle Datensätze löschen“** in der **Tabellenkonfiguration**.
- Konfigurieren Sie die **Tabellenbereinigung**, indem Sie zu **Auto Flushes** (sys_auto_flush.list) navigieren und einen neuen **Auto-Flush-** Datensatz erstellen.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

**Hinweis:**
Verwenden Sie `truncateTable` niemals in einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschvorgänge in Produktions- oder freigegebenen Umgebungen ausführen.

- Erstellen Sie in HI eine Anforderung, damit die Daten gelöscht werden.

### Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Anwendungs-Tags oder einer der Zuweisungsgruppen im Konfigurationselement [cmdb_ci] oder Plattformzuweisungsgruppen zu, um die durchschnittliche Zeit bis zur Zuweisung zu reduzieren.

### Angreifbare Anwendungselemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, AVIs mit **Zuweisen mit**zuzuweisen:

**Hinweis:**
Die Funktion für Zuweisungsempfehlungen in Vulnerability Response ist für Application Vulnerability Responsenicht verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benutzergruppe: Mit dieser Option können Sie eine der vorhandenen Now Platform® Benutzergruppen auswählen.
- Benutzergruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder im Listenmenü unter **Benutzergruppenfeld**angezeigt.
  - Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder fortgeschrittene ServiceNow.

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist, oder eine AVI, die durch die Einhaltung gesetzlicher Vorschriften behandelt werden muss). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um AVIs der Gruppe zuzuweisen, die ermittelt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt.

## Bewertungsprozess für Zuweisungsregeln

Wenn eine neue AVI erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln dafür ausgewertet. Eine AVI wird nur einmal ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jede neue, aktualisierte oder erneut geöffnete AVI verwendet:

- Für jede Schwachstellenzuweisungsregel wird die AVI mit dem Zuweisungsfilter verglichen, wobei die Regel der niedrigsten Ordnung zuerst verwendet wird.
- Wenn die Bedingung erfüllt ist, wird der AVI eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung mit allen anderen Regeln finden, wird die AVI der Standardzuweisungsgruppe zugewiesen, sofern eine Standardregel vorhanden ist.

**Hinweis:**
Wenn keine Standardregel vorhanden ist, bleibt die AVI nicht zugewiesen.

**Zuweisungstyp**, ob manuell oder **Regel** und **Zuweisungsregel,** ist im **Slushbucket** „Formularlayout“ im Formular für angreifbare Elemente in Anwendungen (AVI) verfügbar. Jede AVI, die ursprünglich durch eine Regel zugewiesen, aber später manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel. Verwenden Sie **Zuweisungsregel** und **Zuweisungstypinformationen**, um Fälle zu identifizieren, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Oder welche Regeln die meisten Neuzuweisungen aufwiesen.

**Hinweis:**
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie die Schaltfläche **Änderungen** übernehmen in der Listenansicht „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen AVIs (mit Ausnahme der manuell zugewiesenen) erneut auszuführen.

### Hinweis:

Wenn die geplante Aufgabe *`Reapply all vulnerability assignment rules`* vor der ersten Verwendung von **Änderungen**übernehmen nicht ausgeführt wurde, werden alle Zuweisungsregeln für alle offenen AVIs ausgeführt, mit Ausnahme der manuell zugewiesenen AVIs. Danach werden bei allen nachfolgenden Verwendungen von **„Änderungen anwenden** “ nur die geänderten Regeln und alle abhängigen Regeln erneut ausgeführt. Änderungen an einer Regel können dazu führen, dass eine AVI mit einer anderen unveränderten Regel übereinstimmt. [store-future: BEGIN review]Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.[End]

Die regelmäßige Aufgabe [*`Reapply all assignment rules`*] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen AVIs angewendet, mit Ausnahme der manuell zugewiesenen. Sie kann **Täglich**, **Wöchentlich**, **Monatlich**, **Regelmäßig**, **Einmal**oder **Bei Bedarf**ausgeführt werden. Je nachdem, wie viele aktive AVIs Sie in Ihrer Umgebung haben, denken Sie daran, das Feld **Ausführen** nach der ersten Ausführung entsprechend festzulegen, um Auswirkungen auf die Leistung zu vermeiden.

### Erstellen oder bearbeiten Sie Application Vulnerability Response Zuweisungsregeln

Sie können Regeln erstellen, um basierend auf Filterbedingungen automatisch angreifbare Elemente in Anwendungen (AVIs) zuzuweisen. Diese Regeln weisen AVIs zu, wenn sie importiert oder manuell erstellt werden.

#### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

#### Warum und wann dieser Vorgang ausgeführt wird

Mit Zuweisungsregeln definieren Sie die Zuweisungsbedingung und die Ausführungsreihenfolge. Sobald eine AVI mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet. Weitere Informationen finden Sie unter Filtern innerhalb Application Vulnerability Management.

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**.
2. Klicken Sie auf **Neu**.
3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

#### Zuweisungsregel für Anwendungsschwachstelle

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppenregel. |
| Aktiv | Gibt an, ob die Zuweisungsregel aktiv ist. |
| Ausführungsbefehl | Reihenfolge, in der die Regeln ausgewertet werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Regeln mit hoher Priorität, Elemente, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist, oder eine AVI sollten von der Compliance mit gesetzlichen Vorschriften behandelt werden, um zuerst ausgeführt zu werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist oder , und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um AVIs der Gruppe zuzuweisen, die ermittelt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt. |
| Beschreibung | Beschreibung der Zuweisungsregel. |
| Bedingung | |
| Bedingungsfelder | Bedingungen, die erfüllt sein müssen. |
| Neues Kriterium | Fügt weitere Bedingungsfilterfelder hinzu, aus denen Sie auswählen können. |
| Zuweisen mit | Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.<br>○ Benutzergruppe: Wählen Sie eine Benutzergruppe aus der Suchtabelle aus.<br>○ Benutzergruppenfeld: Wählen Sie im Listenmenü ein Benutzergruppenfeld aus.<br>○ Skript: Erstellen oder bearbeiten Sie ein Skript.<br>**Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert Kenntnisse von ServiceNow. |

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import bewertet.

## Risiko in Application Vulnerability Response automatisch berechnen

Anwendungsschwachstellen-Rechner automatisieren die Berechnung der anfänglichen Risikowerte für die Felder in angreifbaren Elementen in Anwendungen (AVIs). Risikoberechnungen bieten Einblicke in die Priorisierung von Remediationen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

### Anwendungsschwachstellen-Rechner

Das Application Vulnerability Response Basissystem enthält zwei Schwachstellenrechner, die die Basis- **Risikopunktzahl** für das angreifbare Anwendungselement festlegen.

- **Basisrisiko-Rechner**
- **Advanced Risk-Rechner**

Anwendungsschwachstellenrechner können erstellt werden, um die Auswirkungen von AVIs basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle, die Klasse des Konfigurationselements (CI) oder das Alter der AVI handelt, können Sie zusätzliche Schwachstellenrechner erstellen, um andere Felder in AVIs festzulegen. Oder Sie können die vorhandenen Schwachstellenrechner anpassen. Ein Rechner kann so geschrieben werden, dass er einen beliebigen Satz von Prioritäten widerspiegelt. Weitere Informationen finden Sie unter Filtern innerhalb Application Vulnerability Management.

AVIs enthalten den Risikopunktzahlwert, der von den **Risikorechnern** abgeleitet wird.

**Hinweis:**
Eine AVI zeigt den **Quellschweregrad** an, aber nicht den normalisierten Schweregrad. Der normalisierte Schweregrad wird von den Rechnern verwendet, um den Risikopunktzahlwert zu erhalten, wird jedoch nicht in **AVIs** angezeigt.

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Alle aktivierten Schwachstellenrechner legen die ausgewählten Felder jedes Mal fest, wenn eine AVI erstellt wird, wenn sich ein zugeordnetes CI oder eine Schwachstelle ändert.

Der **Basisrisiko** -Rechner berechnet die Risikopunktzahl für **AVIs** anhand des normalisierten Schwachstellenschweregrads.

**Hinweis:**
Pro Zielfeld (**Risikopunktzahl**) kann jeweils nur ein Rechner aktiv sein.

Das **Basisrisiko** ist standardmäßig aktiviert. Der **Advanced Risk Calculator** ist standardmäßig deaktiviert.

## Regeln des Anwendungsschwachstellen-Rechners

Der Basissystem- **Rechner des Risikorechners** enthält Rechnerregeln, die jeder Schweregradstufe (Keine bis Kritisch) basierend auf dem Schweregrad einen Wert (0 bis 100) für die **Risikopunktzahl** zuweisen. Dem**Schweregrad „Unbekannt“** wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, und wie **beim erweiterten Risikorechner**können neue Rechnerregeln oder neue Risikoregeln erstellt werden.

Der **Advanced Risk Calculator** -Rechner des Basissystems enthält eine spezialisierte Schwachstellen-Rechnerregel mit der Bezeichnung **Standardrisikoregel**. Sie berechnet die **Risikopunktzahl** basierend auf mehreren Werten:

- Schwachstellenschweregrad
- OWASP Top 10
- SANS Top 25

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel.

Sie können die in der **Standardrisikoregel** zu verwendenden Werte anpassen und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der **Risikopunktzahl**zählt.

Jede Regel hat eine Einstellung für die **Reihenfolge**. Die erste Übereinstimmung mit den Bedingungen aktualisiert jedoch das Feld **Risikopunktzahl** in der AVI. Nicht geskriptete



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rechnerregeln haben in der Regel weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

## Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen werden eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Exploit-Informationen usw. zugewiesen. Die Geschäftsregel *`Update Risk Rating from Risk Score`* in der Tabelle „Angreifbares Element“ ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert war.

| Wert (Risikobewertung) | Gewichtung (Risikopunktzahl) |
|---|---|
| 1 | 90–100 |
| 2 | 70–89 |
| 3 | 40–69 |
| 4 | 1–39 |
| 5 | 0 |

Ab Version 18.0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als avr_risk_rating bereitgestellt. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wurde so geändert, dass Sie die Einträge in den Werten der Tabelle „Risikopunktzahlgewichtungen“ für die Risikobewertungsberechnung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Gewichtungen der Risikopunktzahl“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (CI) von „Nicht mit Internetzugriff“ in „Mit Internetzugriff“ ändert.
- Wenn die zugeordneten Common Vulnerabilities and Exposures (CVEs) oder Drittanbietereinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer CVE Known Exploit Vulnerability (KEV) verknüpft sind

### Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die für Ihre Organisation eindeutigen Schwachstellen- und Asset-Daten verwenden. Durch Auswahl der Felder, die in der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

### Vorbereitungen

Erforderliche Rolle: sn_vul.app_manage_risk_score_configuration

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner**.
2. Klicken Sie auf der Seite „Schwachstellenrechner“ auf **Advanced Risk Calculator**.
3. Navigieren zu **Seite „Schwachstellenrechner“.** > **Registerkarte „Schwachstellenrechner – Regeln“** > **Standardrisikoregel**.
4. **Wahlweise:** Legen Sie im Abschnitt „Risikorechnerkriterien“ der Seite „Schwachstellenrisikoregel“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung in der Gesamtrisikopunktzahlberechnung fest.
5. Um die Regel zu deaktivieren, müssen Sie das Kontrollkästchen **Aktiv** deaktivieren.
6. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
7. Füllen Sie die Felder des Formulars aus.

**Formular „Risikoregelfeld“.**

| Feld | Beschreibung |
|---|---|
| Referenztabelle auswählen | Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen:<br>○ Angreifbares**Anwendungselement**: Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus per Dot-Walking zugänglich sind<br>○ **Angreifbares Anwendungselement – Konfigurationselement**: Fügen Sie Dot-Walkable-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci).<br>○ **Angreifbares Anwendungselement – Schwachstelle**: Fügen Sie Dot-Walkable-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittparteieintrag. Diese Felder sind nicht Teil der Basistabelle „Schwachstelleneintrag“.<br>○ Referenztabelle für angreifbare**Anwendungselemente**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) sind, oder Tabellen, die einen Verweis auf das angreifbare Element enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ **Konfigurationselement-Referenztabelle**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar.<br>○ **Schwachstellen-Referenztabelle**: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vul_entry sind, oder Tabellen, die einen Verweis auf sn_vul_entry enthalten. Diese Felder sind nicht direkt vom AE aus punktweise durchlaufbar.<br>○ **Benutzerdefinierte Bedingungen**: Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der mit dem Internet verbundene Filter, ob ein Configuration Item (CI) extern oder intern ist. |
| Tabelle | Feld, das nur angezeigt wird, wenn eine der folgenden Optionen in der Referenztabelle Wählen ausgewählt wird:<br>○ **Angreifbares Anwendungselement -> Konfigurationselement**<br>○ **Angreifbares Anwendungselement -> Schwachstelle**<br>○ **Referenztabelle für angreifbare Anwendungselemente**<br>○ **Referenztabelle für Konfigurationselemente**<br>○ **Referenztabelle für Schwachstellen** |
| Feld | Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll. |
| Zusammenfassung | Feld, das nur angezeigt wird, wenn eine Referenztabelle aus Referenztabelle wählen ausgewählt wird. Wählen Sie den minimalen oder maximalen Wert aus, der für Berechnungen berücksichtigt werden soll, wenn Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird. |
| Gewichtung | Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein. |
| Definieren Sie die Wertgewichtung | Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Die Gewichtungen müssen Ganzzahlen zwischen 0 und 100 sein.<br><br>**Hinweis:**<br>Dieses Feld wird nicht angezeigt, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt ist. |
| Bedingungstabelle | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Wählen Sie eine Bedingung aus der Liste aus. |
| Feldname | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Geben Sie einen Namen für die Risikokriterien ein. |
| Bedingung | Feld, das nur angezeigt wird, wenn in der Referenztabelle Wählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen. |

8. Klicken Sie auf **Absenden**.
9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

**Example:**
Fügen Sie den Quellschweregrad als Kriterium für eine Risikoregel hinzu.

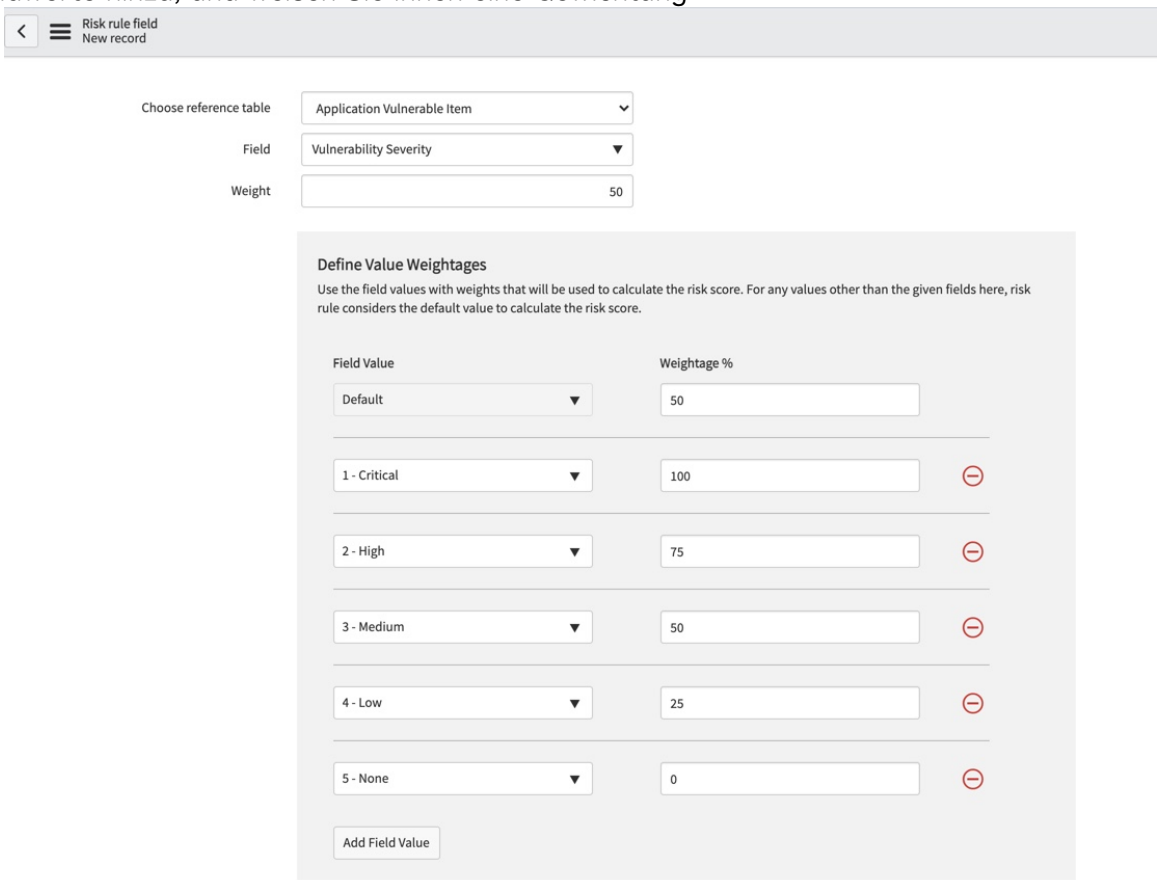
Anwendungsfall: Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden in das Feld Quellenschweregrad in der Tabelle „ **sn_vul_entry** “ eingetragen. Verwenden Sie dieses Feld für Risikopunktzahlberechnungen. Gehen Sie wie folgt vor, um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden:

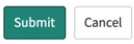
1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Aktiv**.
3. Um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen, klicken Sie auf **Kriterien**hinzufügen.
4. Wählen Sie in der Liste Referenztabelle auswählen die Option Angreifbares **Anwendungselement**aus.
5. Wählen Sie in der Liste Feld die Option **Vulnerability.Severity**aus.
6. **Geben Sie** im Feld Gewichtung die relative Bedeutung dieses Felds innerhalb der Risikoregel ein. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung




zu. 


8. Klicken Sie auf **Absenden**.

### Zugehörige Informationen

Vulnerability Response-Rechner und Schwachstellen-Rechnerregeln

## Erstellen Sie einen Anwendungsschwachstellen-Rechner

Ein Anwendungsschwachstellen-Rechner ist eine vordefinierte Formel, um ein Zielfeld zu berechnen, wenn bestimmte Kriterien erfüllt sind. Rechner, die die Risikopunktzahl des angreifbaren Elements (AVI) der Anwendung berechnen, können **Risikoregelnenthalten**. Risikoberechnungen bieten Einblicke in die Priorisierung von Remediationen.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

**Hinweis:**

Möglicherweise stellen Sie eine Leistungsverschlechterung fest, wenn Sie Anwendungsschwachstellen-Rechner ausführen, die Skripts enthalten.

Ordnen Sie Ihre Regeln so, dass die einfachsten Regeln zuerst ausgeführt werden. Führen Sie Skripts nur für die Elemente aus, die nicht mit einer Bedingung und einem Vorlagenwert oder einer Risikoregel behandelt werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

### Formular „Schwachstellenrechner“.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Anwendungsschwachstellen-Rechners. |
| Tabelle | Wird automatisch mit dem Namen der AVI-Tabelle ausgefüllt. |
| Anwendung | Automatisch ausgefüllt mit Vulnerability Response. |
| Zielfeld | Zu berechnendes Feld. |
| Beschreibung | Textbeschreibung des Rechners. |
| Aktiv | Schalten Sie den Rechner ein oder aus. |

4. Klicken Sie mit der rechten Maustaste auf den Header, um **Speichern**.
   Der Abschnitt „ **Regeln des Schwachstellenrechners“** wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf **Neu**klicken.

**Hinweis:**
Informationen zum Formular „ **Neue Risikoregeln“** (nur verfügbar, wenn das **Feld Ziel Risikopunktzahllautet**) finden Sie in Schritt 10.

6. Füllen Sie die Felder entsprechend aus.

### Formular „Schwachstellenrechner – Regel“

| Feld | Beschreibung |
|---|---|
| Name | Name der Rechnerregel. |
| Bestellung | Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rechner | Automatisch mit dem übergeordneten Rechner ausgefüllt. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie diese Checkbox deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden. |
| Erweiterte Ansicht | Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte aus **Bedingungstyp** und **Werttyp**ausgewählt werden. |

7. Füllen Sie die Felder auf der Registerkarte **Wenn diese Bedingung erfüllt** ist entsprechend aus.

### Registerkarte „Wenn diese Bedingung erfüllt ist“

| Feld | Beschreibung |
|---|---|
| Bedingungstyp | Verfügbar, wenn Sie die **erweiterte Ansicht**auswählen. Zur Auswahl stehen: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Filter: Verwendet Filterbedingungen.<br>○ Filtergruppe: Informationen zum Definieren der Rechnerkriterien finden Sie unter Filtergruppen erstellen und definieren.<br>○ Skript: Skriptbedingung, die verwendet wird, um zu bestimmen, wann dieser Rechner angewendet werden soll.<br>**Hinweis:** Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zur Liste der **Anwendungsschwachstellenrechner** zurück. Untersuchen Sie die Datensätze des Schwachstellenrechners, die im Lieferumfang des Basissystems enthalten sind. |
| Bedingung | Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll oder nicht.<br>Wenn Sie entweder die Bedingungstypen **Filtergruppe** oder **Skript** auswählen, wird dieses Feld ausgeblendet. |

8. Klicken Sie auf die Registerkarte **Diese Werte festlegen**, und füllen Sie die Felder im Formular entsprechend aus.

**Legen Sie diese Felder auf der Registerkarte fest**

| Feld | Beschreibung |
|---|---|
| Werttyp | Verfügbar, wenn Sie die **erweiterte Ansicht**auswählen. Zur Auswahl stehen:<br>○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen.<br>○ Skript: Wird verwendet, um die Werte in jedem Feld festzulegen. |
| Skriptwerte | Verfügbar, wenn Sie den **Werttyp Skript** ausgewählt haben.<br>Definiert, auf welche Werte die Berechnungen angewendet werden sollen. |
| Vorlage | Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten.<br>Wenn Sie einen der **Werttypen Skript** auswählen, wird dieses Feld ausgeblendet. |

9. Wenn Sie alle Eingaben abgeschlossen haben, klicken Sie auf **Absenden**.

**Hinweis:**
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie die **Schaltfläche Rechner erneut anwenden** verwenden. Er durchläuft alle aktiven AVIs. Wenn dieser Rechner zum Festlegen des Werts verwendet wird, wird der Wert für diese AVIs neu berechnet. Da das erneute Anwenden eines Rechners sehr lange dauern kann, wird dies mit einer regelmäßigen Aufgabe erledigt.

10. Füllen Sie im Formular **„Neue Risikoregeln“** die entsprechenden Felder aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

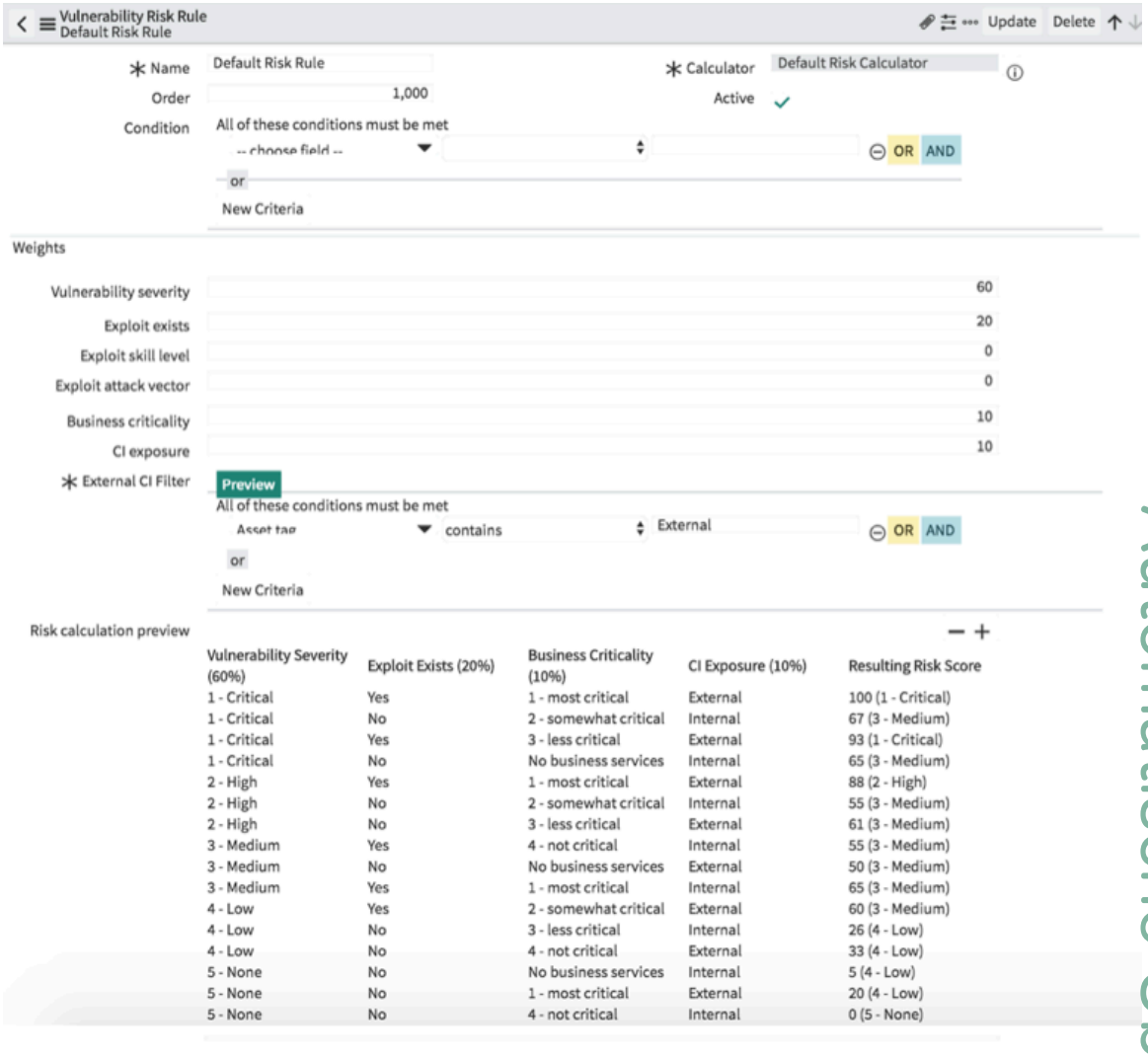
Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der aus diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollen, die Gewichtung auf 0 fest.

Wenn Sie die Gewichtungen aktualisieren, zeigen Szenarien die verbleibenden Gewichtungen sowie die erwarteten Ergebnisse der **Risikopunktzahl** an.

| Feld | Beschreibung |
|---|---|
| Name | Name der Rechnerregel. |
| Bestellung | Die Reihenfolge, in der der Rechner ausgeführt werden soll. Ein Rechner mit einem Reihenfolgeeintrag von 100 wird vor einem Rechner mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Rechner | Automatisch mit dem übergeordneten Rechner ausgefüllt. |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie diese Checkbox deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt werden. |
| Bedingung | Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll.<br>Wenn Sie entweder die Bedingungstypen **Filtergruppe** oder **Skript** auswählen, wird dieses Feld ausgeblendet. |
| **Gewichtungen** | |
| Schwachstellenschweregrad | Prozentsatz des Ergebnisses, der aus dem Schweregrad stammt. |
| OWASP Top 10 | Prozentsatz des Ergebnisses, der auf das Vorhandensein der Schwachstelle in der OWASP Top 10-Liste zurückzuführen ist. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0. |
| SANS Top 25 | Prozentsatz des Ergebnisses, der aus dem Vorhandensein der Schwachstelle in der SANS-Top-25-Liste stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, setzen Sie die Gewichtung auf 0. |
| Laufende Summe | Automatisch berechnete Prozentsätze. Wenn dieser Wert 100 erreicht, zeigt die Szenariovorschau Beispiel-Risikopunktzahlen in verschiedenen Szenarien an. |
| Beispielszenarien | Wenn alle Gewichtungen 100 % ergeben, werden Risikopunktzahl-Szenarien angezeigt, die eine Vorschau der Risikopunktzahl in einigen der möglichen Szenarien bieten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**11.** Klicken Sie auf **Absenden**.

## Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu

Die SchweregradzuordnungApplication Vulnerability Response wandelt Quellschweregradfelder von Drittparteien in erkennbare Felder innerhalb von Vulnerability Responseum.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

### Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response Integrationen von Drittparteien wie Veracode Vulnerability Integration stellen Schweregradzuordnungen bei der Installation bereit. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für benutzerdefinierte oder nicht standardmäßige Drittparteizuordnungen in Ihrer Umgebung vorgesehen und erfordert Application Vulnerability Response und ServiceNow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

#### Feldzuordnung

| Feld | Beschreibung |
|---|---|
| Quelle | Der Name der Quelle für die Schweregradzuordnung. |
| Quellwert | Der Quellschweregradwert. |
| Zielwert | Der Zielschweregradwert. Die Auswahlmöglichkeiten lauten wie folgt:<br>○ 1 - Kritisch<br>○ 2 – Hoch<br>○ 3 – Mittel<br>○ 4 – Niedrig<br>○ 5 – Keine |

4. Wiederholen Sie Schritt 3 für jeden Quellschweregrad.
5. Klicken Sie auf **Absenden**.

#### Filtern innerhalb Application Vulnerability Management

Rechner und Zuweisungsregeln verwenden während des Imports Bedingungen, die mit dem **Bedingungsgenerator**erstellt wurden. Änderungen an den Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

Die im Lieferumfang des Basissystems enthaltenen Regeln und Rechner sind auf Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern erfordert Sorgfalt und erfordert möglicherweise sowohl ServiceNow als auch Application Vulnerability Response. Allerdings sind einige Anleitungen verfügbar.

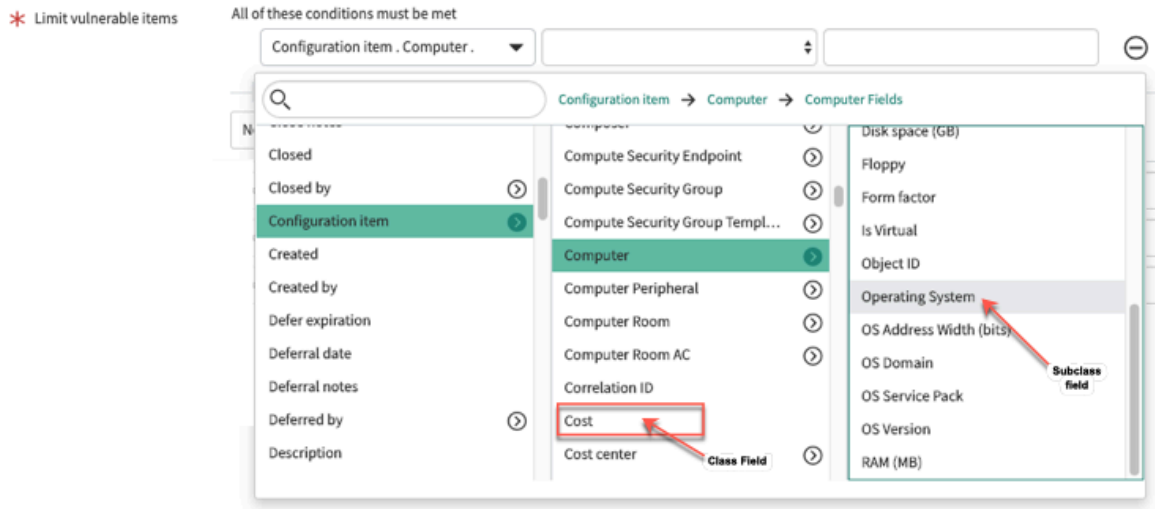
### Vermeiden Sie die Filterung basierend auf Unterklassenfeldern

Einige Tabellen unterstützen die Erweiterung. Ein Beispiel hierfür ist die Tabelle „CMDB CI“ [cmdb_ci]. Tabellen wie cmdb_ci_hardware und cmdb_ci_computer erweitern diese Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann die Erstellung und Auswertung dieses Filters teuer sein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Dropdown-Menü „Bedingungsfilter“**




Beispiel: Filtern nach **Konfigurationselement** > **Kosten** würde die Leistung nicht beeinträchtigen, da **Kosten** ein Klassenfeld und kein Unterklassenfeld von **Konfigurationselement**ist.

**Konfigurationselement** > **Computer**ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser Prozess kann viele Millisekunden dauern, was sich schnell summiert, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigt.

**Hinweis:**
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann Auswirkungen auf die Leistung haben. Die Verwendung von [ist] ist, wo immer möglich, effizienter.

## Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response

Anwendungskorrektur-Zielregeln definieren den erwarteten Zeitrahmen für die Korrektur von angreifbaren Elementen in Anwendungen (AVIs) und bieten einen Zeitrahmen für die Korrektur der Schwachstelle. Wenn beispielsweise ein angreifbares Anwendungselement eine kritische Risikobewertung enthält, muss die Schwachstelle in diesem Element innerhalb von 15 Tagen behoben werden.

App-Sec-Manager können Anwendungskorrektur-Zielregeln erstellen, indem sie Folgendes definieren:

- Das Korrekturziel.
- Das Erinnerungsziel.
- [store-future: BEGIN review]Die Erinnerungs- und Benachrichtigungsempfänger – Wer benachrichtigt werden soll, wenn die AVIs das Erinnerungs- oder Korrekturzieldatum überschritten haben und nicht korrigiert wurden.[End]

App-Sec-Manager können das Korrekturzieldatum im AVI-Formular und in Listenansichten anzeigen. Für **AVIs**im Status „Zurückgestellt“, „ **Gelöst**“ oder „ **Geschlossen** “ werden jedoch keine Daten aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das **Korrekturzieldatum** ist in der AVI-Listenansicht wie folgt farbcodiert als Punkte:

- AVIs, die ihr Benachrichtigungsdatum noch nicht erreicht haben, werden in Grün angezeigt.
- AVIs, die sich dem Korrekturzieldatum nähern, werden in Orange angezeigt.
- AVIs, die nach dem Korrekturzieldatum liegen, werden rot angezeigt.

[store-future: BEGIN review]Gemäß der Anwendungskorrekturzielregel wird eine Zusammenfassungs-E-Mail gesendet, wenn eine oder mehrere AVIs sich ihrem Korrekturzieldatum nähern oder das Korrekturzieldatum verstrichen ist.[End]

## Standardregeln

Application Vulnerability Response Im Lieferumfang von sind drei Standardregeln enthalten, die standardmäßig inaktiv sind:

- Regel für die Einstufung kritischer Risiken: Ein Korrekturziel mit der Risikobewertung „ **1 – Kritisch** “, einem Korrekturziel von 15 Tagen und einer Erinnerung von **7** Tagen vor dem Zieldatum.
- Regel für die Einstufung mittlerer bis hoher Risiken: Ein Korrekturziel mit einer Risikobewertung von **2 – Hoch** oder **3 – Mittel**, ein Korrekturziel von 30 Tagen und eine Erinnerung von **7** Tagen vor dem Zieldatum.
- Regel für die Einstufung weniger kritischer Risiken: Ein Korrekturziel mit einer Risikobewertung von **4 – Niedriges** Risiko, einem Korrekturziel von 45 Tagen und einer Erinnerung von **7** Tagen vor dem Zieldatum.

## Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert ist, werden die aktuellen Korrekturzieldaten für die AVIs gelöscht, auf die sie angewendet wurde. Wenn eine AVI eine aktive Regel erfüllt, wird diese Regel angewendet. Andernfalls hat die AVI keine Regel oder kein Zieldatum und ihr Status ist **Kein Ziel**.

Wenn Regeln gelöscht werden, werden das Korrekturzieldatum und zugehörige Felder in geschlossenen **AVIs** beibehalten. Das Korrekturzieldatum und zugehörige Felder in nicht geschlossenen **AVIs** werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

## Szenario mit Korrekturregeln

Wenn mehrere Korrekturzielregeln auf dieselbe AVI angewendet werden, wird die restriktivste Regel angewendet.

Beispiel: Wenn eine AVI die Bedingung für zwei Anwendungskorrekturzielregeln erfüllt:

Szenario: AVI zuletzt geöffnet am 01.03.2018 um 10:00:00.

- Anwendungskorrektur-Zielregel 1: Zuletzt geöffnet am 03.07.2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen. Das berechnete Korrekturzieldatum ist der 16.03.2018 10:00:00.
- Anwendungskorrektur-Zielregel 2: Zuletzt geöffnet am 10.03.2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen. Das berechnete Korrekturzieldatum ist der 11.03.2018 10:00:00.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Szenario gilt die Anwendungskorrektur-Zielregel 2 für die AVI, da sie das restriktivere Datum hat. 10 Tage seit der ersten Identifizierung der AVI im Vergleich zu 15 Tagen.

**Hinweis:**

Anwendungskorrekturziele werden aus dem Datum von „ **Zuletzt geöffnet** “ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Sie können dieses Feld dem AVI-Formular aus dem Slushbucket „Formularlayout“ hinzufügen. Dies ist das Datum, an dem die AVI zuletzt in Ihrer Instanz geöffnet wurde.

Ab V17.1 werden Korrekturziele aus dem **Ziel ab (Datum)**berechnet. Der Standardwert bleibt **Zuletzt geöffnet am**.

**Hinweis:**

Sobald die Anwendungskorrekturzielregel definiert ist, werden die Korrekturzieldaten von der geplanten Aufgabe *`Evaluate remediation targets`* oder der Schaltfläche **Changes** übernehmen in der Listenansicht der Korrekturzielregeln berechnet.

## Über die geplante Aufgabe „Korrekturziele auswerten“

*`Evaluate remediation targets`* wird einmal täglich um 4:00:00 Uhr ausgeführt.

*`Evaluate remediation targets`* durchläuft alle aktiven Schwachstellenregeln, beginnend mit den Regeln mit dem frühesten Korrekturzieldatum. Es werden alle AVIs betrachtet, die:

- Sie befinden sich nicht im Status „ **Geschlossen**“, **„Zurückgestellt“**oder **„Gelöst“**.
- Hat kein Korrekturzieldatum.
- Sie haben ein Korrekturzieldatum, das nach dem Datum in der Anwendungskorrekturzielregel liegt.

*`Evaluate remediation targets`* fügt ein Korrekturzieldatum hinzu, wenn keines vorhanden ist, oder wenn diese Regel ein früheres Datum als das im Datensatz enthält, wird das vorhandene Zieldatum aktualisiert. Schließlich werden die Felder Korrekturzieldatum und **Korrekturstatus** im **AVI-** Formular aktualisiert. Bei inaktiven Regeln löscht **Korrekturziele** auswerten die Korrekturfelder in der AVI.

## Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, verwenden Sie die Schaltfläche **Änderungen anwenden** auf der Listenseite „Korrekturzielregeln“, um alle geänderten Regeln für alle aktiven offenen **AVIs**mit Ausnahme derer im Status „ **Geschlossen** “, „Zurückgestellt“ oder „ **Gelöst** “ erneut auszuführen.

**Hinweis:**

Wenn die geplante Aufgabe *`Evaluate remediation targets`* ausgeführt wird, können Sie keinen erneuten Anwendungsprozess initiieren. Wenn jedoch bereits ein Prozess zum erneuten Anwenden ausgeführt wird und die geplante Aufgabe ausgelöst wird, werden sie parallel ausgeführt.

Die Prozesse zum erneuten Anwenden in Vulnerability Response und Application Vulnerability Response sind unabhängig und können parallel ausgeführt werden.

### Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur

Fördern Sie die zeitnahe Korrektur von Schwachstellen mit hohem Risiko, indem Sie eine Korrekturzielregel auf der Ebene des angreifbaren Elements (AVI) einrichten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

**Hinweis:**
Im Lieferumfang des Basissystems sind drei Korrekturzielregeln enthalten.

- Regel für die Einstufung kritischer Risiken
- Regel für die Einstufung weniger kritischer Risiken
- Regel für die Einstufung mittlerer bis hoher Risiken

Diese Regeln sind standardmäßig inaktiv. Wenn Sie eines bearbeiten möchten, anstatt ein neues zu erstellen, denken Sie daran, vor dem Speichern das KontrollkästchenAktiv zu aktivieren.

### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Nachbesserungszielregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel. |
| Ziel (Tage) | Geben Sie die Anzahl der Tage an, innerhalb derer die AVIs seit dem letzten Öffnen korrigiert werden sollen. |
| V17.1: Ziel ab (Datum) | Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur das Datums- oder das Datums- und Uhrzeittypfeld angeben. Der Standardwert ist Zuletzt geöffnetes Datum. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1185029 . |
| Aktiv | Standardmäßig ist die **Checkbox Aktiv** aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn diese Checkbox deaktiviert ist, gilt diese Regel nicht für neue AVIs, die im System erstellt werden. |
| Benachrichtigen (Tage vor dem Fälligkeitsdatum) | Anzahl der Tage vor der angestrebten Korrekturzeit, für die eine Erinnerung festgelegt werden soll. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „In Ausführung“. Wenn das Benachrichtigungsdatum überschritten ist und das Korrekturzieldatum erreicht ist, wird der Status als „Ziel erreicht“ angezeigt.<br>**Hinweis:**<br>Wenn dieses Feld auf 0 festgelegt ist, wird nur die Benachrichtigung **„Ziel verfehlt** “ festgelegt. |
| Regel gilt für | Wählen Sie mithilfe des Bedingungsfilters die Kriterien für die Anwendung der Regel auf die AVIs aus. Um Auswirkungen auf die Leistung zu vermeiden, testen Sie Ihre Bedingungen im vollständigen Produktionsmaßstab. Mit Tests können Sie bestimmen, wie lange die Ausführung der Aufgabe „ **Korrekturziele evaluieren** “ unter Berücksichtigung der Bedingungen und der Größe Ihres Configuration Management Database (CMDB)dauert. |
| Aktualisierungsverlauf | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Aktivitäten | Wird für die erstmalige Erstellung einer Regel nicht verwendet. Anschließend werden hier Systemarbeitsnotizen protokolliert. |

4. Klicken Sie auf **Absenden**.
   Diese Regel wird bei der nächsten Ausführung der geplanten Aufgabe `Evaluate remediation targets`wirksam. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird oder wenn in der Listenansicht der Korrekturzielregeln die Schaltfläche **Änderungen** übernehmen verwendet wird. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Weitere Informationen zur regelmäßigen Aufgabe und zum **Anwenden von Änderungen** finden Sie unter, Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.

### Zeigen Sie den Status des Korrekturziels eines angreifbaren Anwendungselements an

Wenn ein angreifbares Anwendungselement (AVI) sein Korrekturzieldatum fast erreicht (oder überschritten) hat, wie durch eine Korrekturzielregel definiert, wird der AVI-Datensatz mit einem Status aktualisiert. Diese Informationen können Ihnen helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

#### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

#### Warum und wann dieser Vorgang ausgeführt wird
Die regelmäßige Aufgabe **„Korrekturziele evaluieren“** wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl von Tagen liegt, bevor die Korrektur überfällig ist, wird dem Datensatz des angreifbaren Elements ein Korrekturstatus hinzugefügt.

#### Prozedur

Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**.
Wenn das Korrekturdatum für die AVI innerhalb des Bereichs der in der Korrekturzielregel festgelegten Bedingungen liegt, überprüfen Sie die Spalten Korrekturzielstatus, die in der Listenansicht der angreifbaren Elemente sichtbar sind. Wenn das Korrekturzieldatum für eine AVI abgelaufen ist, wird im AVI-Formular eine Anmerkung angezeigt.

**Hinweis:**
Informationen zum Anzeigen der Anzahl **derAVIs**mit den Status „Ziel erreicht“, „Wird ausgeführt“ und „**Vergangenes Ziel**“ finden Sie im Dashboard für Anwendungsschwachstellenmanagement [PA].

#### Zugehörige Informationen

Erstellen oder bearbeiten Sie Zielregeln für die Anwendungskorrektur

## Penetrationstests

Penetrationstests in Application Vulnerability Response ermöglichen es Anwendungsbesitzern, die Sicherheitslage ihrer Anwendung zu bewerten. Es handelt sich um das manuelle Testen einer Anwendung durch das Team für ethisches Hacken.

## Erforderliche Rollen

Penetrationstests erfordern die folgenden Rollen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**App-Sec-Manager**: Enthält Sicherheitsmanager und Anwendungsbesitzer, die die Penetrationstest-Bewertungsanforderungen verwalten. Sie enthält die folgenden granularen Rollen:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

**Ethischer Hacker**: Enthält Mitglieder des Teams für ethisches Hacken, die Penetrationstests von Anwendungen durchführen. Sie umfasst die folgenden granularen Rollen:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Weitere Informationen zu diesen Rollen finden Sie unter Application Vulnerability Response -Benutzergruppen und -Rollen.

Ab Version 19.0 von Vulnerability ResponseVeracode Vulnerability Integrationsind die Penetrationsbewertungstests in Veracode Vulnerability Integration bei Verwendung von [] manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstest-Bewertungsanforderungen verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstest-Bewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

## Lebenszyklus von Penetrationstests

Als Anwendungsbesitzer können Sie das Ethical Hacking-Team um eine Penetrationstestbewertung Ihrer Anwendung bitten. Das Team für ethisches Hacken reagiert auf diese Anforderung und erstellt Penetrationstestergebnisse. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Anwendungselemente (AVIs).

Der Penetrationstest-Workflow deckt den Penetrationstest-Lebenszyklus ab, von der Testanforderung bis zur Lösung der Ergebnisse des Teams für ethisches Hacken.

## Fordern Sie eine Penetrationstestbewertung an

Ab v19.0 können Sie in neue Anforderungen erstellen oder vorhandene Anforderungen kopieren **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**.

Vor v19.0 können Sie als Anwendungsbesitzer mithilfe des ITSM-Servicekatalogs eine Penetrationstestbewertung für Ihre Anwendung anfordern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Überprüfen der Penetrationstest-Bewertungsanforderung

Das Team für ethisches Hacken überprüft und bewertet die Anwendung und den Umfang der Penetrationstest-Bewertungsanforderung und fügt sie dem vorhandenen Rückstand hinzu.

### Umgebung wird vorbereitet

Das Team für ethisches Hacken sendet dann eine Anforderung an den Anwendungsbesitzer, eine Umgebung bereitzustellen, in der er mit dem Testen beginnen kann. Sobald die Umgebung bereit ist, informiert der Anwendungsbesitzer das Team für ethisches Hacken.

Weitere Informationen zum Konfigurieren von Testanforderungen finden Sie unter Konfigurieren Sie Penetrationstests.

### Testen und Melden der Penetrationstestergebnisse

Das Team für ethisches Hacken testet die Anwendung und meldet die Ergebnisse dem Anwendungsbesitzer. Das Team für ethisches Hacken definiert auch die Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) für die Ergebnisse der Penetrationstests anhand des Korrekturzieldatums. Diese Ergebnisse sind die manuell erstellten AVIs. Der Anwendungsbesitzer überprüft wiederum die vom Team für ethisches Hacken erstellten AVIs. Sie planen die Korrekturen und weisen sie dem Anwendungsteam zu.

**Hinweis:**
Korrekturzielregeln gelten nicht für Penetrationstestergebnisse.

Das Team für ethisches Hacken kann eine Bibliothek von Anwendungsschwachstelleneinträgen (AVEs) erstellen und diese beim Melden der AVIs wiederverwenden. Sie können auch den Status der Penetrationstestergebnisse nachverfolgen.

### Behebung und Validierung der Penetrationstestergebnisse

Nachdem die Penetrationstestergebnisse vom Anwendungsteam korrigiert und gelöst wurden, werden die Korrekturen manuell validiert und vom Team für ethisches Hacken geschlossen.

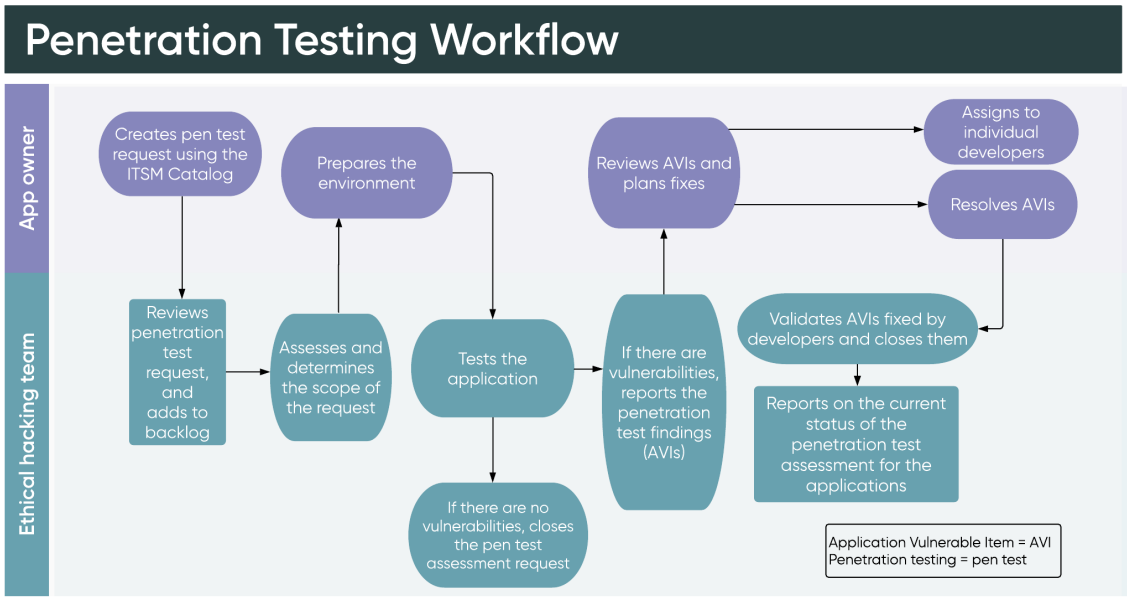
### Application Vulnerability Management-Berichte

Verwenden Sie die im Application Vulnerability Management PA-Dashboard verfügbaren Berichte, um die Ergebnisse der Penetrationstests nachzuverfolgen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Penetrationstest-Lebenszyklus




## Penetrationstest-Bewertungsanforderung aus vorhandenen Anforderungen erstellen (v19.0)

Ab v19.0 erstellen Sie Penetrationstest-Bewertungsanforderungen direkt aus der Liste der vorhandenen Anforderungen. Sie können auch vorhandene Anforderungen im Status „Geschlossen“ in diese Liste kopieren, um Anforderungen zu erstellen.

### Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

### Warum und wann dieser Vorgang ausgeführt wird

Ab Version 19.0 von Vulnerability ResponseVeracode Vulnerability Integrationsind die Penetrationsbewertungstests in Veracode Vulnerability Integration bei Verwendung von [] manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstest-Bewertungsanforderungen verknüpft, die Sie in Application Vulnerability Responsekonfigurieren. Weitere Informationen zu Penetrationstest-Bewertungen von Veracodefinden Sie unter Veracode Vulnerability Integration.

### Prozedur

1. Navigieren zu **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden im neuen Formular beibehalten. Aktive angreifbare Elemente in Anwendungen (AVIs) werden automatisch in die neue Anforderung kopiert. Wählen **Sie Anforderung kopieren und erstellen** aus Datensätzen im Status Geschlossen aus.
3. Wählen Sie Neu, und füllen Sie die Felder aus.

#### Formular „Anforderung für Penetrationstestbewertung“

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutiger Bezeichner, der für die Penetrationstest-Bewertungsanforderung generiert wird. |
| Status | Wählen Sie einen Wert basierend auf dem Status der Anforderung aus. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Angefordert von | Person, die die Bewertung der Anwendung anfordert. |
| Zuweisungsgruppe | Gruppe, die ausgewählt wurde, um an den Ergebnissen des Penetrationstests zu arbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.<br><br>Informationen zum Konfigurieren von Gruppen finden Sie unter Konfigurieren Sie Penetrationstests. |
| Anwendung | Wählen Sie mithilfe der Suchoption eine Anwendung aus. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Ergebnissen des Penetrationstests arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |
| Anwendungstyp | Wählen Sie eine Option aus:<br>○ Webservice (bekannt als API vor v16.1)<br>○ Web-Anwendung<br>○ Thick Client<br>○ Mobile (Wenn Sie **Mobile**auswählen, wird die Registerkarte Mobile am unteren Rand des Formulars mit zusätzlichen Feldern angezeigt.) |
| Sprint | Zeigt die Sprints mit verfügbarer Bandbreite an, um die Bewertungsanforderung basierend auf dem ausgewählten Feld „Bewertungstyp“ zu erfüllen.<br><br>Weitere Informationen zum Ändern der Sprint-Kapazität und des Testumfangs finden Sie unter Konfigurieren Sie Sprints für Penetrationstests und Konfigurieren Sie Bewertungstypen für Penetrationstests. |
| v19.0: Anwendungsgröße | Wählen Sie die Größe der Anwendung aus, die Sie testen möchten.<br>○ Klein<br>○ Mittel<br>○ Groß<br>○ Standard (Wählen Sie diese Option aus, wenn Sie sich bezüglich der Größe nicht sicher sind.)<br><br>Weitere Konfigurieren Sie Penetrationstests<br>Weitere Informationen zum Ändern der Sprint-Kapazität und zum Testen des |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Umfangs mit Anwendungsgröße und Sprint-Kapazität. |
| Erstellt | Datum und Uhrzeit der Erstellung der Anforderung. |
| Bewertungstyp | Wählen Sie den Typ der Bewertung aus:<br>○ Vollständiger Penetrationstest<br>○ Fokussierter Test<br>○ Erneut testen<br>Weitere Informationen zu Testkombinationen und Testumfang finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests. |
| Aktualisiert | Datum und Uhrzeit der letzten Aktualisierung der Anforderung. |
| Demo-Datum | Datum, an dem diese Anwendung demonstriert werden kann. |
| Produktbereitstellung geplant am | Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion. |
| Anwendungsversion/-release für die Bereitstellung geplant | Version der Anwendung, die für die Bereitstellung in der Produktion geplant ist. |
| v19.0: Registerkarte „Anwendung im Besitz eines Drittanbieters oder Joint-Venture-Unternehmens“.<br>Wenn Sie Ja für dieses Feld auswählen, wird die Registerkarte Lieferanten-/Joint-Venture-Informationen angezeigt. Füllen Sie die zusätzlichen Felder aus. | |
| Gibt es eine Klausel, die es uns ermöglicht, Pen-Tests durchzuführen? | Der Begriff „Klausel“ kann sich auf Teststandards beziehen, die alle Vereinbarungen enthalten, die zwischen zwei oder mehr Parteien bestehen, die Sie hinzufügen möchten. Wenn Sie **Ja**auswählen, fügen Sie die Klausel hinzu. |
| Die Klausel, die die Berechtigung zum Durchführen von Pen-Tests angibt | |
| Vollständiger offizieller Name und Adresse des Lieferanten | |
| Angriffserkennungssystem | |
| Technischer Kontakt des Lieferanten | |
| Wurden die protokollierten Informationen auf böswillige Aktivitäten überprüft? | |
| Wird die Anwendung von einem anderen Drittanbieter gehostet? | |
| Kontakt des Lieferanten, der den Pen-Test abzeichnet | |
| Registerkarte „Anwendungsdetails“. | |
| Zweck der Anwendung | Beschreibung der Funktionalität der Anwendung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Details des Technologiestapels | Vollständiger Technologiestapel von Front-End bis Back-End, Datenbanken und anderen Schlüsseltechnologien. |
| Ist Drittanbieteranwendung? | Bestätigt, ob diese Anwendung einem Drittanbieter gehört. |
| Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann. | Arten vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel PII-Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern. |
| Authentifizierungstyp | Gibt an, ob diese Anwendung die LDAP-Authentifizierung, ihre eigene native Authentifizierung oder andere Formen der Authentifizierung verwendet. |
| Fällt die Anwendung unter ein Compliance-Programm? | Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt. |
| Kontakte im Anwendungsteam | Mitglieder des Anwendungsteams, die vom Team für ethisches Hacken bei Fragen kontaktiert werden sollen. |
| Liste der Compliance-Programme | |
| Zugehörige Schnittstellen oder Anwendungen von Drittparteien | |
| IP-Adresse | |
| Ungefähre Anzahl der Benutzer in der Produktion? | |
| Automatisiertes Skript vorhanden? | |
| Ist die Produktionsversion dieser App nach außen gerichtet? | |
| v 19.0: Geschäftsauswirkung | |
| Finanzieller Schaden | Wählen Sie einen aus der Liste aus. |
| Nichteinhaltung | Wählen Sie einen aus der Liste aus. |
| Reputationsschaden | Wählen Sie einen aus der Liste aus. |
| Datenschutzverletzung | Wählen Sie einen aus der Liste aus. |
| Registerkarte „Testdetails“. | |
| Zu testende URLs | URLs, die in Penetrationstests enthalten sein müssen. |
| Auszuschließende URLs | URLs, die von Penetrationstests ausgeschlossen werden müssen. |
| Wurde diese Anwendung zuvor getestet? | Gibt an, ob diese Anwendung bereits Penetrationstests unterzogen wurde. |
| Grund für erneuten Test | Grund für die Anforderung einer Neubewertung des Penetrationstests, wenn die Anwendung zuvor getestet wurde. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Wann wurde die Anwendung getestet? | Zeitrahmen, in dem die Anwendung Penetrationstests unterzogen wurde. |
| Details des Test-Accounts | Details des Test-Accounts, der vom Team für ethisches Hacken für Penetrationstests verwendet werden kann. |
| Anwendungsrollen | Rollen, die von der Anwendung für ihre Benutzer unterstützt werden. |
| Meistverwendete Rollen | Am häufigsten verwendete Rollen in der Anwendung. |
| Registerkarte „Zusätzliche Kommentare“. | |
| Arbeitsnotizen | |

4. Wählen **Sie Speichern**, um Ihre Änderungen zu speichern, oder **Absenden**, um die Anforderung zu initiieren.

### Penetrationstest-Bewertungsanforderung erstellen (vor v19.0)

Initiieren Sie eine Penetrationstest-Bewertungsanforderung für Ihre Webanwendungen oder APIs. Diese Anforderungen werden an das Team für ethisches Hacken übermittelt, das dann diese Anwendungen testet und die Ergebnisse der Penetrationstests manuell meldet.

#### Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

#### Warum und wann dieser Vorgang ausgeführt wird
Der Anwendungsbesitzer löst eine Penetrationstest-Bewertungsanforderung aus, um seine Anwendung oder APIs manuell zu scannen. Das Team für ethisches Hacken testet die Anwendung und erstellt manuell Penetrationstestergebnisse. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Elemente (AVIs).

Die Standardzuweisungsgruppe für das Penetrationstestergebnis ist die Gruppe, die im Feld „Anwendungsteam“ der zugehörigen Penetrationstest-Bewertungsanforderung konfiguriert ist. Der Zuweisungstyp des Penetrationstestergebnisses ist „Manuell“. Die Zuweisungsregeln können die Zuweisung dieser Penetrationstestergebnisse nicht überschreiben.

Ab v19.0 können Sie Penetrationstest-Bewertungsanforderungen direkt aus der Tabelle „Penetrationstest-Bewertungsanforderungen“ [sn_vul_pen_test_assessment_request_list] erstellen. Weitere Informationen finden Sie unter Penetrationstest-Bewertungsanforderung aus vorhandenen Anforderungen erstellen (v19.0).

#### Prozedur

1. Navigieren Sie vor Version 19.0 zu **Alle** > **Selfservice** > **Servicekatalog** > **Services** > **Anforderung für Penetrationstestbewertung**.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden beibehalten. Aktive angreifbare Elemente in Anwendungen (AVIs) werden automatisch in die neue Anforderung kopiert.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Anforderung für Penetrationstestbewertung“

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutiger Bezeichner, der für die Penetrationstest-Bewertungsanforderung generiert wird. |
| Angefordert von | Person, die die Bewertung der Anwendung anfordert. |
| Übergeordnete Bewertungsanforderung | Ursprüngliche Penetrationstest-Bewertungsanforderung, die zum Erstellen der untergeordneten Anforderung verwendet wurde. Sie wird mithilfe einer geschlossenen Bewertungsanforderung erstellt. Nur im untergeordneten Bewertungsanforderungsformular sichtbar. |
| Anwendung | Wählen Sie mithilfe der Suchoption eine Anwendung aus. |
| Anwendungstyp | Wählen Sie eine Option aus:<br>○ Webservice (bekannt als API vor v16.1)<br>○ Web-Anwendung<br>○ Thick Client<br>○ Mobile (Wenn Sie Mobile auswählen, wird die Registerkarte Mobile am unteren Rand des Formulars mit zusätzlichen Feldern angezeigt.) |
| v19.0: Anwendungsgröße | Wählen Sie die Größe der Anwendung aus, die Sie testen möchten.<br>○ Klein<br>○ Mittel<br>○ Groß<br>○ Standard (Wählen Sie diese Option aus, wenn Sie sich bezüglich der Größe nicht sicher sind.) |
| Bewertungstyp | Wählen Sie den Typ der Bewertung aus:<br>○ Vollständiger Penetrationstest<br>○ Fokussierter Test<br>○ Erneut testen<br>Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests. |
| Zweck der Anwendung | Beschreibung der Funktionalität der Anwendung. |
| Details des Technologiestapels | Vollständiger Technologiestapel vom Front-End bis zum Back-End, Datenbanken und andere Schlüsseltechnologien. |
| Ist Drittanbieteranwendung? | Bestätigt, ob diese Anwendung einem Drittanbieter gehört. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann. | Arten vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel PII-Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern. |
| Authentifizierungstyp | Gibt an, ob diese Anwendung die LDAP-Authentifizierung, ihre eigene native Authentifizierung oder andere Formen der Authentifizierung verwendet. |
| Fällt die Anwendung unter ein Compliance-Programm? | Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt. |
| Kontakte im Anwendungsteam | Mitglieder des Anwendungsteams, die vom Team für ethisches Hacken bei Fragen kontaktiert werden sollen. |
| Demo-Datum | Datum, an dem diese Anwendung demonstriert werden kann. |
| Produktbereitstellung geplant am | Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion. |
| Anwendungsversion/-release für die Bereitstellung geplant | Version der Anwendung, die für die Bereitstellung in der Produktion geplant ist. |
| v19.0: Anwendung im Besitz eines Drittanbieters oder Joint-Venture-Unternehmens | Wenn Sie für dieses Feld Ja auswählen, wird die Registerkarte Lieferanten-/Joint-Venture-Informationen mit zusätzlichen Feldern angezeigt.<br><br>Der Begriff „Klausel“ kann sich auf Teststandards beziehen, die Vereinbarungen zwischen zwei oder mehr Parteien enthalten. |
| Status | Wählen Sie einen Wert basierend auf dem Status der Anforderung aus. |
| Zuweisungsgruppe | Gruppe, die ausgewählt wurde, um an den Ergebnissen des Penetrationstests zu arbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Ergebnissen des Penetrationstests arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |
| Sprint | Zeigt die Sprints mit verfügbarer Bandbreite an, um die Bewertungsanforderung basierend auf dem ausgewählten Feld „Bewertungstyp“ zu erfüllen. |
| Erstellt | Datum und Uhrzeit der Erstellung der Anforderung. |
| Teststartdatum | Datum und Uhrzeit des Testbeginns. |
| Aktualisiert | Datum und Uhrzeit der letzten Aktualisierung der Anforderung. |
| Testdetails | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zu testende URLs | URLs, die in Penetrationstests enthalten sein müssen. |
| Auszuschließende URLs | URLs, die von Penetrationstests ausgeschlossen werden müssen. |
| Wurde diese Anwendung zuvor getestet? | Gibt an, ob diese Anwendung bereits Penetrationstests unterzogen wurde. |
| Grund für erneuten Test | Grund für die Anforderung einer Neubewertung des Penetrationstests, wenn die Anwendung zuvor getestet wurde. |
| Wann wurde die Anwendung getestet? | Zeitrahmen, in dem die Anwendung Penetrationstests unterzogen wurde. |
| Details des Test-Accounts | Details des Test-Accounts, der vom Team für ethisches Hacken für Penetrationstests verwendet werden kann. |
| Anwendungsrollen | Rollen, die von der Anwendung für ihre Benutzer unterstützt werden. |
| Meistverwendete Rollen | Am häufigsten verwendete Rollen in der Anwendung. |

4. Wählen Sie **Absenden**.
   Eine E-Mail-Benachrichtigung wird an das Team für ethisches Hacken gesendet, dass die Anforderung für die entsprechende Anwendung erstellt wurde.

### Replizieren Sie eine Penetrationstestanforderung im Status „Geschlossen“.

Erstellen Sie eine Penetrationstest-Bewertungsanforderung, indem Sie eine Anforderung im Status „Geschlossen“ replizieren. Aktive angreifbare Anwendungselemente (AVIs) werden in die neue Anforderung kopiert.

#### Vorbereitungen
Erforderliche Rolle: Anwendungsteam

#### Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Anforderungen für Penetrationstestbewertung** > **Alle**.
2. Wählen Sie eine Anforderung im Status Geschlossen aus.
3. Wählen **Sie Anforderung kopieren und erstellen aus**.
   Eine neue Anforderung wird erstellt, und die aktiven AVIs werden mit aktualisierten Daten in diese Anforderung kopiert. Um den ursprünglichen Status der AVIs aus der übergeordneten Anforderung anzuzeigen, navigieren Sie zur Registerkarte **Snapshot der Penetrationstestergebnisse**.

### Penetrationstestergebnisse basierend auf Bewertungsanforderungen erstellen (vor v19.0)

Erstellen Sie Penetrationstestergebnisse basierend auf der Penetrationstest-Bewertungsanforderung. Bei diesen Ergebnissen handelt es sich um manuell erstellte Application Vulnerability Items (AVIs).

#### Vorbereitungen
Erforderliche Rolle: Ethical Hacker



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Servicekatalog** > **Services** > **Anforderungen für Penetrationstestbewertung**.
2. Um eine AVI für eine Penetrationstest-Bewertungsanforderung zu erstellen, wählen Sie die entsprechende Anforderung aus.
3. Wählen Sie im Abschnitt „Angreifbare Anwendungselemente“ die Option **Neu**aus.
4. Füllen Sie die Felder des Formulars aus.

**Formular „Angreifbares Anwendungselement“ (Penetrationstest-Ansicht)**

| Feld | Beschreibung |
|---|---|
| Nummer | Automatisch generierter AVI-Bezeichner für diesen Datensatz. |
| Bewertungsanforderung | Penetrationstest-Bewertungsanforderung, der diese AVI zugeordnet ist. |
| Schwachstelle | Schwachstelle, die mithilfe der Suchoption aus der Tabelle „Schwachstelleneinträge“ ausgewählt wurde. |
| Risikobewertung | Quantifizierte **Risikopunktzahl**, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikobewertungen finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen.<br>Ab V16.1 entspricht der Wert standardmäßig dem Schweregrad der Schwachstelle. |
| Auswirkungen auf Compliance-Programme? | Bestätigt, ob es Auswirkungen auf ein Compliance-Programm gibt. Auswahlmöglichkeiten sind Ja und Nein. |
| Liste der betroffenen Compliance-Programme | Dieses Feld wird angezeigt, wenn der Wert des Felds „Wirkt sich auf Compliance-Programme aus“ auf *Yes*festgelegt ist. Listet die betroffenen Compliance-Programme auf. |
| Geplante(s) Release/Korrekturversion | Release bis, wenn die Ergebnisse des Penetrationstests gelöst werden müssen. |
| Status | Der Standardwert ist **Offen**, wenn die AVI erstellt wird. Weitere Informationen zur Zuordnung von Status finden Sie unter Status des angreifbaren Elements in der Anwendung (AVI).. |
| Zuweisungsgruppe | Gruppe, die für die Arbeit an dieser AVI ausgewählt wurde. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser AVI arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Korrekturziel | Datum, bis zu dem die AVIs korrigiert werden müssen, seit sie zuerst identifiziert wurden. Dieses Feld wird nur angezeigt, wenn zutreffend.<br><br>Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response. |
| Erstellt | Zeitstempel der Erstellung des angreifbaren Anwendungselements (AVI). |
| Aktualisiert | Zeitstempel der Aktualisierung des angreifbaren Anwendungselements (AVI). |
| Geöffnet von | Benutzer, der dieses Penetrationstestergebnis erstellt hat. |
| Sicherheitsteamkontakt | Ansprechpartner im Ethical Hacking-Team. |
| Kurzbeschreibung | Kurze Erläuterung des Ergebnisses des Penetrationstests. |
| Details | |
| Technische Details | Technische Details des Penetrationstestergebnisses. |
| Auswirkung | Bewertung der Auswirkungen des Penetrationstestergebnisses. |
| Schritte zum Reproduzieren | Dokumentieren Sie die Schritte zum Reproduzieren und Überprüfen des Penetrationstestergebnisses. |
| Empfehlung | Notieren Sie die empfohlenen Aktionen in diesem Feld. |
| Notizen | |
| Arbeitsnotizen | Fügen Sie Notizen hinzu, um Informationen zu Statusübergängen und anderen Feldaktualisierungen zu kommunizieren. |
| V16.1: Betroffene URLs | Weitere Informationen zu den betroffenen URLs. |
| V16.1: Betroffene Parameter | Weitere Informationen zu den betroffenen Parametern. |
| V16.1: Betroffene Funktionalitäten | Weitere Informationen zu den betroffenen Funktionalitäten. |

5. Um das Formular zu speichern, wählen Sie **Absenden**.

### Erstellen Sie einen Anwendungsschwachstelleneintrag

Erstellen Sie einen Anwendungsschwachstelleneintrag für die für das Penetrationstestergebnis angegebene Schwachstelle. Anwendungsschwachstellen sind Schwachstellen in den benutzerdefinierten Softwareanwendungen.

**Vorbereitungen**
Erforderliche Rolle: Ethical Hacker



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response bezieht eine Schwachstelle auf eine Anwendung, um das Penetrationstestergebnis zu erstellen. Bei diesen Ergebnissen handelt es sich um manuell erstellte angreifbare Elemente (AVIs). Sie können einen vorhandenen Eintrag wiederverwenden oder während Penetrationstests manuell einen Eintrag für jede Schwachstelle erstellen.

## Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Bibliotheken** > **Drittpartei**.
2. Wählen Sie auf der Seite „Anwendungsschwachstelleneinträge“ die Option **Neu**aus.
3. Füllen Sie die Felder des Formulars aus.

### Formular „Anwendungsschwachstelleneintrag“ (Penetrationstest-Ansicht)

| Feld | Beschreibung |
|---|---|
| ID | Bezeichner für diesen Schwachstelleneintrag. |
| Schweregrad | Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow-Drittpartei-Integrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu. |
| Primäres CVE | Verweis auf das Common Weakness Enumeration-Element, in das diese Schwachstelle am besten passt. |
| Kategoriename | Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung. |
| Schwachstellendetails | |
| Angriffsvektor | Angreifbarster Angriffsvektor für diese Schwachstelle. |
| Angriffskomplexität | Metrik, die die Bedingungen beschreibt, die außerhalb der Kontrolle des Angreifers liegen und für die Ausnutzung der Schwachstelle erfüllt sein müssen. |
| Umfang | Metrik zur Messung der Fähigkeit einer Softwareschwachstelle, Ressourcen über ihre Grenzen hinaus zu beeinträchtigen. |
| Integrität | Metrik zur Messung der Auswirkung auf die Integrität einer erfolgreich ausgenutzten Schwachstelle. |
| CVSS-Vektor | Offenes Framework zur Erfassung der Merkmale und des Schweregrads von Softwareschwachstellen. |
| Erforderliche Berechtigungen | Berechtigungsebene, die ein Angreifer besitzen muss, um die Schwachstelle erfolgreich ausnutzen zu können. |
| Anwenderinteraktion | Anforderung für menschliche Interaktion, um eine Schwachstelle erfolgreich auszunutzen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Vertraulichkeit | Auswirkung auf die Vertraulichkeit der Informationsressourcen aufgrund einer erfolgreich ausgenutzten Schwachstelle. Diese Ressourcen werden von einer Softwarekomponente verwaltet. |
| Verfügbarkeit | Auswirkung auf die Verfügbarkeit der betroffenen Komponente infolge einer erfolgreich ausgenutzten Schwachstelle. |
| CVSS-Basispunktzahl | Numerische Darstellung (0–10) für den Schweregrad eines Anwendungsschwachstelleneintrags. |
| Bedrohung | Beschreibung der Bedrohung durch diese Schwachstelle. |
| Beschreibung der Verringerung | Beschreibung der Schritte zum Mindern der Schwachstelle. |

4. Um das Formular zu speichern, wählen Sie **Absenden**.

**Hinweis:**
AVEs werden in der Tabelle „Anwendungsschwachstelleneintrag“ (sn_vul_app_vul_entry) erstellt. Die Tabelle „Anwendungsschwachstelleneintrag“ ist ein untergeordnetes Element der Tabelle „Schwachstelleneintrag“ (`sn_vul_entry`). Daher werden die erstellten AVEs auch der Tabelle „Schwachstelleneintrag“ hinzugefügt.

## Platform Analytics-Lösungen für Application Vulnerability Response

Platform Analytics-Lösungen enthalten vorverpackte Platform Analytics -Inhalte zur Verwendung mit anderen Now Platform -Produkten. Dieser Platform Analytics-Lösung enthält wichtige Metriken für die Analyse Ihres Application Vulnerability Management-Prozesses.

### Übersicht

Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist im ServiceNow® Store als separates Abonnement verfügbar. Die Anwendung wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Das Application Vulnerability Response-Inhaltspaket ist Teil des Performance Analytics for Vulnerability Response-Inhaltspakets.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren der Anwendung Performance Analytics for Vulnerability Response finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

### Wichtige Begriffe

**Performance Analytics (PA)**

Lösung, die Management-Dashboards, Berichte zu KPIs und Metriken erstellt und wichtige Geschäftsfragen beantwortet, um die Qualität zu steigern und die Kosten zu senken.

**Angreifbares Anwendungselement (AVI)**

Eine Anwendungsschwachstelle, die von einem Drittanbieter-Schwachstellenscanner gemeldet wird, der in einem Konfigurationselement (Configuration Item, CI) vorhanden ist

**PA-Indikator**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definiert eine Leistungsmessung, die in regelmäßigen Abständen einer Aktivität oder eines Organisationsverhaltens durchgeführt wird, z. B. Top 10 Anwendungen mit den kritischsten angreifbaren Anwendungselementen.

**PA-Indikatorquelle**

Datensätze, die Datensätze aus einer Tabelle oder Datenbankansicht filtern, z. B. AVI Aktiv.

- Das Dashboard „Meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis hin zur Eindämmung oder Korrektur.
- Zeigen Sie die Erreichungsraten der Korrekturziele an, und bestimmen Sie effizient, welche angreifbaren Elemente in Anwendungen (AVIs) das größte Risiko für Ihre Organisation darstellen.

## Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Die folgenden Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um bei der Bestimmung von Korrekturplänen und Statusfortschritten zu helfen. Sie können sich auf die KPIs konzentrieren, die mit kritischen betroffenen Anwendungen und Schwachstellen mit hoher Transparenz verknüpft sind.

- Das Dashboard für Application Vulnerability Management (PA) kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends beträgt drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.
- Das Dashboard „Meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis hin zur Eindämmung oder Korrektur.

**Hinweis:**
Das Dashboard „Meine Anwendungsschwachstellen“ ist eine Teilmenge des Dashboards „Übersicht“ und nur verfügbar, wenn sich ein Mitglied der Security Champion-Benutzergruppe bei einer Instanz anmeldet. Weitere Informationen zum Dashboard „ Meine Anwendungsschwachstellen“ finden Sie unter Dashboard „Meine Anwendungsschwachstellen“.

## Application Vulnerability Management (PA)-Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Anwendungsfälle

| Anwender | Dashboard-Verwendung |
| --- | --- |
| Schwachstellenmanager | Mit dem Dashboard Application Vulnerability Management kann das Schwachstellenmanagement bestimmen, welche angreifbaren Elemente (AVIs) das größte Risiko für ihre Organisationen darstellen.<br><br>Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um sie bei der Bestimmung von Korrekturplänen und Statusfortschritten zu unterstützen. Konzentrieren Sie sich auf die KPIs, die mit kritischen betroffenen Anwendungen und Schwachstellen mit hoher Transparenz verbunden sind. |

## Erforderliche Now Platform Rollen, Setup und Dashboard-Registerkarten

Das Dashboard „Application Vulnerability Management“ (PA) ist als Teil des Inhaltspakets „Performance Analytics for Vulnerability Response“ enthalten. Das Inhaltspaket „Performance Analytics for Vulnerability Response“ wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Sie ist im ServiceNow® Store als separates Abonnement verfügbar.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren der Anwendung Performance Analytics for Vulnerability Response finden Sie unter Anwendung Performance Analytics for Vulnerability Response [PA] installieren und konfigurieren.

Um das Dashboard anzuzeigen, navigieren Sie als Benutzer, der den Benutzergruppen „Security Champion“, „App-Sec-Manager“ oder „Entwickler“ zugewiesen ist, zu **Application Vulnerability Response** > **Übersicht**.

**Hinweis:**
Das Dashboard „Meine Anwendungsschwachstellen“ ist eine Teilmenge des Dashboards „Übersicht“ und nur verfügbar, wenn sich ein Mitglied der Security Champion-Benutzergruppe bei einer Instanz anmeldet. Weitere Informationen zum Dashboard „Meine Anwendungsschwachstellen“ finden Sie unter Dashboard „Meine Anwendungsschwachstellen“.

Ab Version 19.0 von Application Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboardübersicht und Dashboardübersicht.

Das Übersichts-Dashboard kommuniziert KPIs für Schwachstellenrisiko und -verbreitung, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends beträgt drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gliedern Sie die Daten im Dashboard Application Vulnerability Management nach **Scan-Typ**, **Anwendung** oder **Geschäftsbereich auf**. Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter, **Elemente auswählen**, um Ihre Auswahl einzugrenzen. Ab Application Vulnerability Response v15.0 wurden den Auswahlmöglichkeiten für den **Anwendungsfilter** Geschäfts- und CI-Anwendungen hinzugefügt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

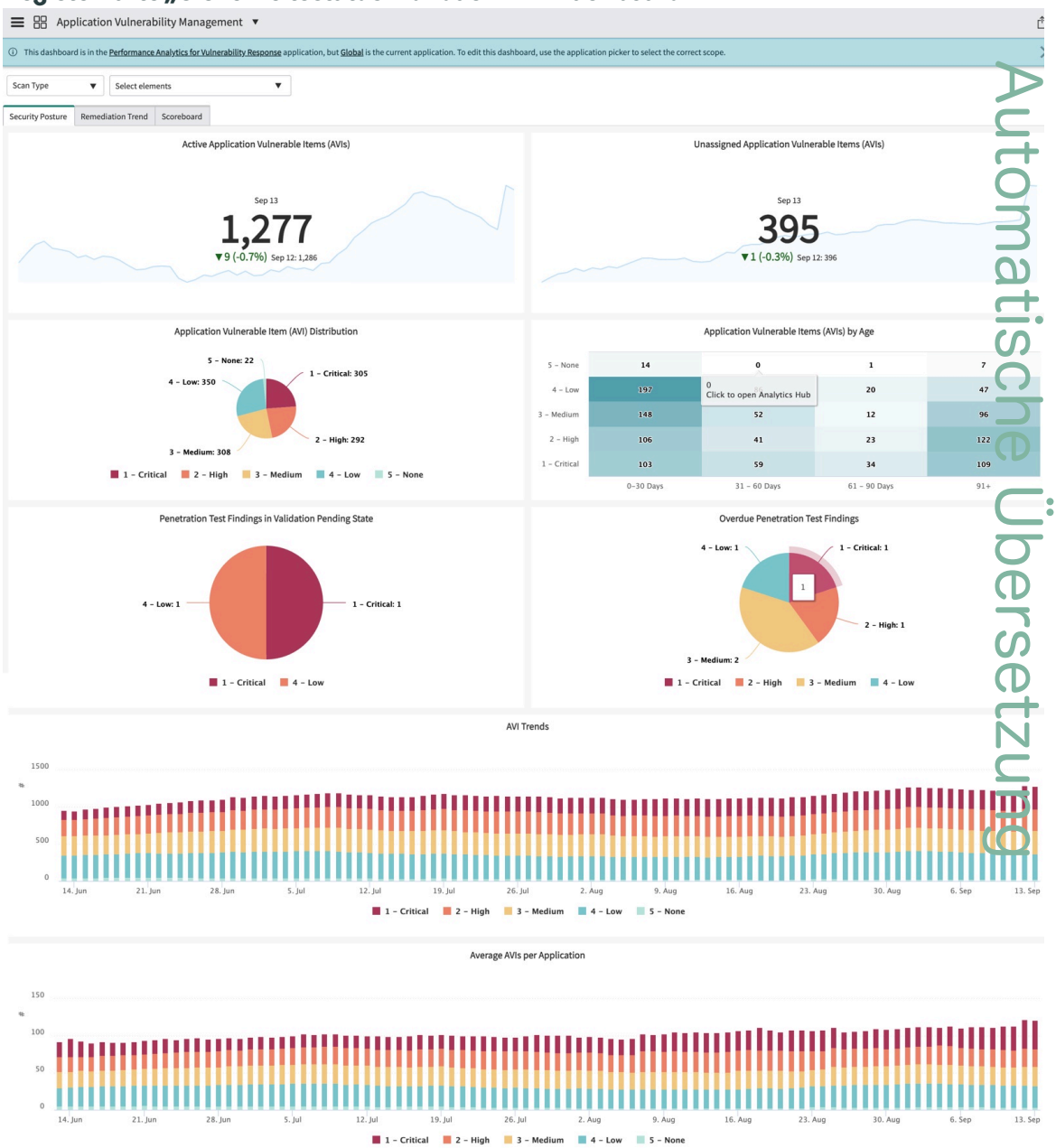
## Registerkarte Sicherheitslage

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturmaßnahmen zu verstehen.

Ab Application Vulnerability Response v15.0 können Sie die Penetrationstest-Ergebnisberichte anzeigen. Penetrationstest-Ergebnisse sind angreifbare Anwendungselemente (AVIs), die basierend auf den Penetrationstest-Bewertungsanforderungen manuell erstellt werden.

**Hinweis:**
Der Scan-Typ für diese Widgets ist „Manuell“.

### Registerkarte „Sicherheitsstatus“ für das AVM-Dashboard

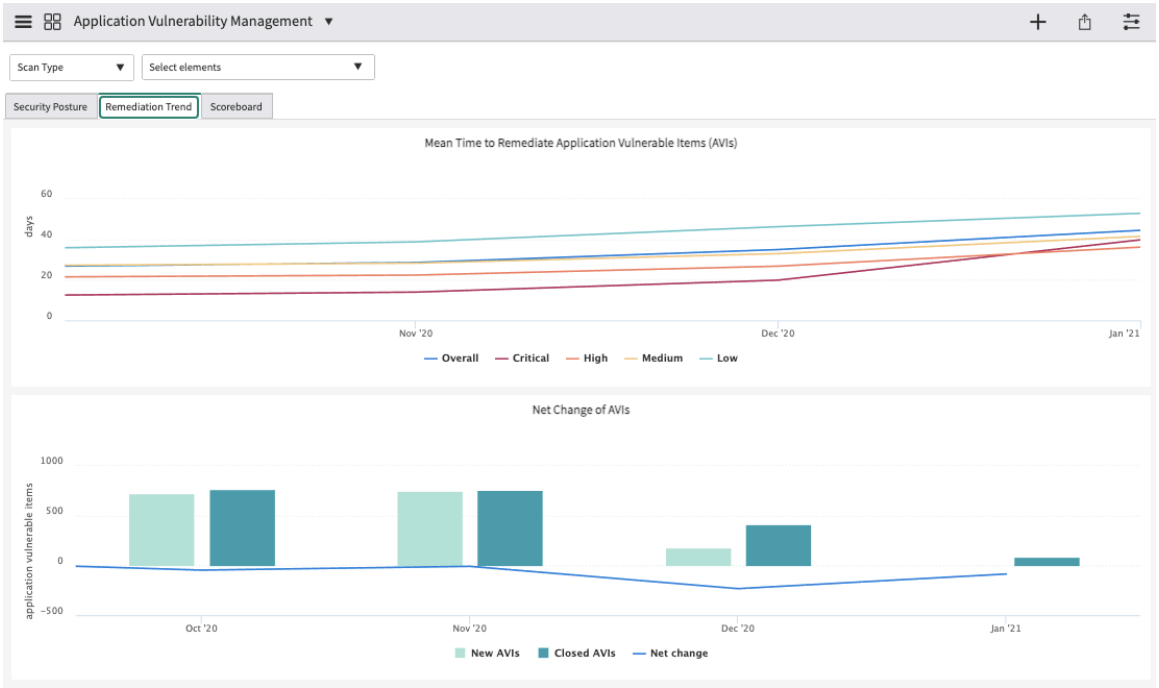



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Korrekturtrend“.

Die Registerkarte Korrekturtrend hilft Ihnen, den Fortschritt Ihrer Korrekturaktionen nachzuvollziehen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

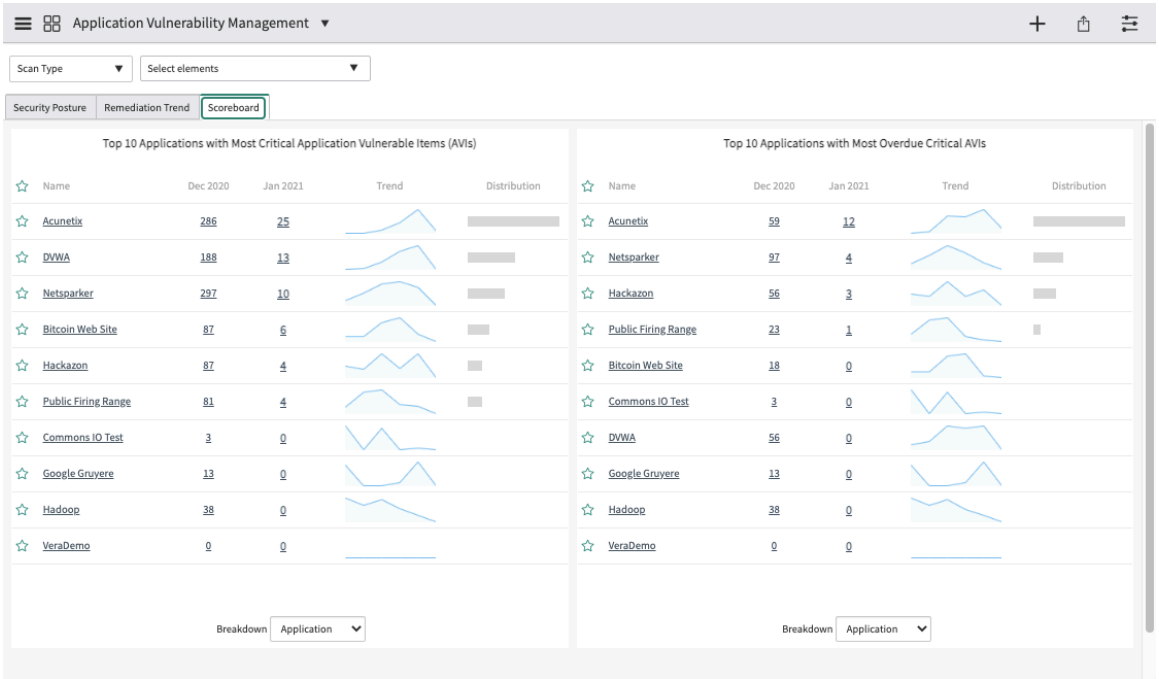
### Registerkarte „Anzeigetafel“.

Die Registerkarte „Scoreboard“ hilft Ihnen, den Fortschritt Ihrer Korrekturmaßnahmen nachzuvollziehen und herauszufinden, welche AVIs bei ihrem Abschluss die meiste Unterstützung benötigen.

Elemente des Scan-Typs:

- Dynamisch: Verwenden Sie nur Metriken aus dem dynamischen Datenimport
- Statisch: Verwenden Sie nur Metriken aus dem statischen Datenimport

Sie können eine oder beide Optionen auswählen.




## Indikatoren

**Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]]. Ziel ist die Minimierung.

**Anwendungsreleases**

Dies ist die eindeutige Anzahl für Anwendungen von AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Angreifbare Anwendungselemente**

Dies ist die Anzahl der angreifbaren App-Elemente AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Durchschnittliche AVIs pro Anwendung**

[Aktive angreifbare Anwendungselemente]] / [[Anwendungsveröffentlichungen]]. Ziel ist die Minimierung.

**Nicht zugewiesene AEs**

Dies ist die Anzahl in der Indikatorquelle AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Fehlerkorrektur von AVIs**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente]] / [[Geschlossene angreifbare Anwendungselemente]]. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Korrektur hoher AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – Hoch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – Hoch]]. Ziel ist die Minimierung.

**Geschlossene angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Maximierung.

**Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]]. Ziel ist die Minimierung.

**Neue angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.New“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]]. Ziel ist die Minimierung.

**Nettoänderung in AEs**

[[Neue angreifbare Anwendungselemente]] – [[Geschlossene angreifbare Anwendungselemente]]. Ziel ist die Minimierung.

**Summierte Dauer der geschlossenen angreifbaren Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Kritische überfällige angreifbare Anwendungselemente**

Dies ist die Anzahl in der Datenquelle „AVI.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Kritische angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „Anwendungen mit aktiven AVIs“, die die folgende Tabelle verwendet: sn_vul_analytics_app_ci_dept_bu. Ziel ist die Minimierung.

## BreakdownsAufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Datenvisualisierungen

### Sicherheitslage

| Name | Typ | Beschreibung |
|---|---|---|
| V15.0: Penetrationstestergebnisse im Status „Validierung ausstehend“. | Kreisdiagramm | Penetrationstest-Ergebnisse im Status „Gelöst“, aber mit ausstehender Validierung, gruppiert nach Risikobewertung. |
| V15.0: Überfällige Penetrationstestergebnisse | Kreisdiagramm | Kritische Penetrationstestergebnisse, die ihr Korrekturzieldatum verpasst haben, gruppiert nach Risikobewertung. |
| Aktive angreifbare Anwendungselemente (AVIs) | Einzelne Punktzahl | Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs). |
| Nicht zugewiesene angreifbare Anwendungselemente (AVIs) | Einzelne Punktzahl | Anzahl der aktiven angreifbaren Anwendungselemente (AVIs) ohne eine Zuweisungsgruppe. |
| Verteilung des angreifbaren Anwendungselements (AVI) | Kreisdiagramm | Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung. |
| Angreifbare Anwendungselemente (AVIs) nach Alter | Heatmap | Anzahl der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung und Alter (in Tagen). |
| AVI-Trends | Symbol „ | Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung. |
| Durchschnittliche AVIs pro Anwendung | Symbol „ | Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung. |

### Trend bei Korrekturen

| Name | Typ | Beschreibung |
|---|---|---|
| Durchschnittliche Zeit bis zur Korrektur von angreifbaren Elementen in Anwendungen (AVIs) | Linie | Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung. |
| Nettoveränderung der AVIs | | Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat. |

### Anzeigetafel

| Name | Typ | Beschreibung |
|---|---|---|
| Top-10-Anwendungen mit den kritischsten angreifbaren Anwendungselementen (AVIs) | Bewertungskarte und Verteilungsleiste | Anwendungen mit der höchsten Anzah an kritischen angreifbaren Elementen in einer Anwendung (AVIs). |
| Top-10-Anwendungen mit den meisten überfälligen kritischen angreifbaren Anwendungselementen (AVIs) | Bewertungskarte und Verteilungsleiste | Anwendungen mit der höchsten Anzahl aktiver angreifbarer Elemente (AVIs), die ihr Korrekturzieldatum überschritten haben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Dashboard „Meine Anwendungsschwachstellen“

Dieses Dashboard enthält wichtige Metriken für die Analyse Ihres Application Vulnerability Management-Prozesses, z. B. die Anzeige der Erreichungsraten der Korrekturziele.

## Erforderliche Now Platform Rollen und Anzeigen des Dashboards

**Hinweis:**

- Dieses Dashboard ist Teil des Inhaltspakets von Application Vulnerability Response. Das Application Vulnerability Response Content Pack ist Teil des Performance Analytics for Vulnerability Response Content Pack.
- Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist im ServiceNow® Store als separates Abonnement verfügbar.
- Das Performance Analytics for Vulnerability Response Content Pack wird nicht automatisch mit der Anwendung Vulnerability Response installiert.

Das Dashboard „Meine Anwendungsschwachstellen“ ist nur verfügbar, wenn sich ein Mitglied der Security Champion-Benutzergruppe bei einer Instanz anmeldet. Weitere Informationen zum Dashboard „Übersicht“ finden Sie unter Dashboard „Application Vulnerability Management“ [PA].

Um das Dashboard anzuzeigen, navigieren Sie zu **Application Vulnerability Response** > **Meine Anwendungsschwachstellen**.

Ab Version 19.0 von Application Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboardübersicht und Dashboardübersicht.

Zeigen Sie Berichte an, die Trenddaten im Zeitverlauf anzeigen. Zeigen Sie regelmäßig Trends wichtiger Metriken an, um Ihre gesamten Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

Das Dashboard „Meine Anwendungsschwachstellen“ ist im Inhaltspaket „Performance Analytics for Vulnerability Response“ enthalten. Das Inhaltspaket „Performance Analytics for Vulnerability Response“ wird nicht automatisch mit der Anwendung Vulnerability Response installiert. Sie ist im ServiceNow® Store als separates Abonnement verfügbar.

## Anwendungsfälle

| Anwender | Dashboard-Verwendung |
|---|---|
| IT-Spezialisten, Korrekturbesitzer oder Analysten, die Schwachstellen beheben, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. | Ein Security Champion verwendet das Dashboard „Meine Anwendungsschwachstellen“, um das Volumen, die Leistung und den Fortschritt der Korrektur von Anwendungsschwachstellen nachzuverfolgen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwender | Dashboard-Verwendung |
| --- | --- |
| | Ermitteln Sie effizient, welche angreifbaren Elemente in Anwendungen (AVIs) das größte Risiko für Ihre Organisation darstellen.<br><br>Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivität, um bei der Bestimmung von Korrekturplänen und Statusfortschritten zu helfen. Sie können sich auf die KPIs konzentrieren, die mit kritischen betroffenen Anwendungen und Schwachstellen mit hoher Transparenz verknüpft sind.<br><br>Erhalten Sie schnell Einblicke in Ihr Schwachstellenrisiko und Ihre Sicherheitslage. Nachverfolgung von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. |

## Dashboard-Registerkarten „Meine Anwendungsschwachstellen“ [PA].

Das Dashboard „Meine Anwendungsschwachstellen“ kommuniziert KPIs für Risiko und Verbreitung von Schwachstellen, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends beträgt drei Monate, kann jedoch in „7 Tage“, „1 Monat“, „3 Monate“, „6 Monate“, „seit Jahresbeginn“, „1 Jahr“ oder „Alle“ geändert werden.

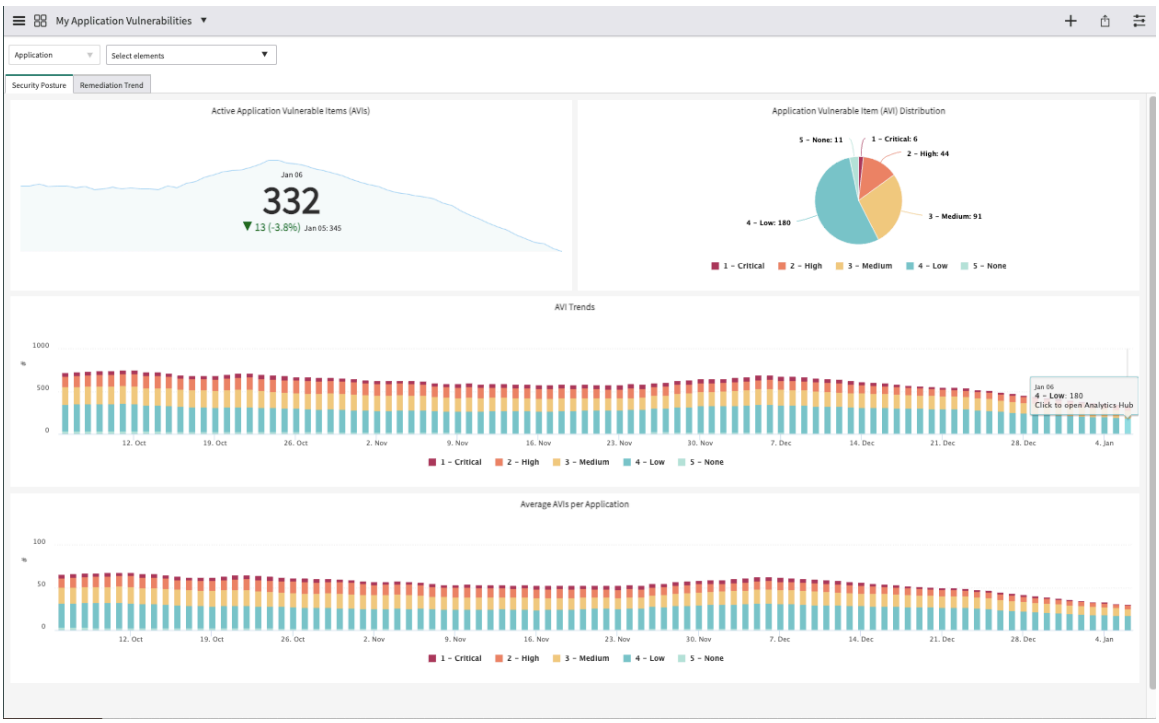
Die Daten werden im Dashboard nach **Anwendung**aufgeschlüsselt. Verwenden Sie die Liste **Elemente** auswählen, um Ihre Auswahl einzugrenzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

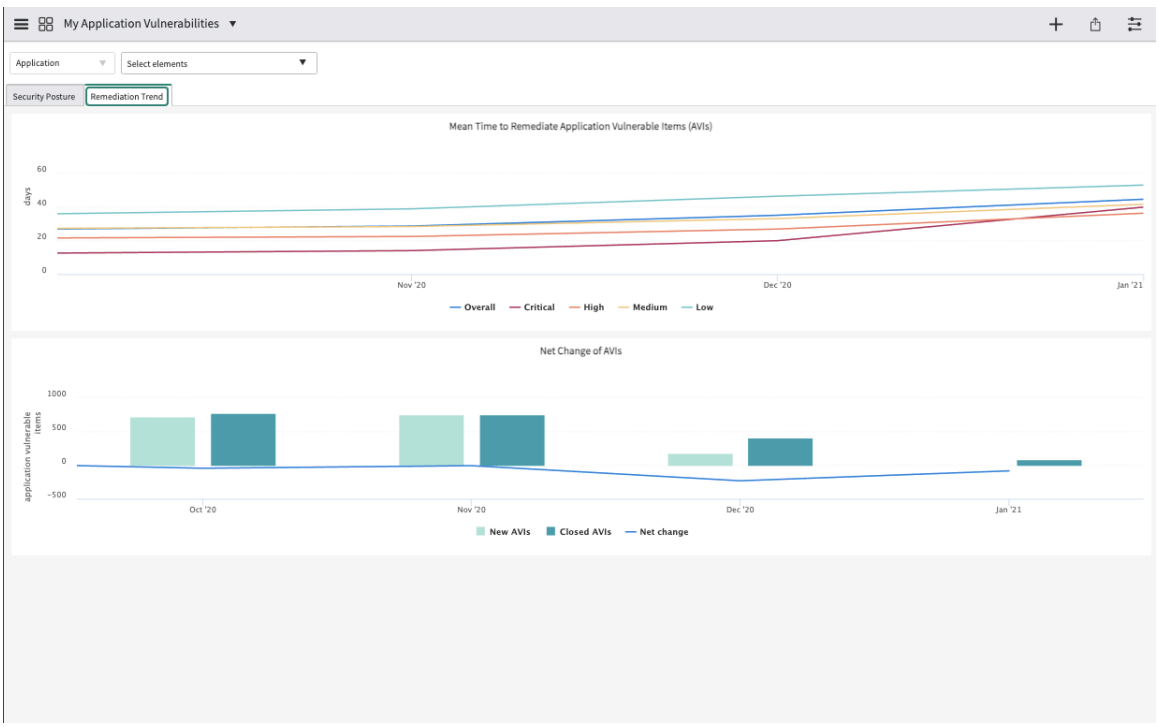
## Registerkarte Sicherheitslage

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturmaßnahmen zu verstehen. Gliedern Sie die Daten im Dashboard „Anwendungsschwachstellenmanagement“ nach **Scan-Typ, Anwendung** oder **Geschäftsbereich auf**. Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter, **Elemente auswählen**, um Ihre Auswahl einzugrenzen.




## Registerkarte „Korrekturtrend“.

Die Registerkarte Korrekturtrend hilft Ihnen, den Fortschritt Ihrer Korrekturaktionen nachzuvollziehen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Indikatoren

**Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]]. Ziel ist die Minimierung.

**Anwendungsreleases**

Dies ist die eindeutige Anzahl für Anwendungen von AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Angreifbare Anwendungselemente**

Dies ist die Anzahl der angreifbaren App-Elemente AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Durchschnittliche AVIs pro Anwendung**

[Aktive angreifbare Anwendungselemente]] / [[Anwendungsveröffentlichungen]]. Ziel ist die Minimierung.

**Nicht zugewiesene AEs**

Dies ist die Anzahl in der Indikatorquelle AVI.Active, die die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Fehlerkorrektur von AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente]] / [[Geschlossene angreifbare Anwendungselemente]]. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Korrektur hoher AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – Hoch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – Hoch]]. Ziel ist die Minimierung.

**Geschlossene angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Maximierung.

**Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]]. Ziel ist die Minimierung.

**Neue angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.New“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs**

[[Summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[Geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]]. Ziel ist die Minimierung.

**Nettoänderung in AEs**

[[Neue angreifbare Anwendungselemente]] – [[Geschlossene angreifbare Anwendungselemente]]. Ziel ist die Minimierung.

**Summierte Dauer der geschlossenen angreifbaren Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „AVI.Closed“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Kritische überfällige angreifbare Anwendungselemente**

Dies ist die Anzahl in der Datenquelle „AVI.Aktiv“, welche die folgende Tabelle verwendet: sn_vul_app_vulnerable_item. Ziel ist die Minimierung.

**Kritische angreifbare Anwendungselemente**

Dies ist die Anzahl in der Indikatorquelle „Anwendungen mit aktiven AVIs“, die die folgende Tabelle verwendet: sn_vul_analytics_app_ci_dept_bu. Ziel ist die Minimierung.

## BreakdownsAufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp

## Datenvisualisierungen

### Sicherheitslage

| Name | Typ | Beschreibung |
|---|---|---|
| Aktive angreifbare Anwendungselemente (AVIs) | Einzelne Punktzahl | Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs). |
| Verteilung des angreifbaren Anwendungselements (AVI) | Kreisdiagramm | Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung. |
| AVI-Trends | Symbol „ | Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung. |
| Durchschnittliche AVIs pro Anwendung | Symbol „ | Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung. |

### Trend bei Korrekturen

| Name | Typ | Beschreibung |
|---|---|---|
| Durchschnittliche Zeit bis zur Korrektur von angreifbaren Elementen in Anwendungen (AVIs) | Linie | Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung. |
| Nettoveränderung der AVIs | | Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat. |

# Application Vulnerability Response Referenzen

Referenzthemen mit Informationen zu Tabellen, Rollen und Eigenschaften, die mit der Anwendung Application Vulnerability Response installiert werden.

Details finden Sie unter:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Application Vulnerability Response -Benutzergruppen und -Rollen
- Mit Application Vulnerability Response installierte Komponenten
- Status des angreifbaren Elements in der Anwendung (AVI).
- Gescannte Anwendungsfelder
- Felder für angreifbares Anwendungselement
- Anwendungsschwachstellen-Felder
- Penetrationsteststatus

## Application Vulnerability Response -Benutzergruppen und -Rollen

Bevor Sie Schwachstellen mit Application Vulnerability Response (AVR) erfolgreich beheben können, müssen Sie Benutzer Benutzergruppen zuweisen.

Rollen definieren, was Sie und Ihre Gruppen in Application Vulnerability Response, Performance Analytics for Vulnerability Responseund Drittanbieterintegrationen mit Application Vulnerability Responseanzeigen und tun können.

### Benutzergruppen

Im Folgenden sind die Standardbenutzergruppen aufgeführt, die Application Vulnerability Responseunterstützen:

- App-Sec-Manager: Enthält Sicherheitsmanager. Ab Application Vulnerability Response v15.0 enthält sie auch Anwendungsbesitzer, die die Penetrationstest-Bewertungsanforderungen verwalten.
- Security Champion: Enthält Verbindungen zwischen der Entwicklungsgruppe und Sicherheitsmanagern.
- Entwickler: Enthält einzelne Beitragende.
- V15.0: Ethical Hacker: Enthält Mitglieder des Teams für ethisches Hacken, die Penetrationstests von Anwendungen durchführen.

Die Systemadministratorrolle [admin] ist erforderlich, um Benutzer den Standardbenutzergruppen von Application Vulnerability Response mithilfe des Benutzeradministrationsmoduls zuzuweisen.

**Hinweis:**

Das Zuweisen von AVR-Benutzern zu den Benutzergruppen Application Vulnerability Response für Application Vulnerability ResponseVulnerability Response ist im Setup-Assistenten von [] nicht verfügbar. Nur Vulnerability Response Rollen werden dort zugewiesen.

In der folgenden Tabelle sind die verfügbaren Application Vulnerability Response Benutzergruppen und die ihnen zugeordneten Rollen aufgelistet. Verwenden Sie diese Tabelle, um zu bestimmen, welche Benutzer welchen Gruppen zugewiesen werden sollen.

| Anwendergruppe | Rollen in dieser Gruppe |
|---|---|
| Security Champion<br><br>Mitglieder dieser Gruppe können: | • sn_vul.app_read_assigned<br>• sn_vul.app_write_assigned<br>• sn_vul.app_update_assignment_group |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendergruppe | Rollen in dieser Gruppe |
| --- | --- |
| • Ihnen zugewiesene angreifbare Anwendungselemente (AVIs) lesen und schreiben.<br>• Weisen Sie eine Ihnen zugewiesene AVI einer anderen Person oder Gruppe zu.<br>• V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren). | • sn_vul.app_update_assigned_to<br>• sn_vul.app_manage_auto_exception_rule |
| App-Sec-Manager<br><br>Mitglieder dieser Gruppe können:<br>• V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren).<br>• Lesen, Schreiben, Löschen und alle Vorgänge für Anwendungskorrekturaufgabenregeln.<br>• Lesen und schreiben Sie alle AVIs.<br>• Konfigurieren Sie AVR, indem Sie Regeln, Rechner und Schweregradzuordnungen erstellen und verwalten.<br>• Konfigurieren Sie Integrationen.<br>• Löschen Sie AVIs.<br>• Weisen Sie AVI Einzelpersonen oder Gruppen zu.<br>• Anwendungen verwalten.<br>• Ermöglicht den Zugriff auf das Anwendungsmodul.<br>• Planen, Konfigurieren und Ausführen der Integration.<br>• Integrationen lesen und ausführen.<br>• Zeigen Sie AVR-Dashboards und -Berichte Performance Analytics an.<br>• V15.0: Penetrationstest-Bewertungsanforderungen verwalten. | • sn_vul.app_manage_auto_exception_rule<br>• sn_vul.app_manage_group_rules<br>• sn_vul.app_read_all<br>• sn_vul.app_write_all<br>• sn_vul.app_update_assignment_group<br>• sn_vul.app_update_assigned_to<br>• sn_vul.app_configure_integrations<br><br>**Hinweis:**<br>Standardmäßig enthält diese Rolle granulare Rollen für die Konfiguration der Drittparteiintegration. Informationen zum Definieren oder Bearbeiten einer App-Sec Manager-Benutzergruppe nach einzelnen oder bestimmten Integrationen finden Sie unter Vulnerability Response Personas und granulare Rollen.<br><br>• sn_vul.app_manage_assignment_rules<br>• sn_vul.app_manage_remediation_target_rules<br>• sn_vul.app_manage_risk_score_configurations<br>• sn_vul.app_manage_applications<br>• sn_vul.app_manage_app_vul_permissions<br>• sn_vul.app_manage_normalized_severity<br>• Version 13.0: sn_vul.app_manage_app_sc<br>• Nur Version 12.0: sn_vul.app_read_application_release<br><br>[In v12.1 entfernt. Nicht verwenden]<br><br>• sn_sec_int.admin<br>• Version 13.0: pa_power_user<br>• pa_viewer |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendergruppe | Rollen in dieser Gruppe |
| --- | --- |
| | **Hinweis:** Ab Vulnerability Response v13.0 ist „pa_viewer“ in „pa_power_user“ enthalten und wird nicht mehr selbst benötigt.<br>• V15.0: sn_vul.app_manage_pen_test_request<br>• V15.0: sn_vul.app_update_state<br>• V15.0: cmdb_read |
| Entwickler<br>Mitglieder dieser Gruppe können:<br>• Ihnen zugewiesene AVR-Datensätze lesen und schreiben.<br>• Weisen Sie eine Ihnen zugewiesene AVI einer anderen Person oder Gruppe zu. | • sn_vul.app_read_assigned<br>• sn_vul.app_write_assigned<br>• sn_vul.app_update_assignment_group<br>• sn_vul.app_update_assigned_to<br>• sn_vul.app_pa_sc_view |
| V15.0: Ethischer Hacker<br>Mitglieder dieser Gruppe können:<br>• Konfigurieren Sie die Standardzuweisungsgruppe und den Beauftragten für Penetrationstest-Bewertungsanforderungen.<br>• Ergebnisse von Penetrationstests verwalten<br>• Verwalten Sie Bewertungsanforderungen für Penetrationstests.<br>• Zeigen Sie angreifbare Anwendungselemente an.<br>• Aktualisieren Sie die Zuweisung für angreifbare Anwendungselemente. | • V15.0: sn_vul.app_update_state<br>• V15.0: sn_vul.app_manage_pen_test_request<br>• V15.0: itil<br>• V15.0: sn_vul.app_read_all<br>• V15.0: sn_vul.app_manage_pen_test_request_config<br>• V15.0: sn_vul.app_manage_manual_avits<br>• V15.0: sn_vul.app_update_assigned_to<br>• V15.0: sn_vul.app_update_assignment_group |

Automatische Übersetzung

### Weisen Sie Benutzer Benutzergruppen in zu Application Vulnerability Response

Weisen Sie Gruppen mithilfe des Benutzeradministrationsmoduls in Ihrer Instanz Benutzer zu.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

So weisen Sie einen Benutzer einer Gruppe zu oder entfernen ihn:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Navigieren zu **Administration** > **Gruppen**.

**b.** Suchen und öffnen Sie die entsprechende Gruppe, z. B. **App-Sec Manager**.
Der Gruppendatensatz wird angezeigt.

**c.** Wählen Sie die Registerkarte **Gruppenmitglieder** aus.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

**d.** Klicken Sie auf **Bearbeiten**.
Das Formular „Mitglieder bearbeiten“ wird angezeigt.

**e.** Wählen Sie in der Liste **„Sammlung“** Benutzer aus, die der Gruppe hinzugefügt oder aus ihr entfernt werden sollen.

**f.** Sobald alle Benutzer der **Gruppenmitgliederliste** hinzugefügt oder entfernt wurden, klicken Sie auf **Speichern**.
Sie kehren zur Registerkarte **Gruppenmitglieder** zurück.

**g.** Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.

**Zugehörige Informationen**

Mit Application Vulnerability Response installierte Komponenten

## Mit Application Vulnerability Response installierte Komponenten

Bei Aktivierung der Funktion Application Vulnerability Response werden verschiedene Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und geplante Aufgaben.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

### Installierte Rollen

Granulare Rollen in Application Vulnerability Response werden standardmäßig bestimmten Benutzergruppen zugewiesen.

**Hinweis:**
Die Verwendung granularer Rollen außerhalb dieser Benutzergruppen erfordert Codierung und fortgeschrittene Application Vulnerability Response - oder ServiceNow -Kenntnisse.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| V20.0: sn_vul.app_manage_auto_exception_rule | Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren). | sn_vul.app_read_auto_exception_rul |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| sn_vul.app_manage_group_rules | Lesen, Schreiben, Löschen und alle Vorgänge für Anwendungskorrekturaufgabenregeln. | • sn_vul.app_read_all<br>• sn_vul.app_read_group_rules |
| V20.0: sn_vul.app_exception_approver | Genehmigt Ausnahmeregeln und Erweiterungsanforderungen für Ausnahmeregeln.<br>Ab v20.0 wurde die granulare Rolle sn_vul.app_read_all für diese Rolle entfernt, sodass Sie auf die Ihnen und Ihrer Gruppe zugewiesenen angreifbaren Anwendungselemente und Korrekturaufgaben zugreifen können, anstatt auf alle angreifbaren Anwendungselemente und Korrekturaufgaben. | sn_vul.app_read_auto_exception_rul |
| sn_vul.app_read_assigned | Zeigen Sie Ihnen zugewiesene angreifbare Anwendungselemente (AVIs) an. | |
| sn_vul.app_read_all | Zeigen Sie alle AVIs und zugehörigen Informationen an. | |
| sn_vul.app_write_assigned | Aktualisieren Sie Ihnen zugewiesene AVIs. | |
| sn_vul.app_write_all | Aktualisiert alle AVIs und zugehörigen Informationen. | |
| sn_vul.app_update_assignment_group | Aktualisieren Sie die AVI-Zuweisungsgruppe. | **Hinweis:** Bei Verwendung außerhalb der Standardbenutzergruppe ist sn_v oder sn_vul.app_write_assigned |
| sn_vul.app_update_assigned_to | Aktualisieren Sie den AVI-Beauftragten. | **Hinweis:** Bei Verwendung außerhalb der Standardbenutzergruppe ist sn_v oder sn_vul.app_write_assigned |
| sn_vul.app_configure_integrations | Konfigurieren Sie Drittanbieterintegrationen. | sn_vul.app_read_all<br>sn_vul.app_read_integrations<br>sn_sec_int.admin<br>sn_vul_veracode.configure_inte<br>sn_vul.configure_nvd_administ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | | [store-future: BEGIN review]sn_vul_fortify.configure<br><br>**Hinweis:**<br>Informationen zum Definieren o<br>einer App-Sec Manager-Benutze<br>einzelnen oder bestimmten Integ<br>Sie unter Vulnerability Respons<br>granulare Rollen. |
| sn_vul.app_read_integrations | Zeigen Sie alle Drittanbieterintegrationen an. | |
| sn_vul_veracode.configure_integration | Definieren, aktualisieren und löschen Sie Veracode-Integrationen. | |
| sn_vul.app_manage_assignment_rules | Definieren, aktualisieren und löschen Sie AVI-Zuweisungsregeln. | sn_vul.app_read_all<br>sn_vul.app_read_assignment_r |
| sn_vul.app_read_assignment_rules | Zeigen Sie Zuweisungsregeln an. | |
| sn_vul.app_manage_remediation_target_rules | Definieren, aktualisieren und löschen Sie AVI-Korrekturzielregeln. | sn_vul.app_read_all<br>sn_vul.app_read_remediation_t |
| sn_vul.app_manage_risk_score_configurations | Definieren, aktualisieren und löschen Sie AVR-Rechner und Risikoregeln. | sn_vul.app_read_all<br>sn_vul.app_read_risk_score_co<br>sn_sec_cmn.calc.write |
| sn_vul.app_read_risk_score_configuration | AVR-Rechner und Risikoregeln anzeigen. | |
| sn_vul.app_manage_applications | Anwendungsdatensätze anzeigen, aktualisieren und löschen. | |
| sn_vul.app_manage_app_sc | Gibt einem Security Champion die Möglichkeit, sich selbst der zugehörigen Liste „Gescannte Anwendung“ hinzuzufügen oder daraus zu entfernen. | |
| sn_vul.app_pa_sc_view | Bietet eine relevante Ansicht für den jeweiligen Security Champion. | |
| sn_vul.app_manage_app_vul_permissions | [internal] Wird von sn_vul.app_manage_applications verwendet. | |
| sn_vul.app_manage_normalized_severity | Aktualisieren Sie die Zuordnung auf den normalisierten Schweregrad. | sn_vul.app_read_normalized_severity |
| sn_vul.app_read_normalized_severity | Normalisierte Schweregraddatensätze anzeigen. | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| [In v12.1 entfernt. Nicht verwenden.] | | |
| sn_vul.app_read_application_release | Zeigen Sie Anwendungs-Release-Datensätze an. | |
| sn_sec_int.admin | Bietet Zugriff auf -Integrationen. | |
| pa_power_user | Bietet Zugriff auf Berichte | pa_viewer |
| sn_vul.app_sec_manager | Priorisiert und verwaltet angreifbare Anwendungselemente. | |
| sn_vul.app_developer | Entwickler, der für die Behebung der Anwendungsschwachstellen verantwortlich ist. | |
| sn_vul.app_create_watch_topic | Erstellen Sie Überwachungsthemen für Anwendungsschwachstellen. | |
| sn_vul.app_read_watch_topic | Lesen Sie die Überwachungsthemen für Anwendungsschwachstellen. | |
| sn_vul.app_edit_watch_topic | Bearbeiten Sie Überwachungsthemen für Anwendungsschwachstellen. | |

## Installierte Scheduled Jobs

Informationen zu Vulnerability Response freigegebenen geplanten Aufgaben finden Sie unter, Mit Vulnerability Response installierte Komponenten.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Ordnen Sie vorhandene AVIs der automatischen Ausnahmeregel zu | Wertet angreifbare Anwendungselemente für Übereinstimmungen mit Ausnahmeregeln aus. |
| Füllen Sie Eintrag und CVE M2M aus | Macht vorhandene Datensätze mit mehreren CWE-Datensätzen konsistent. Einmal nach dem Upgrade ausführen, um auszufüllen, und dann deaktivieren. |
| Synchronisieren Sie die primäre CWE erneut | Für benutzerdefinierte primäre CWE-Berechnungen. Nach dem Upgrade einmal ausführen, um die Synchronisierung erneut durchzuführen, und dann deaktivieren. |
| Rollup der Werte für angreifbare Anwendungselemente zu Schwachstelle und Gruppe | Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Anwendungselemente. |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Anwendungs-Release [sn_vul_app_release] | Enthält Informationen zur Anwendungsversion |
| Version 13.0: | Enthält die Datensätze der Security Champion-Gruppe Application Vulnerability Response. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Anwendungssicherheits-Champions<br><br>[sn_vul_app_m2m_app_sc] | |
| Anwendungsschwachstelleneintrag<br><br>[sn_vul_app_vul_entry] | Enthält Anwendungsschwachstelleneinträge |
| Anwendungsschwachstellenintegration<br><br>[sn_vul_app_integration] | Enthält Application Vulnerability Response Integrationsdatensätze. |
| Ort für Anwendungsschwachstellen-Scan<br><br>[sn_vul_app_vul_scan_location] | Enthält Informationen zum Scan-Standort einer Drittpartei |
| Zusammenfassung von Anwendungsschwachstellen-Scan<br><br>[sn_vul_app_vul_scan_summary] | Enthält Zusammenfassungsinformationen zu Drittpartei-Scans |
| Angreifbares Anwendungselement<br><br>[sn_vul_app_vulnerable_item] | Enthält AVI-Datensätze.<br><br>Ab v19.0 werden die folgenden Spalten für Software-Stücklisten hinzugefügt:<br>• sn_sbm_config_rule<br>• sn_sbom_component<br>• vex_justification<br>• vex_detail<br>• vex_response<br>• vex_state<br>• sca_type (SBOM-SCA) |
| Gescannte Anwendung<br><br>[sn_vul_app_scanned_application] | Enthält Anwendungsinformationen. |
| Statuszuordnung<br><br>[sn_vul_app_state_map] | Enthält die Statuszuordnung von Drittanbieterintegrationen zu AVI-Status (Application Vulnerable Item) |
| Schwachstellen-CWEs<br><br>[sn_vul_m2m_entry_cwe] | Verknüpft CVE-Daten mit Einträgen zu angreifbaren Anwendungen. |
| Anwendungskorrekturaufgabe – Manifest<br><br>sn_vul_app_rt_manifest | Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle durch geplante Aufgaben durchgeführt. |
| Anwendungskorrekturaufgabe | Enthält Anwendungskorrekturaufgaben |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| sn_vul_app_vulnerability | |
| Element der Anwendungskorrekturaufgabe<br><br>sn_vul_app_m2m_vul_group_item | M2M-Tabelle zwischen AVI und Anwendungskorrekturaufgaben. |
| Version 21.0:<br><br>Angreifbare Anwendungselemente<br><br>sn_vul_app_vulnerable_item | Enthält AVI-Datensätze. |
| Version 21.0:<br><br>Paket<br><br>[sn_vul_app_package] | Enthält Details zum Anwendungspaket |
| Version 21.0:<br><br>Lizenzen<br>sn_vul_app_license | Enthält Anwendungslizenzen. |
| Version 21.0:<br><br>Anwendungskorrekturaufgaben<br><br>sn_vul_app_vulnerability | Enthält Anwendungskorrekturaufgaben |

## Status des angreifbaren Elements in der Anwendung (AVI).

Application Vulnerability Response bietet jederzeit ein Statusmodell für den Status Ihrer angreifbaren Elemente in Anwendungen (AVIs). Wenn Sie wissen, wie sich die einzelnen Status aufeinander beziehen und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie Ihre AVIs korrigiert werden müssen.

## Status des angreifbaren Anwendungselements

Zu verstehen, wie Status funktionieren, hilft beim Erstellen oder Bearbeiten von AVI-Regeln (Application Vulnerable Items). AVIs haben mehrere mögliche Status, die dem importierten Korrekturstatus aus der Drittanbieterintegration zugeordnet werden. In einer AVI ist das **Feld** Status schreibgeschützt.

### Application Vulnerability Response Status-Flow-Diagramm

| Status | Beschreibung |
|---|---|
| Offen | Status bei Erstellung. In diesem Status können Sie:<br>**V16: Weitere Details abrufen**<br>Rufen Sie die folgenden Informationen zu einer aus Fortify importierten AVI ab: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

| Status | Beschreibung |
|---|---|
| | • Schwachstellenzusammenfassung<br>• Erklärung der Schwachstelle<br>• Empfehlung<br>• Referenzen<br>• Anforderung<br>• Antwort<br><br>**V16: Als falsch positiv markieren**<br>Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist.<br>**V16: Ausnahme anfordern**<br>Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und einen Grund an, und geben Sie optional zusätzliche Informationen an. Die Korrektur des Elements wird bis zu dem Datum zurückgestellt, bis zu dem eine Ausnahme angefordert wird.<br>**V15: Schließen**<br>Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt die AVI.<br>**V15: Lösen**<br>Markieren Sie eine geöffnete AVI als Gelöst, um sie in den Status „Gelöst“ zu verschieben. Sie müssen im Dialogfeld „Angreifbares Anwendungselement lösen“ Lösungsnotizen hinzufügen. |
| Zurückgestellt | **V15: Wird** durch die Option „ **Ausnahme anfordern** “ ausgelöst. Als Teil des Genehmigungs-Workflows lautet der Status „Zurückgestellt“ In Überprüfung und kann erst nach Genehmigung geschlossen werden.<br><br>In diesem Status können Sie:<br>**V16: Weitere Details abrufen**<br>Rufen Sie die folgenden Informationen zu einer aus Fortify importierten AVI ab: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)

| Status | Beschreibung |
| --- | --- |
| | • Schwachstellenzusammenfassung<br>• Erklärung der Schwachstelle<br>• Empfehlung<br>• Referenzen<br>• Anforderung<br>• Antwort<br><br>**Erneut öffnen**<br>Überführt eine geschlossene oder aufgelöste AVI zurück in den Status „Offen“.<br>**Schließen**<br>Wählen Sie den Status Geschlossen, einen Grund und zusätzliche Informationen aus. Schließt die AVI. |
| Wird untersucht | Wählen Sie diese Option aus der **Liste** Status aus. In diesem Status können Sie:<br>**V20.0**<br>Stellen Sie eine Korrekturaufgabe oder einen AVI-Datensatz manuell in den **Status „Warten auf Implementierung“**um.<br>**V16: Weitere Details abrufen**<br>Rufen Sie die folgenden Informationen zu einer aus Fortify importierten AVI ab:<br>• Schwachstellenzusammenfassung<br>• Erklärung der Schwachstelle<br>• Empfehlung<br>• Referenzen<br>• Anforderung<br>• Antwort<br><br>**V16: Als falsch positiv markieren**<br>Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass eine Schwachstelle im System vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist.<br>**V16: Ausnahme anfordern**<br>Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (Bis) und |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)**

| Status | Beschreibung |
| --- | --- |
| | einen Grund an, und geben Sie optional zusätzliche Informationen an. Die Korrektur des Elements wird bis zu dem Datum zurückgestellt, bis zu dem eine Ausnahme angefordert wird.<br>**V15: Schließen**<br>Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt die AVI.<br>**V15: Lösen**<br>Markieren Sie eine geöffnete AVI als Gelöst, um sie in den Status „Gelöst“ zu verschieben. Sie müssen im Dialogfeld „Angreifbares Anwendungselement lösen“ Lösungsnotizen hinzufügen. |
| Warten auf Implementierung | Sie können Datensätze nur manuell in diesen Status überführen, indem Sie „Warten auf Implementierung“ aus AVI und Korrekturaufgabendatensätzen im Status „Wird untersucht“ auswählen. In diesem Status können Sie:<br>**Offen**<br>Überführt AVI zurück in den Status „Offen“.<br>**Wird untersucht**<br>Rufen Sie weitere Informationen zur Lösung ab. Wechselt zu „Wird untersucht“.<br>**Lösen**<br>Markieren Sie eine geöffnete AVI als Gelöst, um sie in den Status „Gelöst“ zu verschieben. Sie müssen im Dialogfeld „Angreifbares Anwendungselement lösen“ Lösungsnotizen hinzufügen.<br>**Schließen**<br>Wählen Sie den Status Geschlossen, einen Grund aus dem Dialogfeld „Angreifbares Element schließen“ aus, und geben Sie zusätzliche Informationen an. Schließt die AVI.<br>In diesem Status können Sie einen Datensatz in „Warten auf Implementierung“ |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Application Vulnerability Response Status-Flow-Diagramm (Fortsetzung)**

| Status | Beschreibung |
|---|---|
| | überführen, wenn Ihre Recherchen und Arbeiten an einer Aufgabe abgeschlossen sind und eine Korrektur zwar für die Implementierung bereit, aber noch nicht verfügbar ist.<br><br>Legen Sie die Felder **Korrekturzusagedatum** und **Korrekturplan fest**.<br><br>Nach der Implementierung lösen oder schließen Sie die Datensätze. |
| Gelöst | Wird über die Schaltfläche „Lösen“ ausgelöst. In diesem Status können Sie:<br><br>**V16: Weitere Details abrufen**<br><br>Rufen Sie die folgenden Informationen zu einer aus Fortify importierten AVI ab:<br><br>• Schwachstellenzusammenfassung<br>• Erklärung der Schwachstelle<br>• Empfehlung<br>• Referenzen<br>• Anforderung<br>• Antwort<br><br>**Erneut öffnen**<br><br>Wechselt zurück in den Status „ **Offen** “.<br><br>**Schließen**<br><br>Wählen Sie den Status **Geschlossen**, einen Grund und zusätzliche Informationen aus. Schließt die Gruppe.<br><br>Notizen und Lösungsinformationen werden auf der Registerkarte **Notizen** angezeigt. |
| Geschlossen | Ausgelöst durch die Schaltfläche Schließen. In diesem Status können Sie:<br><br>Erneut öffnen: Wechselt in den Status „Offen“ zurück. |

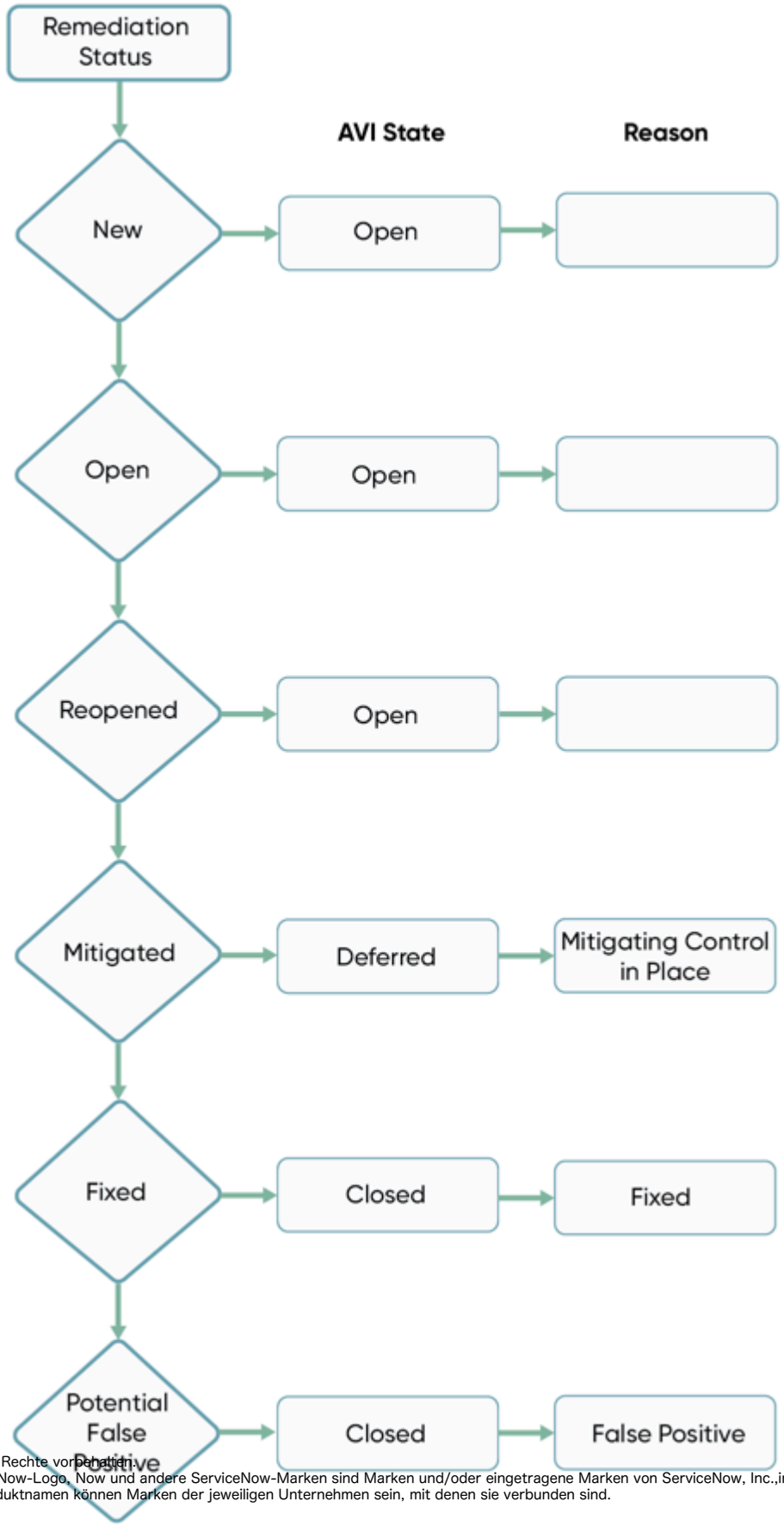
Die Zuordnung für Status pro Integration wird wie folgt angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Statuszuordnung für Veracode

**Hinweis:**
Diese Statuszuordnung ist nur anwendbar, wenn die Option zur Selektierung in ServiceNow nicht ausgewählt ist.

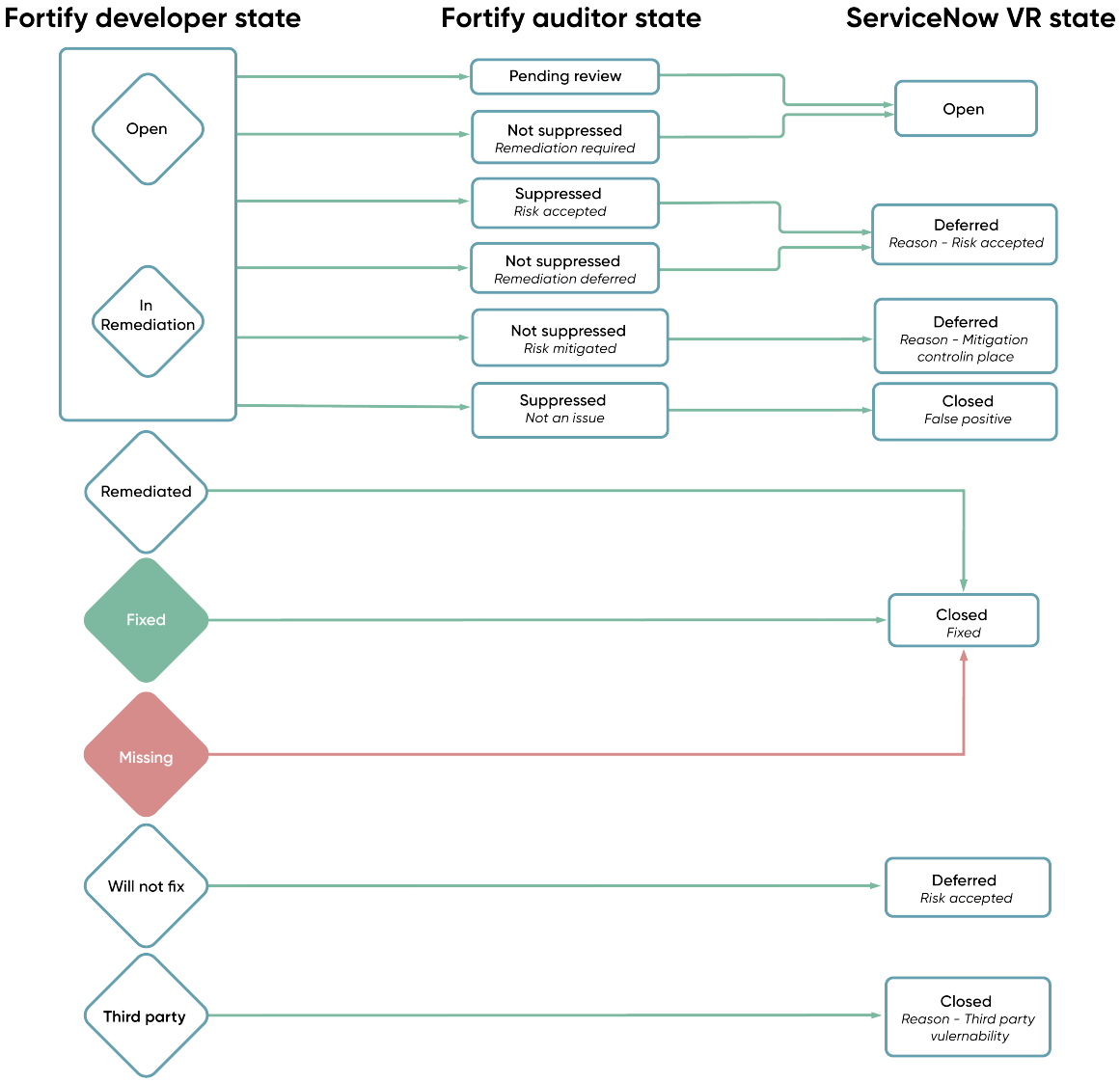



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Statuszuordnung für Fortify

**Hinweis:**
Diese Statuszuordnung ist nur anwendbar, wenn die Option zur Selektierung in ServiceNow nicht ausgewählt ist.




Automatische Übersetzung

## Application Vulnerability Response Beispiele für Korrekturaufgabenregeln

Beispiel für eine Korrekturaufgabenregel mit dem Bedingungsgenerator.

## Eine Regel für Korrekturaufgaben mit Schwachstelle, Produktmodell, IP-Adresse und Zuweisungsgruppe

1. Legen Sie im Bedingungsgenerator für einen neuen Datensatz die Bedingung als fest **Schwachstelle** > **ist** und geben Sie eine bekannte Schwachstelle ein.

   Schwachstellen werden aus den Integrationen „Nation Vulnerability Database“ (NVD) und „Common Weakness Enumeration“ (CWE) importiert, wie in Application Vulnerability Response konfigurierenbeschrieben.

2. Wählen Sie im Abschnitt **Gruppieren nach die Option Angreifbares Anwendungselement** für das Feld **Angreifbare Anwendungselemente gruppieren aus** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Feld Verwenden die Option **Zuweisungsgruppe aus**.

   Verwenden Sie Zuweisungsregeln, um das Feld **Zuweisungsgruppe** automatisch für die Verwendung in der Regel für Korrekturaufgaben festzulegen. Sie können eine mit der Anwendung bereitgestellte Regel verwenden oder eigene Zuweisungsregeln einrichten. Weitere Informationen finden Sie unter Weisen Sie angreifbare Anwendungselemente in Application Vulnerability Response automatisch zu.

4. Wählen Sie eine andere Bedingung aus, z. B. Konfigurationselement „Angreifbares Anwendungselement“ im Feld **Angreifbares Anwendungselement gruppieren aus** und IP-Adresse oder Produktmodell im Feld **Wird** verwendet.
5. Wählen Sie im Abschnitt „Zuweisung“ für Korrekturaufgabe Feld nach Feld zuweisen die Option Nach Feld gruppieren **aus**.
6. Wählen Sie im Feld **Gruppieren nach die Option Zuweisungsgruppe aus**.

   Wie in diesem Abschnitt beschrieben, weist diese Auswahl angreifbare Elemente basierend auf den Bedingungen, die Sie im Abschnitt „Gruppieren nach“ festgelegt haben, verschiedenen Gruppen zu. Obwohl die AVIs die Schwachstelle gemeinsam nutzen, werden sie basierend auf dem CI-Produktmodell oder nach IP-Adresse verschiedenen Gruppen zugewiesen.

7. Wählen Sie **Absenden** aus, um Ihre Regel zu speichern.

## Gescannte Anwendungsfelder

Anwendungen werden während des Imports unter gespeichert **Administration** > **Anwendungen** in Application Vulnerability Response.

## Gescannte Anwendungsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt, sofern nicht anders angegeben. **Abteilungs-** und **Supportgruppeneinträge** können von einem App-Sec-Manager manuell hinzugefügt oder bearbeitet werden.

| Feld | Beschreibung |
|---|---|
| Name | Importierter Name der Anwendung. |
| Version | Importierte Version der Anwendung, falls zutreffend. |
| Betriebsstatus | Importierter Betriebsstatus der Anwendung. |
| Abteilung | Importierte Abteilung, zu der die Anwendung gehört. Wenn leer, kann es manuell hinzugefügt werden. |
| Geschäftsbereich | Importierter Geschäftsbereich, zu dem die Abteilung gehört. Wenn das Feld **Abteilung** ausgefüllt wird, wird dieses Feld automatisch mit dem Geschäftsbereich gefüllt, zu dem die Abteilung gehört. Andernfalls bleibt es leer und schreibgeschützt. |
| Support-Gruppe | Importierte Supportgruppe, zu der die Anwendung gehört. Wenn leer, kann es manuell hinzugefügt werden. |
| Beschreibung | Importierte Beschreibung der Anwendung. |
| Letzte Compliancеprüfung der Richtlinie am | Datum, an dem die Anwendung zuletzt von Veracode auf Richtlinienkonformität gescannt wurde Es wird in den verketteten Integrationen der Anwendungslistenintegration verwendet, in denen Unterstützung für die Delta- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Erfassung für Anwendungen verfügbar ist, indem dieses Datum mit der Delta-Startzeit der jeweiligen Integrationen verglichen wird.<br><br>**Hinweis:**<br>Daten werden für Anwendungen abgerufen, die aus Veracode abgerufen werden, deren Wert für „Datum der letzten Compliancеprüfung der Richtlinie“ größer oder gleich der „Startzeit“ (delta_start_time) der verketteten Integrationen ist. |
| **Zugehörige Liste (nur für App-Sec-Manager oder Security Champion sichtbar)** | |
| Security Champion | Listet die Anwendungen auf, die einem Sicherheits-Champion zugeordnet sind. App-Sec-Manager können Mitglieder zur Liste hinzufügen oder daraus entfernen. |

## Felder für angreifbares Anwendungselement

Angreifbare Elemente in Anwendungen (AVIs) werden während der Importe von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

## Felder für angreifbare Anwendungselemente

Mit Ausnahme der Felder **Zuweisungsgruppe**, **Zugewiesen an** und **Notizen**sind alle anderen Felder in der AVI schreibgeschützt.

| Feld | Beschreibung |
|---|---|
| Nummer | Automatisch generierter AVI-Bezeichner für diesen Datensatz. |
| Überprüfungstyp | Typ des Scanners, der diese AVI gefunden hat.<br><br>Die Auswahlmöglichkeiten lauten wie folgt:<br>• Dynamisch<br>• Statisches Objekt<br>• SCA |
| Risikobewertung | Quantifizierte **Risikopunktzahl**, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikobewertungen finden Sie unter, Risiko in Application Vulnerability Response automatisch berechnen. |
| Risikopunktzahl | Berechneter Betrag des Risikos, das die AVI für Ihre Umgebung darstellt.<br><br>Weitere Informationen finden Sie unter Risiko in Application Vulnerability Response automatisch berechnen. |
| Datum der Korrekturzusage | Das Datum, an dem **AVIs**korrigiert werden sollen, nachdem sie in den Status „Wird untersucht“ verschoben wurden. Dieses Feld wird nur angezeigt, wenn sich die AVI im Status Wird **untersucht**befindet. |
| Korrekturziel | Datum, bis zu dem die AVIs korrigiert werden sollen, seit sie zuerst identifiziert wurden. Wird nur angezeigt, wenn zutreffend. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response. |
| Korrekturstatus | Status der Fehlerkorrektur für die AVI. Sie wird von der AVI mit dem nächsten Fälligkeitsdatum bestimmt, sofern zutreffend.<br>Zu den Status gehören:<br>• In Ausführung<br>• Ziel rückt näher<br>• Vergangenes Ziel |
| Kategoriename | Name der Kategorie der Schwachstelle. |
| Schwachstelle | ID der Schwachstelle, die diesem angreifbaren Anwendungselement zugeordnet ist. |
| Anwendungs-Release | Version der Anwendung. |
| Anwendungsmodul | Betroffene Anwendung in DAST-Scan. Für SAST-Scans ausgeblendet. |
| Standort<br>Version 14.0: SAST | DAST: URL-Speicherort der Schwachstelle in der Anwendung.<br>SAST: Dateipfad und Zeilennummer der Schwachstelle in der Anwendung. |
| Status | Dieses Feld ist bei der Erstellung standardmäßig auf „ **Offen** “ festgelegt. Weitere Informationen zur Zuordnung von Status finden Sie unter Status des angreifbaren Elements in der Anwendung (AVI).. |
| Grund | [Nur sichtbar, wenn sich das AIV im Status „ **Geschlossen** “ befindet.] Erklärung des Status. |
| Zuweisungsgruppe | Gruppe, die für die Arbeit an dieser AVI ausgewählt wurde. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser AVI arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden |
| Erste ermittelte | Datum, an dem die Drittparteiquelle das angreifbare Anwendungselement erstmals gefunden hat. |
| Zuletzt gefunden | Datum, an dem die Drittparteiquelle das angreifbare Anwendungselement zuletzt gefunden hat. |
| Geschlossen | [Nur sichtbar, wenn sich die AVI im Status „ **Geschlossen** “ befindet.] Datum, an dem die AVI geschlossen wurde. |
| Geschlossen von | [Nur sichtbar, wenn sich die AVI im Status „ **Geschlossen** “ befindet.] Entität, die die AVI geschlossen hat. |
| Zusammenfassung | Importierte Beschreibung der Schwachstelle. |
| **Ergebnisse**<br>Schreibgeschützte Daten, die aus einer Drittanbieterintegration importiert werden. | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| AVIT-ID der Quelle | Importierter Bezeichner für die Quell-AVI. |
| Quellenschweregrad | Importierter Schweregrad aus der Quellanwendung. |
| Zieldatum für Quellenkorrektur | Importdatum, bis zu dem die Quelle die Korrektur der AVI erwartet. |
| Quellenminderungsstatus | Importierter Mitigationsstatus aus der Quellanwendung. |
| Quellenkorrekturstatus | Korrekturstatus aus der Quellanwendung importiert. |
| Quellermittlungsstatus | [Nur sichtbar, wenn ausgefüllt] Importierter Problemstatus aus der Quellanwendung. |
| SDLC-Status | Importierter Status des Softwareentwicklungs-Lebenszyklus. |
| Entspricht Richtlinie | Importierter Compliance-Status. Wenn kein Status angegeben ist, wird dieses Feld auf **Nicht zutreffend** festgelegt. |
| Quell-Link | URL der Quell-AVI. |
| Quellhinweise | Importierte Notizen aus der Quelle. |
| Schwachstellenzusammenfassung | Zusammenfassung aus der Quelle importiert. |
| Erklärung der Schwachstelle | Importierte Erklärung aus der Quelle. |
| Empfehlung | Importierte Empfehlung aus der Quelle. |
| Referenzen | Importierte Referenzen aus der Quelle. |
| **HTTP-Anforderung/-Antwort (nur für DAST-Scans sichtbar)** | |
| Quellenanforderung | HTTP-Anforderung |
| Quellenantwort | HTTP-Antwort |
| **Notizen** | |
| Korrekturplan | Details dazu, wie die AVIs korrigiert werden. Der Plan muss bis zum **Datum der Korrekturzusage** implementiert werden. Dieses Feld wird nur angezeigt, wenn sich die AVI im Status Wird **untersucht** befindet. |
| Zusätzliche Kommentare/ Arbeitsnotizen | Alle relevanten Informationen. Wählen Sie das Textfeld für Arbeitsnotizen aus, um Informationen hinzuzufügen.<br><br>Ab Vulnerability Response v20.0 können Sie Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Anwendungselement hinzufügen. |



## Penetrationsteststatus

Anwendungsbesitzer können eine Penetrationstestbewertung für ihre Anwendungen anfordern und den Fortschritt des Teams für ethisches Hacken überwachen, bis die Anforderung gelöst ist.

Die Penetrationstest-Bewertungsanforderung durchläuft die folgenden Übergangsstatus, bis sie gelöst wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Phasen der Penetrationstest-Bewertungsanforderung

| Feld | Beschreibung |
|---|---|
| Penetrationsteststatus | |
| Offen | Status, wenn die Bewertungsanforderung vom Anwendungsbesitzer erstellt wurde. |
| Umfangsdefinition | Das Team für ethisches Hacken bewertet die Anforderung und den Umfang der Anwendung. |
| Vorbereitung der Umgebung | Der Anwendungsbesitzer erstellt eine Umgebung mit Rollen und anderen Informationen und stellt sie dem Ethical Hacking-Team zum Testen bereit. |
| Tests | Das Team für ethisches Hacken testet die Anwendung manuell, um die Ergebnisse des Penetrationstests zu identifizieren. |
| V16.1: Test wird ausgeführt | Das Team für ethisches Hacken gibt an, dass derzeit Tests durchgeführt werden. Wenn dieser Status ausgewählt ist, wird die Option **Test in Warteschleife** im Formular verfügbar. |
| V16.1: Tests in Warteschleife | Dieses Feld wird nur angezeigt, wenn der Status Test wird ausgeführt ausgewählt ist. Das Team für ethisches Hacken steuert die Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) der Penetrationstest-Bewertungsanforderungen, indem es bei Bedarf diesen Status auswählt. Dadurch wird sichergestellt, dass genaue SLAs gemeldet werden. |
| V16.1: Tests werden überprüft | Das Team für ethisches Hacken gibt an, dass der Test abgeschlossen ist und von einem Fachexperten überprüft wird. |
| Geschlossen | Das Team für ethisches Hacken schließt die Penetrationstest-Bewertungsanforderungen, nachdem die Penetrationstestergebnisse gemeldet wurden.<br>**Hinweis:**<br>Ab V16.1 können Sie die Option **Anforderung kopieren und erstellen** im Formular verwenden, um die Anforderung im Status „Geschlossen“ zu replizieren und eine neue Anforderung zu erstellen. Details finden Sie unter Replizieren Sie eine Penetrationstestanforderung im Status „Geschlossen“.. |
| V16.1: Abgebrochen | Der Anwendungsbesitzer bricht die Penetrationstest-Bewertungsanforderung ab. |
| V16.1: Entwurf | Der Anwendungsbesitzer erstellt eine Anforderung und speichert sie als Entwurf, bevor er die Anforderung übermittelt. |
| Status des angreifbaren Anwendungselements | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Phasen der Penetrationstest-Bewertungsanforderung (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| Offen | Wenn das Team für ethisches Hacken die Penetrationstestergebnisse identifiziert und erstellt, lautet der Status „Offen“. |
| Gelöst | Wenn das Anwendungsteam die Ergebnisse des Penetrationstests auflöst, wird der Status in Gelöst geändert.<br>**Hinweis:** Wenn das Penetrationstestergebnis gelöst wurde, aber noch vom Team für ethisches Hacken validiert werden muss, lautet der Substatus `Validation Pending`. |
| Geschlossen | Das Team für ethisches Hacken validiert, dass die Ergebnisse des Penetrationstests gelöst wurden, und ändert den Status in „Geschlossen“. |

## Statuszuordnung für Zurückstellungen und Falschmeldungen in verwalten Application Vulnerability Response

Sie können verwalten, wie die **Quellstatus** für angreifbare Elemente (AVIs), die von Veracode Vulnerability Integration und Fortify Vulnerability Integration importiert werden, nach dem Import in Ihrer Instanz zugeordnet werden.

Ab v20.0 von Vulnerability Responsehaben Sie mehr Optionen für die Selektierung Ihrer importierten AVIs mit ServiceNow -Workflows.

Wenn Sie Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration oder Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integrationverwenden, erhalten Sie auf den Integrationskonfigurationsseiten zwei Optionen, die Sie bei der Verwaltung von Ausnahmen und falsch positiven Meldungen in Ihrer Instanz unterstützen.

- Verwalten Sie Ausnahmen in ServiceNow
- Verwalten Sie Falschmeldungen in ServiceNow

Erforderliche Rolle: App-Sec-Manager.

## Anwendungsfall für Ausnahmemanagement

AVIs werden aus diesen Integrationen mit **Quellstatus** importiert. Nach dem Import werden diese Status den Status „ **Ziel“** und **„Zielgrund“** in Ihrer Instanz zugeordnet, da in einigen Fällen keine genauen Übereinstimmungen zwischen den Quellstatus Ihres Scanners und den von Ihrer Instanz verwendeten Status vorhanden sind.

Zum Beispiel werden **Quellstatus**wie **Wird nicht**korrigiert, Korrektur zurückgestellt, **Risiko akzeptiert**und **Risiko gemindert** aus Fortify Vulnerability Integration dem Status Zurückgestellt mit dem **SubstatusRisiko akzeptiert** oder **ausgleichende Steuerung** in Ihrer Instanz zugeordnet.

Auf den Konfigurationsseiten für diese Integrationen haben Sie die folgenden Optionen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Kontrollkästchen aktiviert | Beschreibung |
|---|---|---|
| Verwalten Sie Ausnahmen in ServiceNow | Y (standardmäßig) | Wenn Sie diese Option aktiviert lassen, müssen Sie Ausnahmen aus AVI-Datensätzen anfordern.<br><br>Importierte **AVIs**, die für den Status „Zurückgestellt“ markiert sind, werden mit dem Ausnahmeverwaltungs-Workflow ServiceNow selektiert.<br><br>**AVIs** mit **Quellstatus**, die normalerweise einem Status „Zurückgestellt“ zugeordnet sind, werden dem **Status** „Ziel“ im Status „ **Offen** “ zugeordnet. |
| | N | Wenn Sie das Kontrollkästchen deaktivieren, bleiben die **Quellstatus** erhalten, die von Ihrem Scanner importiert wurden.<br><br>Diese **AVIs** werden dem Zielstatus „ **Zurückgestellt**“ und einem **Zielgrund** -Status in Ihrer Instanz zugeordnet. Sie werden nicht vom Ausnahme-Workflow selektiert, da sie nicht dem Status „Ziel für **Selektierung** “ und dem Status „ **Ziel für Selektierungsgrund** “ zugeordnet sind.<br><br>Die UI-Aktion **„Ausnahme anfordern** “ ist im AVI-Datensatz nicht verfügbar, da sich der Datensatz bereits im Status **„Zurückgestelltes** Ziel“ befindet. |

## Anwendungsfall für Falsch positive Ergebnisse

Für falsch positive Ergebnisse aus Veracode Vulnerability Integration werden Quellstatus wie „ **Falsch positiv** “ oder „ **Potenziell falsch positiv** “ dem Status „ **Geschlossenes Ziel** “ mit dem Substatus „ **Falsch positiv**“ zugeordnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Kontrollkästchen aktiviert | Beschreibung |
|---|---|---|
| Verwalten Sie Falschmeldungen in ServiceNow | Y (standardmäßig) | Wenn Sie diese Option ausgewählt lassen, müssen Sie ein **Falsch positives Ergebnis** aus AVI-Datensätzen anfordern.<br><br>Importierte AVIs, die für den Status „ **Falsch positiv** “ oder „ **Potenziell falsch positiv** “ markiert sind, werden mit dem Ausnahmeverwaltungs-Workflow ServiceNow selektiert.<br><br>**AVIs** mit **Quellstatus**, die normalerweise einem **geschlossenen** Zielstatus zugeordnet sind, werden einem **Ziel** -Selektierungsstatus in **Offen**zugeordnet.<br><br>Die UI-Aktion **„Falsch positiv** “ ist im AVI-Datensatz verfügbar. |
| | N | Wenn Sie das Kontrollkästchen deaktivieren, bleiben die **Quellstatus** erhalten, die von Ihrem Scanner importiert wurden.<br><br>Diese **AVIs** werden in Ihrer Instanz dem Zielstatus **Geschlossen** und dem **Zielgrund** -Status **Falsch positiv** zugeordnet.<br>Sie werden nicht vom falsch positiven Workflow selektiert.<br><br>Die UI-Aktion **„Falsch positiv** “ ist für den AVI-Datensatz nicht verfügbar, da sich der Datensatz bereits im Status „ **Geschlossenes** Ziel“ befindet. |

## Application Vulnerability Response Referenzen

Die folgenden Begriffe werden in Application Vulnerability Responseverwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Angreifbare Anwendungselemente (AVIs)**

Paarungen von Schwachstelleneinträgen und potenziell angreifbaren Anwendungen in Ihrer Unternehmensumgebung.

**Zuweisungsregeln**

Regeln, die verwendet werden, um AVIs basierend auf Ihren definierten Kriterien zuzuweisen.

**Common Platform Enumeration (CPE)**

Ein strukturiertes NIST NVD-Benennungsschema für Systeme, Software und Pakete der Informationstechnologie.

**Common Vulnerabilities and Exposures (CVE)**

Dictionary der öffentlich bekannten Informationssicherheitsschwachstellen und -risiken.

**Common Weakness Enumeration (CWE)**

Liste der von der Community entwickelten Softwareschwachstellentypen.

**Integrationen**

Geplante Aufgaben, die Berichtsdaten aus CWE oder einem Drittanbietersystem wie Veracodeabrufen, um Schwachstellendaten abzurufen.

> **Hinweis:**
> Wenn die Integration der NIST National Vulnerability Database in Vulnerability Response aktiviert und konfiguriert ist, ist die CVE-Ergänzung für CWEs verfügbar, aber nicht erforderlich. Weitere Informationen zur Integration der NIST National Vulnerability Database finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern.

**National Vulnerability Database (NVD)**

Repository der US-Regierung mit standardbasierten Schwachstellenmanagementdaten, die mithilfe des Security Content Automation Protocol (SCAP) dargestellt werden.

**Nachbesserungszielregeln**

Regeln, die verwendet werden, um AVIs-Zieldaten für die Korrektur basierend auf Ihren definierten Kriterien zuzuweisen.

**Sicherheitsrisiko-Rechner**

Rechner, die zur Priorisierung und Kategorisierung von Anwendungsschwachstellen basierend auf Ihren definierten Kriterien verwendet werden.

## Ausnahmeregel Beispiel für Application Vulnerability Response

Eine Beispielregel, die auf einer bekannten Schwachstelle für eine Ausnahmeregel basiert.

| Feld | Beschreibung |
|---|---|
| Name | Ein eindeutiger Name, mit dem Sie den Zweck identifizieren und die Regel leicht finden können, z. B. `Veracode-1 cwe-22exception`. |
| Status | Schreibgeschützt: Entwurf |
| Gültig ab | Datum, an dem diese Regel zum Zurückstellen von AVIs aktiv ist. |
| Ausführungsbefehl | Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert hat Vorrang vor einem höheren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Gültig bis | Datum, an dem die Korrekturaufgabe die Annahme neuer VIs beendet. |
| Zurückgestellt bis | Datum, bis zu dem die Korrekturaufgaben und AVIs zurückgestellt werden. An diesem Datum wird die AVUL geschlossen, alle AVIs werden aus der Aufgabe entfernt und erneut geöffnet. Gruppenregeln werden erneut auf diese AVIs angewendet. |
| Grund | Grund für die Erstellung dieser Ausnahmeregel. Wählen Sie eine Option aus der Liste aus, z. B. **Korrektur nicht verfügbar**. |
| Zuweisungsgruppe | Gruppe, die für die Nachverfolgung der zurückgestellten VIs zugewiesen ist, z. B. APP Sec Manager. |
| Zusätzliche Informationen | Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen. In diesem Beispiel AVIs zurückstellen mit der Schwachstelle – Veracode-1-22. |
| Bedingung | Filterbedingungen, um anzugeben, welche AVIs dieser Regel entsprechen. In diesem Beispiel lautet die Schwachstelle Veracode-1-22. |
| Für vorhandene Daten ausführen | Option, mit der Sie diese Regel für vorhandene Daten ausführen können, wenn sie zum ersten Mal ausgeführt wird.<br><br>Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der regelmäßigen Aufgabe *`Associate existing AVIs with Auto Exception Rule`* ausgeführt, beginnend mit neuen Daten.<br><br>Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten am **Gültig ab** -Datum ausgeführt. |



## Application Vulnerability Response -Produktansicht

Das AVR-Produkt (Application Vulnerability Response) erfasst die von den Tools für Anwendungssicherheitstests erkannten Schwachstellen und Schwachstellen und bietet einen Überblick über die Sicherheitslage aller Anwendungen in Ihrer Umgebung.

Mit AVR können Sie die Risiken mit den Fehlerkorrektur-Workflows reduzieren. Das Ziel dieser Produktansicht besteht darin, Ihnen zu helfen, zu verstehen, wie AVR-Schlüsselentitäten mit dem CSDM-Core-Framework funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Aktualisierte Terminologie

Ab AVR v19.0 wurden die folgenden Schlüsseltabellen und Spaltennamen aktualisiert. Daher werden in der Dokumentation sowohl Verweise auf die älteren als auch auf die neueren Namen angezeigt.

**Aktualisierte Liste der Begriffe, Tabellen und Feldnamen für AVR**

| Vor AVR v19.0 | Ab AVR v19.0 |
|---|---|
| CI-Suchregeln | Suchregeln |
| Formular „CI-Suchregel“ | Formular „Suchregel“ |
| CI-Übereinstimmungsregel | Übereinstimmungsregel |
| Tabelle durchsuchen | CI-Tabelle durchsuchen |
| Feld durchsuchen | CI-Feld durchsuchen |
| Anwendungs-Release | Erkannte Anwendungen |
| Anwendungs-Release-Tabelle | Tabelle „Erkannte Anwendungen“ |
| Business-Relevanz | Geschäftsrelevanz – Quelle |

## Voraussetzungen

Installieren Sie die neuesten Versionen der folgenden Anwendungen:

- Security Support Common
- Vulnerability Response
- Security Integration Framework
- Security Support Orchestration
- Scanner-Integrationen wie Veracode und Fortify

## AVR und CSDM 4.0

Vor AVR v19.0 wurde bei der Erfassung von Anwendungsschwachstellen die Anwendung, für die die Schwachstellen erfasst wurden, mithilfe der CI-Suchregeln für die gescannten Anwendungen (sn_vul_app_scanned_application) gesucht. Wenn der Anwendungsnamen-Datensatz nicht vorhanden ist, wird ein Eintrag vorgenommen.

Ab AVR v19.0 werden zur Anpassung an das CSDM 4.0-Framework die Produktmodelltabellen anstelle der Tabelle „Gescannte Anwendungen“ verwendet. Wenn die Anwendung die Version hat, erfolgt die Suche in der Tabelle „Softwaremodell“. Wenn keine Version vorhanden ist, erfolgt die Suche in der Tabelle „Anwendungsmodell“. Sowohl das Anwendungsmodell als auch das Softwaremodell sind untergeordnete Tabellen der Tabelle „Produktmodell“, der Grundlagentabelle in CMDB. Im folgenden Screenshot wird das Produktmodell erläutert.

## Systemeigenschaft

Um den produktmodellbasierten CSDM 4.0-Suchprozess zu verwenden, legen Sie die Systemeigenschaft *sn_vul.use_product_model* auf *true*fest.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Überlegungen zu Systemeigenschaften**

| Name der Systemeigenschaft | Systemeigenschaftswert | Suchzielwert | Überlegungen |
|---|---|---|---|
| sn_vul.use_product_model | Wahr | Wählen Sie den Wert **Produktmodell aus** | Neue Benutzer sollten den Wert **Produktmodell** auswählen, um die Suchregeln für Produktmodelle des CSDM 4.0-Frameworks zu verwenden. |
| | false | Wählen Sie den Wert **Konfigurationselement aus** | Bestehende Benutzer können den CI-Suchprozess und die vorhandenen **CI-Suchregeln**weiterhin verwenden. |

**Hinweis:**
Um den Suchzielwert festzulegen, navigieren Sie zur Seite „ **Suchregel** “ > **[Suchregel für AVR-Integration]** > Feld „ **Suchziel** “.

### Suchregeln in AVR

Im CSDM 4.0-Framework werden produktmodellbasierte Suchregeln anstelle von CI-Suchregeln verwendet, um Einträge in den entsprechenden Produktmodellklassen zu erstellen. Ebenso können Sie für Skripts die Suchregeln im Rahmen des CSDM 4.0-Modells definieren.

Ab AVR v19.0 müssen Sie beim Erstellen einer **Suchregel** im Feld Suchziel definieren, ob Sie den Konfigurationselement- oder den Produktmodell-Ansatz verwenden möchten. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

### Erkannte Anwendungen

Navigieren zu **Alle** > **Erkannte Anwendungen**. In der Tabelle „Erkannte Anwendungen“ werden die von den Scannern erfassten Anwendungen angezeigt. Wenn die Systemeigenschaft `sn_vul.use_product_model` auf `true`festgelegt ist, können Sie die entsprechenden Produktmodelle für die Anwendungen anzeigen.

### AVR-Überlegungen

#### Vorhandensein doppelter CI- oder Produktmodelldatensätze

Vergewissern Sie sich, dass die Systemeigenschaft `sn_vul.use_product_model` für den Suchvorgang ordnungsgemäß konfiguriert wurde. Stellen Sie sicher, dass Sie beim Konfigurieren des Suchregelformulars entweder **Konfigurationselement** oder **Produktmodell** als Suchziel auswählen.

## Container Vulnerability Response

Die Anwendung ServiceNow® Container Vulnerability Response importiert angreifbare Container-Elemente (CVITs) und ermöglicht gemäß den Regeln die Behebung von Container-Schwachstellen. Schwachstellendaten werden aus internen und externen Quellen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

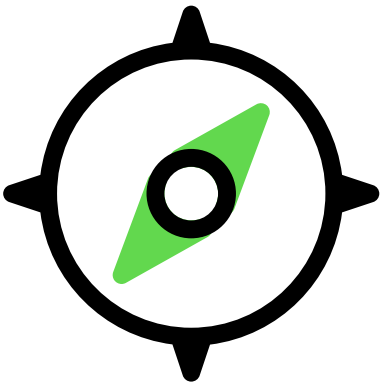
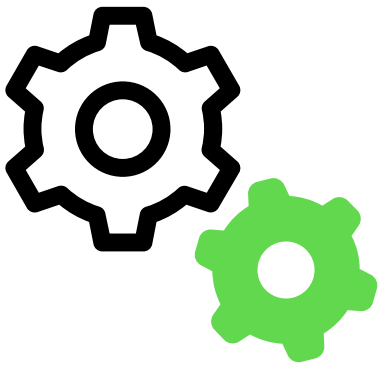
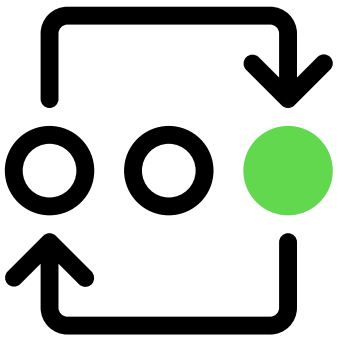
abgerufen, z. B. aus der National Vulnerability Database (NVD) oder aus Integrationen von Drittanbietern.

Ab Version 18.0 von Vulnerability Responsekönnen Sie CVITs in Vulnerability Manager Workspace bzw. IT Remediation Workspace überwachen und korrigieren. Weitere Informationen finden Sie unter Arbeitsbereich des Schwachstellenmanagers und IT Remediation Workspace erkunden.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

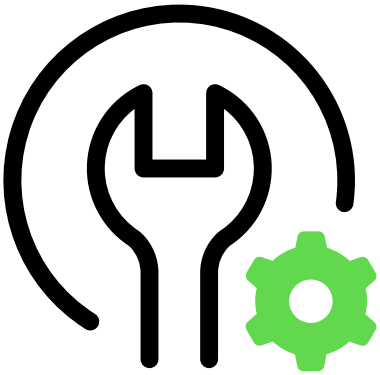
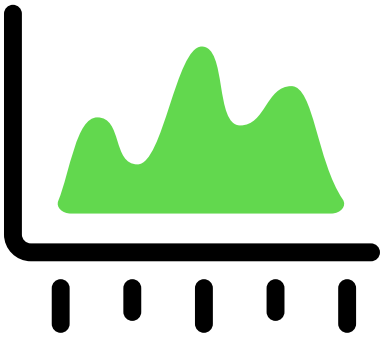
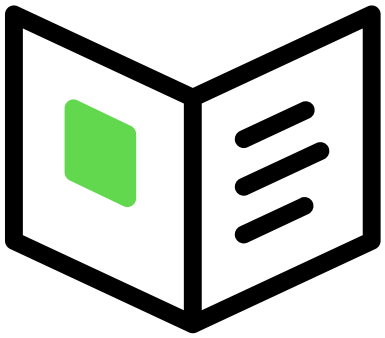
### Container Vulnerability Response

| Erkunden | Konfigurieren | integrieren |
|---|---|---|
|  |  |  |
| Erfahren Sie mehr über die Konzepte und Funktionen von Container Vulnerability Response. | Konfigurieren Sie Container Vulnerability Response. | Erweitern Sie Container Vulnerability Response durch die Integration mit anderen Anwendungen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Container Vulnerability Response (Fortsetzung)

| Beheben | Analytik und Berichterstellung | Referenz |
| --- | --- | --- |
|  |  |  |
| Erfahren Sie, wie Sie Container-Schwachstellen beheben können. | Zeigen Sie Container Vulnerability Response-Analysen an | Rufen Sie Details zu Komponenten von Container Vulnerability Response wie Feldern, Tabellen und Eigenschaften ab. |

### Vorteile

Die Anwendung Container Vulnerability Response bietet die folgenden Vorteile:

- Integration mit Container-Sicherheitsprodukten von Drittanbietern wie Prisma Cloud Compute von Palo Alto Networks.
- Importiert Schwachstellendaten für die Images, die zur Laufzeit bereitgestellt werden, und erweitert die Schwachstellendaten mit kontextbezogenen Informationen zur Laufzeit (Hosts, Kubernetes-Cluster, Services und Namespaces).
- Stellt eine Liste der Referenzen bereit, die aus Schwachstellen auf die relevanten Kubernetes-Entitäten in Configuration Management Database (CMDB) mithilfe von ServiceNow Kubernetes Discovery erstellt wurden.
- Bietet ein umfassendes Dashboard für die Berichterstellung, das Einblicke in die Schwachstellen- und Korrekturtrends bietet.

### Schlüsselfunktionen

Die Anwendung Container Vulnerability Response verwaltet in den Containern erkannte Schwachstellen. Sie bietet die folgenden Funktionen:

- Verweist auf Docker-Image aus CVITs, anstatt Container auszuführen.
- Konfigurieren Sie die Granularität von CVITs für die Nachverfolgung auf Image-, Kubernetes-Cluster-, Namespace- oder Serviceebene.
- Verfolgen Sie neue Image-Versionen nach, um behobene Schwachstellen zu identifizieren. Alle in älteren Versionen gemeldeten Schwachstellen werden in ServiceNow automatisch behoben, wenn neue Image-Versionen zur Laufzeit bereitgestellt werden.
- Verfolgen Sie CVITs in Basis-Images getrennt von Anwendungs-Images nach, um eine unabhängige Korrektur zu ermöglichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie Ausnahmeanforderungen oder falsch positive Anforderungen, die durch einen mehrstufigen Genehmigerprozess überprüft werden können.
- Definieren Sie Ausnahmeregeln, um CVITs automatisch zurückzustellen.

## Anwendungsfälle

Container sind eine großartige Möglichkeit, Anwendungen in mehreren Umgebungen mit geringerem Overhead und erhöhter Portabilität bereitzustellen und zu skalieren. Allerdings können Schwachstellen in Container-Images ein Risiko für den zugrunde liegenden Host und letztlich für die Infrastruktur darstellen, in der Container von diesen Images gestartet wurden. Zwar gibt es viele Container-Sicherheitsprodukte, die Container-Images auf Schwachstellen scannen, aber es gibt einige Überlegungen und Probleme im Zusammenhang mit der Behebung der Schwachstellen. Container Vulnerability Response kann bei der Lösung verschiedener Probleme oder Anwendungsfälle im Zusammenhang mit der Behebung von Container-Image-Schwachstellen helfen. Erkunden Sie Möglichkeiten, das Modul Container Vulnerability Response zu nutzen:

**Laufzeitkontext**

Schwachstellen in Container-Images können erkannt werden, indem das Image in den folgenden Phasen des Anwendungslebenszyklus gescannt wird.

- Phase 1: Wenn Images in der CI/CD-Pipeline erstellt werden.
- Phase 2: Wenn Images in der Registrierung veröffentlicht werden
- Phase 3: Wenn Images zur Laufzeit bereitgestellt werden.

Während es wichtig ist, Schwachstellen in Phase 1 und Phase 2 so früh wie möglich zu identifizieren, ist es ebenso wichtig, die Images zu scannen, die in einer Laufzeitumgebung bereitgestellt werden. Es bietet die folgenden Vorteile:

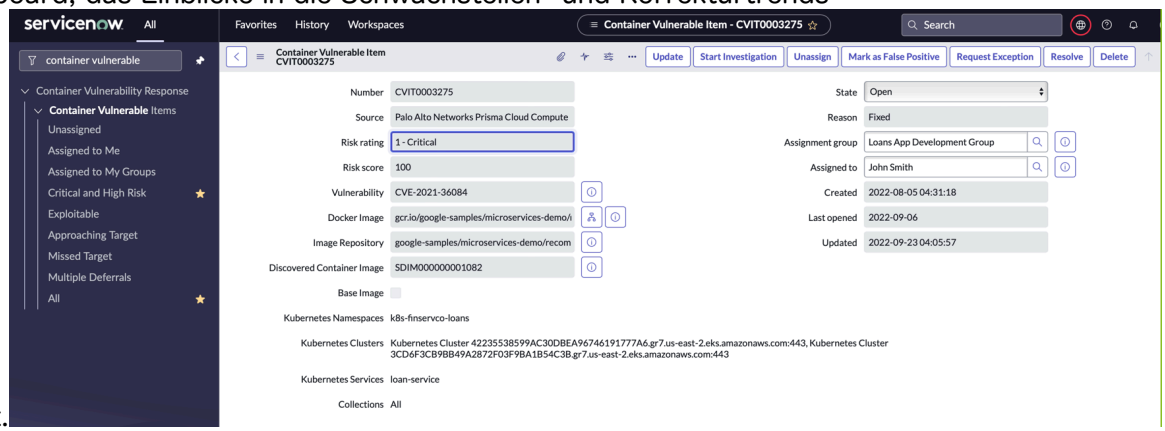
- Identifizieren neuer allgemeiner Schwachstellen und Gefährdungen (CVEs), die veröffentlicht wurden
- Bietet genaue Transparenz der Risikosituation der bereitgestellten Anwendungen.
- Priorisierung von Schwachstellen, die behoben werden müssen. Der Laufzeitkontext in Bezug auf die Anwendungsservices oder Geschäftsservices, die aufgrund einer Schwachstelle betroffen sind, kann bei der Priorisierung helfen.

Container Vulnerability Response ist in Container-Sicherheitsprodukte wie Prisma Cloud Compute aus Palo Alto Networks integriert, um die Schwachstellendaten für die Images abzurufen, die zur Laufzeit bereitgestellt werden, und erweitert die Schwachstellendaten um kontextbezogene Informationen zur Laufzeit, z. B. Hosts, Kubernetes-Cluster, Services und Namespaces Diese Container-Images werden bereitgestellt. Kunden, die die Kubernetes-Erkennung ServiceNow verwenden, können die aus Schwachstellen erstellten Verweise auf die relevanten Kubernetes-Entitäten in ihrem Configuration Management Database (CMDB)anzeigen. Zusätzlich zur Anreicherung der Metadaten bietet ServiceNow auch ein umfassendes Berichts-



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard, das Einblicke in die Schwachstellen- und Korrekturtrends bietet.




### Identifizieren Sie den Besitzer

#### Voraussetzungen

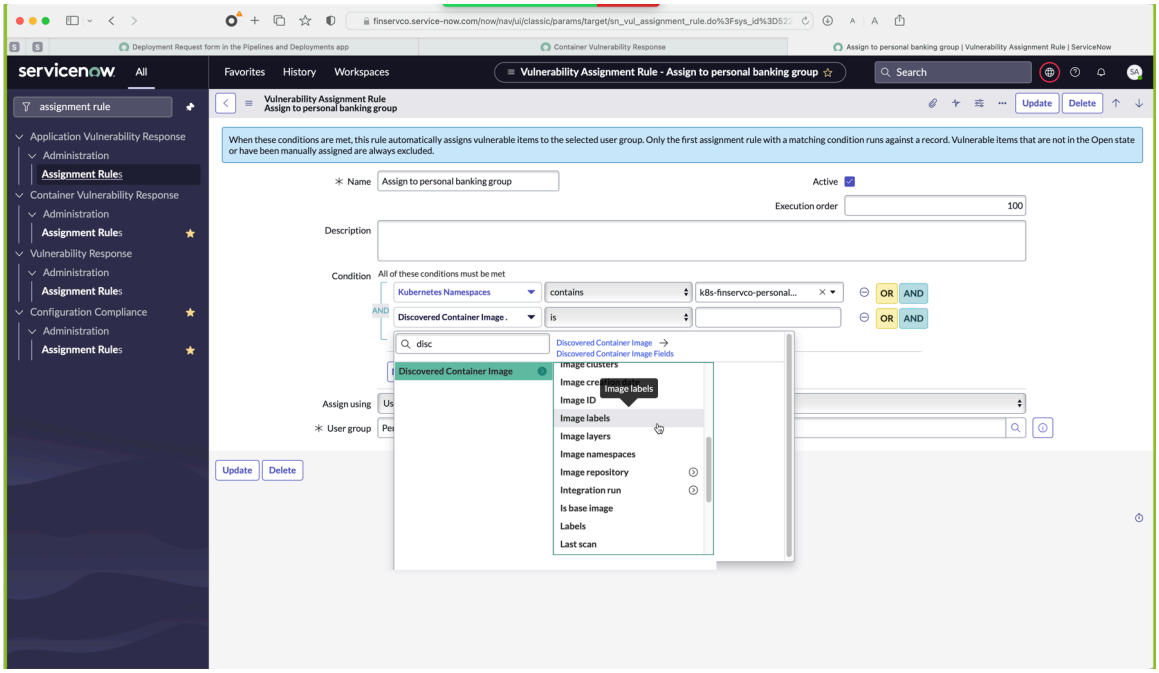
- **Kubernetes-Metadaten und -Referenzen**: Damit Container Vulnerability Response Kubernetes-Metadaten (Namespace, Cluster usw.) und Verweise auf Configuration Management Database (CMDB) -Einträge ausfüllt, müssen Sie die Kubernetes-Erkennung aus Information Technology Operations Management (ITOM) implementieren. Die Kubernetes-Erkennung füllt das Docker-Image, die ausgeführten Docker-Container, Pods, Kubernetes-Cluster usw. in CMDB. Container Vulnerability Response identifiziert das Docker-Image in CMDB basierend auf der Image-ID, identifiziert dann die zugehörigen Kubernetes-Entitäten und füllt die Verweise auf diese Entitäten aus angreifbaren Elementen.
- **Cloud-Metadaten und Docker-Image-Bezeichnungen**: Container Vulnerability Response füllt auch Docker-Image-Bezeichnungen, Cloud-Konto-IDs und Regionen, in denen ein Image bereitgestellt wird. Diese Daten werden im Datensatz „Erkanntes Container-Image“ verwaltet, das dem angreifbaren Element zugeordnet ist. Es gibt keine Voraussetzungen für das Ausfüllen dieser Daten. Container Vulnerability Response verwendet die von Container-Sicherheitsprodukten zurückgegebenen Daten (z. B. Palo Alto Prisma Cloud Compute), um diese Einträge auszufüllen.

Die Verantwortung für das Patchen einer Schwachstelle in einem Container-Image kann von Organisation zu Organisation variieren. Diese Informationen können an verschiedenen Stellen erfasst werden. Einige Organisationen verwenden Docker-Image-Bezeichnungen, um die Anwendungsteams zu identifizieren, die ein bestimmtes Container-Image besitzen, während andere Organisationen den Kubernetes-Namespace oder das Cloud-Konto verwenden können, in dem ein Container-Image bereitgestellt wird, um den richtigen Besitzer zu identifizieren.

Container Vulnerability Response stellt die erforderlichen Datenmodellelemente bereit, damit Docker-Image-Bezeichnungen, Kubernetes-Cluster-/Service-/Namespace-Metadaten oder Cloud-Account-Metadaten (Cloud-Account-ID, Region, Anbieter usw.) in den Zuweisungsregeln erfasst und verwendet werden können. Modul und weisen Schwachstellen basierend auf den Metadaten des Images oder der Laufzeitumgebung automatisch dem richtigen Anwendungsteam zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Verfolgen Sie Schwachstellen in den Basis-Images nach

### Voraussetzungen

Damit die Eigenschaft „Basis-Image“ in Container Vulnerability Responseausgefüllt wird, müssen Basis-Images explizit in der Konsole Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute konfiguriert werden. Weitere Informationen zum Konfigurieren von Basis-Images in Prisma Cloud finden Sie unter https://docs.paloatonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/base_images.

Container Vulnerability Response ermöglicht die Erstellung separater Schwachstellendatensätze für eine Basisschicht, sodass sie einem anderen Team zugewiesen werden können.

Verfolgen Sie Schwachstellen, die in einem Basisbetriebssystem-Image (z. B. Alpin) identifiziert wurden, anhand der in anderen Ebenen des Container-Images erkannten Schwachstellen nach. Viele Organisationen haben dedizierte Teams, die dafür verantwortlich sind, Basis-BS-Images zu patchen und für alle Anwendungsteams verfügbar zu machen.

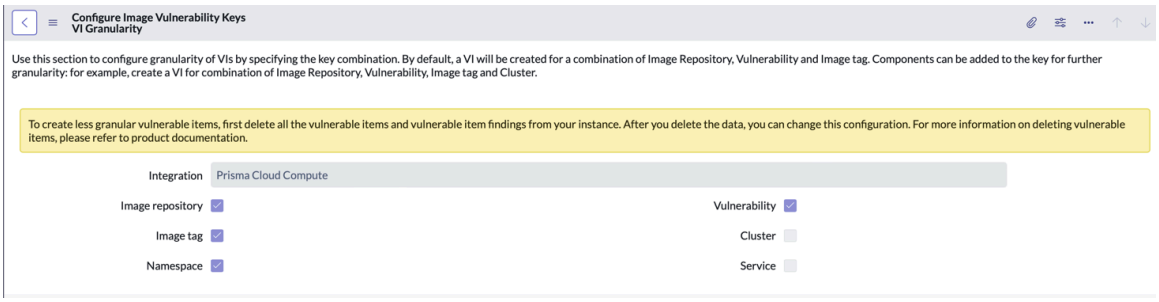
## Definieren Sie die Granularität für angreifbare Elemente

Automatische Übersetzung

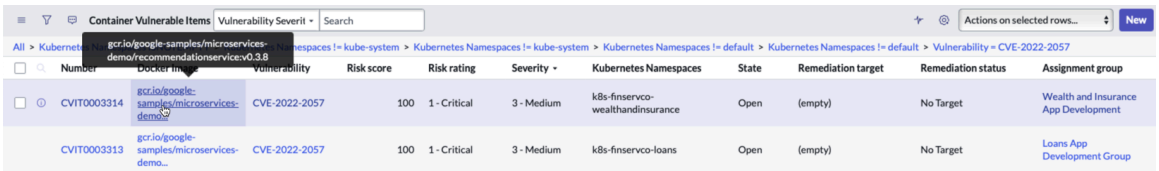
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Voraussetzungen

Konfigurieren Sie die Granularität von CVITs, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**.




Standardmäßig wird für jede eindeutige Kombination aus CVE und Docker-Image-Version (Referenz + Tag) ein angreifbares Element erstellt. Einige Docker-Images können jedoch in mehr als einem Kubernetes-Namespace bereitgestellt werden, und jeder Namespace kann verschiedenen Geschäftsbereichen oder Teams gehören. Jedes Team kann seinem eigenen Rhythmus für die Einführung neuer Versionen von Container-Images folgen, um Schwachstellen zu beheben. Um diesem Szenario Rechnung zu tragen, können Sie mit Container Vulnerability Response die Granularität für angreifbare Elemente definieren: Gibt an, ob für jeden Kubernetes-Namespace/-Cluster/-Service ein angreifbares Element erstellt werden soll, auch für jede eindeutige Kombination aus Docker-Image-Version und Schwachstelle.




Im Beispiel sehen Sie zwei angreifbare Elemente, die für dieselbe Kombination aus Docker-Image und CVE erstellt wurden. Einer für den Kubernetes-Namespace „k8s-finservco-loans“ und der andere für „k8s-finservco-wealthandinsurance“.

## Identifizieren Sie betroffene Services mithilfe der Tag-basierten Serviceidentifizierung

### Voraussetzungen

- Identifizieren Sie verschiedene Services in Ihrer Anwendung, und definieren Sie die Tags/Schlüssel-Wert-Paare, die diese Services darstellen.
- Stellen Sie Docker-Images und Kubernetes-Pods mit diesen Tags oder Bezeichnungen bereit.
- ITOM Kubernetes Discovery bereitstellen Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Bezeichnungen.
- Stellen Sie ITOM Kubernetes Discovery bereit
- Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Schlüssel-Wert-Paaren.
- Importieren von Schwachstellendaten in ServiceNow mit Container Vulnerability Response



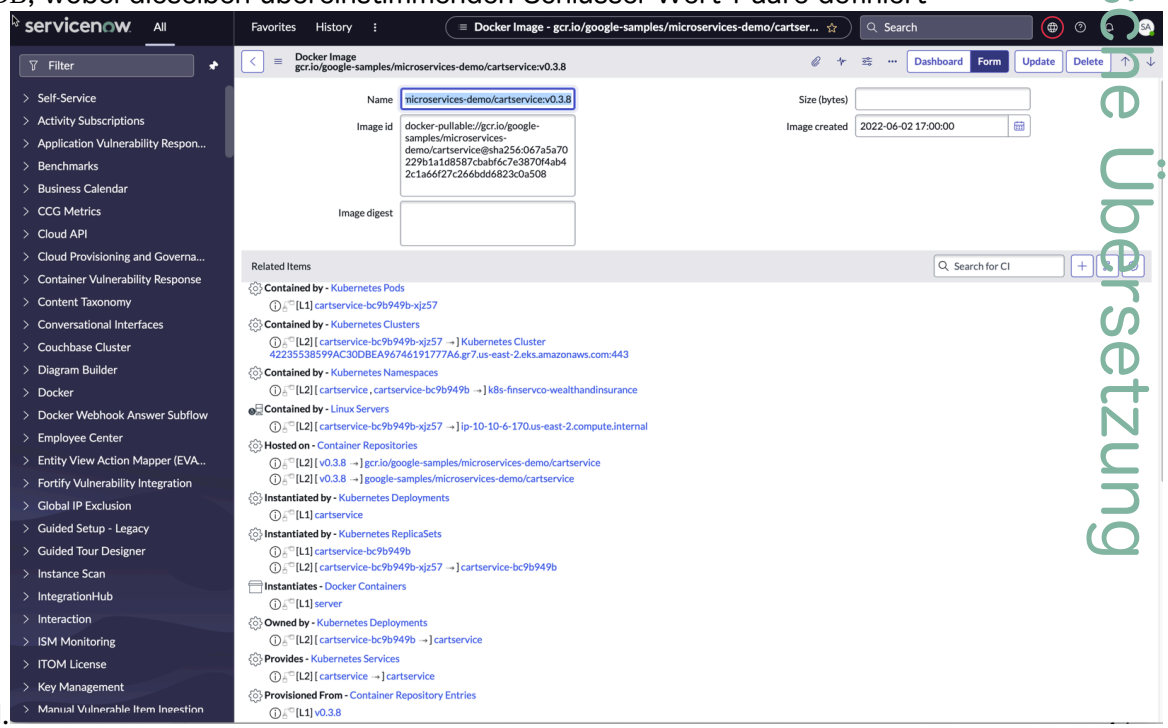
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Risikoberechnung für angreifbare Elemente kann anhand des CI (Docker-Image) und der Relevanz der zugehörigen Services in CMDBerfolgen. Um jedoch die Identifizierung betroffener Services zu erleichtern, bietet Container Vulnerability Response eine Tag-basierte Serviceidentifizierung.

Wenn Kubernetes-Pods oder -Entitäten mit Schlüsselwerten oder Bezeichnungen veröffentlicht werden, die den Schlüsselwerten entsprechen, die in einem Tag-basierten Service in ServiceNowdefiniert sind, stellt Container Vulnerability Response automatisch die Beziehung zwischen einem Docker-Image und dem betroffenen Anwendungsservice her und verwendet den Relevanz dieses Anwendungsservice in der Risikoberechnung.

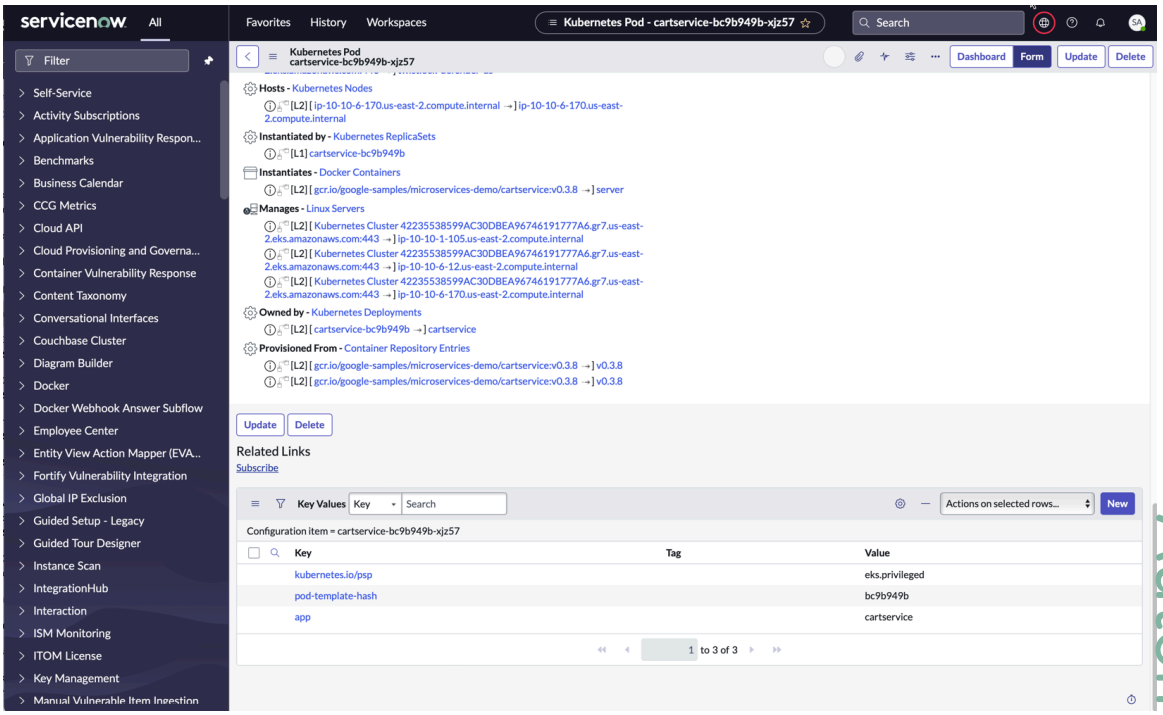
Der Flow lautet wie folgt:

1. Container Vulnerability Response importiert Schwachstellendaten aus dem Container-Sicherheitsprodukt.
2. Für jedes angreifbare Containerelement füllt Container Vulnerability Response das Docker-Image aus CMDB, das die Schwachstelle aufweist.
3. Container Vulnerability Response prüft dann die Docker-Image-Bezeichnungen oder die mit Kubernetes-Pods veröffentlichten Bezeichnungen/Schlüsselwerte, in denen dieses Image bereitgestellt wird. Dieses Image ist in CMDB verfügbar, wenn die Kubernetes-Erkennung ausgeführt wird.
4. Container Vulnerability Response sucht dann nach „Tag-basierten Services“ in CMDB, wobei dieselben übereinstimmenden Schlüssel-Wert-Paare definiert sind.

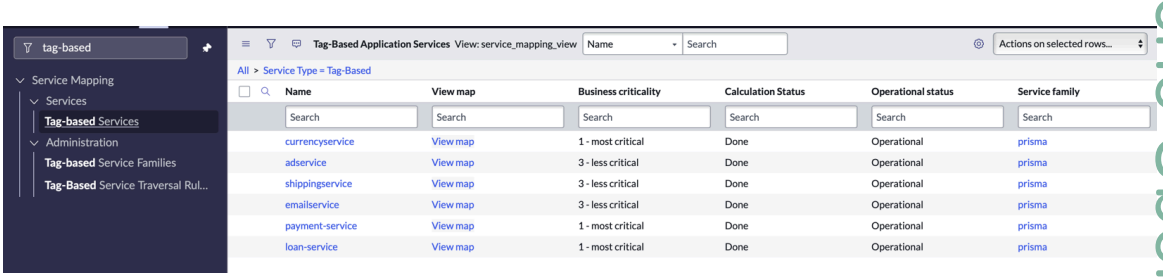


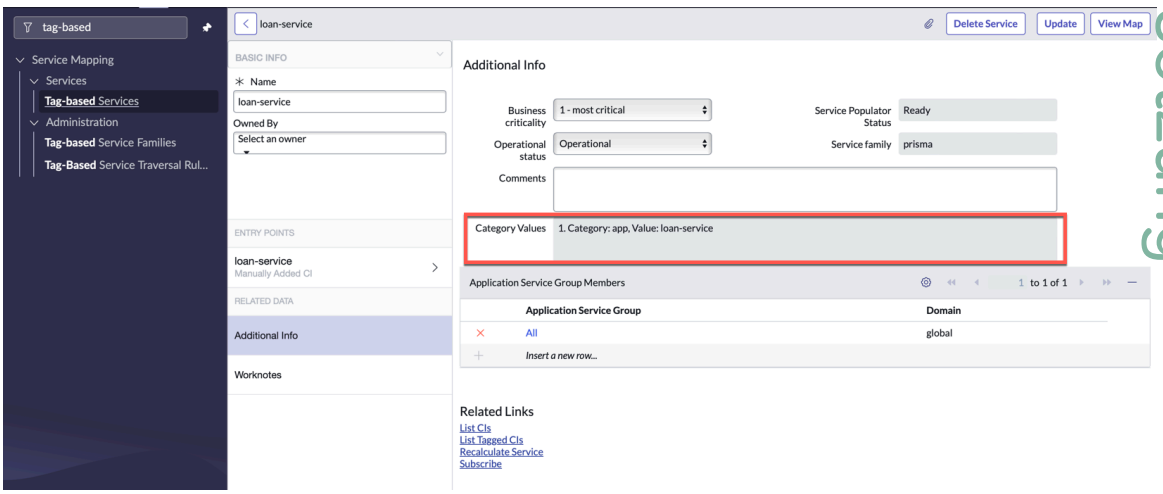

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**5.** Container Vulnerability Response verwendet die „Geschäftskritikalität“ des übereinstimmenden „Tag-basierten Service“ (falls vorhanden), um das Risiko eines angreifbaren Containerelements zu berechnen.




## Nachverfolgung von Schwachstellen

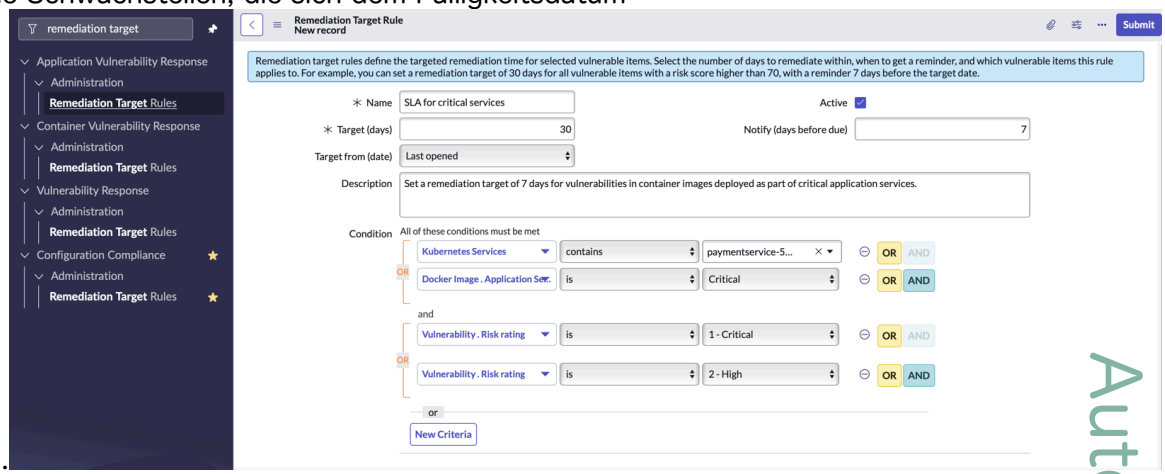
### Korrekturziele werden festgelegt

ServiceNow ermöglicht Schwachstellenmanagern die Definition von „Korrekturzielregeln“, um Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) für die Behebung von in Container-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Images gefundenen Schwachstellen definieren zu können. Das Korrekturzieldatum kann basierend auf einer Bedingung/einem Kriterium für Image-Metadaten oder Schwachstelleninformationen definiert werden. Korrekturbesitzer erhalten E-Mail-Benachrichtigungen über die Schwachstellen, die sich dem Fälligkeitsdatum nähern.




### Behobene Schwachstellen identifizieren

Im Gegensatz zu Host-Schwachstellen, die durch Anwenden eines Patches auf einem Host behoben werden können, können Container-Schwachstellen nicht gepatcht werden. Neue Versionen von Container-Images müssen erstellt und bereitgestellt werden, um die älteren Versionen zu ersetzen. Die neuen Versionen haben einen anderen Bezeichner (Image-ID) als die vorherigen Versionen, was es schwierig macht, nachzuverfolgen, welche Schwachstellen bereits behoben wurden.

ServiceNow identifiziert Schwachstellen, die in früheren Versionen der Container-Images gemeldet wurden, aber in der aktuellen Version des Images behoben wurden, und verschiebt diese Schwachstellen automatisch in den Status „Geschlossen/Behoben“, sodass Sicherheitsteams immer einen genauen Einblick in die aktuelle Risikosituation haben.

## Ausnahmen verwalten

Anwendungsteams oder Korrekturbesitzer für die Schwachstellen benötigen aus den folgenden Gründen möglicherweise die Möglichkeit, eine Ausnahme anzufordern.

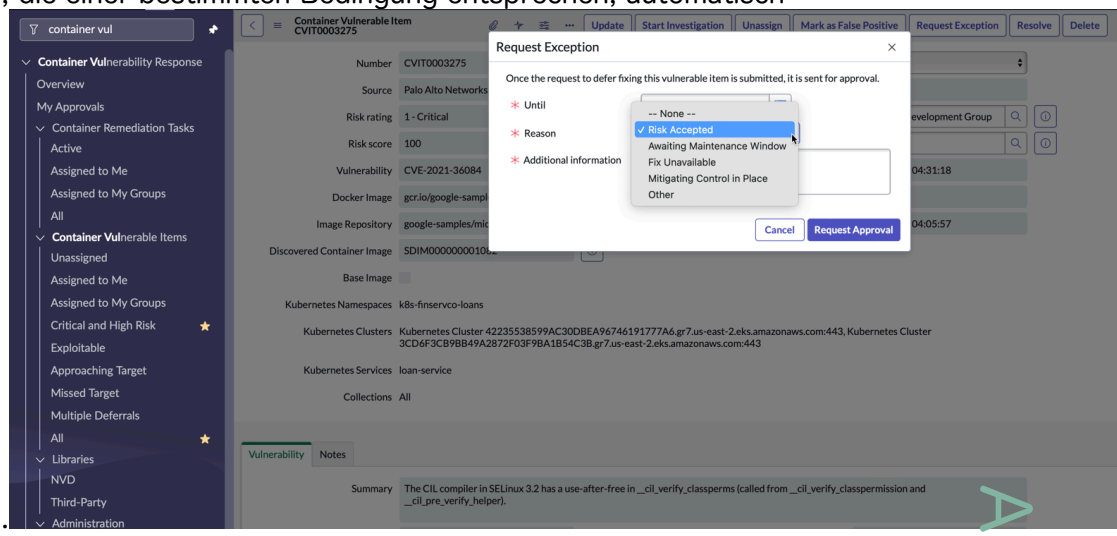
- Eine Verringerungskontrolle ist bereits vorhanden
- Risiko akzeptiert
- Warten auf das Wartungsfenster, um die Korrektur zu veröffentlichen.

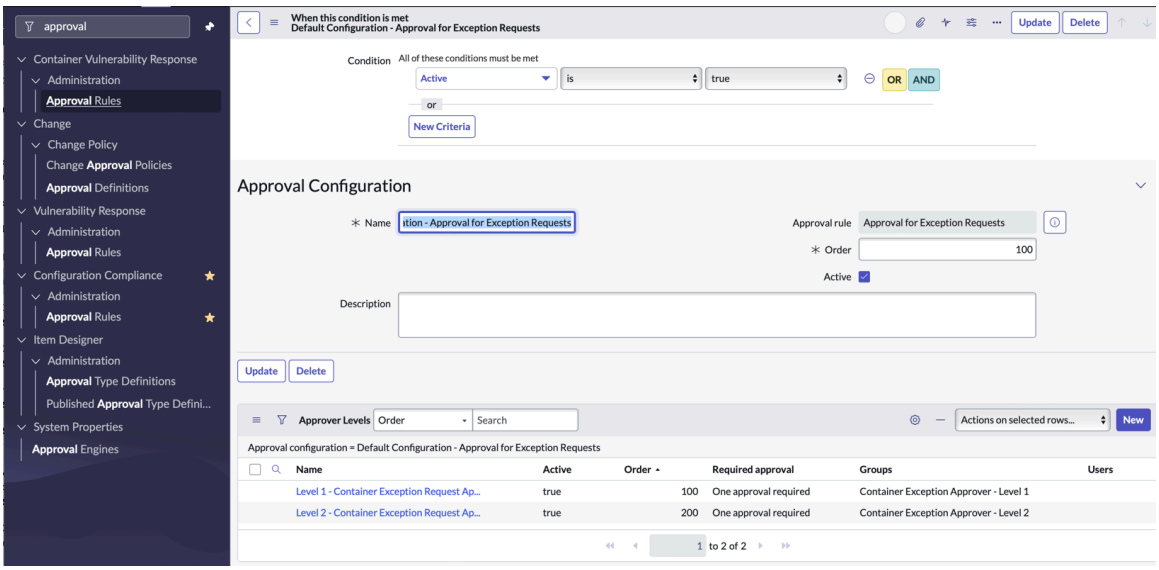
ServiceNow ermöglicht es Sicherheitsadministratoren, mehrere Genehmigerebenen für Ausnahmeanforderungen zu definieren. Sie können auch automatische Ausnahmeregeln definieren, die verwendet werden können, um

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen, die einer bestimmten Bedingung entsprechen, automatisch zurückzustellen.




## Neuigkeiten

Weitere Informationen zu den Neuerungen und Änderungen in Washington DCfinden Sie in den Versionshinweisen zu Washington DC.

## Erste Schritte

- Eine Übersicht über Security Operations in Ihrer Instanz Now Platform finden Sie unter Sicherheitsvorgänge verstehen.
- Informationen zu allen Security Operations -Anwendungen, die im ServiceNow Store] zum Download verfügbar sind, finden Sie unter Sicherheitsvorgänge und im ServiceNow Store.

# Container Vulnerability Response erkunden

Die Anwendung Container Vulnerability Response importiert angreifbare Containerelemente (CVITs). Gemäß den Regeln können Sie mit der Funktion die Container-Schwachstellen beheben. Container Vulnerability Response ist über ein separates Abonnement verfügbar.

Im Gegensatz zu herkömmlichen Anwendungen packen Container den gesamten Anwendungsquellcode zusammen mit seinen Abhängigkeiten in eine Binärdatei, die als Container-Image bezeichnet wird. Das Image wird in einer Registrierung veröffentlicht,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um eine Option zum Ausführen dieses Image als Anwendung oder Containerinstanz auf einer beliebigen Plattform bereitzustellen. Die Phasen in einem Lebenszyklus vor der Bereitstellung von Containern sind:

1. Container-Image erstellen: Das Container-Image wird erstellt und auf einen Quellcode oder eine abhängige Bibliothek verwiesen.
2. Containerimage erstellen
3. Container-Image veröffentlichen: Die Container-Image-Datei wird in einer Registrierung veröffentlicht. Jedes Image hat eine eigene eindeutige ID, die auf dem Inhalt des Image basiert. Diese Images werden im Modus nach der Bereitstellung aus der Registrierung in die Laufzeitumgebung abgerufen. Die Images werden dann als Containerinstanzen auf dem Host in der Produktionsumgebung ausgeführt.

## Container-Images werden gescannt

Ein Container-Image kann vor oder nach der Bereitstellung auf Schwachstellen gescannt werden. Wenn Container-Images während der Phase vor der Bereitstellung gescannt werden, erhalten Sie möglicherweise viele Schwachstellenwarnungen, die möglicherweise nicht Ihrer sofortigen Aufmerksamkeit bedürfen. Das Scannen nach Schwachstellen während der Phase nach der Bereitstellung bietet jedoch größere Vorteile, z. B.:

- Bietet Transparenz in Bezug auf das mit den bereitgestellten Anwendungen verbundene Risiko.
- Bereitstellung einer fokussierten Ansicht nur für die Images in der Produktionsumgebung.
- Identifizierung und Priorisierung der Schwachstellen, auf die sofort reagiert werden muss.
- Gruppierung und Zuweisung von Schwachstellen basierend auf den Metadaten des Image. Beispielsweise können ein Image-Repository, eine Image-Bezeichnung und andere Attribute im Zusammenhang mit dem Container-Image für Gruppierungs- und Zuweisungsregeln verwendet werden.

Jedes Container-Image weist die folgenden Schlüsselkomponenten auf:

- Container- oder Image-Repository: Stellt das Docker-Image mit einem bestimmten Repository oder Namen dar. Sie hostet alle Versionen des Image.
- Docker-Image: Stellt eine bestimmte Version des Build-Docker-Image dar.
- Docker-Container: Stellt eine ausgeführte Instanz des Docker-Image dar. Jede Version hat eine eindeutige ID und mehrere Instanzen der Container, die in der Produktionsumgebung ausgeführt werden.

## Container Vulnerability Response Module

Das Modul Container Vulnerability Response enthält Details zu Folgendem:

**Angreifbare Container-Elemente**

Die angreifbaren Containerelemente (CVITs) werden gruppiert und basierend auf Zuweisung, Relevanz, Ausnutzbarkeit und Korrekturstatus aufgelistet.

**Bibliotheken**

Erhalten Sie Zugriff auf die National Vulnerability Database (NVD) und Bibliotheken von Drittanbietern. Während die NVD-Bibliothek Informationen bereitstellt, die auf die ID des angreifbaren Elements beschränkt sind, stellt die Bibliothek einer Drittpartei die meisten Details zu einem angreifbaren Element bereit. Informationen im NVD-Bildschirm werden nur ausgefüllt, wenn die NVD-Integration ausgelöst wird.

**Administration**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Modul „Administration“ enthält Informationen zu den Zuweisungsregeln der angreifbaren Elemente, den Korrekturzielregeln und den Integrationen von Container-Schwachstellen. Darüber hinaus können Sie auch die Dauer konfigurieren, nach der ein angreifbares Element automatisch geschlossen werden soll. Sie können den Abschnitt VI-Granularität konfigurieren verwenden, um die Granularität von CVITs zu konfigurieren, indem Sie die Tastenkombinationen angeben. Standardmäßig wird eine CVIT für eine Kombination aus einem Image-Repository, einem Image-Tag und einer Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise eine CVIT für eine Kombination aus Image-Repository, Image-Tag, Schwachstelle und Cluster erstellen.

### Verfügbare Versionen

| Release-Version | Releasehinweise |
|---|---|
| Container Vulnerability Response v2.1<br>Container Vulnerability Response v2.06<br>Container Vulnerability Response v2.0.4 | |

## Container Vulnerability Response konfigurieren

Bevor Sie Container Vulnerability Response in Ihrer Instanz von Now Platform ] ausführen, müssen Sie sie konfigurieren.

### Vulnerability Response und Configuration Compliance für Container installieren

Bevor Sie die Anwendung Vulnerability Response und Configuration Compliance für Container in Ihrer Instanz von Now Platform ausführen, müssen Sie die Berechtigung erhalten und die Anwendung aus dem ServiceNow Storeherunterladen. Installieren Sie die Anwendung in Ihrer Instanz Now Platform, und führen Sie einige Installationsschritte im Setup-Assistenten aus.

#### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass die Anwendung installiert und aktiviert ist. | Um zu überprüfen, ob sie aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere |



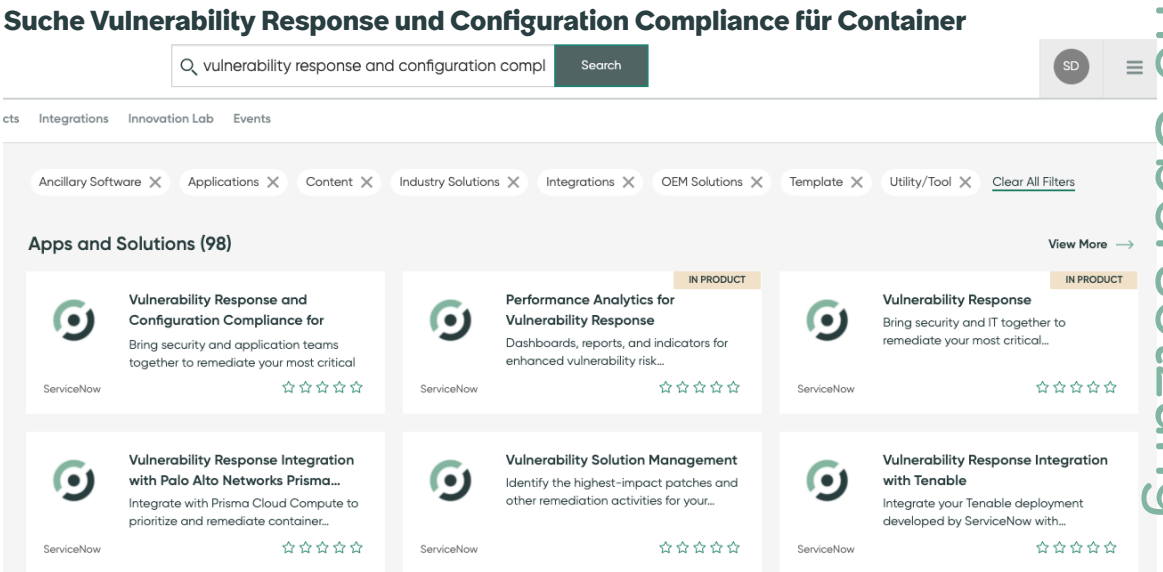
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Setupaufgaben | Beschreibung |
| --- | --- |
| | Informationen unter Vulnerability Response installieren. |
| Vergewissern Sie sich, dass Ihnen die erforderlichen Rollen ServiceNow für Ihre Instanz zugewiesen sind. | Die Administratorrolle ist für die Installation erforderlich.<br><br>Wenn nicht bereits zugewiesen, weist der Systemadministrator [admin] auch die Rolle „Schwachstellenadministrator“, „sn_vul.vulnerability_admin“ oder „sn_vul.admin (veraltet)“ zu. |

Erforderliche Rolle: admin

### Prozedur

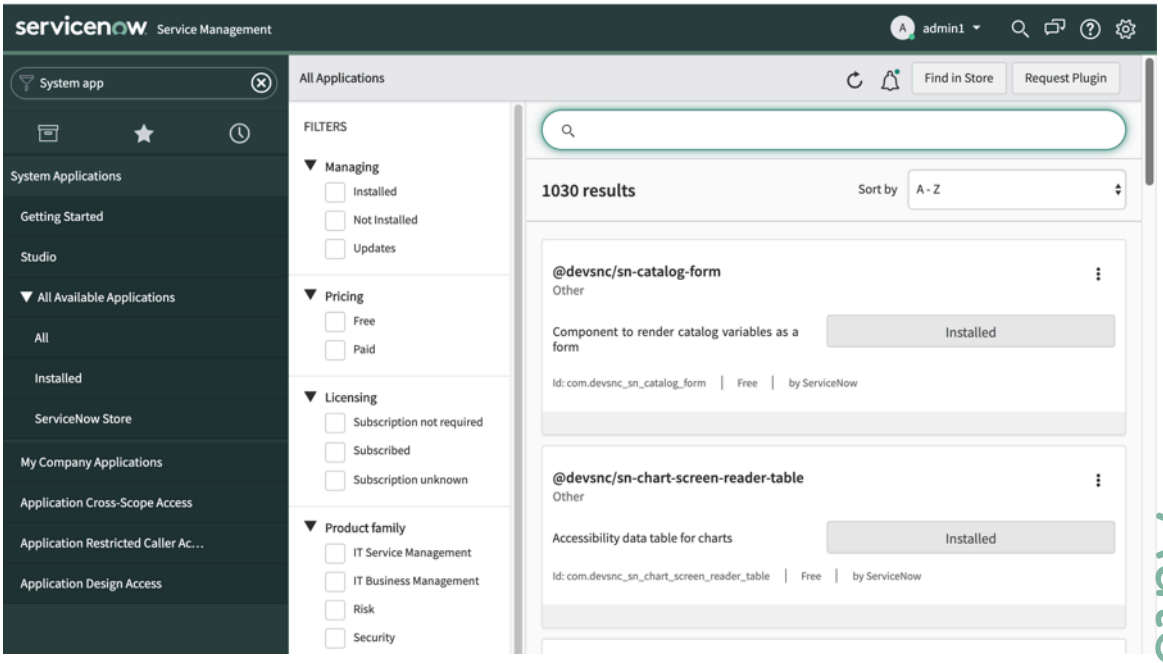
1. Um die Berechtigung zu erhalten und die Anwendung Vulnerability Response und Configuration Compliance für Container herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Anmelden**.
3. Geben Sie in der Suchleiste Vulnerability Response und Configuration Compliance für Containerein.
4. Klicken Sie unter „Apps und Lösungen“ auf die Kachel Vulnerability Response und Configuration Compliance für Container.




5. Klicken Sie auf **Installation anfordern**.
6. Melden Sie sich bei der Now Platform-Instanz an, auf der Sie die Anwendung Vulnerability Response und Configuration Compliance für Container installieren möchten.
7. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




8. Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Vulnerability Response und Configuration Compliance für Container, wählen Sie eine Version aus der Liste aus, und klicken Sie auf **Installieren**.
   Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle installierten Abhängigkeiten werden angezeigt.
9. Klicken Sie auf **Schließen**.

## Konfigurieren Sie Exception Management für Container Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme und fügen Sie der Ausnahme oder falsch positiven Anforderung mithilfe des Moduls Container Vulnerability Response einen Fragebogen hinzu. Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Container Vulnerability Response angefordert. Sie können eine Ausnahme auch mit der GRC: Policy and Compliance Management -Integration anfordern.

### Vorbereitungen

Erforderliche Rolle: sn_vul_container.manage_exception_configuration

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Container Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Policy and Compliance Management installiert ist, GRC: Policy and Compliance Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Policy and Control-Ziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird dieser an die Person gesendet, die die Ausnahme oder falsch positive Anforderung auslöst. Sie können entweder den Standardfragebogen verwenden oder einen Fragebogen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „ **Ausnahmeverwaltungskonfiguration“** aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste **Ausnahmen** verwalten mit auswählen. Sie können entweder Vulnerability Response oder GRC: Policy and Compliance Managementauswählen.
3. Wenn Sie die Option Vulnerability Response ausgewählt haben, geben Sie die folgenden Informationen ein:

#### Vulnerability Response Felder

| Feld | Beschreibung |
|---|---|
| Dauer | Zeitraum, für den eine Ausnahme angefordert werden kann. |
| Einheit | Zeiteinheit für den angegebenen Zeitraum. |
| Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |
| Fragebogen aktivieren, um Ausnahme anzufordern | Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung. |
| Fragebogen, um Ausnahme anzufordern | Zeigt den Fragebogen an, den Sie ausgewählt haben, um eine Ausnahme anzufordern. Der Ausnahmefragebogen wird standardmäßig angezeigt. |

**Hinweis:**
Wenn Sie GRC: Policy and Compliance Managementauswählen, werden die Felder Dauer und Einheit ausgeblendet, da Governance, Risk und Compliance diesen Flow verarbeitet.

4. Wählen Sie **Speichern**.

### Konfigurieren Sie Genehmigungsregeln für Exception Management

Verwenden Sie ab Vulnerability Response v15.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung, Ausnahmeregeln und die Verwaltung falsch positiver Meldungen zu genehmigen. Wenn Sie Vulnerability Response (VR) zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Container-Elemente
- Ausnahmeregel
- Falsch positive Werte für Korrekturaufgaben
- Falsch positive Werte für angreifbare Container-Elemente



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow.

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Tabelle | Tabelle, auf die die Regel angewendet wird. |
| Anwendung | Der Standardwert ist Vulnerability Response. |
| Regeltyp | Gibt den Regeltyp an. Beispiele: Ausnahmeverwaltung, Falschmeldungen oder Ausnahmeregel. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungsregeln. |
| Ablaufdatum der Genehmigung (Tage)<br>Ab v2.5 von Container Vulnerability Response | Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann. |
| Genehmiger benachrichtigen (Tage)<br>Ab v2.5 von Container Vulnerability Response | Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen. |

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

**Hinweis:**
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management.

**Example:**
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden wurden.

## Schnellstarttests für Container Vulnerability Response

Überprüfen Sie, ob Container Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demokonten erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird. Weitere Informationen zum Einrichten und Ausführen der Testsuite für [Führen Sie die Test-Suite Automated Test Framework (ATF) für aus Vulnerability Response ] finden Sie unter Container Vulnerability Response.

Container Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Container Vulnerability Response (sn_vul_container).

### Container Vulnerability Response-Tests

| Test | Beschreibung | Release-Version |
|---|---|---|
| CVR: Zuweisungsregeln | Ermittelt, ob angreifbare Elemente in Containern mit einem Mustersatz von Zuweisungsregeln zur Korrektur erfolgreich automatisch einer Zuweisungsgruppe zugewiesen werden können. | Vancouver |
| CVR: Ausnahmeregel | Testet Ausnahmeregeln. | Vancouver |
| CVR: Flow „Als falsch positiv markieren“ | Testet, ob der Flow „Als falsch positiv markieren“ für das angreifbare Container-Element funktioniert. | Vancouver |
| CVR: Nachbesserungszielregeln | Erstellt eine Fehlerkorrektur-Zielregel. | Vancouver |
| CVR: Flow „Ausnahmeanforderung“ | Testet, ob der Flow „Ausnahmeanforderung“ wie erwartet funktioniert. | Vancouver |
| CVR: Schwachstellenrechner | Testet den Container-Schwachstellenrechner. | Vancouver |

**Zugehörige Informationen**

Schnellstarttests

## Führen Sie die Test-Suite Automated Test Framework (ATF) für aus Container Vulnerability Response

Führen Sie die Test-Suite Automated Test Framework (ATF) aus, nachdem Sie die Anwendung Container Vulnerability Response installiert oder aktualisiert haben.

### Vorbereitungen

Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz wie vorgesehen funktioniert.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Demokonten erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.

- Führen Sie die folgenden Schritte aus, um den Test zu aktivieren:
  1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**.
  2. Wenn diese Option nicht ausgewählt ist, aktivieren Sie das Kontrollkästchen **Test-/Testsuite-Ausführung** aktivieren.
  3. Klicken Sie auf **Speichern**.
  4. Wenn der Bereich im Header nicht auf **Container Vulnerability Response** festgelegt ist oder der Bereich nicht im Header angezeigt wird, klicken Sie auf das Einstellungssymbol.
  5. Klicken Sie im Fenster „Systemeinstellungen“ auf **Entwickler**.
  6. Wenn nicht ausgewählt, klicken Sie auf **Anwendungsauswahl in Header anzeigen,** und schließen Sie das Fenster.
  7. Klicken Sie in der Liste, die neben Systemadministratorangezeigt wird, für das Feld auf **Container Vulnerability Response**.

Erforderliche Rolle: admin oder atf_test_admin

### Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Tests**.
2. Suchen Sie in der Paketliste **nach Vulnerability Response und Configuration Compliance für Container**.
3. Wählen Sie einen Test aus, um den Datensatz zu öffnen.
4. Aktivieren Sie im geöffneten Datensatz das Kontrollkästchen **Aktiv**.
5. Wählen Sie in der zugehörigen Liste „Testschritte“ in der Spalte Aktiv die Option true aus.
6. Klicken Sie auf **Aktualisieren**.
7. Öffnen Sie den Test erneut, und klicken Sie auf **Tests und Testsuite-Ausführung hier aktivieren**.
8. Aktivieren Sie Test-/Test-Suite-Eigenschaften und Test-Debugging-Eigenschaften.
9. Klicken Sie auf **Speichern**.
10. Wenn die Schaltfläche **Test** ausführen nicht angezeigt wird, aktualisieren Sie Ihren Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf Test ausführen, um den **Test** zu starten.
    Nach einiger Zeit zeigt das Dialogfeld „Test ausführen“ einen erfolgreichen Test an. Klicken **Sie auf Zu Ergebnis wechseln,** um weitere Informationen zu erhalten.

### Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von Container Vulnerability Responsefortfahren.

Weitere Informationen zu automatisierten Tests für Container Vulnerability Response und automatisierten Tests, Test-Suites und zum Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF) .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Integration von Container Vulnerability Response mit anderen Anwendungen

Erweitern Sie die Fähigkeiten von Container Vulnerability Response durch Integration mit anderen Anwendungen.

Container Vulnerability Response ist in Container-Sicherheitsprodukte integriert, um Schwachstellendaten für die Images abzurufen, die zur Laufzeit bereitgestellt werden. Anschließend werden die Schwachstellendaten mit kontextbezogenen Informationen zur Laufzeit erweitert, z. B. Hosts, Kubernetes-Cluster, Services und Namespaces, in denen diese Container-Images bereitgestellt werden. Mit der Kubernetes-Erkennung von ServiceNow können Sie die Referenzen anzeigen, die aus Schwachstellen für die relevanten Kubernetes-Entitäten in Ihrem Configuration Management Database (CMDB)erstellt wurden. Neben der Anreicherung der Metadaten bietet ServiceNow auch ein umfassendes Dashboard für Berichte, das Einblicke in die Schwachstellen- und Korrekturtrends bietet.

Container Vulnerability Response bietet Integrationen mit den folgenden Anwendungen:

- Integration „Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute“
- Informationen zur Integration von [ Atlassian Jira mit Vulnerability Response

## Zusätzliche Hinweise für -Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 2.1.2 von Container Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

## Integration „Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute“

Mit der Prisma Cloud Compute-Integration können Sie Container-Images scannen, um Schwachstellen zu erkennen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 16.1 von Vulnerability Responsekönnen Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in der Anwendung Container Vulnerability Response verwenden, um Container-Image-Schwachstellendaten für bereitgestellte Container zu importieren. Anschließend können Sie Berichte zu Schwachstellen und angreifbaren Elementen in den Dashboards Vulnerability Response anzeigen. Diese Schwachstellen können dann priorisiert und behoben werden.

Wenn sich das Produkt Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden. Weitere Informationen finden Sie unter Systemanforderungen für MID Server .

## Anzeigen der Integrationen

Sie können die Integrationen anzeigen, die Teil von Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computesind. Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Integrationen**.

Die folgenden Integrationen sind verfügbar.

| Ausführungssequenz | Zeitplan | Integration | Beschreibung |
|---|---|---|---|
| 1 | Täglich | Integration von Prisma-Cloud-Computing-Basis-Images | Ruft die Schwachstellen für Basis-Images aus der Prisma-API ab und meldet die Schwachstellen der Basis-Images separat. Außerdem werden Image-Ergebnisse und angreifbare Elemente erstellt, die auf die Basis-Images verweisen. |
| 2 | Täglich | Integration von Prisma-Cloud-Computing-Schwachstellen | Ruft Container-Schwachstellen ab. Erstellt Ergebnisse und CVITs sowie erkannte Container-Images. |
| 3 | Bei Bedarf | Integration von Prisma-Cloud-Computing-Containeranzahlen | Ruft Containeranzahlen für alle Nicht-Basis-Images ab. |

## Basis-Image-Konfiguration in Prisma

In der Prisma-Konsole können Sie die Registrierung konfigurieren und dann die Basis-Images aus diesen Registrierungen konfigurieren. Wenn im Basis-Image eine Schwachstelle vorhanden ist, wird beim Ausführen der Integration von Prisma Cloud Compute-Basis-Images das Kontrollkästchen **Basis-Image** aktiviert, um anzuzeigen, dass die Schwachstellen im Basis-Image vorhanden sind.

## VI-Granularität konfigurieren

Um die Granularität von CVITs zu konfigurieren, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **VI-Granularität konfigurieren**und geben die Tastenkombinationen an. Standardmäßig wird eine CVIT für eine Kombination aus Image-Repository, Image-Tag und Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise eine CVIT für eine Kombination aus Image-Repository, Image-Tag, Schwachstelle und Cluster erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozess der Prisma-Integration

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ausgeführt wird, wird überprüft, ob in der Tabelle der National Vulnerability Database (NVD) eine allgemeine Schwachstelle und Gefährdung (Common Vulnerability and Exposure, CVE) vorhanden ist. Wenn sie bereits vorhanden ist, werden die vorhandenen Informationen verwendet. Wenn das CVE jedoch nicht gefunden wird, werden Platzhalterdatensätze in der NVD-Tabelle generiert. Beim Erstellen dieser Platzhalter-NVD-Datensätze werden zunächst nur das CVE und sein Name ausgefüllt. Andere Details werden nicht mit der Annahme ausgefüllt, dass die NVD-Integration diese Details später ausfüllt. Wenn der Integrationsinstanzparameter *update_nvd* auf „true“ festgelegt ist, werden die Platzhalter-NVD-Datensätze aktualisiert. Standardmäßig ist der Instanzparameter auf „false“ festgelegt. Zumindest bis die NVD-Integration ausgeführt wird und diese Details ausgefüllt werden, ist jedoch ein gewisses Verständnis des CVE erforderlich, z. B. dessen Schweregrad, oder einige grundlegende Informationen zum Problem. Um diese Anforderung zu erfüllen, werden die Felder **Exploit vorhanden** und **Korrekturnotizen** mit den aus Prisma abgerufenen Details ausgefüllt. Darüber hinaus ist diese Konfiguration anpassbar, sodass Sie andere Felder angeben können, die Sie im NVD-Eintrag basierend auf den von Prisma bereitgestellten Informationen ausfüllen möchten.

### wird vorbereitet Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Sie können sich auf Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute vorbereiten, indem Sie Setup-Aufgaben ausführen.

## Bevor Sie beginnen

Um die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute zu installieren und zu konfigurieren, können Sie die folgende Prüfliste drucken. Vergewissern Sie sich, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und die Schwachstellendaten in Ihre Now Platform® -Instanz importieren.

**Prüfliste zur Vorbereitung der Integration**

| Aufgabe | Beschreibung |
|---|---|
| ☐ | Vergewissern Sie sich, dass Sie über die folgenden Informationen verfügen:<br>• API-Basis-URL<br>• Benutzername und Passwort.<br><br>Diese Anmeldeinformationen werden verwendet, um die Schwachstellen aus der Prisma Cloud Compute-Integration abzurufen. Weitere Informationen finden Sie unter https://pan.dev/compute/api/<br><br>**Hinweis:**<br>MID-Server ist optional.<br><br>Die für die Prisma Cloud Compute-Integration verwendeten Benutzeranmeldeinformationen benötigen eine Berechtigung zum Überwachen der Images. Siehe folgenden Code:<br>`{"permission":"monitorImages","saas":true,"self-hosted":true}` |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

| Aufgabe | Beschreibung |
|---|---|
| ☐ | Wenn noch nicht installiert und aktiviert, installieren Sie die Anwendung Vulnerability Response, bevor Sie die Drittanbieteranwendung installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 16.1 von Vulnerability Response oder höher. |
| ☐ | Rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in Ihrer Instanz von Now Platform® herunter. |
| ☐ | Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren werden.<br><br>Vergewissern Sie sich, dass Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support von ServiceNow. |
| ☐ | Vergewissern Sie sich, dass Sie über die folgenden Gruppen oder Benutzer verfügen, um die Integrationen zu verwalten und die angreifbaren Elemente zu beheben:<br><br>**Administrator**<br>Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Wenn sie nicht zugewiesen ist, weist der Administrator den Container-Schwachstellenadministrator (sn_vul_container.vulnerability_admin) und andere Rollen zu.<br><br>**sn_vul_container.vulnerability_admin**<br>Schließt die Konfiguration der Prisma Cloud Compute-Integration ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Container Vulnerability Response (CVR) und ihre Datensätze. Dieser Administrator konfiguriert Integrationen und Regeln in Container Vulnerability Response.<br><br>**Vulnerability Response-Gruppe**<br>Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben sn_vul.read_all, sn_vul_container.read_all.<br><br>**Besitzergruppe der Container-Korrektur**<br>Standardmäßig ist die Gruppe „Container-Korrekturbesitzer“ verfügbar. Benutzer, die dieser Gruppe zugewiesen sind, erben sn_vul_container.remediation_owner. Der Container-Korrekturbesitzer behebt Container-Schwachstellen, die ihm oder einer Gruppe zugewiesen sind, der er angehört. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

| Aufgabe | Beschreibung |
|---|---|
| | **Schwachstellenanalyst**<br>Benutzer, die der Gruppe „Container-Schwachstellenanalyst“ zugewiesen sind, erben sn_vul.vulnerability_analyst. Der Schwachstellenanalyst überwacht die Korrektur aller angreifbaren Elemente.<br>Wenn dies noch nicht geschehen ist, ziehen Sie es möglicherweise vor, zusätzliche Gruppen zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen. Weitere Informationen finden Sie unter Benutzergruppen erstellen . |
| ☐ | Installieren Sie die Vulnerability Response -Integration mit NVD, und führen Sie die NIST National Vulnerability Database Integration - API aus (nur CVE). |

Sie sind bereit für Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

### Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte durch, damit das Produkt Prisma Cloud Compute ordnungsgemäß in Container Vulnerability Responseintegriert wird. Diese Anwendung ist als separates Abonnement verfügbar.

### Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Erforderliche Rolle: admin

### Prozedur

1. Melden Sie sich bei der Instanz an, in der Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. Suchen Sie in ServiceNow StoreVulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute nach der Anwendung [].
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

**Hinweis:**
Lesen Sie bei Bedarf die Abschnitte **Sonstige Anforderungen** und **Abhängigkeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Aktualisieren Sie die Felder **Instanzname** und **Grund für die Instanz**, und klicken Sie auf **Validate Instance**(Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.

### Ergebnisse
Ihre Anwendung wird automatisch in Ihrer Instanz installiert.

### Nächste Maßnahme
Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute ..

## Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute .

Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Importieren Sie Daten aus Prisma Cloud Compute. Sie können die importierten Daten verwenden, um Schwachstellen für Ihre Docker-Images zu priorisieren und zu beheben.

### Vorbereitungen
Erforderliche Rolle: admin

### Prozedur
1. Öffnen Sie die E-Mail von ServiceNow, die Sie über die Integration erhalten haben.
2. Melden Sie sich als Administrator bei Ihrer Instanz an.
3. Befolgen Sie die Anweisungen in der E-Mail, um Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Computezu erhalten.
4. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**.
   Füllen Sie die Felder im Formular „Prisma Cloud Compute-Konfiguration“ aus. Weitere Informationen finden Sie unter Formular „Prisma Cloud Compute-Konfiguration“.
5. Wählen Sie in der Liste „Projekte“ entweder **Alle Projekte** oder **Bestimmte Projekte** aus, um entweder alle Projekte oder ausgewählte Projekte zu konfigurieren.
   Wenn Sie **Spezifische Projekte**auswählen, können Sie die Projekte aus der Liste Verfügbar auswählen.
6. Schließen Sie die Konfiguration ab, indem Sie entweder auf **Fertig stellen** oder auf **Anmeldeinformationen speichern und testen**klicken.
   - Wenn Sie ein Projekt konfiguriert haben, klicken Sie auf **Fertig stellen**.
   - Wenn Sie kein Projekt konfiguriert haben, klicken Sie auf **Speichern und Anmeldeinformationen testen**
7. Zeigen Sie die neu erstellte Instanz an, indem Sie zu navigieren **Prisma-Cloud-Computing-Integration** > **Administration** > **Integrationsinstanzen**.
8. Zeigen Sie die Projekte an, die Sie zuvor konfiguriert haben, indem Sie auf **Integrationsinstanzparameter**klicken.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Führen Sie die neu erstellte Integrationsinstanz aus, um die folgenden Daten zu importieren:
   - Docker-Images: Listet die Docker-Images auf, die mit einer Identifizierungs- und Abgleich-Engine (Identification and Reconciliation Engine, IRE) erstellt werden. Jedes Docker-Image enthält auch Informationen zur Beziehung zwischen den Repositorys und den installierten Versionen.
   - Erkannte Container-Images: Das Modul „Erkannte Container-Images“ enthält Informationen zur Image-ID, zum Docker-Image und zum Image-Repository. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. Sie können hier auch die Anzahl der Projekte und Container anzeigen. Für ein erkanntes Container-Image können Sie Cloud-Metadaten anzeigen, z. B. Cloud-Provider, Cloud-Region, Cloud-Konto-ID und Cloud-Ressourcen-IDs.
   - Container-Image-Pakete: Enthält Informationen zu den Paketen, in denen die Schwachstellen vorhanden sind. Die Details des Binärpakets werden auch als durch Kommas getrennte Werte bereitgestellt.
   - Container-Image-Ebenen: In diesem Bildschirm wird der Datensatz für jede Image-Ebene angezeigt.
   - Container-Image-Ergebnisse: Dieser Bildschirm zeigt die Liste der Ergebnisse zusammen mit Informationen zu den zugehörigen Schwachstellen, Image-Ebene, Docker-Image, Image-Repository und erkanntem Image an. Derzeit sind die Schwachstelleninformationen auf die ID beschränkt. Zusätzliche Informationen werden ausgefüllt, wenn die NVD-Integration ausgelöst wird.
   - Angreifbare Container-Elemente: Jedes Ergebnis weist eine entsprechende Schwachstelle auf. Die CVITs werden basierend auf der Granularität weiter erstellt.
10. Konfigurieren Sie die Granularität eines angreifbaren Elements.
    a. Navigieren zu **Prisma-Cloud-Computing-Integration** > **Image-Schwachstellenschlüssel konfigurieren**
    b. Konfigurieren Sie die Granularität der CVITs, indem Sie die erforderlichen Kontrollkästchen aktivieren. Die angreifbaren Elemente werden basierend auf den ausgewählten Schlüsseln beim nächsten Import erstellt.

**Hinweis:**
Standardmäßig wird eine CVIT für eine Kombination aus Image-Repository, Schwachstelle und Image-Tag erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um die Granularität zu erhöhen. Sie können beispielsweise eine CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image-Tag und Cluster erstellen. Sobald die angreifbaren Elemente oder die Ergebnisse der angreifbaren Elemente erstellt wurden, können die Kontrollkästchen nicht mehr bearbeitet werden.

## Container-Schwachstellen werden korrigiert

Die Überwachung der Fehlerkorrektur ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen von angreifbaren Containerelementen (CVITs) endet. Container Vulnerability Response bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

### Container Vulnerability Response Rechnerregeln

Schwachstellenrechner automatisieren die Berechnung der Anfangswerte für die Felder in angreifbaren Containerelementen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste übereinstimmende Rechner wird verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um Schwachstellenrechner anzuzeigen und zu erstellen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Sicherheitsrisiko-Rechner**.

Das Container Vulnerability Response Basissystem enthält zwei Schwachstellenrechner, die die Basis-Risikopunktzahl für das angreifbare Containerelement festlegen. Die folgenden Rechnergruppen sind im Basissystem verfügbar:

- Schwachstellenschwere: Berechnet die Risikopunktzahl für angreifbare Elemente anhand des normalisierten Schwachstellenschweregrads.
- Standardrisikorechner: Basiert auf der Risikoregel.

## Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen werden eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Exploit-Informationen usw. zugewiesen. Die Geschäftsregel *`Update Risk Rating from Risk Score`* in der Tabelle für angreifbare Containerelemente ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Containerelemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert war.

| Wert (Risikobewertung) | Gewichtung (Risikopunktzahl) |
|---|---|
| 1 | 90–100 |
| 2 | 70–89 |
| 3 | 40–69 |
| 4 | 1–39 |
| 5 | 0 |

Ab Version 18.0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle „Risikopunktzahlgewichtungen“ [sn_sec_cmn_risk_scorew_weights] als cvr_risk_rating bereitgestellt. Diese Typen werden als Teil der Geschäftsregeln oder Skripteinbindungen in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wurde so geändert, dass Sie die Einträge in den Werten der Tabelle „Risikopunktzahlgewichtungen“ für die Risikobewertungsberechnung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Gewichtungen der Risikopunktzahl“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn sich ein Konfigurationselement (CI) von „Nicht mit Internetzugriff“ in „Mit Internetzugriff“ ändert.
- Wenn die zugeordneten Common Vulnerabilities and Exposures (CVEs) oder Drittanbietereinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer CVE Known Exploit Vulnerability (KEV) verknüpft sind

Weitere Informationen finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.

## Container Vulnerability Response Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Container-Elemente (CVITs) automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

So erstellen und zeigen Sie Zuweisungsregeln für angreifbare Containerelemente an. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Zuweisungsregeln**. Wenn Sie eine Zuweisungsregel erstellen, können Sie die Bedingungen festlegen. Wenn diese Bedingungen erfüllt sind, weist die Regel die angreifbaren Containerelemente automatisch der ausgewählten Benutzergruppe zu. Nur die erste Zuweisungsregel mit einer übereinstimmenden Bedingung wird für einen Datensatz ausgeführt.

**Hinweis:**
Angreifbare Container-Elemente, die sich nicht im Status „Offen“ befinden oder manuell zugewiesen wurden, werden immer ausgeschlossen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

## Container Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Containerelements (CVIT). Diese Regeln ähneln der Art und Weise, wie SLAs einen Zeitrahmen für die Behebung der Schwachstelle selbst bereitstellen.

Um Korrekturzielregeln für Container-Schwachstellen zu erstellen und anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Nachbesserungszielregeln**.

Die Korrekturzielregeln definieren die Zielkorrekturzeit für ausgewählte angreifbare Containerelemente (CVITs). Legen Sie eine Frist für die Behebung der Schwachstelle fest, indem Sie die Anzahl der Tage für die Behebung auswählen. Legen Sie eine Erinnerung für die Korrektur fest, und legen Sie die angreifbaren Containerelemente fest, für die die Regel gilt. Sie können ein Korrekturziel für die Tage festlegen, innerhalb derer die Korrektur erforderlich ist, und eine Erinnerung festlegen, bevor Sie sich dem Zieldatum nähern. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln.

## Ausnahmeverwaltung in Container Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Containerelement (CVIT), das gemäß der Richtlinie nicht behoben werden kann.

Für einige Container-Schwachstellen (CVIT) ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen der Nichtbehebung der Schwachstelle anerkennen und akzeptieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Lebenszyklus einer Ausnahme

**Definition einer Ausnahme**

Eine Ausnahme ist eine Anforderung, die Korrektur einer CVIT oder RT für einen bestimmten Zeitraum zurückzustellen. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

**Eine Ausnahme wird angefordert**

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine CVIT oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird die **CVIT** oder RT in den Status „Zurückgestellt“ versetzt.

**Eine Ausnahmeanforderung wird genehmigt**

CVIT oder RTs, die nicht sofort korrigiert werden können, werden von Schwachstellenanalysten überprüft, auf Risiko bewertet und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Die Genehmigung einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

### Hinweis:

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

Sobald eine Ausnahmeanforderung für eine CVIT oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen
- Aktualisieren Sie die Felder **Zuweisung an** oder **Zuweisungsgruppen**

**Nachverfolgung einer Ausnahmeanforderung**

Nach dem Auslösen der Ausnahme können Sie ihren Status mithilfe der Registerkarte Statusänderungsgenehmigungen von **CVIT** oder RT nachverfolgen. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen CVITs in dieser RT nicht nachverfolgen.

**Ablauf einer Ausnahmeanforderung**

Wenn eine Ausnahmeanforderung für eine bestimmte CVIT oder RT abläuft, wird die betroffene CVIT oder RT in den Status „ **Offen** “ zurückgesetzt.

Wenn eine einzelne CVIT oder alle CVITs in einer RT beim nächsten Scan erfolgreich sind, ändern sich die **CVITs** und ggf. das Feld „RT-Status“ in **Geschlossen** mit dem Substatus **Fest**.

## Konfigurieren Sie Genehmigungsregeln

Zeigen Sie Genehmigungsregeln an, und konfigurieren Sie sie, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**. Fordern Sie eine Ausnahme für die CVITs an, die nicht sofort behoben oder zurückgestellt werden können, indem Sie die betroffenen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen, Konfigurationselemente (CIs) oder CVITs identifizieren. Automatisieren Sie den CVIT-Zurückstellungsprozess. Übereinstimmende CVITs basierend auf diesen Regeln zurückstellen, wenn das System diese CVITs identifiziert.

Die folgenden Genehmigungsregeln werden standardmäßig geliefert:

- Genehmigung für Ausnahmeanforderungen: Im Basissystem wird eine Standardkonfiguration mit zwei Genehmigungsebenen bereitgestellt. Immer wenn eine Ausnahmeanforderung für ein angreifbares Element vorliegt, wird die Genehmigungsanforderung an die Benutzer oder Gruppen in Ebene 1 gesendet. Nach der Genehmigung durch Genehmiger der Ebene 1 wird die Genehmigungsanforderung an die Genehmiger der Ebene 2 gesendet.

  **Hinweis:**
  Sie können die Standardebenen ändern und nach Bedarf bearbeiten. Ab Container Vulnerability Response v2.0.6 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme- oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*oder *sn_vul_container.container_false_positive_approver_group*, um den Eigenschaftswert zu ändern.

- Genehmigung für Ausnahmeregeln: Hat keine Konfiguration, aber zwei Genehmigungsebenen.
- Genehmigung für falsch positive Ergebnisse: Es gibt eine Konfiguration mit einer Genehmigungsebene.

**Hinweis:**
Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Containerelement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Containerelement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Ausnahmen in anfordern und genehmigen Container Vulnerability Response

Sie können anfordern, dass die Korrektur eines angreifbaren Containerelements (CVIT) für einen bestimmten Zeitraum zurückgestellt wird. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen von anderen Benutzern genehmigen.

Informationen zum Anfordern oder Genehmigen einer Ausnahme finden Sie unter:

- Fordern Sie eine Ausnahme für ein angreifbares Containerelement an
- Fordern Sie mit eine Ausnahme für Container-Schwachstellen an GRC: Policy and Compliance Management



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, dass eine Ausnahme angefordert wurde. Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Containerelement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Containerelement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

#### Fordern Sie eine Ausnahme für ein angreifbares Containerelement an

Fordern Sie eine Ausnahme für ein angreifbares Containerelement (CVIT) an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn ein Patch für einen Computer nicht verfügbar ist.

### Vorbereitungen

Erforderliche Rolle: Entwicklergruppe

### Prozedur

1. Navigieren zu **Container Vulnerability Response** > **Angreifbare Container-Elemente** > **Alle**.
2. Wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „Wird untersucht“ befinden.
3. Klicken Sie im Formular „Angreifbares Container-Element“ auf **Ausnahme anfordern**.
   [store-future: BEGIN review]

   ### Hinweis:

   Abhängig davon, ob Vulnerability Response oder GRC: Policy and Compliance Management im ausgewählt ist **Container Vulnerability Response** > **Ausnahmenverwaltung** Im Bildschirm „“ ändert sich das Formular „Ausnahme anfordern“.

   [End]
4. [store-future: BEGIN review]Wenn Vulnerability Response im Bildschirm „Exception Management“ ausgewählt ist, gehen Sie wie folgt vor.[End]

   a. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der im ausgewählten Zeitraum liegen **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** -Bildschirm. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „Offen“ zurück.<br><br>**Hinweis:**<br>Wenn ab Version 1.2 von Container Vulnerability Responsedie Korrektur eines angreifbaren Elements mithilfe der Ausnahmeverwaltungsfunktion zurückgestellt wurde und das Element vom Scanner erneut geöffnet wird, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum bestehen. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft *sn_vul.container.auto_defer_cvit_in_active_e* auf „true“ fest. Außerdem bleibt das Datum für „Zurückgestellt bis“ bestehen, auch nachdem die CVIT geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle ist sn_vul_container.manage_exception_configuration für Lesen und Schreiben. |
| Grund | Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt:<br>▪ Risiko akzeptiert<br>▪ Warten auf Wartungsfenster<br>▪ Behebung nicht verfügbar<br>▪ Ausgleichende Steuerung vorhanden<br>▪ Sonstige<br>Informationen zum Hinzufügen neuer Grundoptionen finden Sie unter Definieren Sie eine Richtliniengrundzuordnung. |
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden. |

Automatische Übersetzung

**b.** Senden Sie die Ausnahmeanforderung, indem Sie auf **Genehmigung**anfordern klicken. Der Status des angreifbaren Containerelements ändert sich in Wird überprüft. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

### Fordern Sie eine Ausnahme für eine Container-Korrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Container-Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort gelöst werden kann.

**Vorbereitungen**

Sie können Ausnahmen in den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle:

sn_vul.remediation_owner, sn_vul.app_security_change oder sn_vul_container.remediation_owner.

Sie können auch Ausnahmen für Container-Korrekturaufgaben in der klassischen Umgebung anfordern.

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben** > **Alle**.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Wählen Sie im Datensatz der Container-Korrekturaufgabe die **Option Ausnahme anfordern**aus.
4. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist. |
| Grund | Begründung für die Anforderung einer Ausnahme. |
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden. |

5. Klicken Sie auf **Genehmigungs-Engine**.

### Fordern Sie mit eine Ausnahme für Container-Schwachstellen an GRC: Policy and Compliance Management

Fordern Sie Richtlinienausnahmen mit der Funktion GRC zur Verwaltung von Richtlinienausnahmen in der Anwendung Policy and Compliance Management aus Container Vulnerability Responsean.

### Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Policy and Compliance Management aus dem ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vul.remediation_owner

Sie können Ausnahmen auch in der klassischen Benutzeroberfläche anfordern:

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (oder **Korrekturaufgaben**)>**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Klicken Sie im ausgewählten Formular auf **Ausnahme anfordern**.

**Hinweis:**
Wenn GRC: Policy and Compliance Management im Bildschirm „Exception Management“ ausgewählt ist, füllen Sie die Felder im Formular „Ausnahme anfordern“ aus. Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahme anfordern“..

a. Senden Sie die Ausnahmeanforderung, indem Sie auf **Genehmigung**anfordern klicken.
Der Status der angreifbaren Elemente ändert sich in Wird überprüft, und eine Richtlinienausnahme wird erstellt. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

b. Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

c. Klicken Sie auf die Nummer der Richtlinienausnahme.

d. **Wählen Sie** im Feld Genehmiger den Namen des Genehmigers aus.

e. Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

f. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie im Feld Risikobewertung die **Risikobewertung** aus.

g. Speichern Sie das Formular.

h. Klicken Sie auf die Registerkarte **Betroffene Steuerungen**.

i. Fügen Sie die Steuerungen hinzu, indem Sie auf **Hinzufügen**klicken.

j. Speichern Sie das Formular.

**Hinweis:**
Sie können eine Compliance-Überprüfung durchführen, indem Sie auf **Compliance-Überprüfung anfordern**klicken.

Das Genehmigungsformular wird an den Genehmiger gesendet.

Der Genehmiger kann die Anforderung entweder genehmigen, indem er auf **Genehmigen klickt**, oder eine zusätzliche Genehmigung anfordern, indem er auf **Zusätzliche Genehmigung**anfordern klickt.

Der Datensatzstatus ändert sich in „Zurückgestellt“. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte **Zurückstellung** enthält zusätzliche Hinweise zum Datensatz.

**Hinweis:**
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

3. Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definieren Sie eine Richtliniengrundzuordnung

Definieren Sie Grundoptionen, die allen Benutzern zur Verfügung stehen, die eine Ausnahme anfordern.

## Vorbereitungen

Erforderliche Rolle: sn_vul.compliance.manager und sn_vul_container.manage_exception_configuration

## Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

   **Hinweis:**
   Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung „Container Vulnerability Response – CVIT“.
3. Klicken Sie in der Liste Grundauswahl auf **Neu**.
4. Klicken Sie auf das Lupensymbol.
5. Fügen Sie eine vorhandene Grundauswahl hinzu, um eine neue zu erstellen.
   - Wenn Sie eine vorhandene Grundauswahl hinzufügen möchten, wählen Sie einen Grund aus.
   - Wenn Sie der Tabelle „Grundauswahlmöglichkeiten“ eine neue Grundauswahl hinzufügen möchten, klicken Sie auf **Neu**, und füllen Sie die Felder im Formular aus.

   **Formular „Grundauswahlliste“**

| Feld | Beschreibung |
|---|---|
| Bezeichnung | Eindeutige Bezeichnung für diese Auswahl. |
| Wert | Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Richtliniengrundzuordnung“ für die entsprechenden Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_vul_policy_reason_mapping.LIST ein. |
| Reihenfolge | Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert. |
| Standard | Option, um anzugeben, dass diese Grundauswahl immer dann verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, sind alle Grundoptionen verfügbar, für die das Feld **Standard** ausgewählt ist. |
| Aktiv | Option zum Anzeigen der Auswahl in der Liste der Grundoptionen. |

6. Klicken Sie auf **Absenden**.

## Ergebnisse

Die Grundauswahl wird hinzugefügt. Die Grundauswahl ist im Feld **Grund** des Anforderungsformulars für Richtlinienausnahmen für die ausgewählte Anwendung verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Genehmigen Sie eine Ausnahmeanforderung in Container Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Containerelemente oder Korrekturaufgaben, die nicht sofort korrigiert werden können. Sie müssen diese Anforderungen auf Risiken bewerten und sie dann zur Zurückstellung genehmigen, bis sie korrigiert werden können.

#### Vorbereitungen

Sie können Ausnahmen und falsch positive Anforderungen im Vulnerability Response -Arbeitsbereich genehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

Erforderliche Rolle: sn_vul.exception_approver

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen:

#### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

### Zurückstellen eines angreifbaren Containerelements in Container Vulnerability Response

Wenn Sie feststellen, dass das mit einem angreifbaren Containerelement ( **CVIT** ) verknüpfte Problem ein geringes Risiko aufweist und ohne weitere Analyse sofort zurückgestellt werden kann, können Sie die Funktion „Zurückstellen“ verwenden.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

#### Warum und wann dieser Vorgang ausgeführt wird

Eine regelmäßige Aufgabe wird täglich ausgeführt und überprüft, ob zurückgestellte angreifbare Elemente vorhanden sind, deren Datum der Wiedereröffnung erreicht wurde. An dem Tag, an dem die Zurückstellung der CVIT abläuft, wird der Datensatz erneut geöffnet.

#### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie **auf Ausnahme anfordern**.
4. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Bis | Wählen Sie das Datum aus, an dem der Status „Zurückgestellt“ abläuft und die Korrekturaufgabe erneut aktiviert wird.<br><br>**Hinweis:**<br>Wenn ab Version 18.0 von Container Vulnerability Responseein zurückgestelltes angreifbares Containerelement (CVIT) geschlossen und von einem Scanner erneut geöffnet wird, bevor das Ausnahmefenster abläuft, wird der Status der CVIT unter Berücksichtigung des aktiven Ausnahmefensters in den Status „Zurückgestellt“ zurückgesetzt. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vul.container.auto_defer_cvit_in_active_ex` auf „true“ fest. Darüber hinaus bleibt das zurückgestellte Bis-Datum bestehen, auch nachdem das angreifbare Element geschlossen wurde oder die Ausnahme abgelaufen ist. Die erforderliche Rolle ist sn_vul_container.manage_exception_configuration für Lesen und Schreiben.<br><br>Nachdem der Datensatz übermittelt wurde und E- Mail-Benachrichtigungen definiert sind, erhalten Mitglieder der Gruppe Container Vulnerability Response eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Nach Ablauf des Zurückstellungsdatums wird das angreifbare Element auf „Offen“ zurückgesetzt und eine zweite E-Mail-Benachrichtigung gesendet. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br><br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Falsch positiv<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

**5.** Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Gruppe wird als Wird **überprüft**markiert. Ein **zugehöriger** Link Erneut öffnen wird angezeigt. Das Datum und der Grund für die Wiedereröffnung werden in Arbeitsnotizen auf der Registerkarte **Status-Change-Genehmigungen** angezeigt.

Ab Container Vulnerability Response v2.3 können Sie relevante Informationen im Feld Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Containerelement hinzufügen.

### Fordern Sie eine Erweiterung für ein zurückgestelltes angreifbares Containerelement an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Containerelement an, bevor es sein Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

#### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**.
2. Öffnen Sie ein zurückgestelltes angreifbares Containerelement.
3. Wählen Sie **Verlängerung anfordern aus**.

> **Hinweis:**
> Die Schaltfläche Verlängerung anfordern ist nur sichtbar, wenn der Status des angreifbaren Containerelements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Korrektur des zurückgestellten angreifbaren Containerelements verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Genehmigung anfordern**.
   Nach der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers wird eine E-Mail ausgelöst.

   **Hinweis:**
   - Die Anforderung durchläuft zwei Genehmigungsstufen.
   - Wenn ein zurückgestelltes angreifbares Containerelement erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden die Notizen für Bis, Grund und Zurückstellung aktualisiert.

### Arbeiten mit einer Ausnahmeregel in Container Vulnerability Response

Sie können eine Ausnahme für angreifbare Containerelemente (CVITs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch die Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden CVITs basierend auf der Regel zurückstellen, wenn das System sie identifiziert.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response
- Genehmigen Sie eine Ausnahmeregelanforderung in Container Vulnerability Response
- Aktivieren einer Ausnahmeregel in Container Vulnerability Response
- Öffnen Sie eine Ausnahmeregel erneut in Container Vulnerability Response
- Aktualisieren Sie eine genehmigte Ausnahmeregel in Container Vulnerability Response
- Löschen Sie eine Ausnahmeregel in Container Vulnerability Response
- Zurückstellen eines angreifbaren Containerelements in Container Vulnerability Response

**Hinweis:**
Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Containerelement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Containerelement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Containerelementen (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

#### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

#### Warum und wann dieser Vorgang ausgeführt wird
Die Regel wird vom „Gültig ab“-Datum bis zum „Gültig bis“-Datum angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppierungsmethode für diese VUL wird als Ausnahmeregel bezeichnet. Die VUL wird im Status „Zurückgestellt“ erstellt. Sie können diese VUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete CVITs werden zurückgestellt und dieser VUL ab dem „Gültig ab“-Datum hinzugefügt, bis die Gruppe am „Gültig bis“-Datum abläuft.

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung übermittelt wurde.

**Hinweis:**

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann zur Genehmigung erneut übermitteln.

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Klicken Sie auf der Seite „Ausnahmeregel für neuen Datensatz“ auf **Neu**, um eine Regel zu erstellen.
3. Füllen Sie die Felder des Formulars „Ausnahmeregel“ aus.

   **Hinweis:**

   Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahmeregel“.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Senden Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in Wird überprüft. Bis Sie die Ausnahmeregel absenden, bleibt sie im Status Entwurf.
6. So zeigen Sie eine Gruppe an, um Ausnahmeregeln zu verwalten:

   a. Navigieren zu **Alle** > **Benutzeradministration** > **Gruppen**.

   b. Klicken Sie in einer Ausnahmeregel auf die Registerkarte **Angeforderte Genehmigungen**, um den Status der Anforderung anzuzeigen.
   Täglich wird eine regelmäßige Aufgabe ausgeführt, die die Ausnahmeregeln für vorhandene Daten ausführt. Alle angreifbaren Elemente, die der Bedingung entsprechen, werden in den Status „Zurückgestellt“ verschoben. Wenn eine genehmigte Ausnahmeregel gelöscht wird, werden alle zurückgestellten angreifbaren Elemente in ihren vorherigen Status zurückgesetzt. Weitere Informationen finden Sie unter Arbeiten mit einer Ausnahmeregel.

[store-future: BEGIN review]

## Genehmigen Sie eine Ausnahmeregelanforderung in Container Vulnerability Response

Bewerten Sie Ausnahmeregelanforderungen von Benutzern, damit Sie diese Anforderungen genehmigen oder ablehnen können.

### Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

### Warum und wann dieser Vorgang ausgeführt wird

Mitglieder der Benutzergruppe des Ausnahmegenehmigers der Ebene 1 können Ausnahmeregelanforderungen der Ebene 1 genehmigen. Ebenso können Benutzergruppenmitglieder von Ausnahmegenehmigern der Ebene 2



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausnahmeregelanforderungen der Ebene 2 genehmigen. Beide Benutzergruppen erben standardmäßig die Rolle des Ausnahmegenehmigers.

**Hinweis:**

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für die Ausnahmenverwaltung und Falschmeldungen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

**Prozedur**

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit ab, und erläutern Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe (RT) im Status „Zurückgestellt“ erstellt. Ab dem Datum „Gültig ab“ wird diese Regel für alle CVITs ausgeführt, die erstellt werden, sowie für diejenigen, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. CVITs, die den definierten Bedingungen entsprechen, werden der RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   **Hinweis:**
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann zur Genehmigung erneut übermitteln.

[End]

### Aktivieren einer Ausnahmeregel in Container Vulnerability Response

Eine Regel wird an ihrem „Gültig ab“-Datum aktiviert. Nach der Aktivierung wird der Ausnahmeprozess für angreifbare Container-Elemente (CVITs) automatisiert.

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen CVITs, die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option Für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten CVITs, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird geändert zu Zurückgestellt.
2. Wenn eine neu erstellte CVIT mit der Ausnahmeregelbedingung übereinstimmt, wird sie in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht darauf ausgeführt.
3. Am Datum „Gültig ab“ werden vorhandene CVITs hinzugefügt, wenn Sie die Option Für vorhandene Daten ausführen aktivieren.
4. Die RT akzeptiert keine neuen CVITs mehr, wenn die Regel am „Gültig bis“-Datum abläuft. Die RT bleibt bis zum Datum „Zurückgestellt bis“ bestehen.
5. Die Ausnahmeregel läuft am „Gültig bis“-Datum ab.

### Öffnen Sie eine Ausnahmeregel erneut in Container Vulnerability Response

Öffnen Sie eine abgelehnte Ausnahmeregel erneut, die Sie jedoch erneut übermitteln möchten. Wenn Sie die Regel erneut öffnen, wird sie in den Status „Entwurf“ versetzt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird
Anschließend können Sie die Regel aktualisieren und erneut zur Genehmigung übermitteln.

### Prozedur
1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut**öffnen.
3. Aktualisieren Sie das Formular, und übermitteln Sie es erneut zur Genehmigung.

## Aktualisieren Sie eine genehmigte Ausnahmeregel in Container Vulnerability Response

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Datumsangaben ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Containerelemente (CVITs) in den Status „Offen“ verschoben werden.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird
Gruppenregeln werden erneut auf diese CVITs angewendet. Senden Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie den Genehmigungsprozess erneut durchläuft.

### Prozedur
1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen**.
3. Klicken Sie im Dialogfeld „Regel abbrechen“ auf **Regel abbrechen**.
   Die Regel wird wieder in den Status „Entwurf“ verschoben, und die zugehörige VUL wird gelöscht.
   Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

## Löschen Sie eine Ausnahmeregel in Container Vulnerability Response

Löschen Sie eine Ausnahmeregel, die nicht mehr benötigt wird. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Containerelement (CVIT) während der Erfassung nicht zurückstellen möchten.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird
Durch das Löschen einer Regel wird die zugeordnete Korrekturaufgabe (VUL) abgebrochen. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

### Prozedur
1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im Dialogfeld „ **Regel** löschen“ auf Regel löschen, um die ausgewählte Regel zu löschen.
   Die zugeordnete Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

### Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie ihr zurückgestelltes Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

#### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, an dem der Status „Zurückstellen“ abläuft und das angreifbare Containerelement erneut aktiviert wird. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein.<br>Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Containerelemente übertragen, die Teil der Korrekturaufgabe sind. Die angreifbaren Containerelemente sollten sich jedoch im Status „Zurückgestellt“ befinden und ihre aktuellen Bis-Daten vor

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem Aktualisierungsdatum liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie ihr Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

#### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Ausnahmeregeln**.
2. Wählen Sie eine zurückgestellte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein.<br>Zur Auswahl stehen:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die angreifbaren Containerelemente aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Korrekturaufgaben, die im Rahmen einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Falsch positives angreifbares Container-Element markieren und genehmigen

Angreifbare Container-Elemente (CVITs) und Korrekturaufgaben (VULs) können als falsch positive Meldungen markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Benutzern genehmigen.

- In als falsch positiv markieren Container Vulnerability Response
- Genehmigen Sie ein falsch positives Ergebnis

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise eine CVIT oder eine Korrekturaufgabe als falsch positiv markiert wird, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail mit der Nachricht, dass eine CVIT oder Korrekturaufgabe als falsch positiv markiert wurde. Ab v2.5 von Container Vulnerability Responsekönnen Sie die Zeitrahmen für die Genehmigung von Falschmeldungen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Containerelement in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Containerelement oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### In als falsch positiv markieren Container Vulnerability Response

Markieren Sie ein angreifbares Containerelement (CVIT) oder eine Korrekturaufgabe als falsch positiv, wenn die vom Scanner ausgegebene Warnung kein tatsächliches Problem ist. Beispiel: Wenn eine CVIT außer Betrieb genommen wurde, der Scanner jedoch immer noch ein damit verbundenes Problem auslöst, markieren Sie sie als falsch positiv.

#### Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Sie können falsch positive Meldungen aus den Vulnerability Response Arbeitsbereichen anfordern. Weitere Informationen finden Sie unter Fordern Sie ein falsch positives Ergebnis in an IT Remediation Workspace.

Sie können auch falsch positive Meldungen in der klassischen Umgebung anfordern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response (oder Korrekturaufgaben)** > **Alle**.
2. Öffnen Sie die **CVIT**, die Sie als falsch positiv markieren möchten, und klicken Sie auf Als falsch positiv markieren.
   Die CVIT muss sich im Status „ **Offen** “ befinden.
3. Geben Sie im Formular „Falsch positiv“ Details in **Zusätzliche Informationen** ein, und klicken Sie auf **Genehmigung anfordern**.
   Die Genehmigungsanforderung wird gesendet, und der Status der CVIT ändert sich in Wird **überprüft**.
   Sowohl die anfordernde Person als auch der Genehmiger werden per E-Mail benachrichtigt.

#### Genehmigen Sie ein falsch positives Ergebnis

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Benutzern genehmigen.

### Vorbereitungen

Erforderliche Rolle: false_positive_approver

Sie können Ausnahmen und falsch positive Anforderungen im Vulnerability Response -Arbeitsbereich genehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Anforderungen in Vulnerability Manager Workspace.

Sie können Ausnahmen und falsch positive Anforderungen auch in der klassischen Umgebung genehmigen:

### Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

**Hinweis:**
Ein falsch positives Ergebnis kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.

## IT Operations Management und Mustererkennung

Wenn die Erkennung aktiviert ist, werden Informationen vom Information Technology Operations Management (ITOM)-Team empfangen. Wenn ITOM Discovery aktiviert ist, werden Kubernetes-Namespaces, Kubernetes-Cluster und Kubernetes-Services angezeigt, wenn Sie ein angreifbares Containerelement (CVIT) öffnen. Andernfalls können Sie Prisma-Nutzlastinformationen anzeigen.

Die Image-Bezeichnungen aus den Prisma-Nutzlasten werden als Schlüssel-Wert-Paare unter dem Docker-Image gespeichert. Die Bezeichnungen in einer Prisma-Nutzlast werden in der Tabelle cmdb_key_value gespeichert. Um diese Funktion zu aktivieren, wird vom ITOM-Team eine Identifizierungsregel für cmdb_ci_docker_image bereitgestellt. Öffnen Sie das Docker-Image, um die Liste der zugehörigen Elemente anzuzeigen. Die meisten Elemente werden vom Team ITOM ausgefüllt. Der Identifizierungseintrag für ein Docker-Image wird so geliefert, dass die Werte als Schlüssel-Wert-Paare angezeigt werden.

Die Geschäftsrelevanz wird basierend auf den Informationen zur Servicerelevanz bestimmt, die vom Team ITOM erhalten wurden. Eine regelmäßige Aufgabe wird ausgeführt, um Daten aus allen Services abzurufen, die einem Image zugeordnet sind. Sie berechnet die Geschäftskritikalität basierend auf der Servicezuordnung. Da die Risikopunktzahl von



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Geschäftskritikalität abhängen kann, wird die Risikopunktzahl auch basierend darauf berechnet.

## Analytics and Reporting-Lösungen für Container Vulnerability Response

Dieser Platform Analytics-Lösung enthält vorverpackte Platform Analytics Inhalte zur Verwendung mit anderen Now Platform -Produkten. Diese Platform Analytics-Lösung bietet einen Überblick darüber, wie Schwachstellen mithilfe der verschiedenen Diagramme verwaltet werden.

### Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Platform Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

#### Zugehörige Informationen

Analytics- und Reporting-Lösungen

### Container Vulnerability Response-Dashboard

Analytics- und Reporting-Lösungen enthalten vorpaketierte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Mit Platform Analytics-Lösung können Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nachverfolgen. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

### Erforderliche Now Platform-Rollen

- Now Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

### Zugriff auf das Dashboard von Container Vulnerability Response

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Container Vulnerability Response** > **Übersicht**.

Ab Version 2.2 von Container Vulnerability Responsekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und wählen Sie das Symbol **Dashboards**. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, wählen Sie die Dropdown-Liste neben dem Dashboard-Namen aus. Weitere Informationen finden Sie unter Dashboardübersicht und Dashboardübersicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

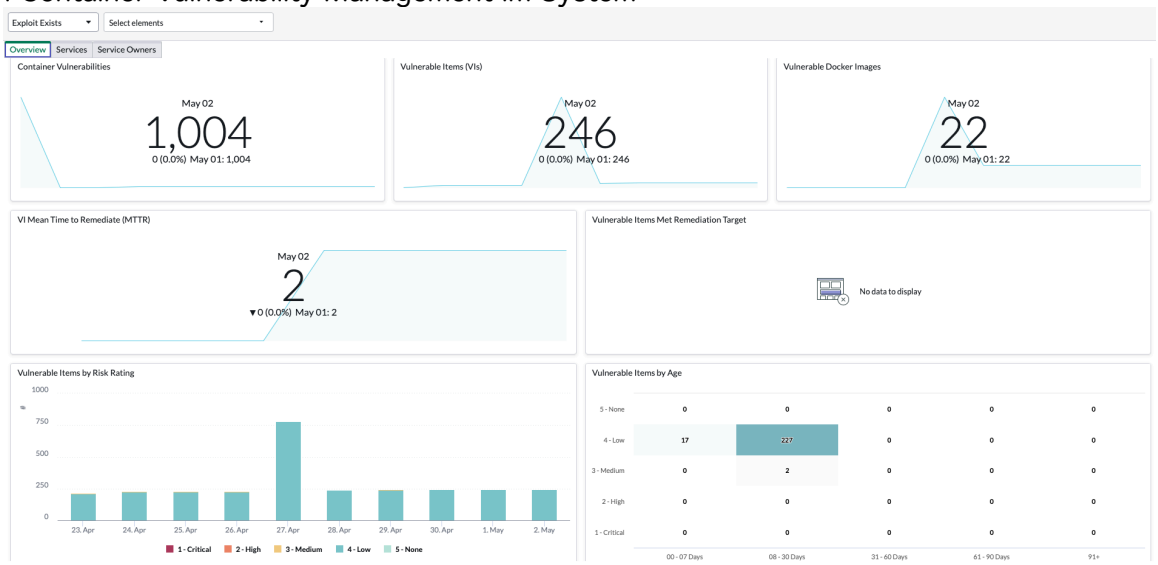
**Hinweis:**

- Wenn Sie ein neuer Benutzer sind, können Sie die Dashboards nur über die Arbeitsbereiche anzeigen.
- Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

## Registerkarten für Container Vulnerability Management

In diesem Dashboard können Sie die in Containern vorhandenen Schwachstellen anzeigen. Sie können die Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.

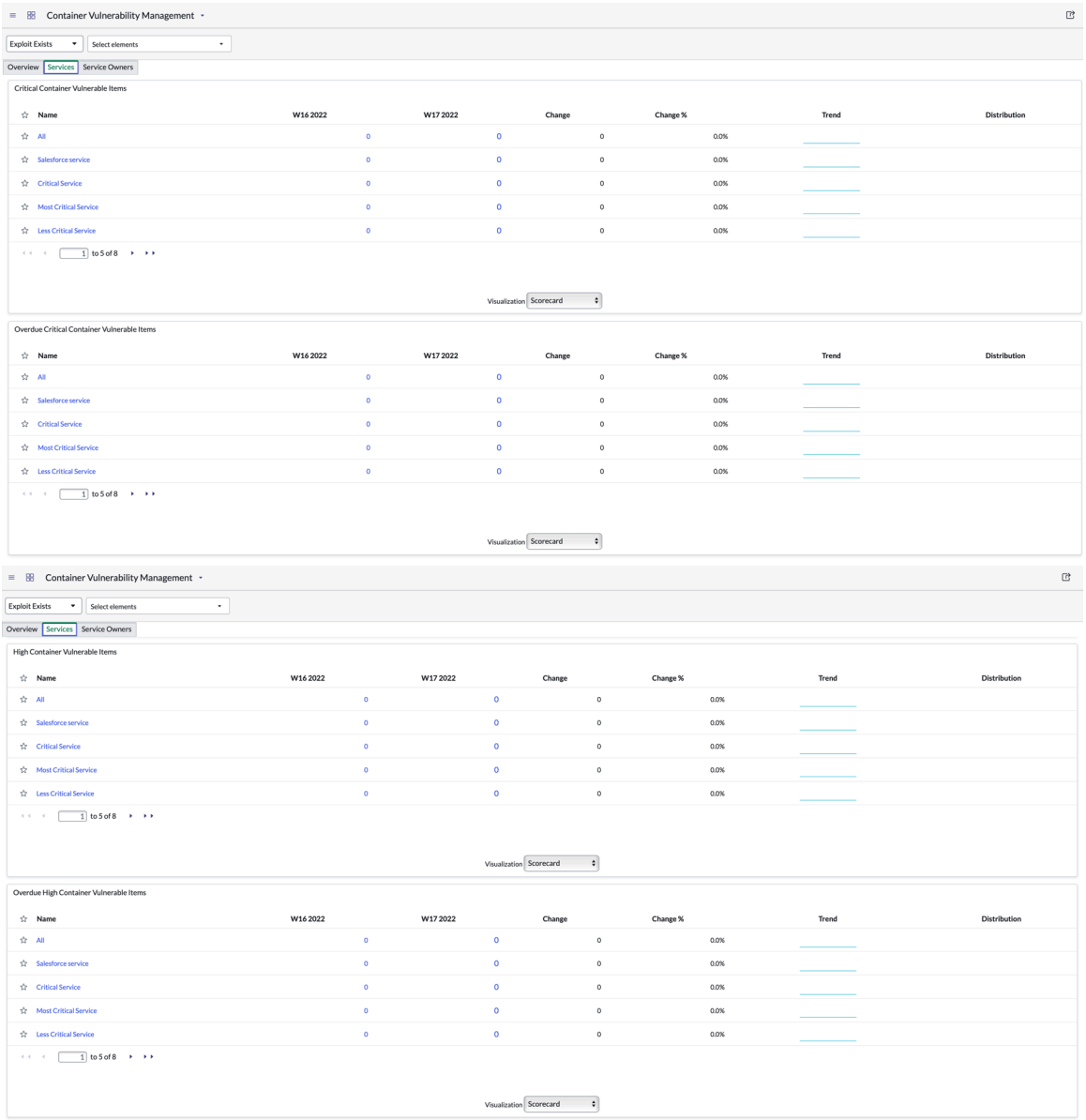
Die Registerkarte **Übersicht** zeigt den Gesamtstatus von Container Vulnerability Management im System an.




Die Registerkarte **Services** zeigt angreifbare Container-Elemente, die sich auf Anwendungsservices auswirken.



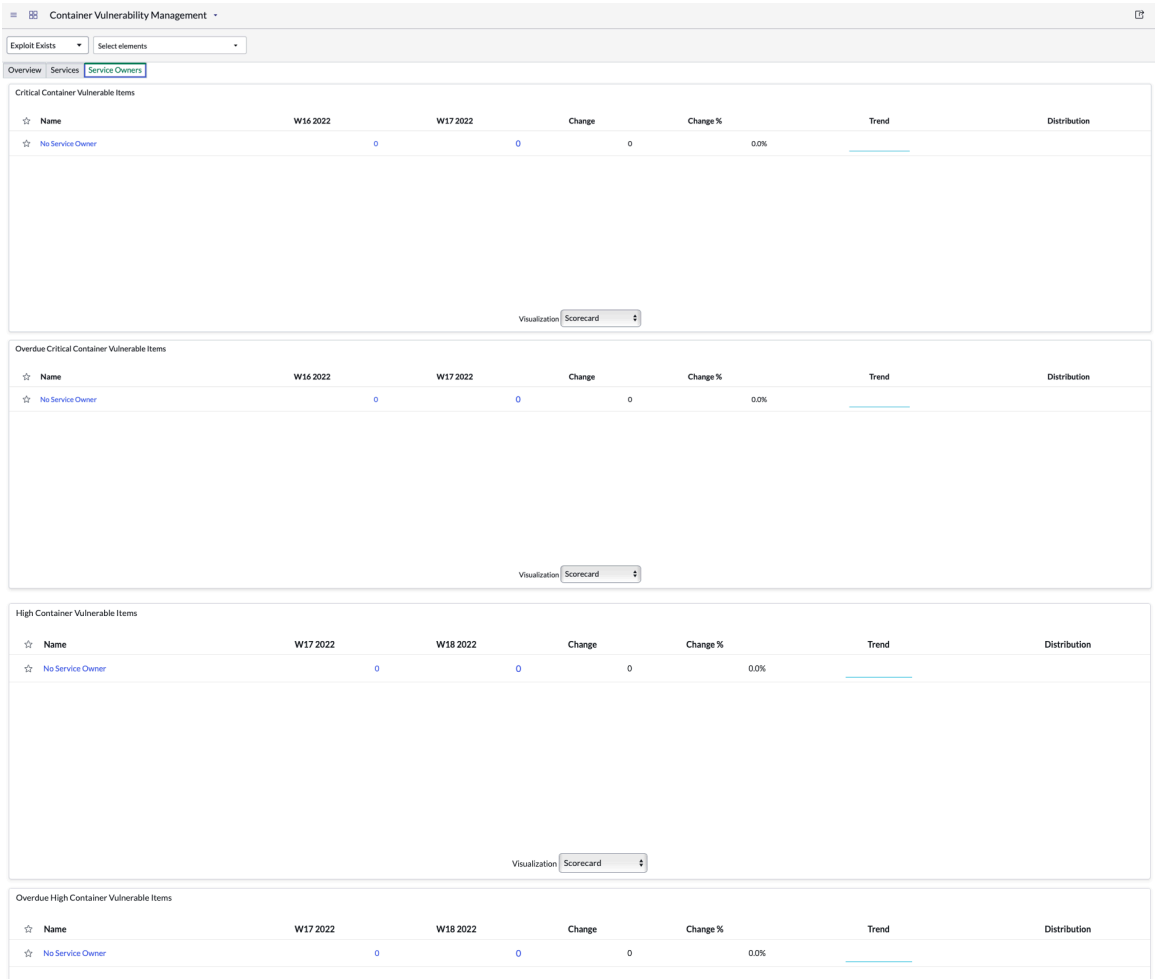
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die Registerkarte „ **Serviceverantwortliche** “ zeigt angreifbare Container-Elemente, die sich auf Serviceverantwortliche auswirken. Registerkarte „Container-Schwachstellenmanagement –

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## BreakdownsAufgliederungen

- Exploit vorhanden
- Exploit-Angriffsvektor
- Exploit-Kompetenzniveau
- Nachbesserungszielstatus
- Risikobewertung
- Status
- Zuweisungsgruppe

Automatische Übersetzung

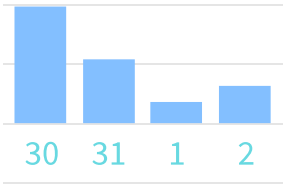
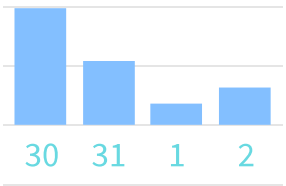
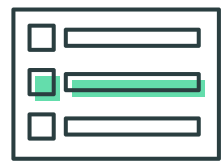
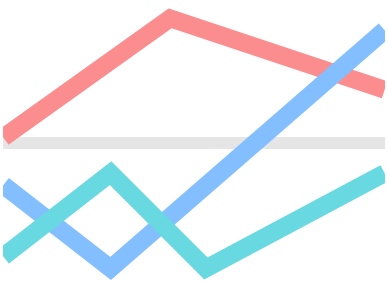
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Datenvisualisierungen

| Name | Typ | Beschreibung |
|---|---|---|
| Container-Schwachstellen | Einzelwert | Anzahl der Container-Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Container-Elementen verknüpft sind. |
| Angreifbare Elemente (AEs) | Einzelwert | Anzahl der aktiven (nicht geschlossener) angreifbaren Containerelemente. |
| Angreifbare Docker-Images | Einzelwert | Anzahl der Docker-Images, die mit aktiven angreifbaren Container-Elementen verknüpft sind. |
| Durchschnittliche Zeit bis zur Fehlerkorrektur (MTTR) für AEs | Einzelwert | Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt. |
| Angreifbare Elemente mit erfülltem Nachbesserungsziel | Einzelwert | Prozentsatz der geschlossenen angreifbaren Containerelemente, deren Korrekturzieldaten im aktuellen und vorherigen Quartal eingehalten wurden. Korrekturziele werden aus dem Datum „Zuletzt geöffnet“ plus der Anzahl der Tage berechnet. |

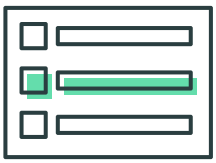
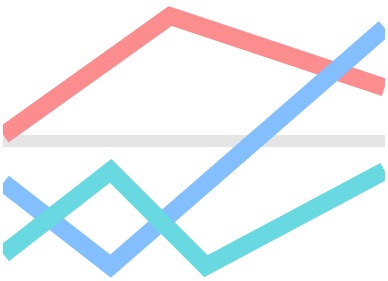
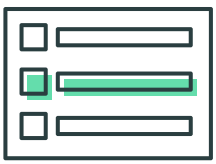
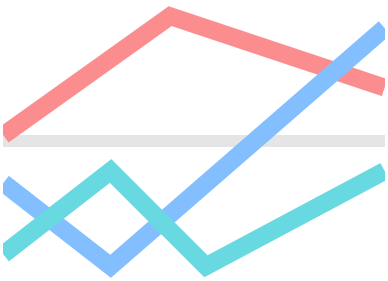
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
| --- | --- | --- |
| Angreifbare Elemente nach Risikobewertung | Leiste   | Anzahl der aktiven angreifbaren Container-Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne. |
| Angreifbare Elemente nach Alter | Leiste   | Anzahl der aktiven angreifbaren Containerelemente, gruppiert nach Risikobewertung und Alter (in Tagen). |
| Kritische angreifbare Container-Elemente | Listen- und   | Anzahl der aktiven angreifbaren Containerelemente mit kritischer Risikobewertung, gruppiert nach Service. |

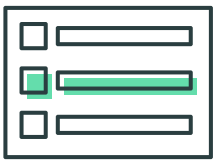
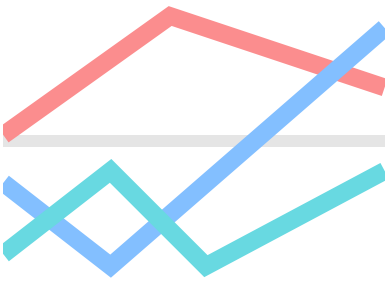
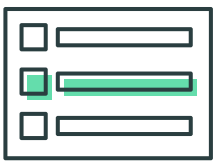
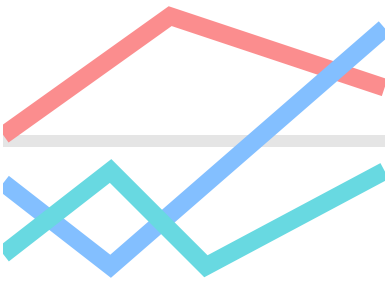
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
| --- | --- | --- |
| Überfällige kritische angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Containerelemente mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Service. |
| Hoch angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Containerelemente mit hoher Risikobewertung, gruppiert nach Service. |

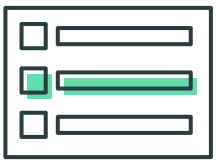
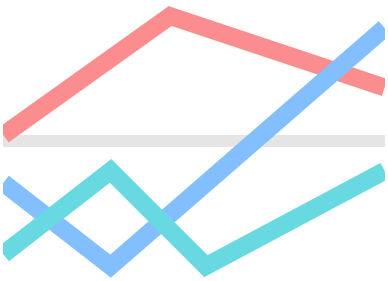
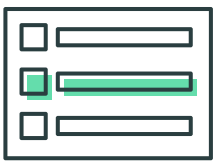
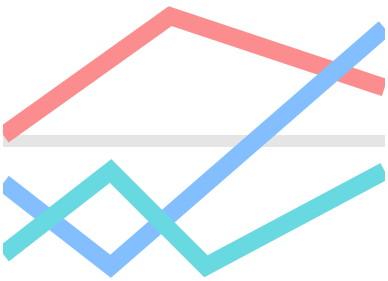
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
| --- | --- | --- |
| Überfällige, hoch angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Service. |
| Kritische angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Containerelemente mit kritischer Risikobewertung, gruppiert nach Serviceverantwortlichem. |

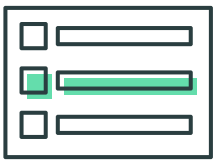
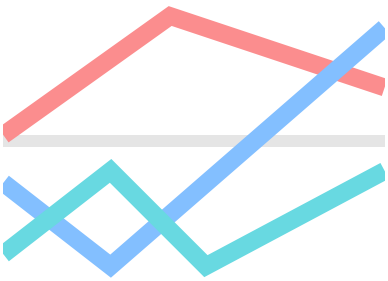
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
| --- | --- | --- |
| Überfällige kritische angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Containerelemente mit kritischer Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Serviceverantwortlichem. |
| Hoch angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Containerelemente mit hoher Risikobewertung, gruppiert nach Serviceverantwortlichem. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
| --- | --- | --- |
| Überfällige, hoch angreifbare Container-Elemente |  und Position  | Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, deren Korrekturzieldaten verstrichen sind, gruppiert nach Serviceverantwortlichem. |

## Container Vulnerability Response – Referenz

Referenzthemen mit Informationen zu Tabellen, Rollen und Eigenschaften, die mit Container Vulnerability Responseinstalliert werden.

### Mit Container Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Container Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

#### Mit Container Vulnerability Response installierte Rollen

Rollen werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Informationen zu unterstützen, die Benutzer und Gruppen in der Anwendung Vulnerability Response anzeigen und tun können. Informationen zur erstmaligen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

Wenn Sie Upgrade-Kunde sind, hat sich der Zugriff für die Benutzer und Gruppen, denen Sie vor v10.3 die Berechtigungen sn_vul.vulnerability_read und sn_vul.vulnerability_write zugewiesen haben, nicht geändert. Benutzern und Gruppen bleiben diese Rollen zugewiesen, bis Sie sie ändern. Ab v10.3 bevorzugen Sie jedoch möglicherweise die Zuweisung granularer Rollen, um mehr Kontrolle darüber zu haben, was Benutzer und Gruppen in der Anwendung Vulnerability Response tun und anzeigen können. Eine Übersicht und weitere Informationen zum Verwalten dieser Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen und Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

| Rollentitel [Name] | Beschreibung |
|---|---|
| sn_vul_container.ci_manager | Verwaltet die Neuklassifizierung abgeglichenen Konfigurationsele |
| sn_vul_container.configure_integrations | Konfiguriert Containerintegration |
| sn_vul_container.configure_vi_granularity | Konfiguriert die Granularität ang Container-Elemente. |
| sn_vul_container.create_vi | Kann angreifbare Container-Elem erstellen. |
| sn_vul_container.delete_vi | Kann manuell erstellte angreifbar Elemente löschen. |
| sn_vul_container.exception_approver | Genehmigt Ausnahmen, Zurücks und Schließungen von angreifbar Containerelementen.<br><br>Ab v2.3 wurde die granular sn_vul_container.read_all fü Rolle entfernt, sodass Sie a Ihnen und Ihrer Gruppe zug angreifbaren Containerelem und Korrekturaufgaben zug können, anstatt auf alle angreifbaren Containerelem Korrekturaufgaben. |
| sn_vul_container.false_positive_approver | Genehmigt oder lehnt das Schlie angreifbaren Containerelementen positiv ab. |
| sn_vul_container.manage_assignment_rules | Definiert und aktualisiert Zuweis angreifbare Container-Elemente. |
| sn_vul_container.manage_auto_close_stale_vi | Konfigurieren Sie die angreifbare das automatische Schließen veral |
| sn_vul_container.manage_auto_exception_rule | Ausnahmeregeln verwalten (Erst Aktualisieren/Löschen). |
| sn_vul_container.manage_normalized_severity | Kann die Zuordnung aktualisiere Schweregrad zu normalisieren. |
| sn_vul_container.manage_permissions | Kann Anwendern Container Vul Response-Rollen zuweisen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung |
|---|---|
| sn_vul_container.manage_remediation_targ… | Definiert und aktualisiert Contain Korrekturzielregeln. |
| sn_vul_container.manage_risk_score_confi... | Definiert und aktualisiert Risikop Rechner, Risikoregeln und Schwa Rollup-Rechner für angreifbare C Elemente. |
| sn_vul_container.read_all | Kann alle angreifbaren Container zugehörige Informationen anzeig |
| sn_vul_container.read_assigned | Kann angreifbare Container-Elem die mir oder meinen Gruppen zug |
| sn_vul_container.read_assignment_rules | Kann Zuweisungsregeln für angr Container-Elemente anzeigen. |
| sn_vul_container.read_auto_exception_rule | Ausnahmeregeln lesen |
| sn_vul_container.read_discovered_image | Kann erkannte Elemente anzeige |
| sn_vul_container.read_integrations | Kann Ergebnisse von Integration anzeigen. |
| sn_vul_container.read_normalized_severity | Kann die normalisierte Schwereg anzeigen. |
| sn_vul_container.read_remediation_target... | Kann Korrekturzielregeln anzeig |
| sn_vul_container.read_risk_score_configu... | Kann Risikopunktzahlrechner, Ri Schwachstellen-Rollup-Rechner Container-Elemente anzeigen. |
| sn_vul_container.remediation_owner | Liest und schreibt angreifbare Co Elemente, die ihnen zugewiesen Schwachstellendatensätze könner einem Benutzer mit dieser Rolle |
| sn_vul_container.update_assigned_to | Kann die Zuweisung von an Containerelementen aktuali<br><br>Erfordert sn_vul_container. sn_vul_container.write_assi |
| sn_vul_container.update_assignment_group | Kann Zuweisungsgruppe fü Container-Elemente aktualis<br><br>Erfordert sn_vul_container. sn_vul_container.write_assi |
| sn_vul_container.update_state | Kann Status angreifbarer E aktualisieren.<br><br>Erfordert sn_vul_container. sn_vul_container.write_assi |

Automatisch übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung |
|---|---|
| sn_vul_container.vulnerability_admin | Konfiguriert alle Regeln, Integrat das Produkt Container Vulnerabi |
| sn_vul_container.vulnerability_analyst | Überwacht die Korrektur aller an Containerelemente. |
| sn_vul_container.write_all | Kann alle angreifbaren Container Korrekturaufgaben aktualisieren. |
| sn_vul_container.write_assigned | Kann angreifbare Containereleme Korrekturaufgaben aktualisieren, meinen Gruppen zugewiesen sind |
| sn_vul_container.read_watch_topic | Kann Überwachungsthemen für C Schwachstellen lesen. |
| sn_vul_container.create_watch_topic | Kann Überwachungsthemen für C Schwachstellen erstellen. |
| sn_vul_container.edit_watch_topic | Kann Überwachungsthemen für C Schwachstellen bearbeiten. |
| sn_vul_container.manage_exception_configuration | Kann Ausnahmeverwaltungskonf verwalten. |

### Mit Container Vulnerability Response installierte Tabellen

Tabellen werden bei der Aktivierung von Container Vulnerability Response (CVR) hinzugefügt.

| Tabelle | Beschreibung |
|---|---|
| Suche nach Container-Image<br>sn_vul_container_image_findings | Speichert Informationen über die zugeordneten Schwachstellen, die Image-Ebene, das Docker-Image, das Image-Repository und das erkannte Image. |
| Container-Image-Ebene<br>sn_vul_container_image_layer | Enthält die Informationen jeder Bildebene. Ein Image ist eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann. |
| Container-Image-Paket<br>sn_vul_container_image_package | Stellt Informationen zu den Paketen bereit, in denen die Schwachstellen vorhanden sind. Die Details des Binärpakets werden auch als durch Kommas getrennte Werte bereitgestellt. |
| Angreifbares Container-Element<br>sn_vul_container_image_vulnerable_item | Enthält Details zu jedem Fund und der entsprechenden Schwachstelle. |
| Erkanntes Container-Image<br>sn_vul_container_image | Stellt Informationen zur Image-ID, zum Docker-Image und zum Image-Repository bereit. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. |
| Suche nach Zuordnungen<br>sn_vul_container_finding_m2m_vul_item | M2M-Beziehung der Container-Image-Ergebnisse und der angreifbaren Container-Elemente (CVITs). |
| Angreifbare Elemente automatisch schließen | Enthält die Informationen zum Schließen der veralteten Container-Image-Ergebnisse und zum Rollup des Status zu den CVITs. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| sn_vul_container_image_auto_close_config | |
| Container-Image-Schwachstellenschlüssel<br>sn_vul_container_image_vulnerability_keys | Enthält die Granularitätskonfiguration für die Erstellung von CVITs aus den Container-Image-Ergebnissen. |
| Docker-bezogene Services<br>sn_vul_container_m2m_ci_services | Enthält alle Business Services, die einem Container-Image zugeordnet sind |
| Anzahlen der VR-Container<br>sn_vul_container_vr_container_counts | Enthält den gleitenden Durchschnitt der Containerinstanzen, die in den letzten 90 Tagen aus einem Container-Image gesponnen wurden. |
| Element der Container-Korrekturaufgabe<br>sn_vul_container_m2m_vul_group_item | M2M-Tabelle zwischen CVIT und Container-Korrekturaufgaben. |
| Container-Korrekturaufgabe<br>sn_vul_container_vulnerability | Enthält Container-Korrekturaufgaben |
| Container-Korrekturaufgabe – Manifest<br>sn_vul_container_rt_manifest | Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle nach geplanten Aufgaben durchgeführt. |

### Mit Container Vulnerability Response installierte regelmäßige Aufgaben

Regelmäßige Aufgaben werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Ordnen Sie vorhandene Container-VIs der automatischen Ausnahmeregel zu | Ordnet die automatische Ausnahmeregel automatisch vorhandenen angreifbaren Containerelementen (CVITs) zu. |
| Überprüfen Sie den Ablauf der Zurückstellung des angreifbaren Container-Elements | Sendet Benachrichtigungen, wenn angreifbare Container-Elemente oder Container-Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen). |
| Anzahl der Vulnerability Response-Container (Anwendung – Vulnerability Response und Configuration Compliance for Containers) | Wird täglich ausgeführt, um die Tabelle sn_vul_container_vr_container_counts auszufüllen, die den gleitenden 90-Tage-Durchschnitt für Container berechnet. |
| CVITs automatisch schließen | Schließt automatisch angreifbare Container-Elemente, die der in der Konfiguration für das automatische Schließen definierten Bedingung entsprechen. Ihr Status wird in „Korrigiert“ geändert. |
| Geschäftsrelevanz für CVIT berechnen | Verarbeitet alle aktiven CVITs und aktualisiert das Feld Geschäftsrelevanz basierend auf den betroffenen Services des Docker-Image der CVIT. |
| Schließen Sie CVITs ab, denen kein Docker-Image zugeordnet ist | Lässt CVITs automatisch ablaufen, denen kein CI zugeordnet ist. Ihr Status wird auf Geschlossen und ihr Substatus auf Abgebrochen gesetzt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Berechnet die zugehörigen VI-Anzahlen für die Container-Korrekturaufgabe | Berechnet die Anzahl der Datensätze für Container-Korrekturaufgaben. |
| Rollup der Werte des angreifbaren Containerelements für Schwachstelle und Gruppe | Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Container-Elemente. |

## Container Vulnerability Response Glossar

Erfahren Sie mehr über Begriffe und Konzepte, die für Container Vulnerability Responsespezifisch sind.

## Wichtige Begriffe

**Behälter**

Eine Softwareeinheit, die den Code und alle seine Abhängigkeiten so verpackt, dass die Anwendung nahtlos und zuverlässig von einer Computerumgebung in eine andere ausgeführt wird.

**Container-Image**

Eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann. Ein Container-Image kann nicht geändert werden und kann daher in jeder Umgebung konsistent bereitgestellt werden.

**Cluster**

Eine Reihe von Worker-Computern, die als Knoten bezeichnet werden, auf denen containerisierte Anwendungen ausgeführt werden.

**Docker**

Software zum Erstellen, Bereitstellen und Verwalten von Anwendungscontainern auf Servern und in der Cloud.

**Docker-Bild**

Eine Vorlagendatei, die Code, erforderliche Bibliotheken, Konfigurationen usw. enthält. Die Datei wird zum Starten von Containerinstanzen verwendet. Es besteht aus einer Vereinigung von Dateisystemen mit Ebenen.

**Docker-Datei**

Eine Textdatei, die Anweisungen zum Erstellen von Container-Images durch Hinzufügen mehrerer Ebenen enthält. Beispiel: Überlagerung von Basis-Ubuntu-, Nginx- und App-Code.

**Docker Compose**

Ein Tool zum Definieren und Ausführen komplexer Anwendungen mit Docker. Mit Compose können Sie eine Multi-Container-Anwendung in einer einzelnen Datei definieren.

**Docker-Container**

Ein Docker-Container ist eine Laufzeitinstanz, die von einem Docker-Image gestartet wird.

**Image-Ebene**

Eine Ebene ist eine Änderung an einem Bild. Sie wird durch eine Anweisung in der Docker-Datei dargestellt. Ebenen werden nacheinander auf das Basis-Image angewendet, um das endgültige Image zu erstellen.

**Image-Repository**

Eine Sammlung von Docker-Images mit verschiedenen Tags oder Versionen.

**Bildbezeichnungen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Reihe von Schlüssel-Wert-Paaren, die mit dem Image als Metadaten gespeichert werden.

**Namespace**

Eine von Kubernetes verwendete Abstraktion zur Unterstützung der Isolierung von Ressourcengruppen innerhalb eines einzelnen Clusters.

**Pod**

Eine Reihe von ausgeführten Containern (eine weitere Abstraktion über einem Container).

**Registry**

Einen gehosteten Service, der Repositorys mit Images enthält.

**Service**

Eine abstrakte Methode, um eine Anwendung, die auf einer Reihe von Pods ausgeführt wird, als Netzwerkservice verfügbar zu machen.

**Tag**

Ein Tag ist eine Bezeichnung, die auf ein Docker-Image in einem bestimmten Image-Repository angewendet wird. Tags geben an, wie verschiedene Images in einem Repository voneinander unterschieden werden.

## Formular „Prisma Cloud Compute-Konfiguration“

Auf das Formular „Prisma Cloud Compute-Konfiguration“ wird über das Modul „Prisma Cloud Compute Integration“ zugegriffen.

Um das Formular „Prisma Cloud Compute-Konfiguration“ anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**.

### Konfiguration des Prisma-Cloud-Computings

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Name der neuen Integrationsinstanz.<br><br>Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen. |
| API-Basis-URL | URL für die Integration mit Prisma Cloud Compute. |
| Benutzername | Benutzername für den Zugriff auf Prisma Cloud Compute. |
| Passwort | Passwort für den Zugriff auf Prisma Cloud Compute. |
| MID-Server | Eine Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. Der MID Server ermöglicht die Kommunikation und die Bewegung von Daten zwischen einer ServiceNow -Instanz und externen Anwendungen, Datenquellen und Services. |
| Projekte verwenden | Option zum Konfigurieren der Projekte. Wenn Sie das Kontrollkästchen aktivieren, können Sie Projekte auf der Konfigurationsseite auswählen und die Integrationen basierend auf den Projekten ausführen, die zum Ausfüllen projektspezifischer Details konfiguriert sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Konfiguration des Prisma-Cloud-Computings (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Wenn diese Checkbox aktiviert ist, wird die Registerkarte **Projekte konfigurieren** aktiviert. Klicken Sie auf **Weiter**, um mit der Konfiguration der Projekte fortzufahren. |

## Formular „Ausnahme anfordern“.

Fordern Sie Richtlinienausnahmen mit der Funktion GRC zur Verwaltung von Richtlinienausnahmen in der Anwendung Policy and Compliance Management aus Container Vulnerability Responsean.

Um das Formular „Prisma Cloud Compute-Konfiguration“ anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (oder **Korrekturaufgaben**)>**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |
| Kontrollziel | Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ geändert wird<br>**Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in Policy and Compliance festgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen . |
| Grund | Grund für die Anforderung einer Ausnahme. |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Ausnahmeregel“

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe von angreifbaren Containerelementen (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Um das Formular „Ausnahmeregel“ anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**.

**Formular „Ausnahmeregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Ausnahmeregel. |
| Gültig ab | Datum, ab dem diese Regel aktiv ist, um die CVITs zurückzustellen. |
| Gültig bis | Datum, ab dem die Korrekturaufgabe keine neuen CVITs mehr akzeptiert. |
| Grund | Grund für die Erstellung dieser Ausnahmeregel. |
| Zuweisungsgruppe | Gruppe, der die Korrekturaufgabe zugewiesen ist, die für die Nachverfolgung der zurückgestellten CVITs erstellt wurde. |
| Zusätzliche Informationen | Zusätzliche Informationen, die die anfordernde Person dem Genehmiger zur Verfügung stellen möchte. Diese Informationen werden in das Beschreibungsfeld der Korrekturaufgabe eingetragen. |
| Bedingung | Filterbedingung für die CVITs, die während der Verarbeitung der CVITs definiert werden kann. |
| Für vorhandene Daten ausführen | Option, mit der Sie diese Regel für vorhandene Daten ausführen können, wenn sie zum ersten Mal ausgeführt wird. |
| Workflow-Phase | Aktueller Genehmigungsstatus der Ausnahmeregel. |
| Status | Status der Ausnahmeregel. |
| Ausführungsbefehl | Eindeutige Reihenfolge für jede Ausnahmeregel. |
| Zurückgestellt bis | Datum, bis zu dem die VULs und CVITs zurückgestellt werden. An diesem Datum wird die erstellte VUL geschlossen, alle CVITs werden aus der Gruppe verschoben und die Gruppenregeln werden erneut angewendet. |



## Configuration Compliance

Die Anwendung ServiceNow® Configuration Compliance ist eine SCA-Anwendung (Secure Configuration Assessment), die Scan-Ergebnisse aus Integrationen mit Konfigurations-Scan-Anwendungen von Drittanbietern zusammenfasst. Sie können Konfigurations-Compliance-Probleme mit Configuration Management Database (CMDB)priorisieren. Configuration Compliance ist eng in den IT-Change-Management-Prozess integriert, um nicht konforme Konfigurationen zu korrigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

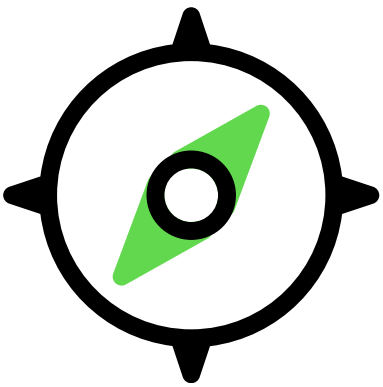
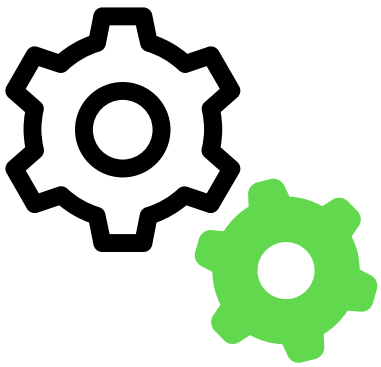
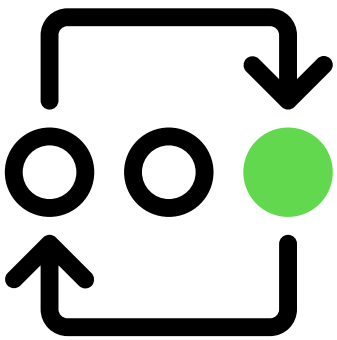
| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Ab Version 18.0 von Vulnerability Responsekönnen Sie Konfigurationsprobleme in Vulnerability Manager Workspace und IT Remediation Workspace überwachen und beheben. Weitere Informationen finden Sie unter Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

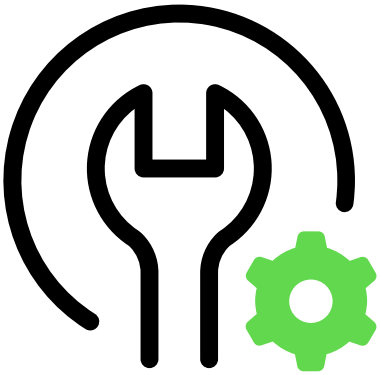
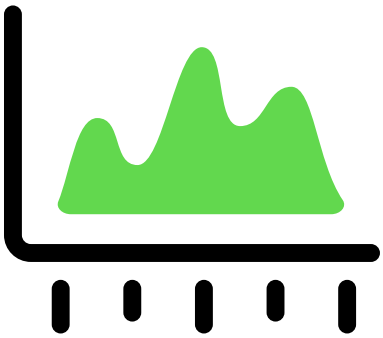
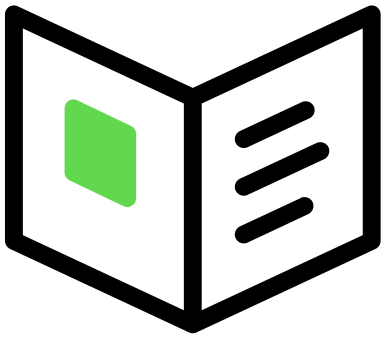
**Configuration Compliance**

| Erkunden | Konfigurieren | integrieren |
|---|---|---|
|  |  |  |
| Erfahren Sie mehr über die Konzepte und Funktionen von Configuration Compliance | Konfigurieren Sie Configuration Compliance | Erweitern Sie Configuration Compliance durch die Integration mit anderen Anwendungen |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Configuration Compliance (Fortsetzung)**

| Beheben | Analysen und Berichte | Referenz |
|---|---|---|
|  |  |  |
| Erfahren Sie, wie Sie nicht konforme Assets mit Configuration Compliance korrigieren können | Zeigen Sie Configuration Compliance-Analysen an | Rufen Sie Details zu Configuration Compliance-Komponenten wie Feldern, Tabellen und Eigenschaften ab |



## Configuration Compliance erkunden

Verwenden Sie Testergebnisse aus SCA-Integrationen (Secure Configuration Assessment) von Drittanbietern, um die Compliance mit Sicherheits- oder Unternehmensrichtlinien zu überprüfen. Identifizieren, priorisieren und beheben Sie nicht konforme Konfigurationselemente.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

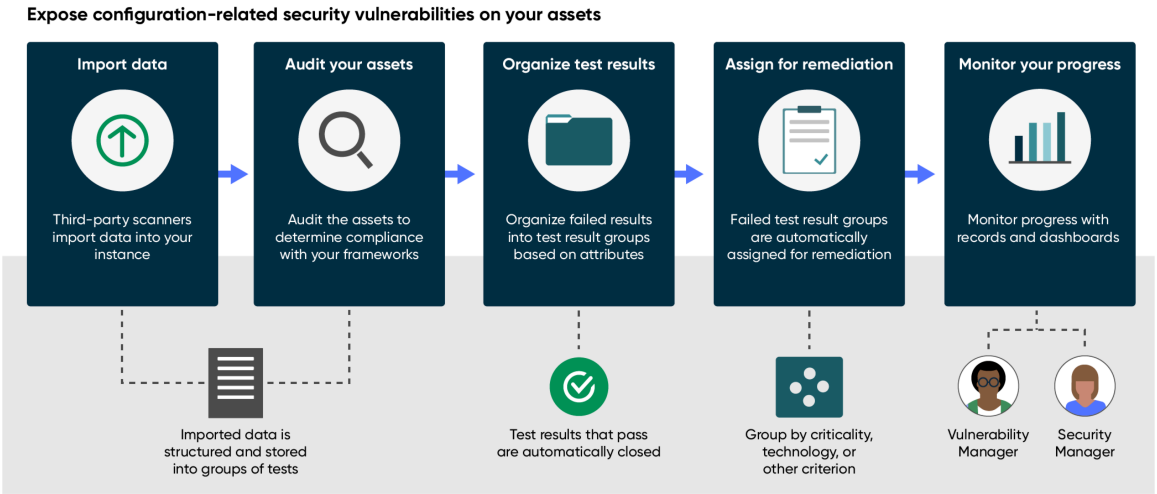
### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Configuration Compliance – Beschreibung

Mit der Anwendung ServiceNow® Configuration Compliance können Sie die kritischsten konfigurationsbezogenen Schwachstellen in Ihrer Umgebung schnell und effizient priorisieren und beheben. Configuration Compliance ist per Abonnement im ServiceNow® Store] verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Hauptfunktionen von Configuration Compliance

Verwenden Sie Configuration Management Database (CMDB) in Ihrem Now Platform®, um die wichtigsten konfigurationsbezogenen Sicherheitsschwachstellen verfügbar zu machen und zu beheben. Konzentrieren Sie Ihre Korrekturressourcen auf Aktivitäten mit der größten Risikominderung. Optimieren Sie den Korrekturprozess für Sicherheit, IT und Ihre Geschäftsprozess-Stakeholder. Die Anwendung Configuration Compliance enthält die folgenden Hauptfunktionen:

- Mit unterstützten Drittanbieterintegrationen werden automatisch Richtlinien, Tests, autoritative Quellen und Technologien importiert. Weitere Informationen zu unterstützten Integrationen finden Sie unter Configuration Compliance-Integrationen.
- Korrelieren Sie Richtlinien und Tests mit Konfigurationselementen (Assets), um konfigurationsbezogene Schwachstellen zu identifizieren und um sicherzustellen, dass Ihre Assets den Richtlinien und Kontrollen entsprechen.
- Vereinheitlichen Sie die Konfigurationsbewertung, -zuweisung und -korrektur für alle Ihre Assets.
- Konfigurations-Scan-Inhalte können aus führenden SCA-Ökosystem-Integrationsanwendungen (Secure Configuration Assessment) importiert werden.
- Konfigurationsergebnisse, Testfehler, können basierend auf den Kompetenzen des Korrekturspezialisten und den Zuständigkeitsbereichen gruppiert und automatisch weitergeleitet werden. Intelligente Workflows und eine enge Integration mit Change Management sorgen für reibungslose Aufgabenübergaben zwischen Gruppen.
- Bei Verwendung mit der Anwendung ServiceNow Governance, Risk und Compliance (GRC) kann für Konfigurationstests in Configuration Compliance ein Rollup zu den entsprechenden GRC-Steuerungen durchgeführt werden.
- Erstellen Sie mit dem erweiterten Change-Management vorab ausgefüllte Change-Anforderungen für die IT direkt aus Configuration Compliance, um Sie bei Ihren Korrekturaufgaben zu unterstützen, die zusätzliche Ressourcen erfordern.
- Mit Dashboards können Sie Metriken zum Korrekturstatus in Testergebnisgruppen, Compliance-Tests und Richtliniendatensätzen anzeigen.

## Configuration Compliance – Benutzer

Configuration Compliance -Aktivitäten können viele Managementebenen betreffen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Systemadministratoren
- Schwachstellenadministratoren
- Schwachstellenmanager
- Schwachstellenanalysten
- Compliance-Administratoren

Configuration Compliance -Aufgaben umfassen die folgenden Rollen.

- sn_vulc.admin – kann lesen, schreiben, löschen
- sn_vulc.write – kann lesen und schreiben
- sn_vulc.remediation_owner – Kann zugewiesene Datensätze lesen und aktualisieren

**Hinweis:**
Die Rolle „sn_vulc.remediation_owner“ wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle „itil“ zugewiesen wird.

- sn_vulc.read – Kann lesen

## Configuration Compliance und Security Operations

Wenn Qualys Vulnerability Integration und Tenable Vulnerability Integration installiert sind, wird der Zugriff auf Vulnerability Response verfügbar. Sie können mehrere Bereitstellungen dieser Integrationen haben. Daten aus jeder Bereitstellung werden identifiziert und sind in einer einzigen Instanz von GRCverfügbar.

## Verfügbare Versionen für Washington DC

| Release-Version | Versionsinformationen |
|---|---|
| Configuration Compliance v14.7, v14.8, v14.9 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Configuration Compliance importierte Daten

Die Anwendung Configuration Compliance importiert Richtlinien, Tests, autoritative Quellen und Testergebnisse aus Drittanbieterintegrationen und speichert sie in Modulen zur Ansicht.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Unterstützte Integrationen

Drittanbieterintegrationen importieren Konfigurationsbewertungsergebnisse, Richtlinien, Tests, Technologien, autoritative Quellen und Testergebnisse in die Anwendung Configuration Compliance. Schwachstellenmanager oder Schwachstellenanalysten können diese Daten verwenden, um konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.

Weitere Informationen zu unterstützten Integrationen finden Sie unter Configuration Compliance-Integrationen.

## Richtlinien

Richtlinien beziehen sich auf autoritative Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Richtlinien. Richtlinien sind in der Regel an einer Technologieklasse ausgerichtet, z. B. Windows, Oracle-Datenbanken, Cisco IOS, und werden häufig vom primären Branchenstandard abgeleitet. Richtlinien können an die Anforderungen der Organisation angepasst werden. Ein einzelner Konfigurationstest kann mehreren Richtlinien angehören.

## Tests

Tests sind Bibliotheken von Datensätzen, die Scans von Computer-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets verwaltet werden soll.

Ein Configuration Compliance -Test ist der Mechanismus, den Integrationsanwendungen von Drittanbietern verwenden, um Assets nach Schwachstellentyp zu gruppieren. Einige VA-Scanlösungen von Drittanbietern wie Qualys verfügen über sehr große Testbibliotheken (bis zu 8.000), die Richtlinien und „Frameworks“ autoritativer Quellen zugeordnet sind.

Ein Test kann viele Werte haben, Eins-zu-Viele, erwartet im Vergleich zu tatsächlichen Werten usw. Ein Test ist alles, was verwendet werden kann, um eine Klasse von Software- oder Hardware-Assets zu identifizieren, die nicht konform ist. Zum Beispiel eine Release- oder Hardwarenummer.

| Integration | Beschreibung |
|---|---|
| Qualys Vulnerability Integration | Die geplante Aufgabe **Qualys PC Controls**ruft die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Steuerungen**.<br><br>**Hinweis:**<br>Wenn Sie die Integration manuell ausführen möchten, führen Sie **Qualys PC-Steuerungen** nach **Qualys PC-Richtlinien**aus. |
| Tenable Vulnerability Integration | Die regelmäßige Aufgabe Tenable.io Compliance-Ergebnisintegration importiert Konfigurationstests (Tests).<br><br>Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integration | Beschreibung |
| --- | --- |
| | Integrationen in der folgenden Reihenfolge aus, bis Sie alle ignorierten Assets mit Bewertungsdaten abgeglichen haben:<br>• Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnissen<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br>• Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br><br>Um den Konfigurationstestdatensatz anzuzeigen, navigieren Sie zu **Configuration Compliance** > **Tests**. Im Datensatz werden importierte Daten im Feld **Kurzbeschreibung** und auf den Registerkarten Korrekturstatus, Beschreibung und Korrektur angezeigt. Daten werden auch in den zugehörigen Links **Zitate**, **Richtlinien**und **Testergebnisse** angezeigt. |

## Technologien

Eine der Techniken, die von Schwachstellenscannern von Drittanbietern zum Erstellen von Testgruppen von Software- und Hardware-Konfigurationselementen für die Analyse verwendet werden, besteht darin, sie nach Technologie zu organisieren. Technologien sind eine importierte Bibliothek von Betriebssystemen, Netzwerkgeräten, Datenbanken und Apps, die Richtlinien zugeordnet sind. Tests haben mehrere Implementierungen für verschiedene Technologien. Die Fehlerkorrektur ist auch technologiespezifisch.

Sie können die anwendbaren Technologien für einen Test anzeigen, um besser zu verstehen, auf welche Arten von Software- oder Hardware-Assets die Steuerung angewendet werden kann. Beispiele für Technologien, die auf Steuerungen angewendet werden können, sind CentOS 7.x, Windows 8.1, Windows 2016 Server usw. Die Liste der Technologien ist schreibgeschützt und entspricht den in der Anwendung Qualys Cloud Platform definierten Technologien.

Technologien werden nur für datenbankbezogene Konfigurationsbewertungen importiert. *db_type* (sofern nicht leer) im Import wird zum Erstellen einer Technologie verwendet. Zeigen Sie Technologien an, die im Abschnitt „Technologien“ in Konfigurationstestdatensätzen, Testergebnisdatensätzen, Richtliniendatensätzen und in ausgefüllt sind **Configuration Compliance** > **Unterstützungsdaten** > **Technologien**.

## Autorisierende Quellen

Configuration Compliance verwendet autoritative Quellen und Zitate, wenn Schwachstellenwarnungen für Tests generiert werden. Autorisierende Quellen sind in der Regel Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. „NIST 800-53 Version 3 (2009) 3: 2009, SA-4“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
In Qualys Vulnerability Integrationwird diese Kombination als -Framework bezeichnet.

Autorisierende Quellen und Zitate (auch als Mandate bezeichnet) werden aus den Schwachstellenscannern von Drittanbietern importiert.

Autorisierende Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -verfahren. Konfigurationstests können durch Bezugsvermerke auf mehrere autoritative Quellen verweisen. Autorisierende Quellen können in Vorbereitung auf ein Audit über die Compliance für einen bestimmten Standard berichten.

| Integration | Beschreibung |
|---|---|
| Qualys Vulnerability Integration | Die regelmäßige Aufgabe **Qualys PC-Richtliniendetails**ruft die autorisierenden Quellen und Bezugsvermerke ab. Sie können diese regelmäßige Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Richtliniendetail**.<br>**Hinweis:**<br>Wenn Sie die Integration manuell ausführen möchten, führen Sie **Qualys PC-Richtliniendetails** nach **Qualys PC-Richtlinien**aus. |
| Tenable Vulnerability Integration | Die regelmäßige Aufgabe Tenable.io Compliance-Ergebnisintegration importiert autoritative Quellen als Teil von Zitatdaten.<br>Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie alle ignorierten Assets mit Bewertungsdaten abgeglichen haben:<br>• Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnissen<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br>• Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br>Daten werden über den zugehörigen Link **Zitate** in Konfigurationstestdatensätzen angezeigt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Testergebnisse

Configuration Compliance berechnet die Testergebnisse nicht, sondern importiert sie als Teil einer Drittanbieterintegration. Sobald sie in Configuration Complianceangezeigt werden, werden sie mithilfe von **Korrekturaufgaben korrigiert**. Weitere Informationen finden Sie unter Configuration Compliance Korrelation.

| Integration | Beschreibung |
|---|---|
| Qualys Vulnerability Integration | Sie können die Testergebnisse auf eine der folgenden Arten abrufen:<br>• Die regelmäßige Aufgabe **Qualys PC-Ergebnisse**ruft die Testergebnisse ab. Sie können diese regelmäßige Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys PC-Ergebnisse**.<br>**Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie **Qualys PC-Ergebnisse** nach **Qualys PC-Richtlinien** und **Qualys PC-Richtliniendetails aus**.<br>Beim Import von **Qualys PC-Ergebnissen** wird der Parameter `Start Time` auf der Registerkarte „ **Integrationsdetails**“ verwendet. Alle anderen Configuration Compliance -Importe übernehmen alle verfügbaren Daten unabhängig von `Start Time`.<br>Wenn der Import der **Qualys PC-Ergebnisse** abgeschlossen ist, wird ein Event ausgelöst, um Berechnungen für das Importende auszulösen. Weitere Informationen finden Sie unter Configuration Compliance Status.<br>• Alternativ können Sie ab V14.5 auch die folgenden Integrationen ausführen, um die Testergebnisse abzurufen: |
| Tenable Vulnerability Integration | Die regelmäßige Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Testergebnisse.<br>Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie alle ignorierten Assets mit Bewertungsdaten abgeglichen haben: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integration | Beschreibung |
|---|---|
| | • Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnissen<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br>• Tenable.io Assets-Integration<br>• Tenable.io Integration von Compliance-Ergebnisauffüllung<br><br>Um den Konfigurationstestdatensatz anzuzeigen, navigieren Sie zu **Configuration Compliance** > **Testergebnisse**. Im Datensatz werden importierte Daten in den Feldern**Test**und **Configuration Item** angezeigt. Daten werden auch auf den Registerkarten **Erwartete Werte**, **Tatsächliche Werte**und **Fehlerkorrektur** angezeigt. Die zugehörigen Links **„Testergebnisgruppen“** und **„Testergebnisverlauf“** werden ausgefüllt. |

### Erkennung von Configuration Compliance

Configuration Compliance -Daten werden aus SCA-Scanneranwendungen von Drittparteien importiert. Sie strukturieren Gruppen von Software- und Hardwaretests in Datensätzen, um die Durchführung von Bewertungen zu beschleunigen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Wenn ein Import abgeschlossen ist, wird ein Event gesendet, um die Aktionen für das Importende anzuzeigen. Für jede aktive Testergebnisgruppe werden die folgenden Aktionen ausgeführt:

- Aufgelöste Gruppen mit fehlgeschlagenen Ergebnissen kehren in den Status **„Warten auf Implementierung“** zurück.
- Testergebnisgruppen, bei denen alle Ergebnisse bestanden haben, sind **Geschlossen**.
- Der Status der Testergebnisse in aktiven Gruppen wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Gruppe ist, wird aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Configuration Compliance Korrelation

Configuration Compliance bietet Priorisierung und Gruppierung von Testergebnissen, um die Behebung von Nicht-Compliance-Problemen zu unterstützen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Asset-orientierte Priorisierung

Konfigurationsscans können eine große Anzahl von Ergebnissen erzeugen. Priorisieren Sie die Ergebnisse, um die maximale Risikominderung zu erzielen. Die Priorität umfasst sowohl die Konfigurationstestrelevanz als auch die Asset-Relevanz. Die Priorität des Konfigurationstestergebnisses wird als Risikopunktzahl zwischen 0 und 100 ausgedrückt. Rechnergruppen berechnen die Risikopunktzahl und können angepasst werden.

Wenn der Import der Drittpartei abgeschlossen ist, sendet Configuration Compliance ein Event, um Aktionen für das Importende anzugeben. Für jede aktive Ergebnisgruppe werden die folgenden Aktionen ausgeführt:

- Aufgelöste Gruppen mit fehlgeschlagenen Ergebnissen kehren in den Status **„Warten auf Implementierung“** zurück.
- Gruppen, in denen alle übergebenen Ergebnisse **Geschlossen**sind.
- Der Status der Testergebnisse in aktiven Gruppen wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Gruppe ist, wird aktualisiert.

## Rangfolge der Korrekturaufgaben

Wenn Testergebnisse zu mehr als einer Gruppe gehören, wird der **Status** eines Testergebnisses anhand einer Rangfolge abgeleitet.

Die **Felder** Status und **Auflösung** im Formular „ **Konfigurationstest“** und das Feld **Ergebnis** im Formular „ **Testergebnis“** werden nach dieser Rangfolge berechnet.

**Hinweis:**

Die Rangfolge der Gruppenmitgliedschaft gilt nur für Elemente, bei denen das Element den Konfigurationstest nicht bestanden hat. **Übergebene** Elemente befinden sich immer im Status „ **Geschlossen – Repariert** “.

Der **Ergebniswert** bestimmt den Status. Gruppen im Status „ **Geschlossen – Repariert“** und **„Geschlossen – Abgebrochen“** werden ignoriert. Der Elementstatus wird aus den Status aller anderen Korrekturaufgaben berechnet, zu denen er gehört, oder auf **Offen**gesetzt, wenn keine andere Gruppe für den Artikel vorhanden ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Order of Precedence for Test Results belonging to multiple Test Result Groups | | | | | | |
|---|---|---|---|---|---|---|
| **Group A** | **Group B** | | | | | |
| | **Open** | **Under Investigation** | **Awaiting Implementation** | **Resolved** | **Deferred** | **Closed-Invalid** |
| **Open** | Open | Under Investigation | Awaiting Implementation | Resolved | Deferred | Closed-Invalid |
| **Under Investigation** | Under Investigation | Under Investigation | Awaiting Implementation | Resolved | Deferred | Closed-Invalid |
| **Awaiting Implementation** | Awaiting Implementation | Awaiting Implementation | Awaiting Implementation | Resolved | Deferred | Closed-Invalid |
| **Resolved** | Resolved | Resolved | Resolved | Resolved | Deferred | Closed-Invalid |
| **Deferred** | Deferred | Deferred | Deferred | Deferred | Deferred | Closed-Invalid |
| **Closed-Invalid** | Closed-Invalid | Closed-Invalid | Closed-Invalid | Closed-Invalid | Closed-Invalid | Closed-Invalid |

## Erstellung von Korrekturaufgaben

Configuration Compliance Korrekturaufgaben werden manuell erstellt.

Es gibt zwei Möglichkeiten, Korrekturaufgaben zu erstellen und **auszufüllen**.

- Über das **Modul „Korrekturaufgaben“** und mithilfe von Filtern, die die Registerkarte „ **Testergebnisse** “ automatisch ausfüllen.

  Diese Methode ist nützlich, wenn Sie wissen, welche Filterung Sie verwenden möchten. Zum Beispiel die Erfassung aller fehlgeschlagenen Testergebnisse mit mittlerer und höherer Relevanz, die sich auf die Windows-basierte Infrastruktur auswirken und nur für die SAP-Lieferkettenanwendung gelten.

- Durch Auswahl von Testergebnissen in der Liste „ **Testergebnisse** “ und Erstellen einer Gruppe aus dem Menü **Aktionen für ausgewählte Zeilen...**

  Diese Methode eignet sich für Ergebnisse, die nicht einfach gefiltert werden können, oder für Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten. Zum Beispiel Ausreißer, die nichts gemeinsam haben.

### Hinweis:

Wenn Sie eine Gruppe aus der Liste „ **Testergebnisse** “ erstellen und sich später entscheiden, einen Filter für diese Gruppe zu verwenden, werden Ihre ursprünglichen Einträge entfernt und durch die Filterergebnisse ersetzt.

## Nicht gruppierte Testergebnisse

**Nicht gruppierte Testergebnisse** enthalten alle nicht bestandenen Testergebnisse, die keine Mitglieder einer aktiven (nicht**geschlossenen**) Gruppe sind. Dieses Modul wird nach jedem Import und immer dann aktualisiert, wenn Testergebnisse einer Gruppe hinzugefügt oder daraus entfernt werden.

### Erkannte Elemente für Configuration Compliance

Assets werden mithilfe von CI-Suchregeln automatisch mit Konfigurationselementen (CIs) abgeglichen, wenn sie mithilfe der Host- und Testergebnisintegrationen importiert werden. Erkannte Elemente geben Ihnen Einblick, wie die Asset-Identifizierung CIs in der CMDBzugeordnet wird.

Erkannte Elemente werden als **abgeglichen**, nicht **abgeglichen**oder **neu klassifiziert**betrachtet. Identifizierte CIs befinden sich im Status **Abgestimmt**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Suche nach potenziellen Übereinstimmungsproblemen zu erleichtern, wird die CI-Suchregel, die mit dem **CI übereinstimmt,** im Feld CI-Übereinstimmungsregel angezeigt.

**Hinweis:**
Die Unterstützung von**CI-Übereinstimmungsregelfeldern** ist nur für die Qualys -Integration verfügbar.

Wenn keine Übereinstimmung gefunden wurde, wird ein CI in der nicht *abgeglichenen CI* -Klasse [sn_sec_cmn_unmatched_ci], [cmdb_ci_unclassed_hardware]oder [cmdb_ci_incomplete_ip] von CMDBerstellt. Wenn das ursprüngliche nicht abgeglichene CI neu klassifiziert wurde, werden die Datensätze für erkannte Elemente aktualisiert, um diesen Status widerzuspiegeln. Weitere Informationen finden Sie unter Nicht abgeglichene CIs und Nicht abgeglichene Konfigurationselemente anzeigen und neu klassifizieren.

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Das Modul listet nicht abgeglichene Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in „Erkannte Elemente“ finden Sie unter Formularfelder „Erkannte Elemente“.

### CI-Änderungen für erkannte Elemente für Configuration Compliance

Der Standardwert der Eigenschaft sn_sec_cmn.update_on_ci_change ist true. Wenn also das Konfigurationselement (CI) für ein erkanntes Element aktualisiert wird, werden auch die Testergebnisse aktualisiert.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die externe ID für das Testergebnis wird aktualisiert, und die Risikopunktzahl, Zuweisungsregeln, Gruppenregeln und Korrekturzielregel werden neu ausgewertet. Wenn ein Testergebnis mit demselben Test und CI vorhanden ist, werden die Testergebnisse mit dem vorhandenen Testergebnis aktualisiert, und das aktuelle Testergebnis wird mit dem Substatus ungültigCIgeschlossen. Arbeitsnotizen werden entsprechend hinzugefügt.

Wenn Sie das CI für das vorhandene Testergebnis nicht aktualisieren möchten, legen Sie die Eigenschaft auf false fest. In diesem Fall wird bei Änderung eines CI ein neues Testergebnis erstellt und das vorhandene als ungültigesCI geschlossen.

### Gleichen Sie nicht abgeglichene erkannte Elemente für ab Configuration Compliance

Erstellen Sie eine regelmäßige Aufgabe, um nicht abgeglichene erkannte Elemente abzugleichen. Wenn ein Testergebnis erstellt wird, ist das Konfigurationselement (CI), das zum Zeitpunkt der Erstellung hinzugefügt wurde, möglicherweise veraltet.

**Vorbereitungen**
Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Wenn sich die Informationen in der CMDB ändern, werden nicht abgeglichene CI-Informationen nicht abgeglichen. Wenden Sie zum Abgleichen CI-Suchregeln auf die Testergebnisse an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.

Eine regelmäßige Aufgabe wird bei Bedarf ausgeführt, um die CI-Übereinstimmungsregel für die erkannten Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach der erneuten Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Testergebnisse werden ebenfalls aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente für Configuration Compliance.

### Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge > Nicht abgeglichene erkannte Elemente abgleichen**.
2. Klicken Sie auf der Seite „Hintergrundaufträge“ auf **Abgleichsauftrag erstellen**.
3. Füllen Sie die Felder des Formulars aus.

**Hinweis:**
Sie können nur das Feld Parameter bearbeiten.

#### Hintergrundauftrag

| Feld | Beschreibung |
|---|---|
| Nummer | Eindeutige Auftragsnummer. |
| Erstellt von | Benutzer, der die Aufgabe erstellt hat. |
| Parameter | Parameter zum Abgleichen der nicht abgeglichenen erkannten Elemente:<br>○ limit: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen.<br>○ firstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichprozess mit dem ersten erkannten Element. |
| Status | Aktueller Status des Hintergrundauftrags. |
| Statusbeschreibung | Beschreibung des aktuellen Status des Hintergrundauftrags. |
| Auftragstyp | Typ des Auftrags. Der Wert ist **Nicht abgeglichene erkannte Elemente abgleichen**. |
| Gestartet um | Zeit, zu der der Auftrag gestartet wurde. |
| Endete um | Zeitpunkt, zu dem der Auftrag abgeschlossen wurde. |
| Auftragsdauer | Gesamtzeit, die für den Abschluss der Aufgabe benötigt wurde. |
| Substatus | Substatus für den ausgewählten Status. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Notizen | Anzahl der verarbeiteten Datensätze. |

4. Klicken Sie auf **Absenden**.

**Hinweis:**

- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen**.
- Sie können nicht abgeglichene CIs nicht abgleichen oder CI-Suchregeln erneut anwenden, während Sie Hosts oder Testergebnisse importieren.

### Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente für an Configuration Compliance

Wenden Sie Suchregeln für Konfigurationselemente (CIs) erneut auf ausgewählte erkannte Elemente aus der Listenansicht der erkannten Elemente an und wählen Sie Aktionen aus. Der Administrator muss möglicherweise eine Suchregel aus mehreren Gründen bearbeiten oder aktualisieren. Wenn sich die Suchregel ändert, können sie sie erneut auf die erkannten Elemente anwenden.

#### Vorbereitungen

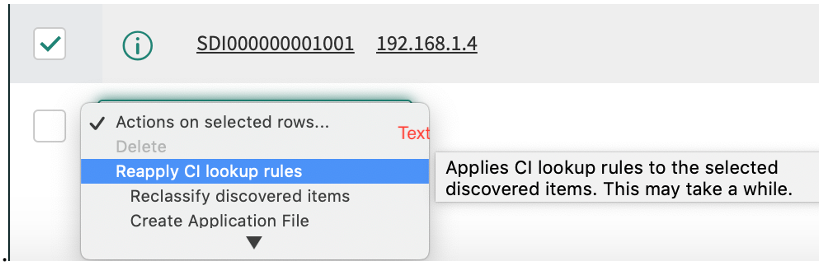
Erforderliche Rollen:

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn sich das CI nach der erneuten Anwendung der CI-Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI und den Testergebnissen aktualisiert. Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente für Configuration Compliance.

#### Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge** > **CMDB** > **Erkannte Elemente**.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie **auf Aktion für ausgewählte Zeilen**.




3. Wählen Sie in der Liste **CI-Suchregeln erneut anwenden** aus.

   Die Regeln werden auf diese erkannten Elemente erneut angewendet.

### Tenable Vulnerability Integration mit Configuration Compliance

Das Produkt Tenable.io von Tenable Vulnerability Integration importiert Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests zur Verarbeitung in der Anwendung Configuration Compliance.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Tenable.io

Tenable Vulnerability Integration wird unterstützt.

Sie können importierte Daten verwenden, um:

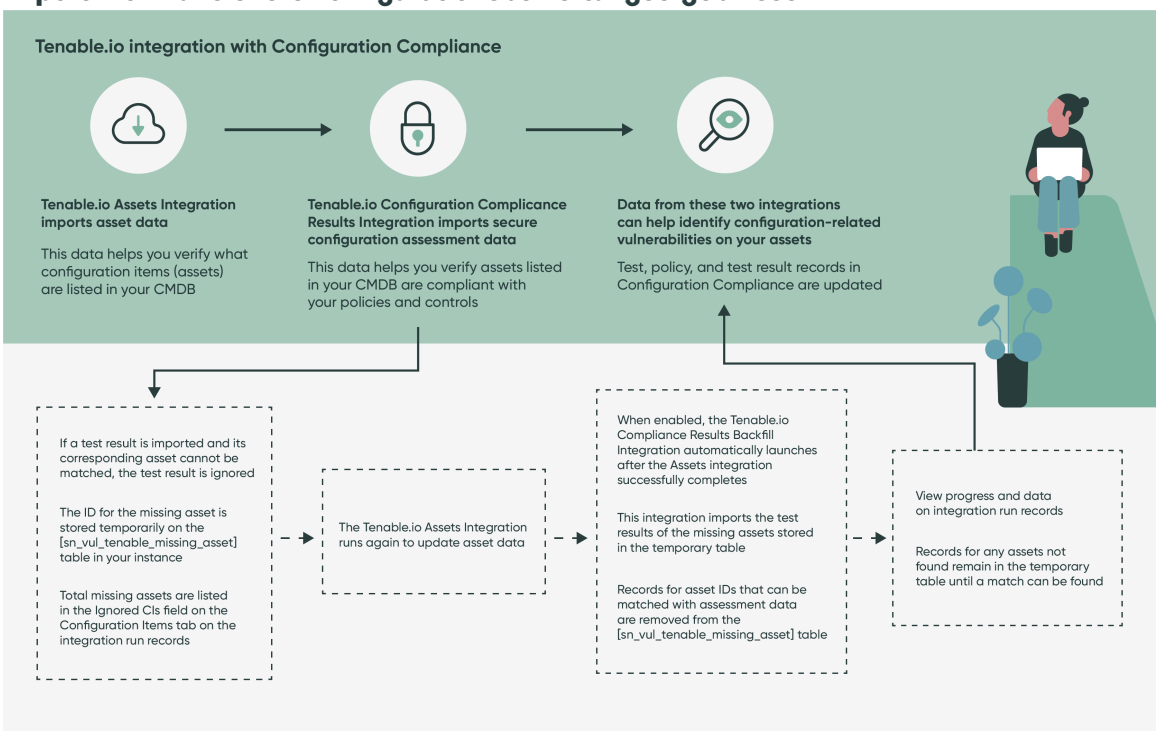
- Identifizieren Sie konfigurationsbezogene Schwachstellen in Ihren Assets, die in Ihrem aufgeführt sind Configuration Management Database (CMDB)
- Vergewissern Sie sich, dass Ihre Assets Ihren Richtlinien und Kontrollen entsprechen.

Asset-Daten, Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests werden mit den folgenden Integrationen importiert:

- Tenable.io Assets-Integration
- Tenable.io Integration von Compliance-Ergebnissen
- Tenable.io Integration von Compliance-Ergebnisauffüllung

Die folgende Abbildung zeigt, wie die Integrationen zusammenarbeiten, um Asset- und Konfigurationsbewertungsdaten zu importieren und alle ignorierten CIs abzugleichen, die während eines Imports übersehen wurden.

**Import-Flow für sichere Konfigurationsbewertungsergebnisse**






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten werden importiert, aktualisiert und in den Testergebnissen, Richtlinien und Konfigurationstestdatensätzen in der Anwendung Configuration Compliance angezeigt.

In einigen Fällen unterscheidet sich die Anzahl der importierten Konfigurationselemente (CIs) für die Tenable.io Assets-Integration und die Tenable.io Compliance-Ergebnisintegration. In diesem Fall werden temporäre Datensätze erstellt und für die ignorierten Asset-IDs gespeichert. Diese Datensätze können später mit importierten Bewertungsdaten durch Importe aus der Compliance-Ergebnisauffüllungsintegration abgeglichen werden.

Angenommen, die Assets-Integration importiert 80 Assets in einer Integrationsausführung, die Compliance-Ergebnisintegration jedoch 100.

**Hinweis:**
Sie können die Anzahl der ignorierten CIs bei Integrationsausführungen überprüfen, indem Sie zu navigieren **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**. Klicken Sie auf den Namen einer Integration, um den Datensatz zu öffnen. Öffnen Sie im zugehörigen Link „Ausführungen der **Schwachstellenintegration** “ einen Integrationsausführungsdatensatz, und wählen Sie die **Registerkarte** Elemente aus, um den Wert im Feld **Ignorierte CIs anzuzeigen**. Dieses Feld verfolgt die Gesamtzahl der ignorierten (fehlenden) Assets aus dem Import.

Durch den Vergleich von Werten in den Feldern **„Ignorierte CIs“** in jedem Integrationsausführungsdatensatz ergibt sich eine Differenz von 20 ignorierten CIs. Daher wird die Auffüllungsintegration automatisch ausgeführt, wie in der vorherigen Abbildung dargestellt. Diese Integration importiert die Konfigurationsbewertungsinformationen für die zusätzlichen 20 Assets, die von der Compliance-Ergebnisintegration gefunden, aber von der Asset-Integration übersehen wurden. Da Bewertungsdaten für fehlende Assets nicht importiert werden, importiert die Tenable.io Compliance-Ergebnisauffüllungsintegration bis zu 200 Asset-IDs pro Integrationsausführung, um die fehlenden Assets mit den entsprechenden Bewertungsdaten abzugleichen. Alle Datensätze, die für fehlende oder ignorierte Assets erstellt und in der temporären Tabelle aufgelistet werden, werden gelöscht, nachdem diese Assets und ihre Daten abgeglichen wurden.

**Hinweis:**
Es kann mehrere Ausführungen dieser Integrationen erfordern, um alle ignorierten Assets zu importieren.

Weitere Informationen zum Aktivieren und Konfigurieren der Tenable.io Asset-Integration finden Sie unter Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten. Weitere Informationen zur Integration finden Sie unter Die Tenable Vulnerability-Integration verstehen.

Tenable.io Integration von Compliance-Ergebnissen und Tenable.io Integration von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste Tenable Integrations (Vertretbare Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen können.

## CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Configuration Compliance Schwachstellenintegrationen von Drittparteien

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Configuration Compliance automatisch Hostdaten, um nach Übereinstimmungen in Configuration



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Management Database (CMDB)zu suchen. Dies geschieht mithilfe von **CI-Suchregeln**. Diese Regeln werden verwendet, um Konfigurationselemente (CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Fehlerkorrektur zu unterstützen.

Beim Importieren von Assets wird zuerst in der Liste „ **Erkannte Elemente** “ anhand von Drittpartei-IDs gesucht, um Übereinstimmungen mit Konfigurationselementen (CIs) aus vorherigen Importen zu finden. Wenn eine Übereinstimmung mit der Host-ID gefunden wird, wird sie als Feld **Konfigurationselement** im Testergebnisdatensatz verwendet.

Sie können mithilfe der Liste „ **Erkannte** Elemente“ sehen, wie importierte Assets CIs zugeordnet werden. Wenn keine Übereinstimmung gefunden wird oder das Feld cmdb_ci leer ist, verwenden die Regeln die anderen Hostinformationen, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als Nicht **abgeglichenes CI**gekennzeichnet. Weitere Informationen zum Umgang mit diesen CIs finden Sie unter Nicht abgeglichene CIs.

Ein neues erkanntes Element wird erstellt und diesem CI zugeordnet.

**Hinweis:**
CI-Suchregeln sind nur für Qualys Integration for Security Operations verfügbar.

CI-Suchregeln können domänengetrennt sein und sind quellenspezifisch. Jede Quelle kann mehrere Bereitstellungen haben. Qualys kann mehrere Bereitstellungen der Qualys-Integration haben. Jede Bereitstellung verfügt über eigene CI-Suchregeln.

**Hinweis:**
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenintegration gemeinsam genutzt. Wenn eine Regel gelöscht oder geändert wird, wirkt sich die Löschung oder Änderung auf alle Bereitstellungen der Schwachstellenintegration aus.

Wenn Sie eine Übereinstimmung versuchen, ist der erste Schritt eine Lieferanten-ID-Suche nach einer genauen Übereinstimmung für Quelle, source_instance und Lieferanten-ID. Dann werden Suchregeln der Reihe nach ausgeführt, von der niedrigsten zur höchsten, und angehalten, wenn eine Regel nur ein einzelnes CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

**Hinweis:**
Um eine Übereinstimmung mit Low-Level-Netzwerkelementen zu vermeiden, wird das übergeordnete CI zurückgegeben, wenn ein übereinstimmendes CI `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`oder `cmdb_ci_ip_address`ist.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist beim Upgrade nicht verfügbar. Informationen zum Upgrade und Anweisungen zum Festlegen der Eigenschaft finden Sie unter CI-Klassen ignorieren.

Um die Suche nach Übereinstimmungsproblemen zu erleichtern, wird die CI-Suchregel, anhand derer eine Übereinstimmung gefunden wird, dem Datensatz „Erkanntes Element“ im Feld „ **CI** -Übereinstimmungsregel“ hinzugefügt. Suchregeln werden zuerst nach dem niedrigsten Wert für die **Reihenfolge** ausgewertet.

Diese Qualys CI-Suchregeln werden mit dem Basissystem geliefert.

- QUALYS-HOST-ID
- FQDN
- NetBIOS



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- DNS
- IP

Diese Microsoft Defender CI-Suchregeln werden mit dem Basissystem geliefert.

- S3-Bucket
- Name
- Ressourcen-ID

Diese Palo Alto Prisma Cloud CI-Suchregeln werden mit dem Basissystem geliefert.

- S3-Bucket
- Name
- Ressourcen-ID

Das Importieren von Testergebnisdaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Abgleichen innerhalb von CMDB verwendet wird, kann zu langen Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie benutzerdefinierte CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln**. Unter Schritte zum Verhindern doppelter oder verwaister Datensätze nach dem Ausführen von Vulnerability Response CI-Suchregeln finden Sie weitere Informationen zum Verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

### Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf der Listenseite „CI-Suchregeln“ auf **Änderungen** übernehmen, um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Keine Übereinstimmung mit einer Regel

Wenn sich das Konfigurationselement (CI) nach der erneuten Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die Testergebnisse werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente für Configuration Compliance.

#### Vorhandene Konfigurationselemente für werden dedupliziert Configuration Compliance

Die Duplikat-CI-Korrektur für Deduplizierungsaufgaben wird mit der Eigenschaft `sn_sec_cmn_src_ci.cmdb_ci` aktualisiert.

Immer wenn eine Deduplizierungsaufgabe zum Aktualisieren der Konfigurationselemente (CIs) verwendet wird, werden auch die erkannten Elemente aktualisiert, die sich auf diese CIs beziehen. Daher werden die Testergebnisse mit dem CI aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente für Configuration Compliance.

### Erstellen von CIs für Configuration Compliance mithilfe der Identification and Reconciliation Engine

Ab Configuration Compliance 11.1 können Sie Konfigurationselemente (CIs) in Configuration Management Database (CMDB) mithilfe der IRE-API (Identification and Reconciliation Engine)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellen. Wenn Sie die IRE-API zum Erstellen von CIs verwenden, können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in CMDBschreiben.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB enthält Basissystemklassen, in denen Daten zu CIs gespeichert werden.

## IRE zur CI-Erstellung verwenden

Wenn vor Version 11.1 weder in der Liste „Erkannte Elemente“ noch in CMDBein übereinstimmendes CI gefunden wurde, wurde ein CI in der Klasse „Nicht abgeglichenes CI“ (sn_sec_cmn_unmatched_ci) erstellt.

Weitere Informationen finden Sie unter Nicht abgeglichene CIs.

Ab Version 11.1 können Sie die IRE-API zum Erstellen von CIs in CMDBverwenden. Anstatt die Klasse „Nicht abgeglichenes CI“ zu verwenden, wird ein CI in der Klasse „Nicht klassifizierte Hardware“ oder „Unvollständige IP – identifiziertes Gerät“ erstellt.

## CMDB CI-Klassen

**Hinweis:**
Um die neuen Klassen zu verwenden, aktivieren Sie das Plugin CMDB CI Class Models. Andernfalls werden CIs in der CI-Klasse Nicht abgeglichen erstellt.

Wenn der Host, den Sie von einem Scanner einer Drittpartei importiert haben, ab Version 11.1 nicht in der Liste „Erkannte Elemente“ oder in CMDBgefunden wird, wird er in einer der folgenden neuen CMDB CI-Klassen gespeichert.

**CMDB CI-Klassen**

| CMDB CI-Klasse | Beschreibung |
|---|---|
| Unvollständige IP-Identifizierung des Geräts (cmdb_ci_incomplete_ip) | CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen nur die IP-Adresse verfügbar ist. |
| Nicht klassifizierte Hardware (cmdb_unclassed_hardware_ci) | CI wird in dieser Tabelle erstellt, wenn eine der folgenden Informationen in den vom Scanner empfangenen Hostinformationen verfügbar ist:<br>• Hostname<br>• IP-Adresse<br>• DNS<br>• NETBIOS<br>• MAC-Adresse |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**CMDB CI-Klassen (Fortsetzung)**

| CMDB CI-Klasse | Beschreibung |
|---|---|
| | **Hinweis:** Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und dem nicht klassifizierten Hardware-CI zugeordnet. Wenn sowohl die IP- als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adress-CI erstellt und dem nicht klassifizierten Hardware-CI zugeordnet. |

Das System verwendet automatisch eine nicht abgeglichene CI-Klasse, wenn einer der folgenden Fälle auftritt:

- Das CI-Klassen-Plugin CMDB ist nicht aktiviert.
- IRE löst beim Erstellen eines neuen CI eine Ausnahme aus.

**Zugehörige Informationen**

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

## Configuration Compliance Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen Testergebnisse automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die Standardzuweisungsregel **An CI-Supportgruppe**zuweisen ist im Basissystem enthalten und weist Testergebnisse der CI **-Supportgruppe**zu. Standardmäßig inaktiv.

Die von den Zuweisungsregeln festgelegten Zuweisungsgruppen werden von **Gruppenregeln** verwendet, um Besitzer Korrekturaufgaben (RTs) zuzuweisen.

## Testergebnisse werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, Testergebnisse mit **Zuweisen mit**zuzuweisen:

- Zuweisungsgruppe: Mit dieser Option können Sie eine der vorhandenen Now Platform® Benutzergruppen auswählen.
- Zuweisungsgruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle cmdb_ci verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Keine: Gibt an, dass für dieses Pflichtfeld kein Standardwert vorhanden ist
- Konfigurationselement: Genehmigungsgruppe
- Konfigurationselement: Zuweisungsgruppe
- Konfigurationselement: Supportgruppe

- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder fortgeschrittene ServiceNow®.

Weitere Informationen zum Erstellen von Zuweisungsregeln finden Sie unter Erstellen oder bearbeiten Sie Configuration Compliance Zuweisungsregeln.

Mit der Rolle „sn_vulc.remediation_owner“ können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die ihnen oder ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Configuration Compliance** > **Testergebnisse** > **Meine offenen Testergebnisse**, oder **Configuration Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.

Die Rolle „sn_vulc.remediation_owner“ kann direkt einem Benutzer zugewiesen werden. Sie wird auch automatisch zugewiesen, wenn Sie einem Benutzer die Rolle „itil“ zuweisen.

## Bewertungsprozess für Zuweisungsregeln

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln dafür ausgewertet. Die Zuweisungsregeln werden nach der CI-Übereinstimmung und der Berechnung der Risikopunktzahl ausgewertet. Ein Testergebnis wird nur beim ersten Import und beim Ändern einer Regel automatisch ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:

- Für jede Testergebnis-Zuweisungsregel wird das Testergebnis mit dem Zuweisungsfilter verglichen, Regel niedrigster Reihenfolge zuerst.
- Wenn die Bedingung erfüllt ist, wird dem Testergebnis eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung zwischen allen Regeln finden, bleibt das Testergebnis nicht zugewiesen.

## Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie die Schaltfläche **Änderungen** übernehmen auf der Listenseite „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen Testergebnisse mit Ausnahme der manuell zugewiesenen erneut auszuführen.

**Hinweis:**
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.

Die regelmäßige Aufgabe [`Reapply all assignment rules`] ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle offenen Testergebnisse anhand aller aktiven Regeln mit Ausnahme der manuell zugewiesenen ausgewertet. Sie kann Täglich, Wöchentlich, Monatlich, Regelmäßig, Einmal oder Bei Bedarf ausgeführt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zuweisungsregeln und Zuweisung von Korrekturaufgaben

Normalerweise weisen Sie Ihre Korrekturaufgabe (RT) derselben Zuweisungsgruppe zu wie die darin enthaltenen Testergebnisse. Das ist es, was die Regeln für Korrekturaufgaben standardmäßig tun.

Wenn Ihre RT-Gruppen beispielsweise nach Konfigurationselementklasse gruppiert sind, kann die erstellte Korrekturaufgabe nach den verschiedenen Zuweisungsgruppen aufgeteilt werden. Eine Oracle Database-TRG kann Gruppe 1 und eine Oracle Database-TRG Gruppe 2 zugewiesen werden.

Wenn die Zuweisungsgruppe auf der Ebene der Korrekturaufgabe geändert wird, werden alle Testergebnisse in dieser Gruppe, die dieselbe Zuweisungsgruppe haben, in der neuen Zuweisungsgruppe aktualisiert. Die Testergebnisse werden als manuell zugewiesen markiert und sind nicht für eine weitere Regelauswertung geeignet.

### Zuweisungen von Configuration Compliance Korrekturaufgaben werden entfernt

Sie können die Felder **Zugewiesen an** und **Zuweisungsgruppe** für Korrekturaufgaben (RT) und die zugehörigen Testergebnisse direkt aus den TRG-Datensätzen löschen, von denen Sie feststellen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

## Übersicht

Ab v14.3 der Anwendung Configuration Compliance können Korrekturbesitzer Datensätze für die Neuzuweisung mit der **Schaltfläche** Zuweisung aufheben aktualisieren.

## Anwendungsfall für sn_vulc.remediation_owner

Wenn Sie der Meinung sind, dass RTs und die zugehörigen Testergebnisse nicht in Ihrem Bereich der Korrektur liegen, oder wenn Sie der Meinung sind, dass Ihnen oder Ihren Gruppen Datensätze fälschlicherweise zugewiesen wurden, sollten Sie sich oder Ihre Gruppen aus den **Feldern Zugewiesen an** und entfernen **Zuweisungsgruppenfelder** in diesen Korrekturaufgabendatensätzen.

## Heben Sie die Zuweisung des Moduls auf

Die **Schaltfläche Zuweisung** aufheben wird in den RT-Datensätzen in einem anderen Status als „“ oder „Geschlossen“ oder „Gelöst“ angezeigt.

Wenn Sie Zuweisung **aufheben auswählen**, werden Sie aufgefordert, alle der Gruppe zugeordneten Testergebnisse neu zuzuweisen und in den Zuweisungstyp Nicht zugewiesen **überzugehen**.

Alle Datensätze, die Sie entweder über die UI-Schaltfläche oder manuell aktualisieren, werden im Modul Nicht zugewiesen unter Configuration Complianceangezeigt.

Informationen zum Neuzuweisen von Datensätzen mithilfe der UI-Aktion [ *`Unassigned`* finden Sie unter Entfernen Sie Zuweisungen aus Testergebnisgruppen für sich oder Ihre Gruppen.

## Systemeigenschaft und Benachrichtigungen

Wenn Sie Administrator mit der Rolle „ **sn_vulc.vulnerability_admin** “ sind und Zuweisung aufheben für einen Datensatz auswählen, löst die Systemeigenschaft *`sn_vulc.unassign_test_result_group.approval_required`* standardmäßig den Datensatz „Statusänderungsgenehmigung“ und den Datensatz „Angeforderte Genehmigung“ aus. Außerdem wird die Anforderung in der Liste „Meine Genehmigungen“ des Genehmigers angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Als Schwachstellenadministrator können Sie die Systemeigenschaft *sn_vulc.unassign_test_result_group.approval_required* auf „ **false** “ setzen, um den Genehmigungsprozess zu deaktivieren.

- Wenn der Genehmiger Ihre Anforderung genehmigt, löscht die Systemeigenschaft *sn_vulc.default_assignment_group* standardmäßig die Felder Zugewiesen an und Zuweisungsgruppe und füllt das Feld Zuweisungstyp mit **Nicht zugewiesen**aus. Als Schwachstellenadministrator können Sie den Wert in der Systemeigenschaft *sn_vulc.default_assignment_group* so ändern, dass die Zuweisungsfelder geleert und dann eine bestimmte Gruppe zugewiesen wird. Beispiel: Wenn ein Benutzer für einen Datensatz die Option Zuweisung **aufheben** auswählt und Sie ihn zur Überprüfung an eine bestimmte Gruppe umleiten möchten, können Sie im Wertfeld der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.
- Wenn der Genehmiger Ihre Anforderung ablehnt, wird der Grund für die Ablehnung auf der Registerkarte **Notizen** angezeigt.

Alternativ dazu, wenn *sn_vulc.default_assignment_group* nicht für eine bestimmte Gruppe konfiguriert ist, werden Benutzer, die Sie der Benutzergruppe „Zuweisung aufheben“ hinzufügen, standardmäßig benachrichtigt, wenn die Zuweisung von Datensätzen aufgehoben wird. Die Systemeigenschaft *sn_vulc.default_notification_group* bestimmt die Benachrichtigungen an diese Gruppe.

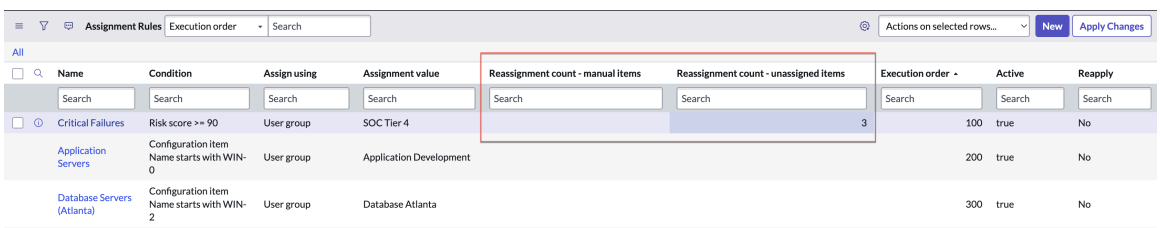
Der Zuweisungstyp ( **Manuell**, **Regel**oder Nicht zugewiesen) ist in den RT-Datensätzen und in der **Listenansicht**verfügbar. Der **Zuweisungstyp Nicht zugewiesen** wird angezeigt, nachdem die Felder **Zugewiesen an** und **Zuweisungsgruppe** durch die Systemeigenschaft der Funktion gelöscht wurden.

## Überwachen Ihrer Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche regelmäßige Aufgabe zählt die Datensätze, wenn sie in den Zuweisungstyp **Nicht zugewiesen** übergehen. Mit dieser Anzahl können Schwachstellenanalysten Zuweisungsregeln überwachen und anpassen, die aufgrund von Zuweisungsregeln mit einer höheren Anzahl nicht zugewiesener RTs möglicherweise keine gute Leistung erbringen.

Die geplante Aufgabe *Reassignment count for assignment rules* wird täglich ausgeführt und verbucht die Gesamtzahl der RTs, die nicht von dieser Funktion für eine bestimmte Zuweisungsregel zugewiesen wurden.

Die Aufgabe zählt auch alle Datensätze, die manuell nicht zugewiesen sind. Sowohl die manuellen Anzahlen als auch die von dieser Funktion erfassten Anzahlen werden in der Liste „Schwachstellenzuweisungsregeln“ in zwei Spalten veröffentlicht: *Reassignment count - manual items* und *Reassignment count - unassigned items*.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Als Schwachstellenadministrator können Sie diese Anzahl anzeigen, indem Sie zu navigieren **Configuration Compliance** > **Administration** > **Zuweisungsregeln**.
2. Wählen Sie das Zahnradsymbol oben rechts in der Liste aus, und wählen Sie die **Anzahl der Neuzuweisungen – manuelle Elemente**und die **Anzahl der Neuzuweisungen – nicht zugewiesene Elemente** zur Anzeige aus.
3. Alle RTs, die ursprünglich durch eine Regel zugewiesen wurden, später jedoch automatisch oder manuell neu zugewiesen wurden, enthalten in der Listenansicht einen Verweis auf die ursprüngliche Regel.

## Configuration Compliance Übersicht über Korrekturaufgaben und Gruppenregeln

Erstellen Sie automatisch Korrekturaufgaben (Remediation Tasks, RTs), um die Ergebnisse mithilfe von Regeln für Korrekturaufgaben in großen Mengen zu analysieren. Die Kriterien, nach denen Gruppen gebildet werden, sind so konfiguriert, dass Sie Testergebnisse nicht manuell Gruppen zuweisen müssen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Korrekturaufgaben verstehen

Korrekturaufgaben stellen eine Reihe von Testergebnissen dar, die korrigiert werden sollen. Das Gruppieren von Testergebnissen bietet viele Vorteile. Sie können Testergebnisse durch die Korrekturstatus verschieben, sie als untersucht markieren, sie zurückstellen und sie mithilfe von Gruppen in Massen als gelöst markieren. Sie können Bedingungen erstellen, um alle Ergebnisse automatisch mit den angegebenen Ergebnissen, Technologien, Risikopunktzahlen und anderen Daten im Zusammenhang mit den Testergebnissen zu gruppieren. Testergebnisse können zu mehr als einer Korrekturaufgabe gehören, sodass Sie flexibel mit einer Gruppe arbeiten und eine andere Gruppe überwachen können. Es hängt alles von Ihren organisatorischen Anforderungen ab. Sie können beispielsweise nach Zuweisung gruppieren und auch eine Gruppe erstellen, die Technologien enthält.

Korrekturaufgaben werden wie folgt erstellt.

- Manuell mit einer von zwei Optionen, um der Gruppe angreifbare Elemente hinzuzufügen.
  - **Manuell**: erstellt eine Gruppe ohne Einträge. Testergebnisse müssen manuell hinzugefügt werden.
  - **Filter**: Erstellt eine Gruppe und verwendet Bedingungen, um Testergebnisse automatisch zu dieser Gruppe hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Manuell hinzugefügte Testergebnisse werden nicht automatisch durch Regeln für Korrekturaufgaben oder Gruppenbedingungen aus Korrekturaufgaben entfernt.

- Automatisch mithilfe von Regeln für Korrekturaufgaben. Diese Option ist die einfachste Option. Nach der Konfiguration erstellen Korrekturaufgabenregeln alle gewünschten Korrekturaufgaben.

Über eine Korrekturaufgabe kann die Gruppe der Testergebnisse einem Benutzer zugewiesen, auf einen späteren Zeitpunkt zurückgestellt, zum Erstellen einer **Change-Anforderung**verwendet werden usw.

**Hinweis:**

Mit der Rolle sn_vulc.remediation_owner können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Configuration Compliance** > **Testergebnisse** > **Meine offenen Testergebnisse**, oder **Configuration Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**.

Wenn festgestellt wird, dass ein neues Testergebnis zu einer Gruppe hinzugefügt werden kann, wird das **Testergebnis** in die zugehörige Liste „Testergebnisse“ der Korrekturaufgabe aufgenommen.

Beim Aktualisieren des Status einer Korrekturaufgabe kann der Status der zugehörigen Testergebnisse so aktualisiert werden, dass er mit dieser Korrekturaufgabe übereinstimmt. Weitere Informationen zu Statusänderungen finden Sie unter Configuration Compliance Status.

## Grundlegendes zu Regeln für Korrekturaufgaben

Mit Regeln für Korrekturaufgaben können Sie definieren, wie Testergebnisse automatisch gruppiert und zugewiesen werden. Die Standardregel **Zuweisungsgruppe Test**ist im Basissystem enthalten, um Testergebnisse basierend auf der **Zuweisungsgruppe eines Testergebnisses und dem Feld Test zu gruppieren.** Diese Regel ist standardmäßig deaktiviert. Sie können nach anderen Wertesätzen in Spalten gruppieren, auf die über das Testergebnis zugegriffen werden kann. Sie können bis zu sechs Schlüssel und eine beliebige Anzahl von Bedingungen verwenden. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie Configuration Compliance Testergebnis-Gruppenregeln.

Sie können Ihre Testergebnisse beispielsweise nach Zuweisungsgruppe oder Technologie und Konfigurationselement (CI) gruppieren. Für Testergebnisse, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Sie können eine Gruppenregel für CIs mit niedrigem Schweregrad oder geringem Risiko haben. Weitere Informationen zu verfügbaren Feldern finden Sie unter Testergebnisfelder.

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln für Korrekturaufgaben ausgewertet. Ein Testergebnis wird nur einmal ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet.

Gruppenregeln werden nach CI-Übereinstimmung, Risikopunktzahlberechnungen und Zuweisungsregeln ausgewertet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für jede Regel für Korrekturaufgaben wird das Testergebnis mit dem Bedingungsfilter verglichen.
- Für jede Regel, bei der die Regelbedingung übereinstimmt, werden die Daten aus den Gruppenschlüsselspalten im Testergebnis abgerufen. Die Regel überprüft, ob eine **offene** Korrekturaufgabe vorhanden ist, die derselben Zuweisungsgruppe wie das Testergebnis zugewiesen ist.

  Wenn die Gruppe gefunden wird, wird das Testergebnis der vorhandenen Gruppe im Status „ **Offen** “ hinzugefügt.

- Wenn keine Gruppe im Status **Offen** gefunden wird, erstellt die Regel eine Gruppe, weist sie basierend auf dem Wert **Benutzergruppe** oder **Schlüssel** in der Regel zu und platziert das Testergebnis darin.

Es kann mehr als eine Testergebnisregel definiert werden, um verschiedene Arten von Ergebnissen zu gruppieren. Da jedes Ergebnis mit den Regelbedingungen verglichen wird, bevor es in eine Gruppe eingefügt wird, können zu viele Regeln Auswirkungen auf die Leistung haben.

Wenn eine Gruppenregel gelöscht wird, haben Sie die Möglichkeit, alle offenen Gruppen zu löschen, die von der Regel erstellt wurden. Dies gilt sowohl für die Regelformularansicht als auch für die Listenansicht.

Wenn die Zuweisung einer Korrekturaufgabe vorgenommen oder geändert wird, werden die Felder **Zuweisungsgruppe** und **Zugewiesen an** auf alle Testergebnisse übertragen, mit Ausnahme derer, bei denen das Testergebnis eine andere Zuweisungsgruppe als die RT hat. Weitere Informationen zu Zuweisungsregeln finden Sie unter Configuration Compliance Übersicht über Zuweisungsregeln. Diese Zuweisungen werden beim nächsten Import automatisch für diese Gruppe verwendet.

## Verfolgen Sie die Anzahl der Zurückstellungen für Testergebnisse und Korrekturaufgaben nach

Verfolgen Sie ab v14.3 im Modul für mehrere Zurückstellungen nach, wie oft ein Testergebnis oder eine Korrekturaufgabe zurückgestellt wurde. Eine regelmäßige Aufgabe, Anzahl der Zurückstellungen **festlegen**, wird täglich ausgeführt, um Anzahlen für Datensätze zu veröffentlichen, die mehr als einmal in der Spalte Zurückstellungsanzahl in den Datensätzen zurückgestellt wurden, die im Modul Mehrere Zurückstellungen aufgelistet sind.

## Rechnergruppen und Rechner für konfigurieren Configuration Compliance

Configuration Compliance-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Configuration Compliance-Rechner

Die Anwendung Configuration Compliance enthält zwei Arten von Rechnern: Risikorechner und Risikopunktzahl-Rollup-Rechner. Diese Rechnergruppen sind standardmäßig aktiviert.

Die Rechnergruppe „Risikopunktzahl“ wurde in „Risikorechner“ umbenannt.

Die Rollup-Rechner für Risikopunktzahlen enthalten Rollup-Rechner für Konfigurationstests und Korrekturaufgaben.

Das Konfigurieren von Risiko- und Rollup-Rechnern für die Korrektur von Testergebnissen und Korrekturaufgaben umfasst die folgenden Aufgaben:

- Erstellen Sie einen Risikorechner
- Erstellen Sie einen Rollup-Rechner für die Risikopunktzahl

Nachdem Sie einen Risikorechner erstellt haben, ist er bei der nächsten Datenerfassung für Berechnungen verfügbar. Nachdem Sie sie erstellt haben, möchten Sie sie möglicherweise auch bei Bedarf anwenden.

Weitere Informationen zu Rechnern und Rechnergruppen finden Sie unter Configuration Compliance Rechnergruppen.

## Configuration Compliance Exception Management – Übersicht

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Leitlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Die Ausnahmeverwaltung umfasst das Anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für eine Korrekturaufgabe, die gemäß der Richtlinie nicht korrigiert werden kann.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einige Schwachstellen ist möglicherweise kein Patch, keine Korrektur oder keine Lösung vorhanden. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen anerkennen und ihnen zustimmen, wenn die konfigurationsbezogene Schwachstelle nicht behoben wird.

## Lebenszyklus einer Ausnahme

Eine Ausnahme ist eine Anforderung, die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum zurückzustellen.

Der Lebenszyklus einer Ausnahme lautet wie folgt:

- Eine Ausnahme wird angefordert
- Eine Ausnahmeanforderung wird genehmigt
- Nachverfolgung einer Ausnahmeanforderung
- Ablauf einer Ausnahmeanforderung

### Eine Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Befreiung für eine Korrekturaufgabe beantragen. Während des Genehmigungsprozesses bleibt die Korrekturaufgabe im Status Wird **überprüft**. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird die Korrekturaufgabe in den Status „Zurückgestellt“ **verschoben**.

### Eine Ausnahmeanforderung wird genehmigt

Korrekturaufgaben, die nicht sofort korrigiert werden können, werden überprüft, auf Risiko bewertet und zur Zurückstellung genehmigt, bis sie korrigiert werden können. Die Genehmigung einer Ausnahmeanforderung kann ein zweistufiger Workflow sein. Wenn nur der Genehmiger der ersten Ebene anwesend ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Configuration Compliance.

**Hinweis:**

Wenn Sie ab Configuration Compliance v13.0 die CC-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern.

Sobald eine Ausnahmeanforderung für eine Korrekturaufgabe genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Schließen
- Löschen

**Hinweis:**

Kommentare zur Ablehnung werden in den Arbeitsnotizen für eine Korrekturaufgabe angezeigt. Wenn eine Ausnahmeanforderung abgelehnt wird, wird diese Korrekturaufgabe in ihren vorherigen Status zurückgesetzt.

### Nachverfolgung einer Ausnahmeanforderung

Automatische Übersetzung

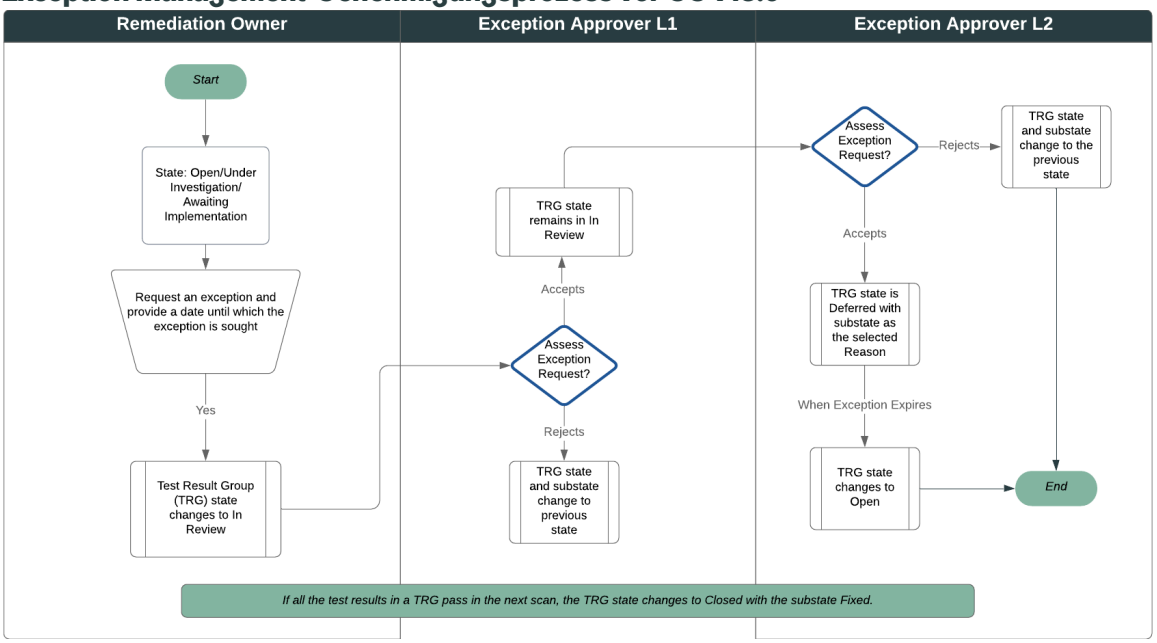
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach dem Auslösen der Ausnahme können Sie ihren Status mithilfe der Registerkarte „ **Statusänderungsgenehmigungen** “ der Korrekturaufgabe nachverfolgen. Wenn eine Aktion für eine Gruppe ausgeführt wird, können Sie den Status der einzelnen Testergebnisse in dieser Gruppe nicht nachverfolgen.

**Ablauf einer Ausnahmeanforderung**

Wenn eine Ausnahmeanforderung für eine Korrekturaufgabe abläuft, kehrt die Gruppe in den Status „ **Offen** “ zurück.

**Exception Management-Genehmigungsprozess vor CC v13.0**




## Configuration Compliance Change-Management

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Testergebnisgruppen (TRGs) in der Anwendung Configuration Compliance erstellen und verwalten.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Change-Anforderungen und der Configuration Compliance -Workflow

Change-Anforderungen und Change-Management sind Teil des Korrekturprozesses des Configuration Compliance -Workflows. Während dieser Korrekturphase können Sie Change-Anforderungen verwenden, um Testergebnisse zu priorisieren, nachzuverfolgen und zu korrigieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung Configuration Compliance arbeitet mit dem IT-Change-Management-Prozess Now Platform® zusammen, um Sie bei der Korrektur nicht konformer Software und Technologien in Ihrer Umgebung zu unterstützen.

Mit Change Management in der Anwendung Configuration Compliance können Sie Testergebnisse vorhandenen Change-Anforderungen zuordnen oder eine Testergebnisgruppe aufteilen und nur für ausgewählte Testergebnisse eine neue Testergebnisgruppe erstellen.

Weitere Informationen finden Sie unter Change-Anforderung in Configuration Compliance erstellen.

## Wichtige Begriffe

**Tests**

Tests sind Bibliotheken von Datensätzen, die Scans von Computer-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets verwaltet werden soll. Ein Test ist alles, was verwendet werden kann, um eine Klasse von Software oder ein Hardware-Asset zu identifizieren, das nicht konform ist.

**Testergebnisse**

Testergebnisse werden von Drittanbieterintegrationen importiert. Sobald sie in Configuration Complianceangezeigt werden, werden sie mithilfe von **Testergebnisgruppen korrigiert**. Gruppen werden gemäß Zuweisungsregeln zur Korrektur zugewiesen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewird das Testergebnis mit „Ergebnis“ *gekennzeichnet*.

**Testergebnisgruppe**

Testergebnisse werden gemäß Zuweisungsregeln in Testergebnisgruppen gruppiert und automatisch den Korrekturbesitzern zur Korrektur zugewiesen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewird das Testergebnis als *Korrekturaufgabe*bezeichnet.

**Richtlinien**

Richtlinien beziehen sich auf autoritative Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Richtlinien.

**Change-Anforderungen**

Change-Anforderungen helfen Ihnen bei der Implementierung kontrollierter Prozesse für die Fehlerkorrektur. Sie können Change-Anforderungen mit Testergebnisgruppen in Configuration Compliance verwenden, um nicht konforme Assets (Konfigurationselemente) zu identifizieren, nachzuverfolgen und zu beheben, die zusätzliche Ressourcen erfordern oder die Sie zurückstellen möchten.

Weitere Informationen zu Testergebnissen und Testergebnisgruppen finden Sie unter Configuration Compliance Übersicht über Korrekturaufgaben und Gruppenregeln.

## Wann Change-Anforderungen in verwendet werden sollen Configuration Compliance

Change-Anforderungen helfen Ihnen, Korrekturaktivitäten für Ihre Testergebnisse zu initiieren und nachzuverfolgen. Wenn Korrekturbesitzer eine große Anzahl nicht korrigierter Testergebnisse oder Konfigurationselemente haben, verwenden sie möglicherweise Change-Anforderungen, um Testergebnisse für die Zurückstellung zu identifizieren. Alternativ

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können sie Testergebnisse und Konfigurationselemente identifizieren und neu gruppieren, die mehr Ressourcen erfordern, als ursprünglich in der ursprünglichen Testergebnisgruppe identifiziert wurden.

**Erstellen Sie Change-Anforderungen aus einer Testergebnisgruppe**

Erstellen Sie eine Change-Anforderung direkt aus einer Testergebnisgruppe für alle Testergebnisse in der Gruppe, oder verwenden Sie Filter, um nur Testergebnisse zu identifizieren, die bestimmten Kriterien entsprechen. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung von Testergebnissen zu beschleunigen, die ein manuelles Eingreifen erfordern.

**Gruppe aufteilen**

Identifizieren Sie aus einer vorhandenen Testergebnisgruppe eine Teilmenge der Testergebnisse, die Sie in eine neue Testergebnisgruppe verschieben möchten. Durch das Erstellen einer neuen TRG können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Testergebnisgruppe zu beeinträchtigen.

**Ordnen Sie Testergebnisse einer vorhandenen Change-Anforderung zu**

Ordnen Sie Testergebnisse vorhandenen Aufgaben zu, um die Erstellung doppelter Change-Anforderungen zu vermeiden, während Sie an der Lösung Ihrer Testergebnisgruppen arbeiten. Durch die Zuordnung einer Testergebnisgruppe zu einer Change-Anforderung, die bereits in Ihrer Instanz verfügbar ist, können Sie vorhandene Aufgabenlisten verwenden.

### Typen von Change-Anforderungen für eine Testergebnisgruppe

Sie können Change-Anforderungen direkt aus Testergebnisgruppen, die Ihnen zugewiesen sind, erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Testergebnisgruppe erstellen:

- Standard Ein vorab autorisierter Change, der geringes Risiko und relativ häufig ist und einem bestimmten Verfahren oder einer Arbeitsanweisung folgt.
- Normal. Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall. Eine Änderung zur Lösung eines schwerwiegenden Incidents.

## Anwendung Configuration Compliance einrichten, installieren und konfigurieren

Bevor Sie die Anwendung in Ihrer Instanz Now Platform® ausführen, müssen Sie zuerst die Anwendung Configuration Compliance aus dem ServiceNow® Storeherunterladen und installieren. Diese Anwendung ist als separates Abonnement verfügbar.

Führen Sie vor der Installation die folgenden Schritte in der Setup-Prüfliste aus, die in der folgenden Tabelle aufgeführt sind. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Weitere Informationen zu veröffentlichten Versionen der Anwendung Configuration Compliance sowie zu Anwendungen von Drittanbietern und ServiceNow, die damit kompatibel sind, finden Sie im Artikel Vulnerability Response Compatibility Matrix and Release Schema Changes [KB0856498] in der HI Knowledge Base.

Weitere Informationen zum Abrufen von Berechtigungen für Store-Apps finden Sie unter Security Operations und ServiceNow Store.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie Prüflistenaufgaben ein

| Setupaufgaben | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Configuration Compliance-Administrator“ [sn_vulc.admin] zu.<br>• Der Configuration Compliance-Administrator [sn_vulc.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.<br>• Der Korrekturbesitzer [sn_vulc.remediation_owner] liest und aktualisiert zugewiesene Datensätze. Die Rolle „sn_vulc.remediation_owner“ wird auch automatisch zugewiesen, wenn einem Benutzer die Rolle „itil“ zugewiesen wird. |
| Unterstützte Integrationen | Bevor Sie Configuration Compliance zur Korrektur von Konfigurationselementen verwenden können, müssen Sie eine Scanner-Integration einer Drittpartei installieren und mindestens einen Netzwerk-Scan durchführen.<br><br>Stellen Sie sicher, dass die Anwendung Vulnerability Response installiert und aktiviert ist, bevor Sie unterstützte Drittanbieterintegrationen konfigurieren. Weitere Informationen finden Sie unter Vulnerability Response installieren.<br><br>Um zu überprüfen, ob Integrationsanwendungen installiert und aktiviert sind, navigieren Sie zu **Abonnement-Management** > **Abonnements** in Ihrer Instanz zur Verfügung. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.<br><br>Weitere Informationen zu Integrationen von Drittanbietern und eine Liste der unterstützten Produkte finden Sie unter Configuration Compliance-Integrationen. |

Qualys Vulnerability Integration



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Qualys Vulnerability Integration bereits auf Ihrem System installiert ist und sich Ihre API-Anmeldeinformationen von denen unterscheiden, die Sie für Configuration Complianceverwenden möchten, rufen Sie den Setup-Assistenten auf (in Vulnerability Response), und weisen Sie sie jeder **Qualys PC-** Integration zu.
- Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** und bearbeiten Sie das Feld **Qualys-API-Anmeldeinformationen** auf der Registerkarte **Qualys-REST-Details**.

Ausführlichere Informationen zu Qualys Vulnerability Integrationfinden Sie unter Qualys Vulnerability Integration verstehen.

Sie sind jetzt bereit, die Anwendung Configuration Compliance zu installieren. Weitere Informationen finden Sie unter Configuration Compliance installieren.

## Configuration Compliance installieren

Bevor Sie Configuration Compliance in Ihrer Instanz von Now Platform® ] ausführen, müssen Sie zuerst die Anwendung Configuration Compliance aus dem ServiceNow Storeherunterladen und installieren. Diese Anwendung ist als separates Abonnement verfügbar.

### Vorbereitungen

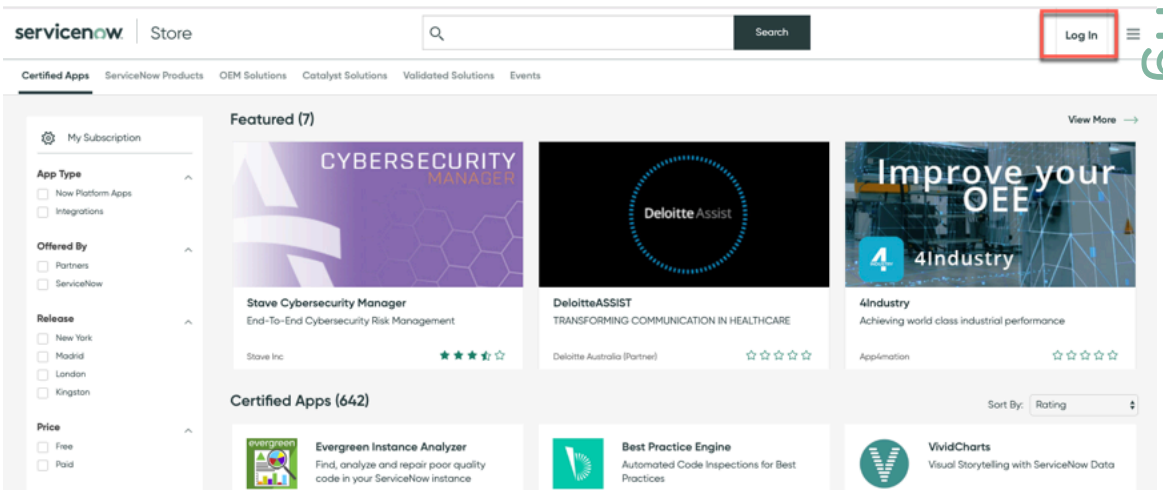
Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Weitere Informationen zu Setup-Aufgaben finden Sie unter Anwendung Configuration Compliance einrichten, installieren und konfigurieren. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Erforderliche Rolle: admin

### Prozedur

1. Um die -Berechtigung zu erhalten und die Kernanwendung Configuration Compliance herunterzuladen, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Anmelden**.

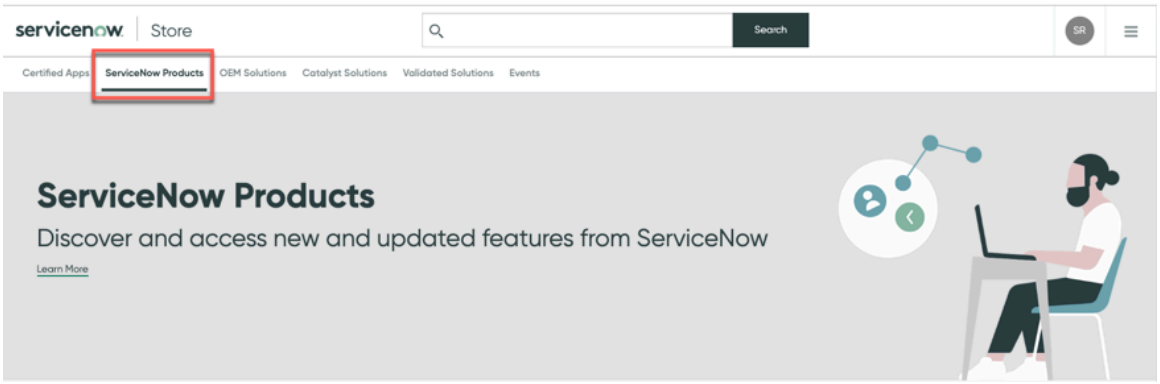



3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.

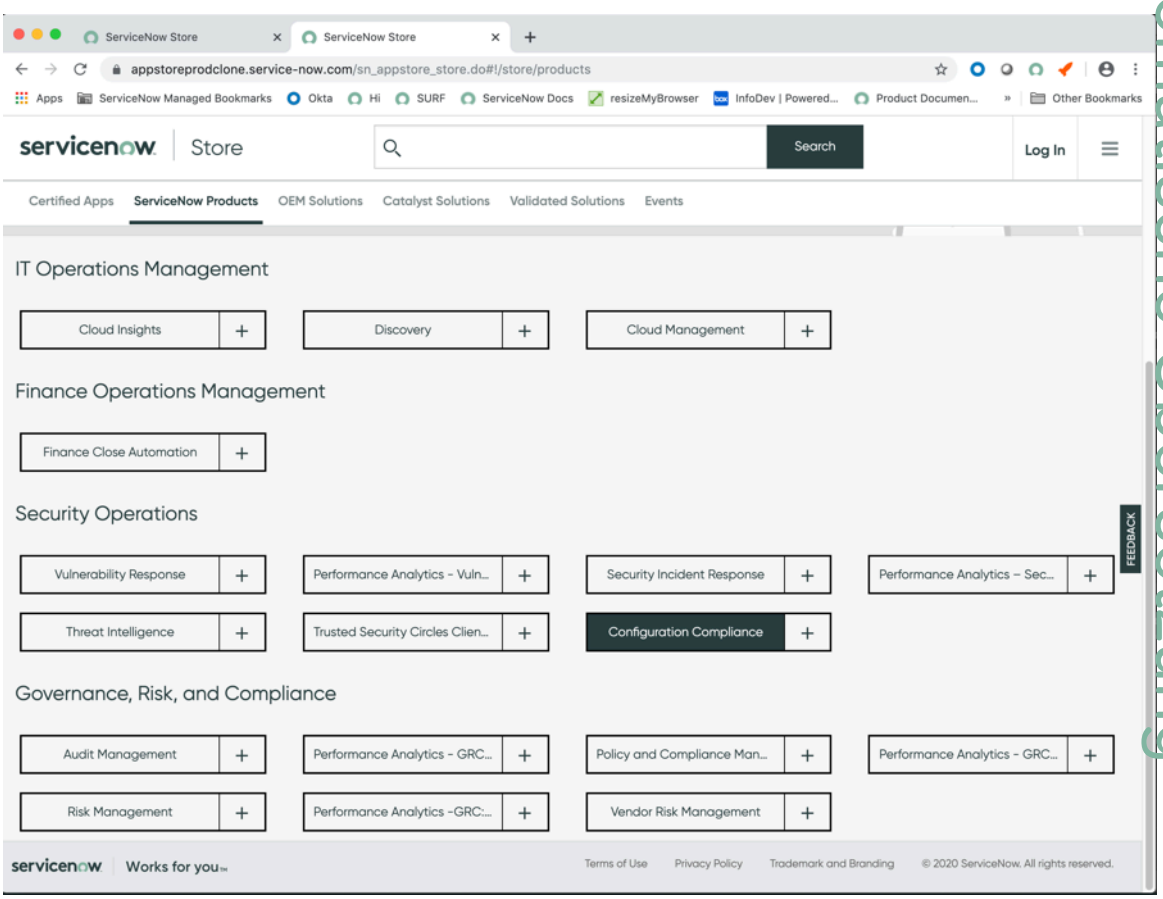
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.


Automatische Übersetzung

4. Wenn diese Option nicht ausgewählt ist, klicken Sie auf der angezeigten Seite auf die Registerkarte **ServiceNow-Produkte**.



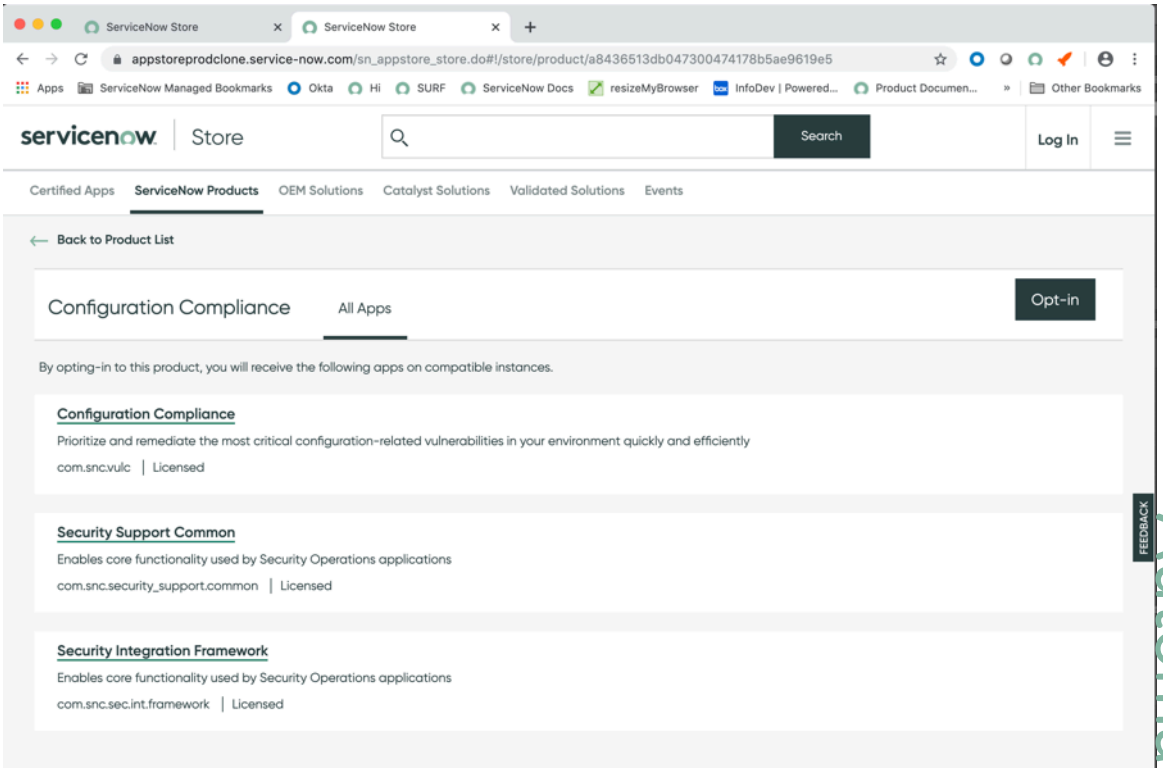

5. Um die zugeordneten Anwendungen anzuzeigen, für die Sie mit der Anwendung Configuration Compliance berechtigt sind, klicken Sie auf der Produktlistenseite auf das Produkt **Configuration Compliance**.



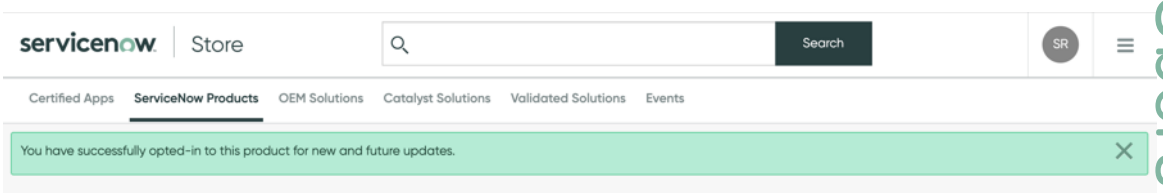

Auf der angezeigten Seite werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Um weitere Informationen zu einer Anwendung zu erhalten, klicken Sie auf einen Link.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Opt-in**, um die Anwendung Configuration Compliance zu erhalten.
7. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Eingabeaufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren**.
   Eine Nachricht wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung entschieden haben.




   Wenn in der Produktliste die Registerkarte ServiceNow Produkte ausgewählt ist, ersetzt ein grünes Häkchen das Pluszeichen rechts neben der Anwendung Configuration Compliance, wie in der folgenden Abbildung dargestellt.

   Nachdem Sie die Nutzungsbedingungen und verwalteten Berechtigungen für eine der Anwendungen auf der Registerkarte „ **ServiceNow-Produkte** “ akzeptiert haben, können Sie auf der Seite „Produktliste“ auf das Pluszeichen (+) klicken, um die Berechtigung zu erhalten und sich für die anderen Anwendungen in diesem zu entscheiden Seite mit einem einzigen Klick.

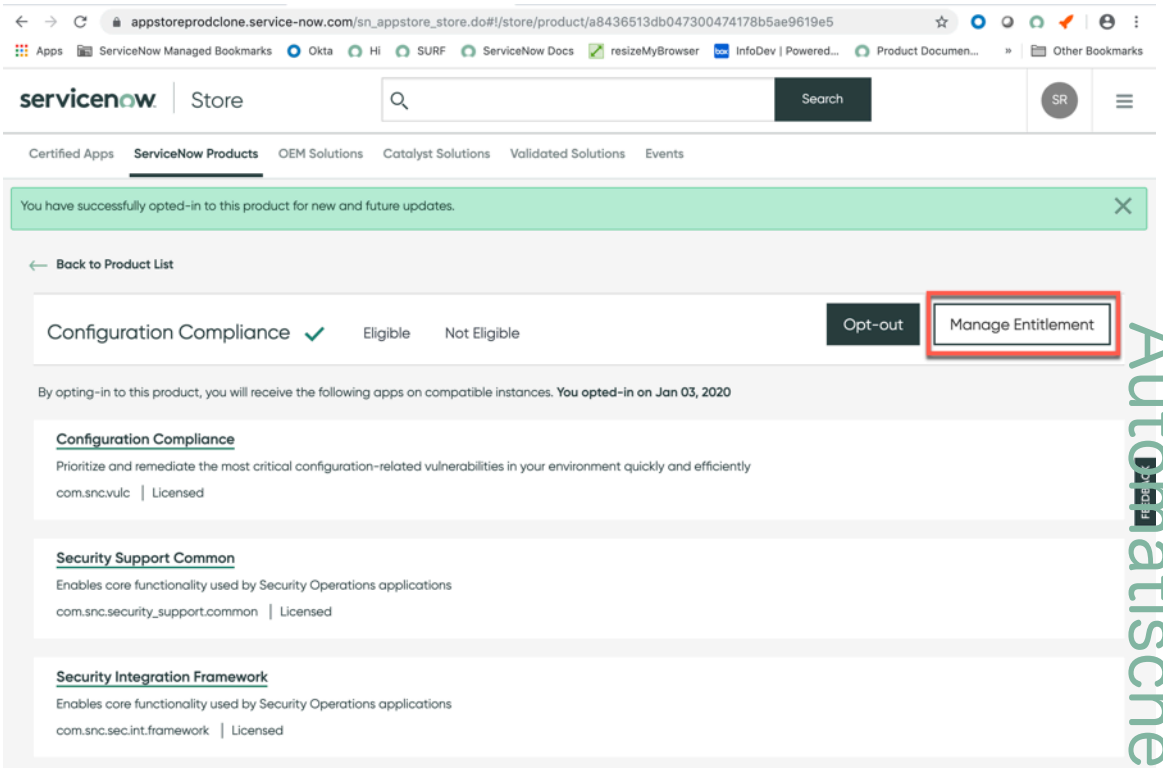
8. Fahren Sie mit Schritt 10 fort, um die Anwendung in Ihrer Now Platform -Instanz zu installieren.
9. **Wahlweise:** Alternativ führen Sie die folgenden Schritte aus, wenn Sie Ihre Berechtigung für die Anwendung Configuration Compliance in anderen Instanzen von Now Platform verwalten möchten.

Automatische Übersetzung

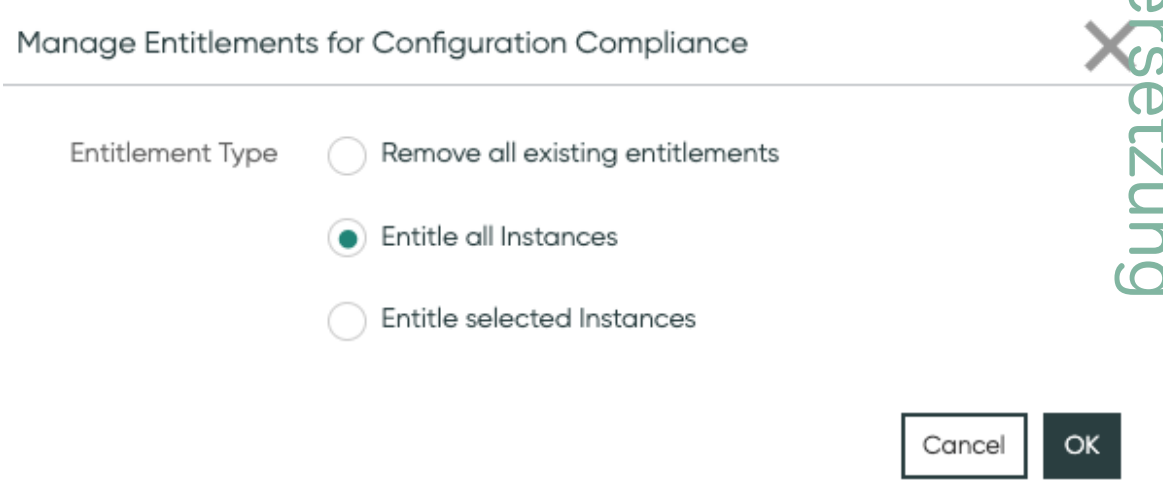
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie in der Produktliste auf die Anwendung Configuration Compliance, um sie anzuzeigen.

**b.** Klicken Sie **auf Berechtigung verwalten**.




**c.** Wählen Sie im angezeigten Dialogfeld „Berechtigungen für Konfigurations-Compliance verwalten“ eine der folgenden Optionen aus:




**d.** Klicken Sie auf **OK** oder **Abbrechen**, um fortzufahren.

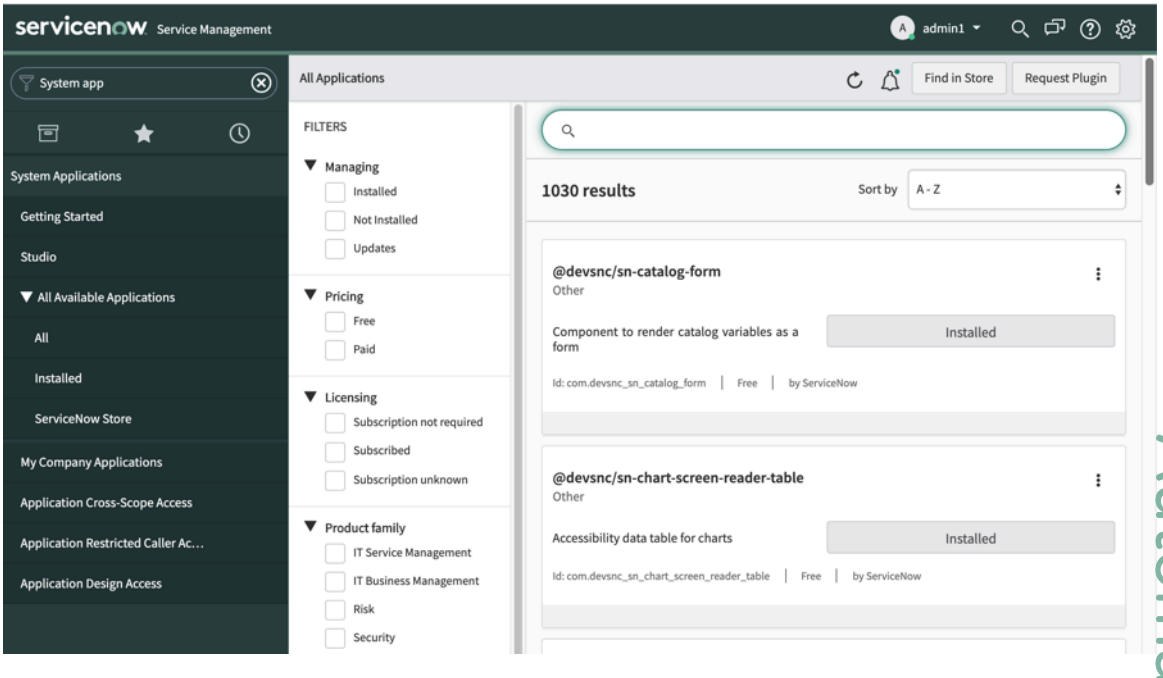
Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihren Now Platform Instanzen zu installieren.

**10.** Melden Sie sich bei der Instanz Now Platform an, auf der Sie die Anwendung Configuration Compliance installieren möchten.

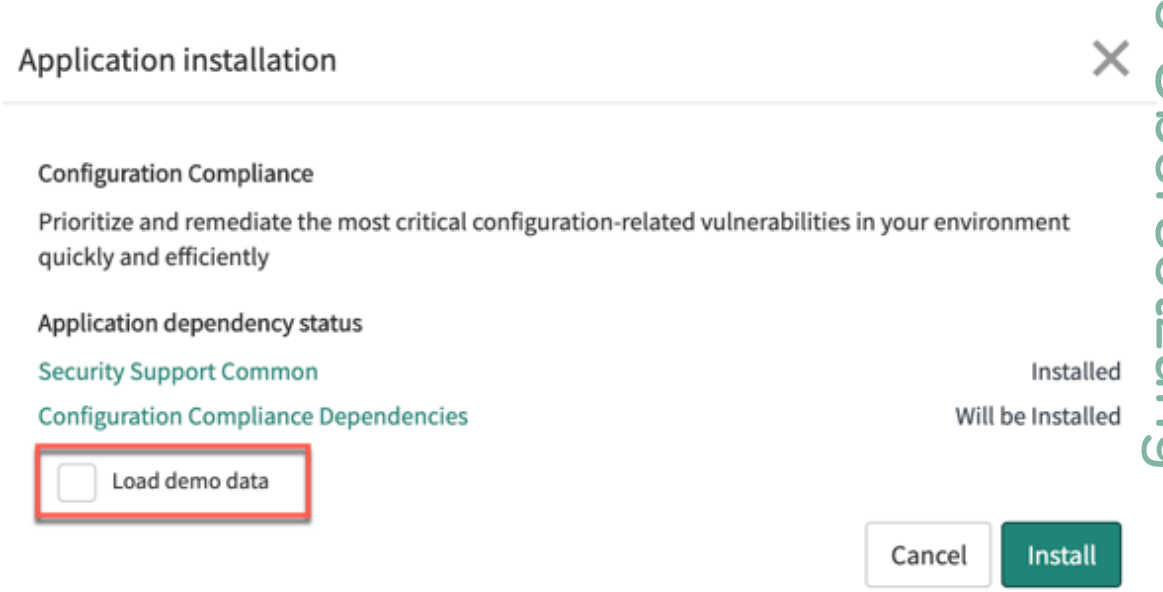
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**11.** Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.




**12.** Suchen Sie in den aufgeführten Anwendungen nach der Anwendung Configuration Compliance (sn_vulc), und klicken Sie auf **Installieren**.
Das Dialogfeld „Anwendungsinstallation“ wird angezeigt. Alle zu installierenden Abhängigkeiten werden angezeigt.




**13.** Wenn Sie Demodaten wünschen, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren**.

### Hinweis:

Wenn Sie das Kontrollkästchen Demodaten laden nicht aktivieren, können die **Demodaten** nachträglich nicht über den **Anwendungsmanager** installiert werden. Weitere Informationen dazu, wie Sie Demodaten nach der Erstinstallation installieren oder erneut installieren, finden Sie im Artikel Workaround to install demo data if application is opened (Workaround zur Installation von Demodaten, wenn die Anwendung bereits installiert ist) [KB0722909] in der Knowledge Base von Now Support.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Installation kann einige Zeit in Anspruch nehmen. Im Dialogfeld „Installieren“ wird eine Meldung angezeigt, nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden.

14. Klicken Sie auf **Schließen**.

Separate SCA-Plugins von Drittanbietern erfassen und transformieren Daten in Configuration Compliance. Bevor Sie Configuration Compliance zur Korrektur von Konfigurationselementen verwenden können, müssen Sie eine Scanner-Integration einer Drittpartei installieren und mindestens einen Netzwerk-Scan durchführen.

Informationen zur Installation von Drittanbieterintegrationen für Configuration Compliancefinden Sie unter Configuration Compliance-Integrationen.

## Mit Configuration Compliance installierte Komponenten

Bei der Aktivierung des Configuration Compliance-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Anwendungsdateien-Tabelle, sodass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert sein, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Befolgen Sie diese Schritte, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Geben Sie im **Filternavigator sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **UND**und dann **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

## Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| Configuration Compliance-Administrator<br><br>[sn_vulc.admin] | Kann Anwendungseigenschaften, Konfigurationen, Aktualisierungsregeln und Integrationen der Configuration Compliance-Anwendung ändern. | sn_vulc.write<br><br>**Hinweis:**<br>Erbt die Rollen, die für die Verwaltung der Datensätze der Anwendung Configuration Compliance erforderlich sind. |
| gelesen<br><br>[sn_vulc.read] | Lesen Sie Listen und Datensätze in Configuration Compliance. | sn_sec_cmn.calc_read |
| write<br><br>[sn_vulc.write] | Schreiben Sie Listen und Datensätze in Configuration Compliance. | • sn_vulc.read<br>• sn_vulc.remediation_owner |
| Schreibzuweisung<br><br>[sn_vulc.write_assignment | In Testergebnis-Zuweisungsfelder schreiben. | Enthalten in der Rolle „sn_vulc.remediation_owner“. |
| Korrekturbesitzer<br><br>sn_vulc.remediation_owner | Zeigen Sie die Berechtigung für Testergebnisse an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie. | Enthalten in der itil-Rolle.<br><br>Enthält:<br>• sn_sec_cmn.read<br>• sn_vulc.write_assignment |
| CC.System<br><br>sn_vulc.import_admin | Führt alle geplanten Aufgaben in der Konfigurations-Compliance-Anwendung aus. | • sn_vulc.write<br>• import_admin<br>• sn_vul_tenable.read_integration |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | **Hinweis:** Dieser Benutzer ist der Standard-Ausführungsbenutzer für jede geplante Aufgabe in Konfigurations-Compliance. | |
| VRCommon.System<br><br>sn_vul_cmn.admin | Standardmäßiger „Run-as“-Benutzer für alle regelmäßigen Aufgaben in der allgemeinen Anwendung Vulnerability Response. | • sn_vul_cmn.write<br>• sn_sec_cmn.admin<br>• report_admin |
| SecCommon.System<br><br>sn_sec_cmn.admin | Standardmäßiger „Run-as“-Benutzer für alle geplanten Aufgaben, die für die Hintergrundaufgabenfunktion in der allgemeinen Anwendung „Security Support“ verwendet werden | • sn_sec_cmn.int_write<br>• sn_sec_cmn.write<br>• workflow_admin<br>• sn_sec_cmn.calc_write<br>• sn_sec_core.read_dictionary<br>• sn_sec_cmn.manage_approval_rules<br>• sn_sec_int.admin<br>• sn_sec_cmn.cap_email_write<br>• sn_sec_cmn.manage_classification_rules<br>• sn_sec_cmn.manage_background_job |
| V14.7: sn_vulc.edit_watch_topic | Bearbeiten Sie Überwachungsthemen für Configuration Compliance. | sn_vulc.read_watch_topic |
| V14.7: sn_vulc.read_watch_topic | Lesen Sie Überwachungsthemen für Configuration Compliance. | cmdb_read |
| V14.7: sn_vulc.create_watch_topic | Erstellen Sie Überwachungsthemen für Configuration Compliance. | sn_vulc.read_watch_topic |

Automatische Übersetzung

## Installierte Scheduled Jobs

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Version 12.0<br><br>Berechnen Sie Korrekturmetriken für alle Testergebnisgruppen | Berechnet und aktualisiert Werte für Statusmetriken in Korrekturaufgabendatensätzen. |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Version 12.0:<br><br>Berechnen Sie Korrekturmetriken für alle Testergebnisse | Berechnet und aktualisiert Werte für Statusmetriken in Testergebnisdatensätzen. |
| Version 12.0:<br><br>Statussynchronisierung von Change-Anforderungen | On-Demand-Auftrag, der die Status aller vorhandenen Korrekturaufgaben (RTs) mit Change-Anforderungen (CHGs) synchronisiert. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, werden auch die Status der zugehörigen Korrekturaufgaben automatisch verschoben. Aktiviert die zukünftige Statussynchronisierung. |
| Version 11.1:<br><br>Überprüfen Sie die Zurückstellung der Testergebnisgruppen Ablauf | Sendet Benachrichtigungen, wenn Korrekturaufgaben abgelaufen sind (und wenn sie in einer Woche ablaufen). |
| Configuration Compliance-CI-Anzahl | Füllt die Anzahl eindeutiger Konfigurationselemente (CIs) und den gleitenden 90-Tage-Durchschnitt in der Tabelle „Anzahl Konfigurationselemente“ [sn_vulc_cc_configuration_item_count] aus. |
| Version 11.1: Korrekturziele bewerten und benachrichtigen | Legt Korrekturzieldaten für alle Testergebnisse fest oder aktualisiert sie. Bestimmt den Status der Korrekturzieldaten anhand von Regeln. Sendet Benachrichtigungen |
| V14.7: Testergebnisgruppen in einheitliche Korrekturaufgabe einfügen | Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Benutzeroberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_remediation_task). |
| Version 12.0:<br><br>Füllen Sie CR-TRG m2m für CR und CR-Parent aus | Füllt Change-Anforderungen für Korrekturaufgaben aus. |
| Entfernt in v11.1: Zurückgestellte Testergebnisgruppen erneut öffnen<br><br>**Hinweis:**<br>Veraltet für Versionen vor 11.1. Nicht verwenden. | Öffnet zurückgestellte Gruppen erneut, wenn das Fälligkeitsdatum abgelaufen ist. |
| Wenden Sie alle Zuweisungsregeln erneut an | Wendet alle Zuweisungsregeln erneut an. |
| Version 14.3: Anzahl der Neuzuweisungen für Zuweisungsregeln | Wird täglich ausgeführt und veröffentlicht die Gesamtzahl der Testergebnisse und Korrekturaufgaben, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen wurden. |
| Bewerten Sie den Status der Testergebnisgruppen neu | Bewertet den Status von Korrekturaufgaben für Einträge neu, bei denen **„asset_state“** den Wert „false“ hat. Wird alle 15 Minuten ausgeführt. |
| Rollup der Risikopunktzahl des Testergebnisses für | Wird stündlich ausgeführt und berechnet die Rollup-Punktzahlen für die geänderten Konfigurationstests und Korrekturaufgaben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Testergebnisgruppe und Konfigurationstest | • Berechnet die Rollup-Risikopunktzahl für alle Tests in sn_vulc_test_manifest und löscht den Manifestdatensatz nach Abschluss.<br>• Berechnet die Rollup-Risikopunktzahl für alle Tests in sn_vulc_result_group_manifest und löscht das Manifest nach Abschluss. |
| Version 12.0:<br><br>Aktualisieren Sie die Richtlinienkorrekturmetriken | Berechnet und aktualisiert Werte für Statusmetriken in Richtliniendatensätzen. |
| Version 14.3: Anzahl der Zurückstellungen festlegen | Erfasst die Anzahl der Zurückstellungen eines Testergebnisses oder einer Korrekturaufgabe. |
| Aktualisieren Sie die Risikobewertung für Testergebnisse | Aktualisiert die Risikobewertung für Testergebnisse. |
| Aktualisieren Sie die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Konfigurationstests. | Aktualisiert die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Configuration Compliance Tests. |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Zuweisungsregel<br><br>[sn_vulc_assignment_regel] | Enthält den Satz von Regeln, die ausgewertet werden, um die Zuweisungsgruppe für Testergebnisse festzulegen. |
| Autoritative Quelle<br><br>[sn_vulc_auth_src] | Speichern Sie importierte autoritative Quellen. |
| Rechner<br><br>[sn_vulc_calculator_risk_score] | Enthält den Rechner, der bestimmte Testergebnisfelder festlegt, wenn bestimmte Bedingungen erfüllt sind. |
| CC-Konfigurationselement: Anzahl<br><br>[sn_vulc_cc_configuration_item_count] | Enthält die Gesamtzahl der Konfigurationselemente. |
| Version 12.0: Change-Anforderungszuordnung<br><br>[sn_vulc_action_associate_cr] | Bereitstellungstabelle für die Zuordnung von Change-Anforderungen zu Korrekturaufgaben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Version 12.0: Erstellung von Change-Anforderungen<br><br>[sn_vulc_action_create_cr] | Staging-Tabelle zum Erstellen von Change-Anforderungsformularen. |
| Version 12.0: Change-Anforderungsformular<br><br>[sn_vulc_cr_form] | Basistabelle für Change Request Management. |
| Zitat<br><br>[sn_vulc_citation] | Enthält importierte Zitate |
| Konfigurationstest<br><br>[sn_vulc_test] | Enthält importierte Konfigurationstestdaten |
| Konfigurationstest-Manifest<br><br>[sn_vulc_test_manifest] | Enthält die Konfigurationstests, für die die Rollup-Risikopunktzahl berechnet werden muss. |
| Version 12.2 Fehlende Asset-Tabelle [sn_vul_missing_asset] | Enthält temporäre Asset-Datensätze für importierte Konfigurations-Compliance-Bewertungsdaten mit nicht abgeglichenen Assets. |
| Konfigurationstest Technologie<br><br>[sn_vulc_test_technologie] | Enthält importierte Konfigurationstesttechnologien |
| Gruppenregel<br><br>[sn_vulc_grouping_rule] | Enthält die Regeln, die die Kriterien definieren, nach denen Gruppen automatisch für eine Reihe von Testergebnissen erstellt werden. |
| Richtlinie<br><br>[sn_vulc_policy] | Enthält importierte Richtlinien |
| Richtlinienkonfigurationstest<br><br>[sn_vulc_policy_test] | Enthält importierte Testdaten für Richtlinienkonfigurationen |
| Korrekturzielregel<br><br>[sn_vulc_ttr_rule] | Definiert den erwarteten Zeitrahmen für die Korrektur eines Testergebnisses. |
| Risikorechner<br><br>[sn_vulc_calculator_group] | Enthält die Gruppierung von Configuration Compliance Rechnern. Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet. |
| Rollup-Rechner für Risikopunktzahl | Enthält Rollup-Rechnerkonfigurationen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| [sn_vulc_risk_score_rollup] | |
| Testergebnisgruppe aufteilen<br>[sn_vulc_action_split_trg] | Bereitstellungstabelle für die Aufteilung von Korrekturaufgaben. |
| Genehmigung der Zustandsänderung<br>[sn_vulc_state_change_approval] | Enthält Prozessdaten zum Genehmigungsstatus |
| Technologie<br>[sn_vulc_technologie] | Enthält importierte Technologien. |
| Relevanz-Zuordnung testen<br>[sn_vulc_test_criticality_map] | Enthält Relevanzzuordnungsdaten |
| Testergebnis<br>[sn_vulc_result] | Enthält importierte Testergebnisse. |
| Testergebnisgruppe<br>[sn_vulc_result_group] | Enthält importierte Korrekturaufgaben |
| Version 12.0:<br>Change-Anforderungen der Testergebnisgruppe | Enthält Change-Anforderungen für Korrekturaufgaben. |
| Manifest der Testergebnisgruppe<br>[sn_vulc_result_group_manifest] | Enthält die Korrekturaufgaben, für die die Rollup-Risikopunktzahl berechnet werden muss. |
| Testergebnisgruppen<br>[sn_vulc_m2m_result_result_group] | Enthält Korrekturaufgabendaten |
| Testergebnisverlauf<br>[sn_vulc_result_history] | Enthält den importierten Testergebnisverlauf. |
| Testergebnis Korrekturstatus | Status des Testergebnisses im Vergleich zur nächsten angewendeten Korrekturzielregel. |
| V14.7: Testanzahlen von Themen überwachen<br>[sn_vulc_wt_test_counts] | Cache-Tabelle für die Registerkarte „Unterschiedliche Konfigurationstests“ im Arbeitsbereich von Vulnerability Manager. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Erstellen oder bearbeiten Sie Configuration Compliance Zuweisungsregeln

Erstellen Sie Regeln, um Testergebnisse basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen Testergebnisse beim Import zu.

## Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

## Warum und wann dieser Vorgang ausgeführt wird

Im Lieferumfang des Basissystems ist die Zuweisungsregel Configuration Compliance enthalten, **An CI-Supportgruppe zuweisen**, die Testergebnisse derselben Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel ist standardmäßig inaktiv. Sie können mithilfe von Filterbedingungen Änderungen vornehmen. Mit Zuweisungsregeln definieren Sie eine oder mehrere Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein Testergebnis mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet.

**Hinweis:**
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch ausgewertet oder manuell über die Schaltfläche **Änderungen** übernehmen in der Liste „Zuweisungsregeln“ ausgewertet.

## Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Zuweisungsregeln**.
2. Öffnen Sie die Regel **An CI-Supportgruppe zuweisen,** oder klicken Sie auf **Neu**.
3. Bearbeiten Sie die Regel **An CI-Supportgruppe zuweisen**, oder füllen Sie im Falle von **Neu**die entsprechenden Felder im Formular aus.

### Configuration Compliance-Zuweisungsregel

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppenregel. |
| Ausführungsbefehl | Reihenfolge, in der die Regeln ausgewertet werden. Die niedrigste Zahl wird zuerst ausgewertet.<br><br>Regeln mit hoher Priorität, Testergebnisse, die einer besonderen Behandlung bedürfen, bei denen das Risiko kritisch ist, oder ein Testergebnis, das von der Compliance-Abteilung behandelt werden sollte, sollten zuerst ausgeführt werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung erforderlich ist und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um Testergebnisse der Gruppe zuzuweisen, die bestimmt, zu welcher Zuweisungsgruppe sie gehören sollen. Diese Gruppe könnte eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel wird zuletzt ausgeführt. |
| Aktiv | Gibt an, ob die Zuweisungsregel aktiv ist. |
| **Bedingung** | |
| Bedingungsfelder | Bedingungen, die erfüllt sein müssen.<br><br>Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Neues Kriterium | Fügt weitere Bedingungsfilterfelder hinzu, aus denen Sie auswählen können. |
| Beschreibung | Text, der die Zuweisungsregel beschreibt. |
| Zuweisen mit | Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.<br>○ Benutzergruppe: Wählen Sie eine Benutzergruppe aus der Suchtabelle aus<br>○ Benutzergruppenfeld: Wählen Sie im Dropdown-Menü ein Benutzergruppenfeld aus.<br>○ Skript: Erstellen oder bearbeiten Sie ein Skript.<br>**Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert Kenntnisse von ServiceNow. |
| Anwendergruppenfeld | Wählen Sie die Benutzergruppe aus, die für die Korrektur von Tests verantwortlich ist, die den Bedingungen der Zuweisungsregeln entsprechen. |

4. Klicken Sie auf **Absenden**.

## Configuration Compliance Korrekturzielregeln

Mit Korrekturzielregeln können Sie die erwarteten Zeitrahmen für die Korrektur von Testergebnissen festlegen. Sie können Benachrichtigungen an Benutzer und Gruppen senden, wenn Zieldaten näher rücken und sie überfällig sind.

Erforderliche Rollen: Configuration Compliance-Administrator (sn_vulc_admin) oder ein Manager mit der Rolle sn_vulc.manage_remediation_target_rules.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Korrekturzielregeln

Eine regelmäßige Aufgabe, *`Evaluate and notify remediation targets`*, wird täglich ausgeführt und verwendet aktive Korrekturzielregeln, um aktive Testergebnisdatensätze auszuwerten. Immer wenn Testergebnisdatensätze, die Testergebnisgruppen zugeordnet sind, aktualisiert oder geändert werden, werden die geänderten Werte von den Zielregeln ausgewertet, und die Änderungen werden zusammengefasst und in den zugehörigen Testergebnisgruppen angezeigt.

Sie können vorhandene Korrekturzielregeln bearbeiten, deaktivieren oder löschen und neue erstellen. Wenn Sie eine neue Regel ändern, deaktivieren oder erstellen, haben Sie die

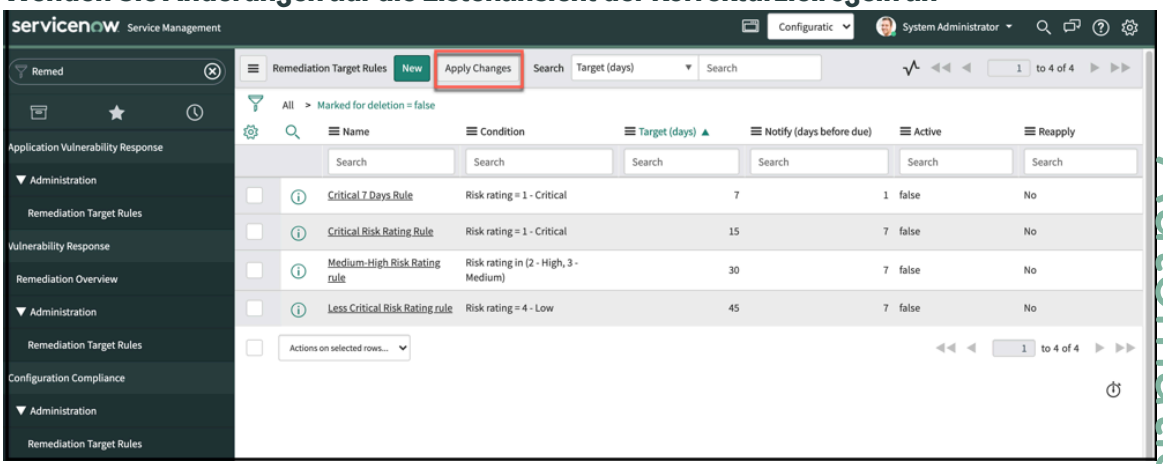


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglichkeit, in der Listenansicht der Korrekturzielregeln auf **Änderungen** übernehmen zu klicken und die Änderungen, die Sie vor der nächsten geplanten Aufgabe vorgenommen haben, manuell anzuwenden. Mit dieser Option können Sie Ihre Testergebnisdatensätze erneut auswerten, ohne warten zu müssen. Wenn Sie Ihre Änderungen nicht manuell anwenden, werden sie bei der nächsten täglichen geplanten Aufgabe übernommen und angewendet.

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Nachbesserungszielregeln** , um Korrekturzielregeln anzuzeigen.

**Wenden Sie Änderungen auf die Listenansicht der Korrekturzielregeln an**




2. Klicken Sie in der Spalte Name auf eine Regel, um den zugehörigen Datensatz zu öffnen.
3. Aktivieren Sie das Kontrollkästchen **Aktiv** im Datensatz der Korrekturzielregel, um deaktivierte Regeln (falsch) zu aktivieren (true).

Wenn Sie eine Zielregel ändern oder hinzufügen, werden Ihre Änderungen verwendet, um alle aktiven Testergebnisse zusammen mit allen anderen Zielregeln auszuwerten, die von Ihren Änderungen betroffen sind, unabhängig davon, ob Sie die Änderungen manuell anwenden oder auf die nächste geplante Aufgabe warten. Wenn Sie die Änderungen manuell anwenden, kann diese Auswertung bei einer großen Anzahl aktiver Testergebnisse einige Zeit in Anspruch nehmen, da alle von Ihren Änderungen betroffenen Regeln für eine Auswertung verwendet werden.

Zum Beispiel ist der Standardwert für angestrebte Korrekturtage 30. Wenn Sie eine neue Regel erstellen, die auch 30 für gezielte Korrekturtage hat, werden diese Regel und alle Zielregeln mit 30 Tagen oder mehr als Zieldatum auf Ihre Testergebnisse angewendet.

## Deaktivierte und gelöschte Zielregeln

Wenn eine Regel aktiv ist, wird true in der Spalte Aktiv in der Listenansicht der Korrekturzielregeln angezeigt. Nachdem eine Regel deaktiviert wurde (false), wird sie nicht mehr auf neue Testergebnisse angewendet. Die regelmäßige Aufgabe verfolgt jedoch weiterhin alle vorhandenen Testergebnisse, auf die die Regel angewendet wurde. Wenn die deaktivierte(n) Regel(n) anschließend reaktiviert wird/werden, wird jedes Testergebnis mit einem leeren Feld **Korrekturzieldatum** anhand der reaktivierten Regeln ausgewertet. Dies schließt Testergebnisse ein, die erstellt wurden, während die Regeln deaktiviert wurden.

Wenn Regeln gelöscht werden, werden das **Korrekturzieldatum** und zugehörige Felder in geschlossenen Testergebnissen beibehalten. Das **Korrekturzieldatum** und zugehörige Felder in nicht geschlossenen Testergebnissen werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine Regel zu deaktivieren, deaktivieren Sie im Datensatz der Korrekturzielregel das Kontrollkästchen Aktiv, und klicken Sie auf **Aktualisieren**. False wird in der Listenansicht der Korrekturzielregeln in der Spalte Aktiv angezeigt.

Um eine Regel zu löschen, klicken Sie im Formular auf **Löschen**, oder wählen Sie in der Listenansicht die Regel oder Regeln aus, und klicken Sie in der Liste **Aktionen für Zeilen aufLöschen**. Die Regel wird nicht mehr in der Liste angezeigt, und die nächste Regel in der Reihenfolge des Vorgangs ersetzt die gelöschte Regel.

Wenn Sie eine Regel deaktivieren oder löschen und Ihre Änderungen vor der nächsten geplanten Aufgabe anwenden, wird die Regelreferenz aus dem Feld gelöscht, das Korrekturdatum und die Statusdaten bleiben jedoch erhalten. Wenn Sie Ihre Änderungen nicht manuell anwenden, wird die Regelreferenz mit der nächsten geplanten Aufgabe aus dem Feld gelöscht.

## Über Zielregeln und die geplante Aufgabe Korrekturziele auswerten und benachrichtigen

Die geplante Aufgabe *`Evaluate and notify remediation targets`* wird einmal täglich um 16:30:00 Uhr ausgeführt. Sie erfasst alle aktiven Korrekturzielregeln und wertet alle aktiven Testergebnisse aus, beginnend mit den Testergebnissen mit dem frühesten Korrekturzieldatum. Sie wertet alle Testergebnisse aus, die die folgenden Kriterien erfüllen:

- Sie befinden sich nicht im Status **„Geschlossen** “.
- Hat kein Korrekturzieldatum.
- Korrekturzieldaten aufweisen, die nach den Daten in den Korrekturzielregeln liegen.
- Werden nach Abschluss eines Scanner-Imports erstellt. Die regelmäßige Aufgabe erfasst und bewertet alle neuen Testergebnisse, die als Ergebnis eines Imports erstellt werden.

Nachdem eine Zielregel definiert wurde, werden die Korrekturzieldaten von der geplanten Aufgabe *`Evaluate and notify remediation targets`* berechnet. Die regelmäßige Aufgabe fügt ein Korrekturzieldatum hinzu, falls keines vorhanden ist, oder, wenn diese Regel ein früheres Datum als das im Datensatz enthält, wird das vorhandene Zieldatum aktualisiert.

Alle abgelaufenen Datensätze und Erinnerungsdaten, die den Zielregeln entsprechen, werden von der Aufgabe abgerufen und Benachrichtigungen werden gesendet. Bei deaktivierten Regeln löscht die Aufgabe die Korrekturfelder in Testergebnisdatensätzen und beendet das Senden von Benachrichtigungen.

## Anzeigen von Zieldaten und Status in Listen- und Formularansichten

Configuration Compliance -Manager können das Korrekturzieldatum sowohl im Testergebnisformular als auch in Listenansichten sehen. Korrekturzielregeln werden auch nach einem Scanner-Import ausgeführt und erneut ausgeführt, wenn ein Testergebnis erneut geöffnet wird.

Die regelmäßige Aufgabe aktualisiert das **Korrekturziel** und den Korrekturstatus in der **Listenansicht** der Testergebnisse sowie die Felder **Korrekturzielregel**, **Korrekturziel**und **Korrekturstatus** im Testergebnisformular.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**

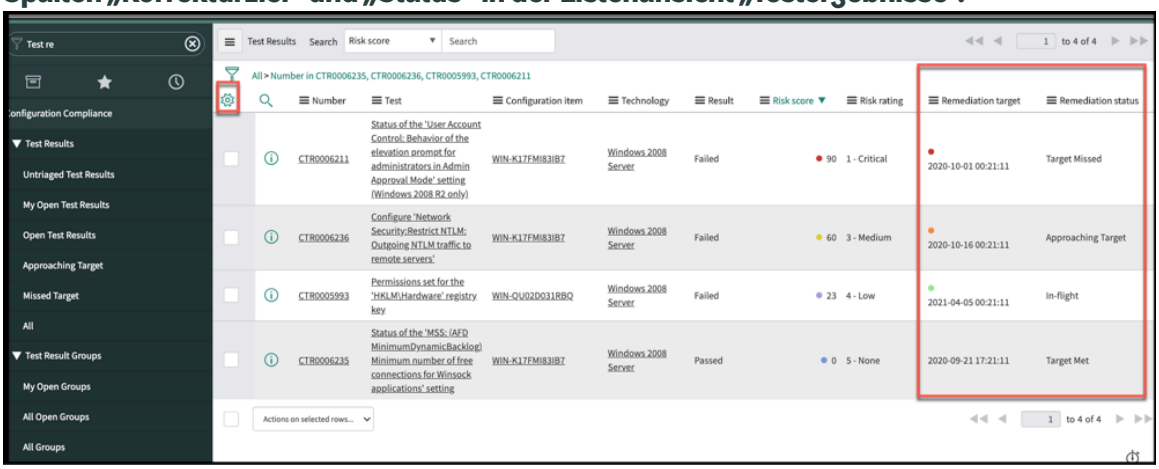
Standardmäßig werden die Spalten **Korrekturziel** und **Korrekturstatus** nicht in der Listenansicht der Testergebnisse angezeigt. Um diese Spalten anzuzeigen, müssen Sie sie auch der Listenansicht hinzufügen. Fügen Sie dem Testergebnisformular auf ähnliche Weise die Felder **Korrekturzielregel**, **Korrekturziel**und **Korrekturstatus** hinzu.

Verwenden Sie die Slushbuckets in den Menüs „Einstellungen“ und „Zusätzliche Aktion“, wie in den folgenden Abbildungen gezeigt, um diese Spalten und Felder anzuzeigen. Klicken Sie für das Menü Zusätzliche Aktion im Testergebnisdatensatz auf das Menüsymbol, gefolgt von **Konfigurieren** und **Formularlayout**, um den Slushbucket anzuzeigen und die Felder von **Verfügbar** in **Ausgewählt**zu verschieben.

Das Korrekturzieldatum wird in der Listenansicht der Testergebnisse als farbige Punkte codiert:

- Testergebnisse, die ihr Benachrichtigungsdatum noch nicht erreicht haben, werden grün angezeigt.
- Testergebnisse, die sich dem Korrekturzieldatum nähern, werden orange angezeigt.
- Testergebnisse, die nach dem Korrekturzieldatum liegen, werden rot angezeigt.

**Spalten „Korrekturziel“ und „Status“ in der Listenansicht „Testergebnisse“.**

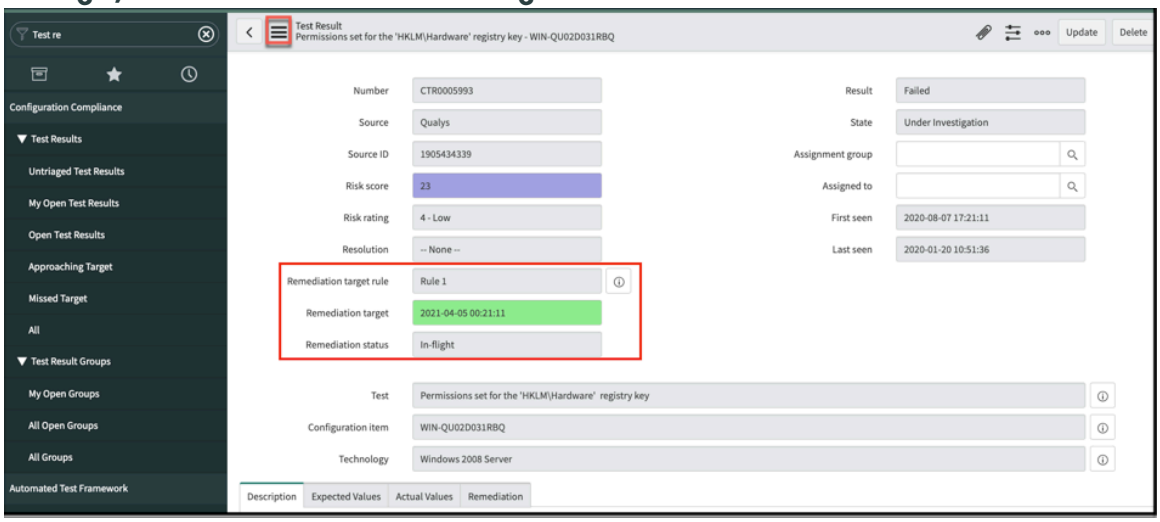



- Ziel verfehlt: Das Zieldatum ist überfällig
- Während der Ausführung: Das Testergebnis wird ausgeführt



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zielregel, Ziel und Statusfelder im Testergebnisdatensatz




Testergebnisdatensätze werden auch visuell im Dashboard Configuration Compliance angezeigt. Navigieren zu **Alle** > **Configuration Compliance** > **Übersicht** und überprüfen Sie das Dashboard auf den Status. Die Übersicht enthält vorhandene Widgets und den Korrekturstatus. Die Farben der Diagramme entsprechen den Farben, die in der Listenansicht „Testergebnisse“ und im Datensatz „Testergebnis“ angezeigt werden.

## Szenario der Korrekturzielregel

Wenn mehrere Korrekturzielregeln auf dasselbe Testergebnis angewendet werden, wird die restriktivste Regel angewendet.

Zum Beispiel, wenn ein Testergebnis, das zuerst am 01.03.2018 identifiziert wurde, die Bedingungen für zwei Korrekturzielregeln erfüllt:

- Korrekturzielregel 1: Definiert am 07.03.2018; Korrekturziel ist 15 Tage seit der ersten Sichtung. Das berechnete Korrekturzieldatum ist der 16.03.2018 10:00:00.
- Korrekturzielregel 2: Definiert am 10.03.2018; Korrekturziel ist 10 Tage seit der ersten Sichtung. Das berechnete Korrekturzieldatum ist der 11.03.2018 10:00:00.

### Hinweis:

Korrekturziele werden aus dem Datum der **letzten** Sichtung plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.

Ab V14.5 werden Korrekturziele aus dem **Ziel ab (Datum)**berechnet. Der Standardwert bleibt **Zuletzt gesehen**.

In diesem Szenario gilt Korrekturzielregel 2 für das Testergebnis, da es das restriktivere Datum hat: 10 Tage seit der ersten Identifizierung des Testergebnisses vs. 15 Tage.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen oder ändern Sie Zielregeln, und wenden Sie Änderungen erneut an

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Nachbesserungszielregeln** zum Anzeigen, Bearbeiten und Erstellen neuer Korrekturzielregeln.
2. Klicken Sie in der Spalte Name auf eine Regel, um eine Zielregel zu öffnen und den Datensatz zu bearbeiten, oder klicken Sie alternativ auf **Neu**, um eine neue Zielregel zu erstellen.
3. Füllen Sie das Formular aus, um den erwarteten Zeitrahmen für die Korrektur zu definieren, geben Sie an, für welche Testergebnisse diese Regel mit Bedingungen gilt, und legen Sie fest, wann Erinnerungen an Benutzer oder Gruppen oder an beide gesendet werden sollen.
4. Klicken Sie auf **Absenden**. Alternativ können Sie bearbeitete Regeln speichern, indem Sie auf **Aktualisieren**klicken.

   Die Listenansicht wird mit Ihrer aktualisierten oder neuen Regel angezeigt. Die Regeln in der Liste werden beginnend mit der Regel mit dem niedrigsten Korrekturzieldatum geordnet und ausgeführt. Wenn Sie eine Regel deaktivieren oder löschen, wird die inaktive oder gelöschte Regel durch die nächste Regel in der Reihenfolge ersetzt.
5. Um Ihre neuen Änderungen jetzt zu übernehmen, klicken Sie auf **Änderungen übernehmen**.

### Configuration Compliance Rechnergruppen

Configuration Compliance -Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Configuration Compliance Rechnergruppen

Aus dem Datensatz des Standardrisikorechners können Rechnerregeln bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können diese Funktion verwenden, um die Konfiguration des Risikorechners anzupassen. Sie können zu Beginn ihrer Bereitstellung mit mehreren Priorisierungsschemata experimentieren und diese Änderungen bei Bedarf anwenden, um zu sehen, wie sie sich auf die Importergebnisse auswirken.

Die Rechnergruppe „Risikopunktzahl“ wurde in „Risikorechner“ umbenannt.

Rollup-Rechner für Risikopunktzahlen sind in Configuration Complianceenthalten. Es gibt zwei Arten von einzelnen Rollup-Rechnern:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Konfigurationstest-Risiko-Rollup**

Rechner, die Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammenfassen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt.

**Rollup der Testergebnisgruppe „Risikopunktzahl“.**

Diese Rechner fassen die Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Gruppe bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt.

Sowohl die Rechnergruppe „Risikopunktzahl“ als auch die Gruppe „Risikopunktzahl-Rollup-Rechner“ sind standardmäßig aktiviert.

Weitere Informationen finden Sie in den folgenden wichtigen Begriffen für Configuration Compliance -Rechner:

**Testergebnis**

Ein Testergebnis ist das Ergebnis des Konfigurationstests für ein Konfigurationselement (CI) und die zugehörige Technologie. Testergebnisse in den Status „Fehlgeschlagen“, „Fehler“ und „Unbekannt“ identifizieren Hardware, Software und Assets, die nicht Ihren Richtlinien entsprechen.

**Testergebnisgruppe**

Testergebnisse werden zum Zeitpunkt des Datenimports basierend auf den vordefinierten Gruppenregeln gruppiert. Diese Korrekturaufgaben ähneln Schwachstellengruppen in Vulnerability Response. Korrekturaufgaben organisieren Testergebnisse in Gruppen für die Massenanalyse und stellen eine Reihe von Elementen dar, die korrigiert werden sollen.

**Risikopunktzahl in einem Testergebnis**

Ein Wert, der von Risikopunktzahl-Rechnern berechnet wird und auf dem Geschäftskontext eines Assets und dem Schweregrad des zugehörigen Tests basiert. Dies ist der Durchschnitt der Geschäftskritikalität des betroffenen Assets, wie in der CMDB definiert, und der Schweregrad des Tests, wie vom Scanner kommuniziert.

Jedem Asset können mehrere Services zugeordnet sein. Die geschäftliche Relevanz eines Assets wird durch den Service mit der höchsten Relevanz bestimmt.

Der berechnete Wert wird in den Risikopunktzahlfeldern der Testergebnisse angezeigt. Die Punktzahlen zeigen Werte zwischen 0 und 100 an. Felder sind auch farbcodiert, um Ihnen den Schweregrad auf einen Blick zu zeigen.

**Risikopunktzahl in Testergebnisgruppe**

Diese Punktzahl wird im Datensatz der Korrekturaufgabe angezeigt und ist der zusammengefasste Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Korrekturaufgabe. Diese Punktzahl ändert sich, wenn Testergebnisse in der Korrekturaufgabe korrigiert werden.

**Risikopunktzahl im Konfigurationstest**

Diese Punktzahl wird bei Konfigurationstests angezeigt und ist der zusammengefasste Wert der Risikopunktzahlen für alle aktiven Testergebnisse mit diesem Konfigurationstest. Diese Punktzahl ändert sich, wenn die mit diesem Konfigurationstest verknüpften Testergebnisse korrigiert werden.

**Risikobewertung**

Das Risiko, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, der Risiken als „Kritisch“ (1) bis



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Keine“ (5) bewertet. Die Punktzahl basiert auf einem Bereich von Risikopunktzahlen und wird in den Risikobewertungsfeldern angezeigt.

**Risikobewertungsbereiche**

| Risikobewertung | Risikopunktzahl |
|---|---|
| 1 - Kritisch | 90 bis 100 |
| 2: Hoch | 70 bis 89 |
| 3: Mittel | 40 bis 69 |
| 4: Niedrig | 1 bis 39 |
| 5: Keine | 0 |

**Rollup-Rechner der Risikopunktzahl**

Es gibt zwei Arten von Rollup-Rechnern:

- Konfigurationstest-Risiko-Rollup: Diese Rechner fassen die Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten.
- Rollup der Risikopunktzahl der Testergebnisgruppe: Diese Rechner fassen die Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Gruppe bereitzustellen. Der Rollup-Wert wird in den Feldern Risikopunktzahl angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten. Ein Beispiel für einen Risikopunktzahl-Rollup-Rechner und wie er Punktzahlen berechnet, finden Sie unter Beispiel für Risiko-Rollup-Berechnung für Configuration Compliance.

**Historische Risikopunktzahl**

Die inhärente Risikopunktzahl für alle bestandenen Testergebnisse in einer Korrekturaufgabe. Dieses Feld zeigt die Höhe des Risikos an, das von einer Testgruppe behoben wurde. Es wird nur angezeigt, wenn sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl 0 ist.

Punktzahlen werden berechnet, wenn sich die Risikopunktzahl ändert oder wenn Testergebnisse einer Korrekturaufgabe hinzugefügt oder daraus entfernt werden.

**Hinweis:**
Damit dieses Skript ordnungsgemäß funktioniert, ist das Plugin Service-Mapping erforderlich. Service-Mapping ist als separates Abonnement verfügbar und erfordert die Aktivierung durch Mitarbeiter von ServiceNow.

## Erstellen Sie eine Rechnergruppe Configuration Compliance .

Configuration Compliance Rechnergruppen werden verwendet, um Rechner basierend auf der gewünschten Verwendung zu gruppieren.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Das Configuration Compliance Basissystem enthält eine Rechnergruppe: **Risikopunktzahl**. Wenn Sie andere Rechner erstellen, können Sie sie dieser Gruppe hinzufügen oder andere Gruppen und Rechner erstellen. Innerhalb jeder Gruppe wird der erste Rechner ausgeführt, der dem Testergebnis entspricht.

Es gibt zwei Rechnergruppen, die in der Anwendung Configuration Compliance enthalten sind:

- Risikorechner
- Rollup-Rechner für Risikopunktzahl

Risikorechner berechnen die Risikopunktzahl und Risikobewertung eines Testergebnisses.

Rollup-Rechner für Risikopunktzahl fassen Risikopunktzahlen für alle Testergebnisse und Korrekturaufgaben mit demselben Konfigurationstest zusammen, um eine Gesamtrisikopunktzahl bereitzustellen.

Sie erstellen auch neue Rechner direkt aus diesen Gruppen.

### Prozedur

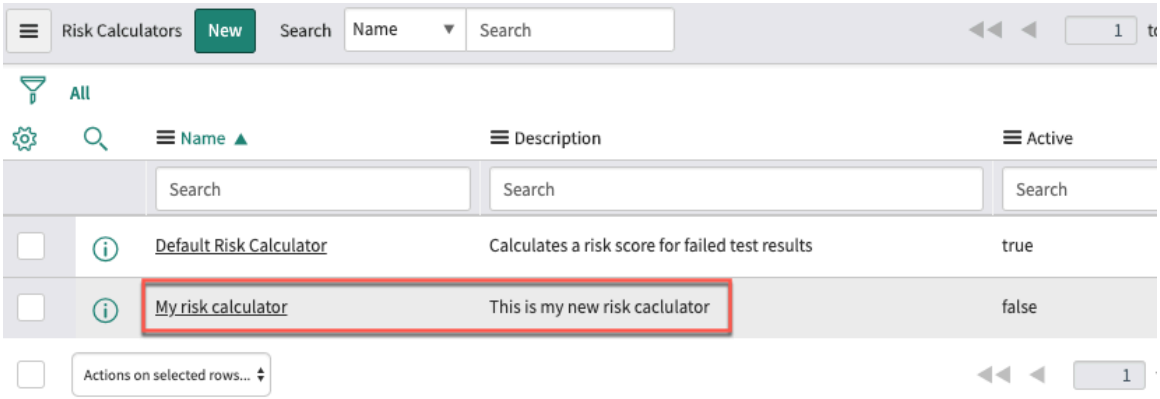
1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Rechnergruppen**.
2. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** und wählen Sie **Risikorechner** oder **Rollup-Rechner**für Risikopunktzahl aus.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Rechners. |
| Beschreibung | Eine Beschreibung dieser Rechnergruppe. |
| Aktiv | Aktivieren oder deaktivieren Sie die Rechnergruppe. |

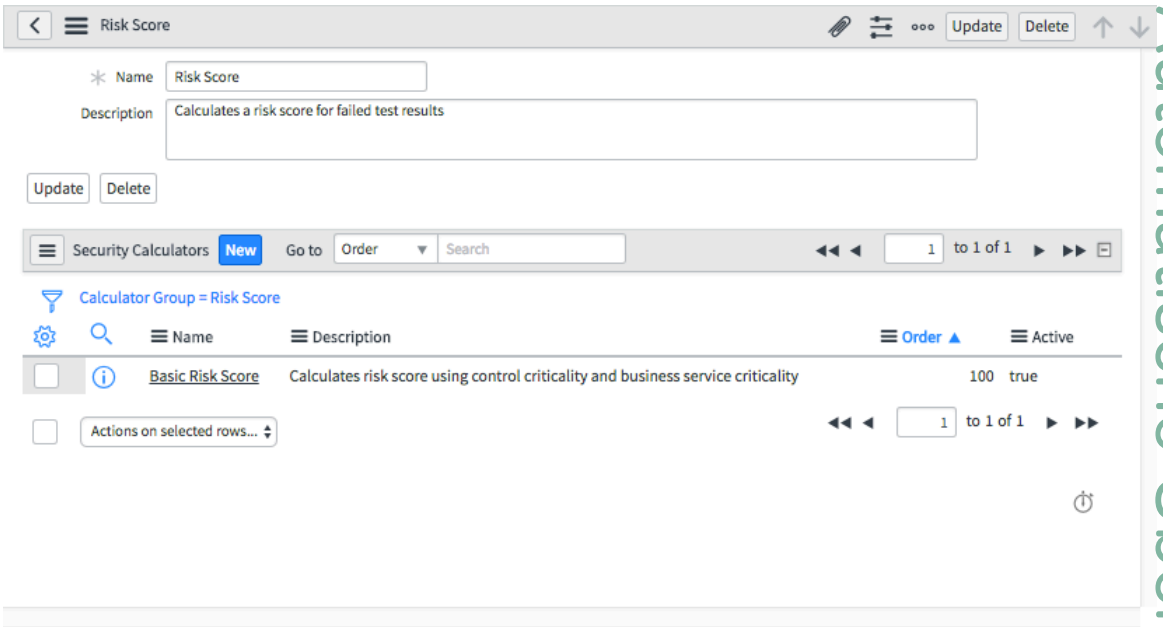
5. Klicken Sie im Header des Formulars mit der rechten Maustaste auf **Speichern**, oder klicken Sie auf **Absenden**.
   Die neue Rechnergruppe wird in der Gruppenliste mit den anderen Rechnern angezeigt. Klicken Sie auf den Namen der neuen Rechnergruppe, um den Datensatz zu öffnen. Weitere Informationen zum Festlegen von Bedingungen und angezeigten Werten und zum erneuten Anwenden von Rechnern finden Sie unter Erstellen, bearbeiten und wenden Sie Risikorechner für erneut an Configuration Compliance.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die zugehörige Liste „ **Sicherheitsrechner“** wird angezeigt.




**6.** Klicken Sie auf **Neu**, um der Gruppe Rechner mit ihren Bedingungen hinzuzufügen.

Die Beachtung der Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird für diesen Datensatz oder dieses Formular nicht unterstützt.

### Configuration Compliance Rechner und Rechnerregeln

Configuration Compliance Automatisieren Sie die Berechnung der Anfangswerte für die Felder in den Testergebnissen. Die Bedingung für jeden Rechner wird der Reihe nach ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

## Configuration Compliance -Rechner

Das Configuration Compliance-Basissystem enthält einen Konfigurations-Compliance-Rechner (**Standardrisikorechner** ), der die Basis- **Risikopunktzahl** für das Testergebnis festlegt. Configuration Compliance-Rechner können erstellt werden, um die Auswirkungen von Testergebnissen basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle oder die Klasse des Konfigurationselements (CI) handelt, können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie zusätzliche Konfigurations-Compliance-Rechner erstellen, um andere Felder in Testergebnissen festzulegen, oder Sie können die vorhandenen Konfigurations-Compliance-Rechner anpassen. Ein Rechner kann so geschrieben werden, dass er einen beliebigen Satz von Prioritäten widerspiegelt.

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel der Reihe nach ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Alle aktivierten Konfigurations-Compliance-Rechner legen die ausgewählten Felder jedes Mal fest, wenn ein Testergebnis erstellt wird, wenn sich ein zugeordnetes CI oder ein Konfigurationstest ändert oder wenn der zugehörige Link **Risikopunktzahl berechnen** in einem Testergebnis verwendet wird. Beispielsweise wird die Risikopunktzahl in Testergebnisdatensätzen automatisch aktualisiert, wenn der Wert für „control.criticality“ in einem importierten Testergebnis aktualisiert wird. Nachdem ein Testergebnisimport eine Testergebnispunktzahl aktualisiert hat, kann der Benutzer die Risikopunktzahl der Testergebnisse neu berechnen, indem er auf die **Schaltfläche Rechner erneut anwenden** klickt.

Wenn Sie aus einem vorhandenen Testergebnis auf den zugehörigen Link Risikopunktzahl berechnen klicken und einer der Rechner aktiviert ist, wird das Feld Risikopunktzahl im Testergebnis aktualisiert.

**Hinweis:**
Der zugehörige Link **Risikopunktzahl** berechnen ist nur sichtbar, wenn mindestens ein Konfigurations-Compliance-Rechner aktiviert ist.

## Configuration Compliance Rechnerregeln

Standardmäßig wird ein Basissystem- **Standardrisikorechner** bereitgestellt. Wenn Sie eine Risikoregel für diesen Rechner erstellen möchten, müssen Sie das Zielfeld des **Standardrisikorechners** auf **Risikopunktzahl**festlegen. Klicken Sie auf die Schaltfläche **Neue Risikoregel**, um eine neue Risikoregel zu erstellen . Dieser erstellt eine spezialisierte Testergebnis-Rechnerregel, die als **Risikoregel** bezeichnet wird, die wiederum die **Risikopunktzahl** basierend auf mehreren Werten berechnet. Standardmäßig werden die folgenden Werte für die Berechnung der Risikopunktzahl alsbetrachtet:

- Business-Relevanz
- Relevanz

Sie können die in der **Standardrisikoregel** zu verwendenden Werte anpassen und festlegen, wie viel Gewichtung jeder dieser Werte erhalten soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis- **Risikopunktzahl**zählt.

Ab Configuration Compliance Version 13.0 können Sie die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Felder und Gewichtungen für die Risikoregel definieren .

## Zuweisen eines Gewichtungsprozentsatzes

Sie können auch einen Gewichtungsprozentsatz (0–100) auf Feldwertebene zuweisen. Sie können beispielsweise jeder Schweregradstufe („Keine“ bis „Kritisch“) einen Gewichtungsprozentsatz zuweisen. Wenn die Relevanzgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für die Relevanzstufe zugewiesen werden:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Gewichtungsprozentsatz zuweisen**

| Relevanz | Risikopunktzahl |
|---|---|
| Kritisch | 100 |
| Hoch | 50 |
| Mittel | 20 |
| Keine | 0 |

Wenn die Relevanz kritisch ist, beträgt die entsprechende Gewichtung 50. Wenn die Relevanz hoch ist, beträgt die Gewichtung 25, bei mittlerer Relevanz beträgt die Gewichtung 10. Wenn die Relevanz keine ist, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie unter unter Beispiel für die Berechnung der Risikopunktzahl für Configuration Compliance.

Jede Regel hat eine Einstellung für **Reihenfolge**. Die erste Übereinstimmung mit den Bedingungen aktualisiert jedoch das Feld **Risikopunktzahl** im Testergebnis. Nicht geskriptete Rechnerregeln haben in der Regel weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

Der Basissystemrechner Configuration Compliance enthält Rechnerregeln, die jeder Relevanzstufe („Keine“ bis „Kritisch“) basierend auf dem Schweregrad einen Wert (0–100) für die **Risikopunktzahl** zuweisen. Dem Schweregrad „Unbekannt“ wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, z. B. der Standardrisikorechner, neue Rechnerregeln oder neue Risikoregeln können erstellt werden.

## Gewichtungen der Schwachstellen-Risikopunktzahl

Allen Schwachstellen werden eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Exploit-Informationen usw. zugewiesen. Die Geschäftsregel `Update Risk Rating from Risk Score` in der Tabelle „Angreifbares Element“ ist für die Berechnung der Risikobewertung verantwortlich. Immer wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17.1 der Anwendung Vulnerability Response (VR) wurden die folgenden Risikobewertungen als Teil der Skripteinbindung VulnerabilityUtilsbereitgestellt, die hartcodiert war.

| Wert (Risikobewertung) | Gewichtung (Risikopunktzahl) |
|---|---|
| 1 | 90–100 |
| 2 | 70–89 |
| 3 | 40–69 |
| 4 | 1–39 |
| 5 | 0 |

Ab Version 18.0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als cc_risk_rating bereitgestellt. Diese Typen werden als Teil der Geschäftsregel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wurde so geändert, dass Sie die Einträge in den Werten der Tabelle „Risikopunktzahlgewichtungen“ für die Risikobewertungsberechnung abfragen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Geschäftsregeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle „Gewichtungen der Risikopunktzahl“ zugreifen, indem Sie im Filternavigator sn_sec_cmn_risk_score_weight eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (CI) von „Nicht mit Internetzugriff“ in „Mit Internetzugriff“ ändert.
- Wenn die zugeordneten Common Vulnerabilities and Exposures (CVEs) oder Drittanbietereinträge (TPEs) für die angreifbaren Elemente (VIs) mit einer CVE Known Exploit Vulnerability (KEV) verknüpft sind

### Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die für Ihre Organisation eindeutigen Test- und Asset-Daten verwenden. Durch Auswahl der Felder, die in der Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

#### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

#### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Risikorechner**.
2. Klicken Sie **auf Standardrisikorechner**.
3. Wählen Sie das Zielfeld als **Risikopunktzahl**aus.
   Die Schaltfläche **Neue Risikoregel** wird in der Tabelle „Rechnerregel“ angezeigt.
4. Klicken Sie auf die Schaltfläche **Neue Risikoregel**, um zum Formular **Configuration Compliance-Risikoregel** zu navigieren.
5. Legen Sie im Abschnitt „Kriterien für Risikorechner“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung in der Gesamtrisikopunktzahlberechnung fest.
6. Deaktivieren Sie die Checkbox **Aktiv**, um die Regel zu deaktivieren.
7. Klicken Sie auf **Kriterien** hinzufügen, um den Kriterien des Risikorechners Risikoregelfelder hinzuzufügen.
8. Füllen Sie die Felder des Formulars aus.

**Formular „Risikoregelfeld“.**

| Feld | Beschreibung |
|---|---|
| Referenztabelle auswählen | Die Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden.<br><br>Wählen Sie unter den folgenden Optionen aus: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Testergebnis: Fügen Sie Felder hinzu, die Sie direkt über das Testergebnis (TR) erreichen können.<br>○ Testergebnis – Konfigurationselement: Fügen Sie durchlaufbare Dot-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle.<br>Diese Felder sind nicht Teil der Basistabelle cmdb_ci.<br>○ Testergebnis – Test: Fügen Sie Dot-Walkable-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittparteieintrag. Diese Felder sind nicht Teil der Konfigurationstest-Basistabelle.<br>○ Testergebnis-Referenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) sind, oder Tabellen, die einen Verweis auf das Testergebnis enthalten. Diese Felder sind nicht direkt aus dem Testergebnis per Dot-Walk ableitbar.<br>○ Konfigurationselement-Referenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci enthalten. Diese Felder sind nicht direkt vom TR aus punktweise durchlaufbar.<br>○ Testreferenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vulc_test sind, oder Tabellen, die einen Verweis auf sn_vulc_test enthalten. Diese Felder sind nicht direkt vom TR aus punktweise durchlaufbar.<br>○ Benutzerdefinierte Bedingungen: Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der mit dem Internet verbundene Filter, ob ein Configuration Item (CI) extern oder intern ist. |
| Feld | Das Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Gewichtung | Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine ganze Zahl zwischen 0 und 100 sein. |
| Tabelle | ○ Testergebnis > Konfigurationselement<br>○ Testergebnis > Test<br>○ Test-Ergebnisreferenztabelle<br>○ Referenztabelle für Konfigurationselemente<br>○ Test-Referenztabelle<br>Dieses Feld wird nur angezeigt, wenn eine der aufgelisteten Optionen im Feld Referenztabelle wählen ausgewählt wird. |
| Zusammenfassung | Wählen Sie den minimalen oder maximalen Wert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird.<br>Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle wählen eine Referenztabelle ausgewählt wird. |
| Definieren Sie die Wertgewichtung | Komponente zum Zuweisen von Gewichtungen zu jedem Feldwert. Definieren Sie für numerische Felder Feldwerte als Bereich (z. B. 1–5). Der Wert muss eine Ganzzahl zwischen 0 und 100 sein.<br>Dieses Feld wird nicht angezeigt, wenn im Feld Referenztabelle wählen die Option Benutzerdefinierte Bedingungen ausgewählt ist. |
| Bedingungstabelle | Wählen Sie eine Bedingung aus der Liste aus.<br>Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. |
| Feldname | Geben Sie einen Namen für die Risikokriterien ein.<br>Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die Option Benutzerdefinierte Bedingungen ausgewählt wird. |
| Bedingung | Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen.<br>Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen die |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Option Benutzerdefinierte Bedingungen ausgewählt wird. |

9. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für das aktive Testergebnis neu zu bewerten.

## Erstellen oder bearbeiten Sie Risiko-Rollup-Rechner für Configuration Compliance

Erstellen Sie einen neuen Risikorechner, oder bearbeiten Sie einen vorhandenen.

### Vorbereitungen
Erforderliche Rolle: Erforderliche Rolle: sn_vulc.admin

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** und wählen Sie **Risikopunktzahl-Rollup-Rechner**aus.
2. Klicken Sie in der angezeigten Liste der Risikopunktzahl-Rollup-Rechner auf einen Rechner, um den Datensatz zu öffnen und das Formular zu bearbeiten.
3. Alternativ können Sie zum Erstellen eines neuen Rechners auf **Neu** klicken und das Formular ausfüllen.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Rollup-Rechners für Konfigurationstest oder Testergebnisgruppe. |
| Beschreibung | Eine Beschreibung für den Risiko-Rollup-Rechner. |
| Skriptwerte | Bearbeiten Sie die Werte im Skript nach Bedarf.<br>**Hinweis:**<br>Das Bearbeiten von Skripts erfordert fortgeschrittene Kenntnisse der Anwendung Now Platform und Configuration Compliance. |

4. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.

Rollup-Rechner sind regelmäßige Aufgaben, die stündlich ausgeführt werden, um Änderungen zu erfassen. Diese geplanten Aufgaben enthalten auch Gesamtrisikowerte für Konfigurationstests und Korrekturaufgaben. Die Rollup-Werte werden in den Feldern „Risikopunktzahl“ angezeigt.

Ein Beispiel dafür, wie ein Risiko-Rollup-Rechner Punktzahlen bestimmt, finden Sie unter Beispiel für Risiko-Rollup-Berechnung für Configuration Compliance.

## Erstellen, bearbeiten und wenden Sie Risikorechner für erneut an Configuration Compliance

Rechnerregeln können bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können diese Funktion verwenden, um die Konfiguration des Risikorechners anzupassen und bei Bedarf Änderungen anzuwenden, um Ergebnisse zu importieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

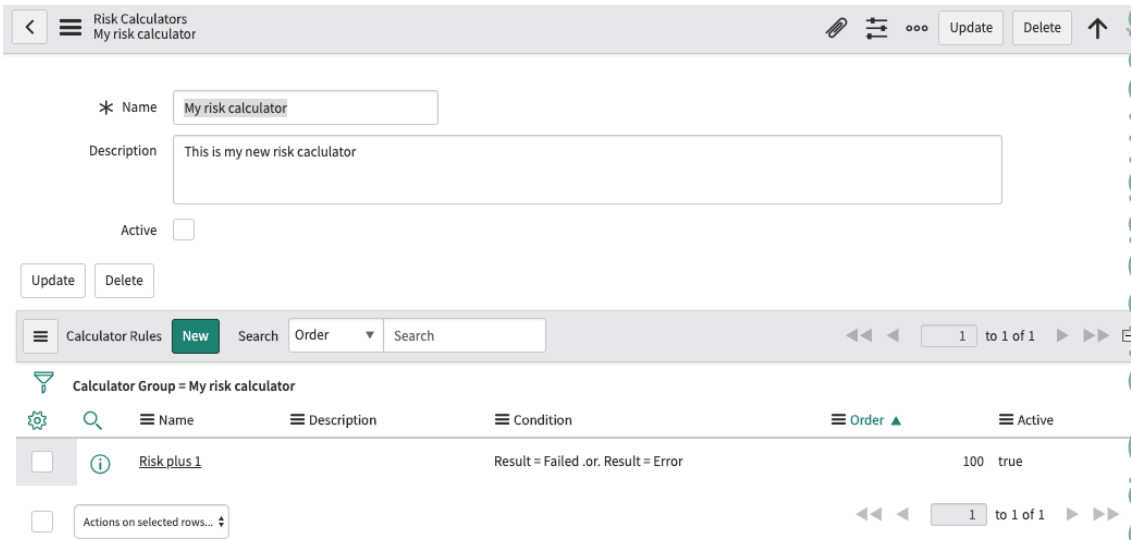
## Prozedur

**1.** Führen Sie die folgenden Schritte aus, um einen neuen Risikorechner zu erstellen.

**a.** Navigieren zu **Alle** > **Configuration Compliance** > **Administration** und wählen Sie **Risikorechner**aus.

**b.** Klicken Sie in der Liste „Risikorechner“ auf **Neu**.

**c.** Geben Sie einen Namen und eine Beschreibung für Ihren neuen Rechner ein, und klicken Sie auf **Absenden**.
Der neue Rechner wird in der Liste „Risikorechner“ angezeigt.




**d.** Klicken Sie in der Liste auf den neuen Rechner, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird, und geben Sie die Felder und Werte an, die in Testergebnisdatensätzen und Korrekturaufgaben angezeigt werden sollen.

**e.** Klicken Sie im angezeigten Datensatz auf **Neu**.

**f.** Füllen Sie die Felder auf den Registerkarten entsprechend aus.

| Registerkarte | Beschreibung |
|---|---|
| Wenn diese Bedingung erfüllt ist | Verwenden Sie den Bedingungen-Generator, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird. Beispiel: Ergebnis ist Fehlgeschlagen oder Ergebnis ist Fehler. |
| Diese Werte festlegen | Verwenden Sie die Vorlage, um die Felder und Werte auszuwählen, die angezeigt werden sollen. |

**g.** Klicken Sie auf **Absenden**.
Der Datensatz wird mit den neuen Rechnerregeln und der Gruppe angezeigt, zu der er gehört.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Führen Sie die folgenden Schritte aus, um einen vorhandenen Rechner erneut anzuwenden, um Ergebnisse zu testen oder die Regeln und angezeigten Werte für einen vorhandenen Risikorechner zu bearbeiten.

   a. Wählen Sie in den Listen „Risikorechner“ oder „Risiko-Rollup-Rechner“ den Rechner aus, den Sie bearbeiten möchten.

   b. Um einen Risikorechner erneut auf die vorhandenen Testergebnisdaten aus dem Datensatz anzuwenden, klicken **Sie auf Rechner**erneut anwenden.
   Alle Testergebnisse, die die Bedingungen des Rechners erfüllen, werden aktualisiert.

   **Hinweis:**
   Abhängig von der Anzahl der Testergebnisse kann diese Aktualisierung einige Zeit dauern.

   c. Um die Bedingungen und Werte zu bearbeiten, klicken Sie links unten in der Spalte Name auf den Namen des Rechners.
   Für Risikorechner werden der Datensatz und die Registerkarten **Wenn diese Bedingung erfüllt ist** und **Diese Werte festlegen** angezeigt.

   d. Füllen Sie das Formular entsprechend aus.

| Registerkarte | Feldbeschreibung |
|---|---|
| Wenn diese Bedingung erfüllt ist | Verwenden Sie den Generator für Filterbedingungen, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt werden soll. |
| Diese Werte festlegen | Wählen Sie eine, um fortzufahren.<br>▪ Werttyp: Vorlage. Wählen Sie Felder aus der Liste und die entsprechenden Werte aus.<br>▪ Skript: Geben Sie Ihre Änderungen mit dem Editor ein.<br>**Hinweis:**<br>Das Bearbeiten von Skripts erfordert fortgeschrittene Kenntnisse der Anwendung Now Platform und Configuration Compliance. |

3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um die neuen Regeln bei Bedarf auf Ihre vorhandenen Testergebnisdaten anzuwenden.

   a. Klicken Sie in der angezeigten Liste „Risikorechner“ auf einen Rechner, den Sie anwenden möchten.
   Der Datensatz wird angezeigt.

   b. Klicken **Sie auf Rechner erneut** anwenden, um Ihre Änderungen zu testen und bei Bedarf auf Ihre Importergebnisse anzuwenden.

4. Zeigen Sie Ihre Änderungen an den Testergebnissen an, und bearbeiten Sie Ihre Rechner nach Bedarf weiter.

### Beispiele für die Berechnung der Risikopunktzahl Configuration Compliance .

Ab v13.0 von Configuration Compliancekönnen Sie die Kriterien für die Standardrisikoregel anpassen. Verwenden Sie Risikopunktzahlen von Drittanbietern wie Qualys und Tenable für die Berechnung der Risikopunktzahl.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drittanbieter wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden in das Feld Relevanz in der Tabelle sn_vulc_test eingetragen. Verwenden Sie dieses Feld für Risikopunktzahlberechnungen. Gehen Sie wie folgt vor, um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden:

### Fügen Sie die Quellenrelevanz als Kriterium für eine Risikoregel hinzu

Verwenden Sie Punktzahlen basierend auf der Relevanz, die von Drittanbietern bereitgestellt werden, um Risikopunktzahlen zu berechnen.

#### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

#### Warum und wann dieser Vorgang ausgeführt wird

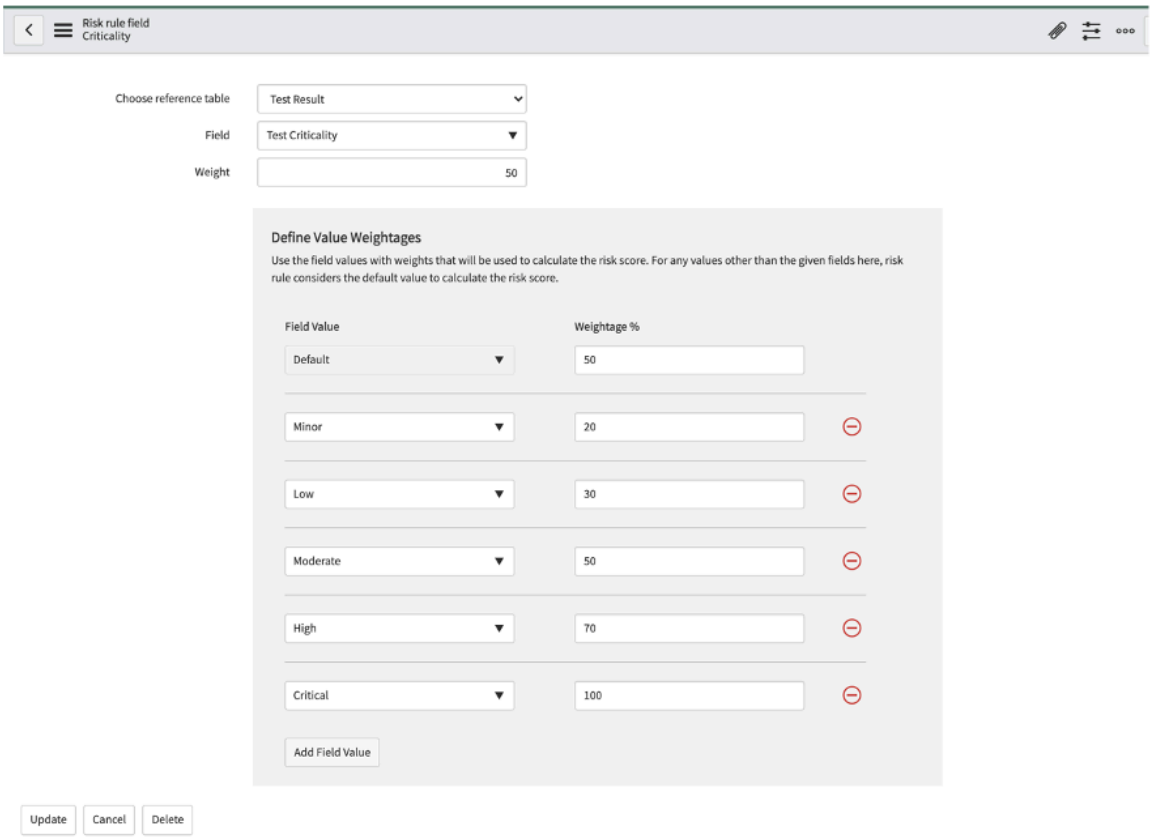
Drittanbieter wie Qualys und Tenable geben ihre eigenen Risikopunktzahlen an. Diese Punktzahlen werden in das Feld Relevanz in der Tabelle sn_vulc_test eingetragen. Verwenden Sie dieses Feld für Risikopunktzahlberechnungen und die Berechnung der Risikopunktzahl.

#### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie zum Formular „Risikoregel“.
3. Deaktivieren Sie die Checkbox **Aktiv**, um die Regel zu deaktivieren.
4. Klicken **Sie auf Kriterien hinzufügen**.
5. **Wählen Sie in der Liste Referenztabelle** wählen die Option **Testergebnis**aus.
6. Wählen Sie in der Liste **Feld** die **Option Test.Relevanz aus**.
7. **Geben Sie** im Feld Gewichtung die relative Wichtigkeit dieses Felds an.
   Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
8. Fügen Sie im Abschnitt **„Wertgewichtungen definieren“ Feldwerte** hinzu, und weisen Sie den Feldern einen Gewichtungsprozentsatz zu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**9.** Klicken Sie auf **Absenden**.

### Geschäftsrelevanz als Kriterium für eine Risikoregel hinzufügen

Geben Sie einen Relevanzwert für Business Services an, und verwenden Sie die Geschäftsrelevanz, um die Risikopunktzahlen zu berechnen.

**Vorbereitungen**
Erforderliche Rolle: sn_vulc.admin

**Warum und wann dieser Vorgang ausgeführt wird**
Angenommen, Ihre Organisation verfügt über viele Geschäftsservices, und ein Configuration Item (CI) wird von den folgenden Services verwendet:

**Relevanz der Business Services**

| Business-Service | Relevanz |
|---|---|
| Cloud-Management | 1 – Am kritischsten |
| E-Commerce | 2 – Einigermaßen kritisch |
| Client-Services | 3: Weniger kritisch |
| Reisekosten und Spesen | 4: Nicht kritisch |

Die Zuordnung zwischen CI und Services wird in der Tabelle „Services“ [cmdb_ci_services] gespeichert. Wenn ein CI einen Konfigurationstest nicht besteht, wird ein Testergebnis (TR)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

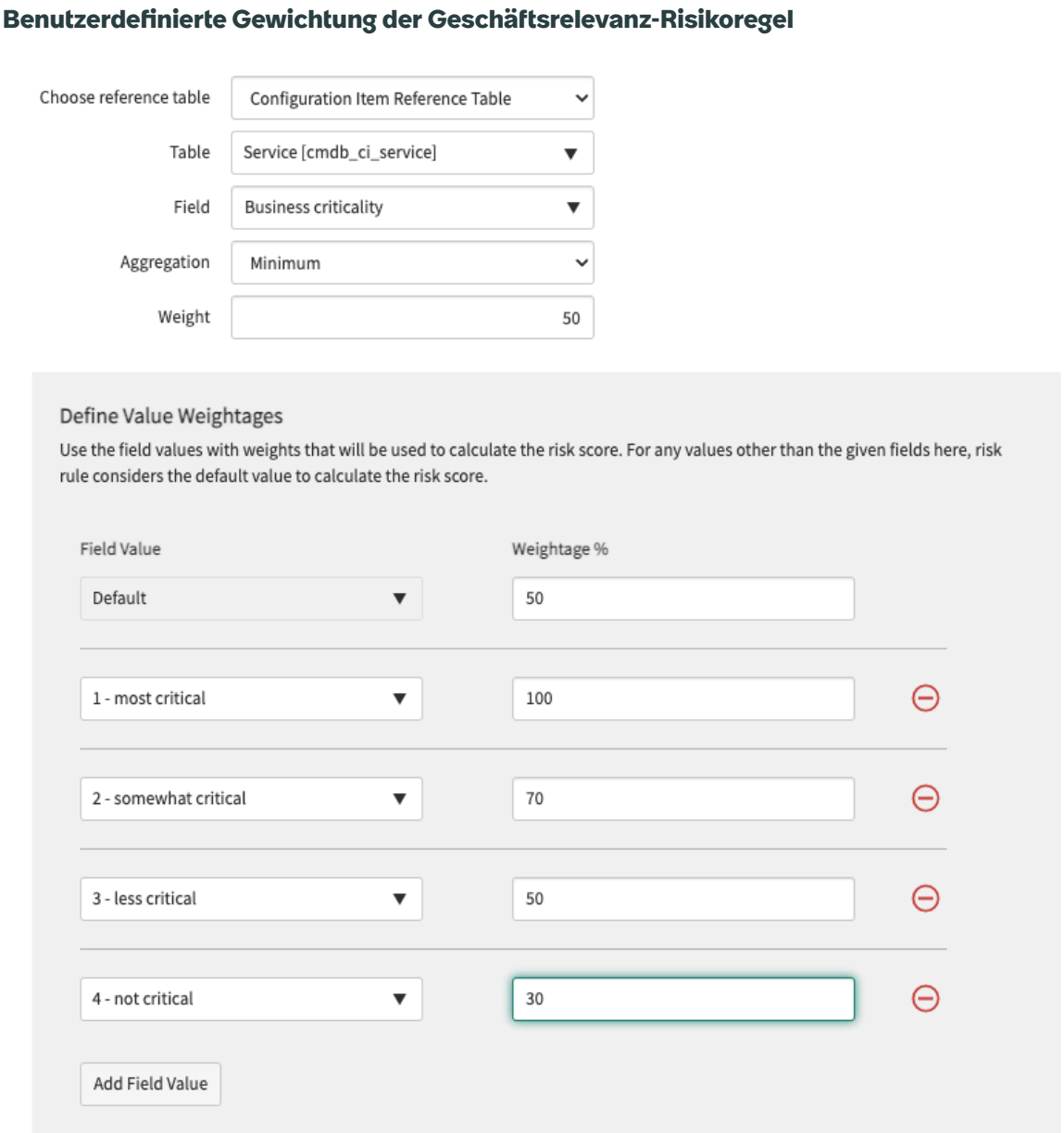
erstellt. Sie können den Wert der Geschäftsrelevanz der betroffenen Services verwenden, um die Risikopunktzahl für diese TR zu berechnen. Befolgen Sie das Verfahren, um den Relevanzwert dieser Services zur Berechnung der Risikopunktzahl zu verwenden.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie im Abschnitt „ **Rechnerregeln** “ zum Formular „Risikoregel“.
3. Deaktivieren Sie die Checkbox **Aktiv**, um die Regel zu deaktivieren.
4. Klicken **Sie auf Kriterien hinzufügen**.
5. **Wählen Sie in der Liste Referenztabelle** auswählen **Konfigurationselement-Referenztabelle**aus.
6. Wählen Sie in der Liste **Tabelle** die **Option Service [cmdb_ci_service] aus**.
7. Wählen Sie in der Liste **Feld** die Option **Geschäftsrelevanz**aus.
8. **Wählen** Sie im Feld Zusammenfassung die Option **Minimum** aus, um den kritischsten Service für diesen Anwendungsfall abzurufen (1 – Am kritischsten Wert) oder **Maximum**, um den am wenigsten kritischen Service für diesen Anwendungsfall abzurufen (4 – Nicht kritischer Wert).
9. **Geben Sie** im Feld Gewichtung die relative Wichtigkeit dieses Felds an.
   Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
10. Fügen Sie im Abschnitt **„Wertgewichtungen definieren“ Feldwerte** hinzu, und weisen Sie Gewichtungen zu.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Automatische Übersetzung

**11.** Klicken Sie auf **Absenden**.

## Fügen Sie dem Risikorechner ein bedingtes Kriterium hinzu

Verwenden Sie benutzerdefinierte Bedingungen für die Risikoregel für die Berechnung der Risikopunktzahl.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Ihre Organisation verfügt über mehrere Konfigurationselemente (CIs), von denen ein externer Benutzer nur auf einige zugreifen kann. Benutzer können Risikopunktzahlgewichtungen für diese nach außen gerichteten CIs hinzufügen.

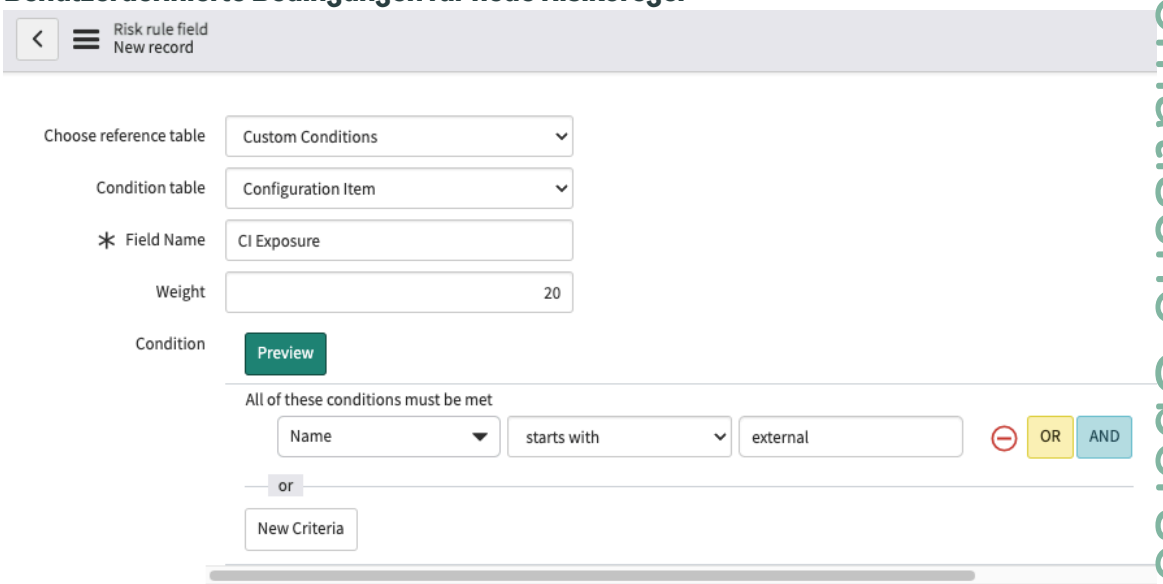
**Hinweis:**
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „external“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Risikorechner**.
2. Navigieren Sie zum Formular „Risikoregel“.
3. Deaktivieren Sie die Checkbox **Aktiv**, um die Regel zu deaktivieren.
4. Klicken **Sie auf Kriterien hinzufügen**.
5. **Wählen Sie in der Liste Referenztabelle** auswählen die **Option Benutzerdefinierte Bedingungen**aus.
6. Wählen Sie in der Liste **BedingungstabelleKonfigurationselement**aus.
7. Geben Sie im **Feld** Feldname CI-Gefahrenpotenzial ein.
8. **Geben Sie** im Feld Gewichtung die relative Wichtigkeit dieses Felds an.
   Der Wert muss eine ganze Zahl zwischen 0 und 100 sein.
9. Wählen Sie im Feld **Bedingung** die Option **Name > beginnt mit**aus, und geben Sie als Wert externalan.

**Benutzerdefinierte Bedingungen für neue Risikoregel**




10. Klicken Sie auf **Absenden**.

#### Zugehörige Informationen

Configuration Compliance-Rechnergruppen

## Beispiel für die Berechnung der Risikopunktzahl für Configuration Compliance

Bestimmen Sie die Risikopunktzahlrechner, um Risikopunktzahlen zu generieren, die die für Ihre Organisation spezifischen Test- und Asset-Daten verwenden.

## Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregelrechner bestimmt werden. Angenommen, ein Risikoregelrechner ist mit den Feldern in dieser Tabelle konfiguriert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bestimmen Sie die Punktzahlen des Risikoregelrechners**

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| Steuerung.Relevanz | 50 | Standard: 0<br>Gering: 20<br>Niedrig: 30<br>Moderat: 50<br>Hoch: 70<br>Kritisch: 100 |
| Business_Relevanz | 50 | Standard: 0<br>Gering: 20<br>Niedrig: 30<br>Moderat: 50<br>Höhe: 70<br>Kritisch: 100 |

Angenommen, die in dieser Tabelle angezeigten Testergebnisse sind im System vorhanden.

**Testergebniszuordnung**

| ID | Business-Relevanz | Kontrollrelevanz |
|---|---|---|
| CTR0000001 | 1: Am kritischsten | Kleiner |
| CTR0000002 | 1: Am kritischsten | Niedrig |
| CTR0000003 | 2: Einigermaßen kritisch | Kleiner |
| CTR0000004 | 2: Einigermaßen kritisch | Mittel |
| CTR0000005 | 3: Weniger kritisch | Niedrig |

Die Risikopunktzahlberechnung für das Testergebnis wird basierend auf der Formel berechnet:

Risikopunktzahl = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100, wobei W die Gewichtung und FV der Gewichtungsprozentsatz des Feldwerts ist.

Die resultierende Risikopunktzahl für diese Testergebnisse ist in der folgenden Tabelle beschrieben:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Risikopunktzahl basierend auf Testergebnissen**

| ID | Geschäftsrelevanz (50 %) | Kontrollrelevanz (50 %) | Resultierende Risikopunktzahl |
|---|---|---|---|
| CTR0000001 | 1 – Am kritischsten (50 % x 100) | Gering (50 % x 20) | 60 |
| CTR0000002 | 1 – Am kritischsten (50 % x 100) | Niedrig (50 % x 30) | 65 |
| CTR0000003 | 2 – Einigermaßen kritisch (50 % x 70) | Gering (50 % x 30) | 45 |
| CTR0000004 | 2 – Einigermaßen kritisch (50 % x 70) | Mittel (50 % x 50) | 60 |
| CTR0000005 | 3 – Weniger kritisch (50 % x 50) | Niedrig (50 % x 30) | 40 |

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie in dieser Tabelle die Ergebnisse:

**Ergebnisse für geänderten Gewichtungsprozentsatz**

| Feld | Gewichtung | Gewichtungsaufgliederung |
|---|---|---|
| Steuerung.Relevanz | 50 | Standard: 0<br>Gering: 20<br>Niedrig: 30<br>Moderat: 60<br>Höhe: 70<br>Kritisch: 100 |
| Business_Relevanz | 50 | Standard: 50<br>1 – Am kritischsten: 100<br>2 – Einigermaßen kritisch: 70<br>3 – Weniger kritisch: 20<br>4 – Nicht kritisch: 30 |

Die Risikopunktzahl für die Testergebnisse nach erneuter Anwendung des Rechners wird in der folgenden Tabelle angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Risikopunktzahl für TR bei erneuter Anwendung des Rechners

| ID | Geschäftsrelevanz (50 %) | Kontrollrelevanz (50 %) | Resultierende Risikopunktzahl |
|---|---|---|---|
| CTR0000001 | 1 – Am kritischsten (50 % x 100) | Gering (50 % x 20) | 60 |
| CTR0000002 | 1 – Am kritischsten (50 % x 100) | Niedrig (50 % x 30) | 65 |
| CTR0000003 | 2 – Einigermaßen kritisch (50 % x 70) | Gering (50 % x 30) | 45 |
| CTR0000004 | 2 – Einigermaßen kritisch (50 % x 70) | Mittel (50 % x 60)<br>*Überarbeiteter Wert | 65<br>*Überarbeiteter Wert |
| CTR0000005 | 3 – Weniger kritisch (50 % x 20)<br>*Überarbeiteter Wert | Niedrig (50 % x 30) | 25<br>*Überarbeiteter Wert |

### Beispiel für Risiko-Rollup-Berechnung für Configuration Compliance

Das folgende Beispiel zeigt, wie Punktzahlen für Risiko-Rollup-Rechner bestimmt werden.

Für den folgenden Rollup-Rechner für Testergebnisgruppen lautet die Formel zur Berechnung der Gruppenrisikopunktzahl des Testergebnisses:

(Maximale Risikopunktzahl/100) * 85 + (Faktor * 15).

Der Faktor in der vorherigen Gleichung wird durch die Anzahl der Testergebnisse bestimmt (siehe folgende Tabelle).

| Anzahl Testergebnisse | Faktor |
|---|---|
| <10 | 0,2 |
| 1-99 | 0,4 |
| 100–1000 | 0,6 |
| 1001–9999 | 0,8 |
| > 1000 | 1 |

Für die folgende Korrekturaufgabe, TRG0003066, mit drei Testergebnissen Risikopunktzahlen beträgt die maximale Punktzahl 90.

| Nummer | Risikopunktzahl | Gruppe | Ergebnis | Status |
|---|---|---|---|---|
| CTR000123 | 90.0 | TRG0003066 | Fehlgeschlagen | Offen |
| CTR000124 | 70 | TRG0003066 | Fehlgeschlagen | Offen |
| CTR000125 | 40 | TRG0003066 | Fehlgeschlagen | Offen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die Korrekturaufgabe, TRG0003066, beträgt die Risikopunktzahl 79, (90/100) * 85 + 0,2 * 15 = Math.floor (76,5 +3) = 79.

Die historische Risikopunktzahl ist null, da die Gruppe noch „Offen“ ist.

Nach der Datenerfassung lauten die Testergebnisse „Bestanden“, und die Gruppe wechselt zu „Geschlossen“, wie in der folgenden Tabelle dargestellt.

| Nummer | Risikopunktzahl | Gruppe | Ergebnis | Status |
|---|---|---|---|---|
| CTR000123 | 0 | TRG0003066 | Bestanden | Geschlossen |
| CTR000124 | 0 | TRG0003066 | Bestanden | Geschlossen |
| CTR000125 | 0 | TRG0003066 | Bestanden | Geschlossen |

Der Verlauf der Testergebnisse wird in der folgenden Tabelle angezeigt.

| Nummer | Risikopunktzahl | Neuestes Ergebnis | Ergebnis |
|---|---|---|---|
| CTRH000111 | 90.0 | CTR000123 | Fehlgeschlagen |
| CTRH000112 | 70 | CTR000124 | Fehlgeschlagen |
| CTRH000113 | 40 | CTR000125 | Fehlgeschlagen |

Die Risikopunktzahl ist 0, da in der Gruppe keine offenen Testergebnisse vorhanden sind.

Die maximale Risikopunktzahl der Ergebnisse, die bestanden haben, + die maximale Risikopunktzahl aus dem Verlauf – 90.

Für die Testergebnisgruppe TRG0003066 beträgt die historische Risikopunktzahl 79.

(90/100) * 85 + 0,2 * 15 = Math.Grundriss (76,5 +3) = 79.

## Erstellen oder bearbeiten Sie Configuration Compliance Testergebnis-Gruppenregeln

Sie können Regeln erstellen, um Testergebnisse basierend auf Filterbedingungen automatisch zu gruppieren. Diese Regeln gruppieren Testergebnisse automatisch, wenn sie importiert werden. Verwenden Sie den Filter, um die nach dieser Regel gruppierten Testergebnisse zu begrenzen, z. B. Auswahl aller Testergebnisse mit Exploits.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem enthält eine Testergebnis-Gruppenregel, **Zuweisungsgruppe, Test**, die Testergebnisse nach Zuweisungsgruppe gruppiert (vorausgefüllt aus **Zuweisungsregeln**) und das Testergebnis-Feld **Test**. Diese Regel kann mithilfe von Filterbedingungen und Gruppenschlüsseln geändert werden. Gruppenschlüssel sind Spalten in der Testergebnistabelle. Wählen Sie bis zu sechs Schlüssel aus, um anzugeben, welche Werte zum Gruppieren der Testergebnisse verwendet werden sollen.

Ab Version 14.7 von Configuration Complianceist die Regel **Zuweisungsgruppe,** Testgruppe für neue Implementierungen deaktiviert.

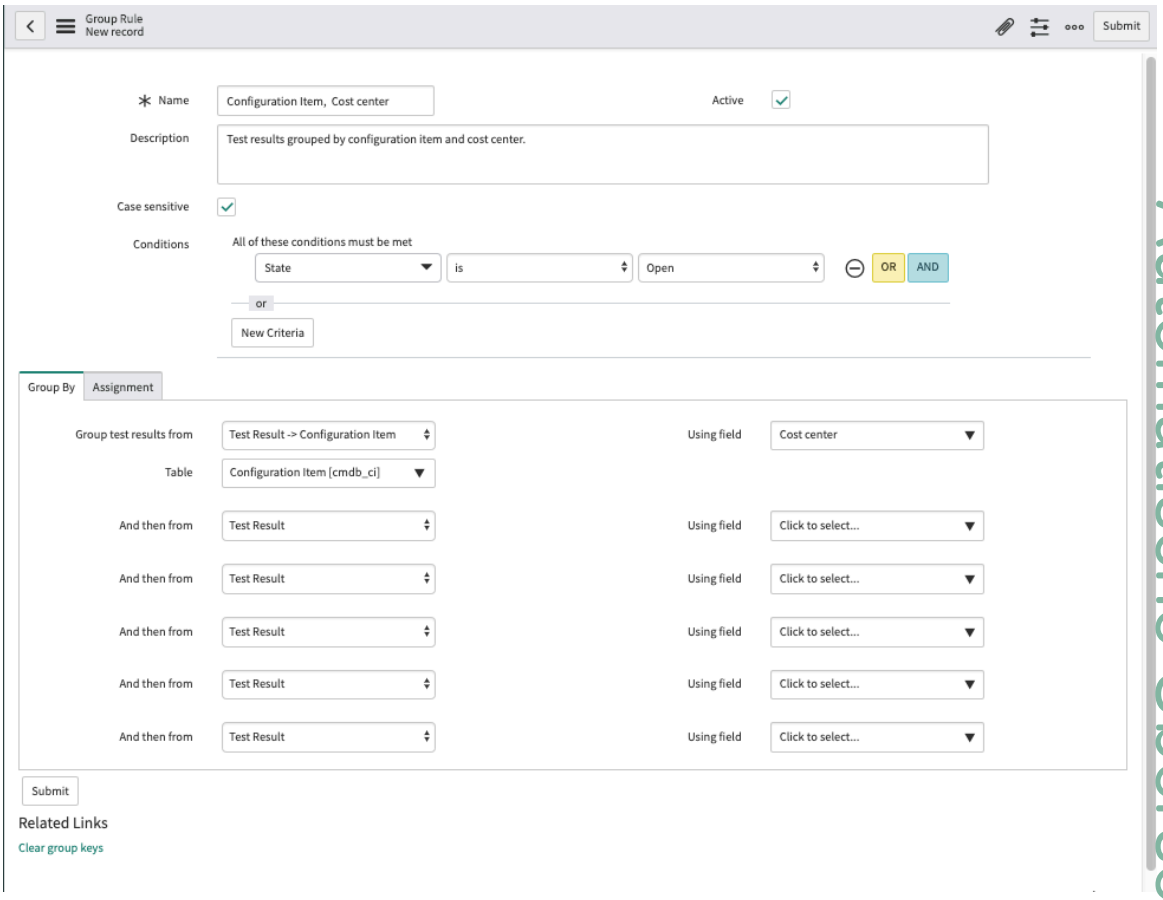


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch oder manuell über die **Schaltfläche Erneut anwenden** im Formular „Gruppenregel“ ausgewertet.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Gruppenregeln**.
2. Öffnen Sie die **Zuweisungsgruppe,** die Testregel, oder klicken Sie auf **Neu**.




3. Wenn **Neu**, füllen Sie die Felder im Formular entsprechend aus.

#### Configuration Compliance Testergebnis-Gruppenregel

| Feld | Beschreibung |
|---|---|
| Name | Name der Gruppenregel. |
| Aktiv | Gibt an, ob die Gruppe aktiv ist. |
| Beschreibung | Textbeschreibung dieser Testergebnis-Gruppenregel. |
| Groß-/ Kleinschreibung beachten | Bestimmt, ob bei der Regelübereinstimmung die Groß-/Kleinschreibung beachtet wird oder nicht.<br>**Hinweis:**<br>Beim Standardwert wird die Groß-/Kleinschreibung beachtet. |
| Bedingungen | Bedingungen, die erfüllt sein müssen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Standardmäßig (Kontrollkästchen „Groß-/Kleinschreibung beachten“ deaktiviert) wird beim**Suchtext**, den Sie im Bedingungsgenerator für Gruppenregel-Datensätze und -Formulare eingeben, nicht zwischen Groß- und Kleinschreibung unterschieden. Sie haben die Möglichkeit, die Suche nach Groß-/Kleinschreibung in Gruppendatensätzen und Formularen zu aktivieren. |
| **Gruppieren nach** | |
| Testergebnisse gruppieren von | Automatisieren Sie die Erstellung von Gruppen basierend auf dieser Regel. Wählen Sie eine der verfügbaren Optionen aus.<br>○ Testergebnis \| Feld wird verwendet<br>○ Testergebnis->Konfigurationselement \| Tabelle \| Feld wird verwendet<br>Wenn ein erweitertes **Tabellenfeld** ausgewählt ist, werden Testergebnisse, die die entsprechende erweiterte Tabelle nicht verwenden, in einer separaten Korrekturaufgabe gruppiert. |
| **Zuweisung** | |
| Weisen Sie Testergebnisgruppen nach zu | Automatisieren Sie die Zuweisung von Gruppen, die basierend auf dieser Regel erstellt wurden. Wählen Sie eine der verfügbaren Optionen aus.<br>○ Gruppen-Key<br>Wenn diese Option ausgewählt ist, wird ein Feld Schlüsselwert angezeigt. Die verfügbaren Felder werden in einem Dropdown-Menü aufgelistet.<br>○ Benutzergruppe<br>Wenn diese Option ausgewählt ist, wird ein Suchfeld für Benutzergruppen angezeigt. |

4. Klicken Sie auf **Absenden**.

**Hinweis:**
**Der** zugehörige Link Gruppieren nach Schlüssel löschen entfernt die Gruppenschlüssel aus der Registerkarte Gruppieren nach im Formular.

## Geben Sie die Dauer einer für eine Korrekturaufgabe angeforderten Ausnahme an

Verwenden Sie Systemeigenschaften, um die Dauer zu begrenzen, für die eine Ausnahme für eine Korrekturaufgabe angefordert wird. Die Korrektur der Korrekturaufgabe wird für den angegebenen Zeitraum zurückgestellt.

### Vorbereitungen
Erforderliche Rolle: sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Die Eigenschaft sn_vulc.exception_max_request_days wird verwendet, um die maximale Anzahl von Tagen anzugeben, für die eine Ausnahme für eine Korrekturaufgabe angefordert werden kann. Der Standardwert beträgt 365 Tage.

**Hinweis:**

Sie können die Eigenschaft sn_vulc.exception_approval_required verwenden, um den Ausnahmegenehmigungs-Workflow für die Korrekturaufgabe zu deaktivieren, wenn er nicht erforderlich ist. Standardmäßig ist diese Eigenschaft aktiviert und ihr Wert ist true.

### Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie auf der Seite „Systemeigenschaften“ nach sn_vulc.exception_max_request_days.
3. Klicken Sie auf den Eigenschaftsnamen, um den Datensatz „Systemeigenschaft“ zu öffnen.
4. Um diesen Datensatz bearbeiten zu können, stellen Sie sicher, dass Configuration Compliance als aktuelle Anwendung ausgewählt ist.
5. Geben Sie einen positiven **Wert** ein, und klicken Sie auf **Aktualisieren**.
   Der Datensatz wird aktualisiert und gespeichert.

## Konfigurieren Sie Exception Management für Configuration Compliance

Begrenzen Sie die Dauer einer angeforderten Ausnahme und fügen Sie der Ausnahme mithilfe des Moduls Configuration Compliance einen Fragebogen hinzu. Standardmäßig wird eine Ausnahme mit dem Modul ServiceNow® Vulnerability Response angefordert. Sie können eine Ausnahme auch mit der GRC: Policy and Compliance Management -Integration anfordern.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response aktiviert ist, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ebenso können Sie, wenn das Modul GRC: Policy and Compliance Management installiert ist, GRC: Policy and Compliance Management auf dem Konfigurationsbildschirm auswählen. Wenn Sie diese Option aktivieren, können Sie eine Ausnahme anfordern, die das Policy and Control-Ziel von GRCangibt.

Wenn Sie einen Fragebogen hinzufügen, wird dieser an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung ausgelöst hat. Sie können entweder den Standardfragebogen verwenden oder einen Fragebogen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Ausnahmenverwaltung**.
2. Wählen Sie im Formular „Ausnahmeverwaltungskonfiguration“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste Ausnahmen verwalten mit auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Vulnerability Response Version 17.1 können Sie entweder Vulnerability Response oder GRC: Policy and Compliance Managementauswählen. Sie müssen das Plugin [ GRC aktivieren, um GRC: Policy and Compliance Management zum Anfordern einer Ausnahme zu verwenden. Das Ändern der Konfiguration hat keine Auswirkungen auf die vorhandenen Daten.

3. Füllen Sie die Felder im Formular basierend auf der von Ihnen ausgewählten Option aus.
   - Wenn Sie die Option Vulnerability Response ausgewählt haben, füllen Sie die Felder im Formular aus.

**Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

| Feld | Beschreibung |
|---|---|
| Dauer | Zeitraum, für den eine Ausnahme angefordert werden kann. |
| Einheit | Zeiteinheit für den angegebenen Zeitraum. |
| Fragebogen aktivieren, um Ausnahme anzufordern | Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung. |
| Fragebogen, um Ausnahme anzufordern | Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Anfordern einer Ausnahme. Der Ausnahmefragebogen wird standardmäßig angezeigt. |

   - Wenn Sie die Option GRC: Policy and Compliance Management ausgewählt haben, füllen Sie die Felder im Formular aus.

**Einstellungen für Formular „VR-Ausnahmeverwaltung“.**

| Feld | Beschreibung |
|---|---|
| Fragebogen aktivieren, um falsch positive Meldung zu markieren | Option zum Hinzufügen eines Fragebogens zur ausgelösten falsch positiven Anforderung. |
| Fragebogen, um falsch positive Meldung zu markieren | Option zum Anzeigen des von Ihnen ausgewählten Fragebogens, um ihn als falsch positiv zu kennzeichnen. Der Fragebogen für eine falsch positive Anforderung wird standardmäßig angezeigt. |

4. Wählen Sie **Speichern**.

## Fügen Sie einen Ausnahmegenehmiger für hinzu Configuration Compliance

Fügen Sie den Genehmigergruppen Benutzer hinzu, damit Sie eine Ausnahme für eine Korrekturaufgabe in Configuration Complianceanfordern können.

### Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird
Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit dem standardmäßigen zweistufigen Genehmigungs-Workflow genehmigt. Das Hinzufügen von Benutzern zur Gruppe der ersten Ebene ist

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

obligatorisch. Wenn sich keine Benutzer auf der zweiten Ebene befinden, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

**Hinweis:**
Wenn es keinen Genehmiger der ersten Ebene gibt, kann keine Ausnahme angefordert werden.

**Hinweis:**
Bis Configuration Compliance v13.0 kann keine Ausnahme angefordert werden, wenn es keinen Genehmiger der ersten Ebene gibt. Wenn Sie jedoch ab Configuration Compliance v13.0 die CC-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für die Ausnahmeverwaltung standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht wieder in Workflow ändern.

### Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Benutzer und Gruppen** > **Gruppen**.
2. Suchen Sie in der Spalte Name nach **Ausnahme**und klicken Sie auf **Ausnahmegenehmiger - Ebene 1 CC**.

   **Hinweis:**
   Ab Configuration Compliance v14.7.5 können Sie die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahmeanforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** und wählen Sie `sn_vulc.exception_approver_L1_CC` oder `sn_vulc.exception_approver_L2_CC`, um den Eigenschaftswert zu ändern.

3. Navigieren Sie im Formular „Gruppenausnahmegenehmiger – Ebene 1 CC“ zu **Gruppemmitglieder** > **Neu** (oder **Bearbeiten**).
4. Füllen Sie die Felder des Formulars aus.

**Benutzerformular**

| Feld | Beschreibung |
|---|---|
| Anwender-ID | Eindeutiger Bezeichner für den Benutzer |
| Vorname | Vorname des Benutzers. |
| Nachname | Nachname des Benutzers. |
| Titel | Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus. |
| Abteilung | Abteilung des Benutzers. |
| Passwort | Dem Benutzer zugewiesenes Passwort. Dieses Passwort kann dauerhaft oder temporär sein. |
| Passwort muss zurückgesetzt werden | Option, mit der Benutzer das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten. |
| Gesperrt | Option, um den Benutzer für die Instanz zu sperren und alle aktiven Sitzungen des Benutzers zu beenden. Das System verhindert, dass Benutzer mit der Administratorrolle sich selbst aussperren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Aktiv | Option zum Aktivieren dieses Benutzers. Nur Sie können einen inaktiven Benutzer in diesen Bereichen sehen:<br>○ Listen der Benutzer<br>○ Auswahlliste für Referenzfelder (Lupensymbol)<br>○ Autovervollständigen-Liste, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben |
| Nur Webservice-Zugang | Option, um diesen Benutzer als nicht interaktiven Benutzer festzulegen. |
| Interner Integrationsbenutzer | Option zum Festlegen dieses Benutzers als internen Integrationsbenutzer. |
| E-Mail | E-Mail-Adresse des Benutzers. |
| Sprache | Bevorzugte Sprache des Benutzers. |
| Kalenderintegration | Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook. |
| Zeitzone | Zeitzone für den Standort dieses Benutzers. |
| Datumsformat | Bevorzugtes Datumsformat des Anwenders. |
| Telefon (geschäftlich) | Geschäftliche Telefonnummer des Benutzers. |
| Mobiltelefon | Mobiltelefon des Benutzers. |
| Foto | Foto, das Sie hochladen können, indem Sie **auf Hinzufügen klicken... klicken**. |

5. Klicken Sie auf **Absenden**.
6. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 5, um einen Ausnahmegenehmiger – Ebene 2 CC zu erstellen.

   **Hinweis:**
   Wählen Sie beim Erstellen eines Genehmigers der zweiten Ebene **Ausnahmegenehmiger – Ebene 2 CC**

7. **Wahlweise:** Wenn Sie **Bearbeiten**auswählen, verschieben Sie Benutzer aus der **Sammlung** in den **Bereich Gruppenmitglieder**, und klicken Sie auf **Speichern**.
   Der Genehmiger muss zu navigieren **Alle** > **Configuration Compliance** > **Meine Freigaben** und Anforderungen genehmigen.

## Erstellen Sie eine Configuration Compliance -Relevanzzuordnung

Configuration Compliance Die -Kritikalitätszuordnung bietet eine Transformationszuordnung für Quellkritikalitätsfelder von Drittparteien zu erkennbaren Feldern im Schweregrad Configuration Compliance.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Relevanz-Zuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

#### Feldzuordnung

| Feld | Beschreibung |
|---|---|
| Quelle | Der Name der Quelle für die Relevanzzuordnung. |
| Quellwert | Der Quellrelevanzwert. |
| Zielwert | Der Zielwert. Auswahlmöglichkeiten:<br>**Kritisch**<br>Das mit der Steuerung verbundene Konfigurationsproblem verursacht eine Unterbrechung eines oder mehrerer geschäftskritischer CIs.<br>**Hoch**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung dar, verursacht jedoch nicht das Herunterfahren wichtiger Netzwerkressourcen.<br>**Mittel**<br>Das mit der Kontrolle verbundene Konfigurationsproblem ist ein Risiko, aber keine unmittelbare Bedrohung.<br>**Niedrig**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung auf niedriger Ebene dar und kann für CIs mit höherem Risiko ignoriert werden.<br>**Kleiner**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt ein geringes Risiko dar und kann bei Bedarf ignoriert werden. |

4. Klicken Sie auf **Absenden**.

## Erstellen Sie E-Mail-Benachrichtigungen

Schwachstellenadministratoren können die Benachrichtigung bearbeiten oder neue hinzufügen und angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhalten soll und welcher Inhalt in der Benachrichtigung enthalten sein soll.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Sie können E-Mail-Vorlagen für verschiedene Arten von E-Mail-Benachrichtigungen erstellen. Weitere Informationen zum Erstellen von E-Mail-Vorlagen finden Sie unter Definieren Sie E-Mail-Vorlagen für Vulnerability Response.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**.
2. Wählen Sie den Benachrichtigungsdatensatz des Korrekturziels aus, oder wählen Sie **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie **Benachrichtigungsvorschau** aus, um die Nachricht anzuzeigen.

### Ergebnisse

Ab v14.11 von Configuration Compliancewerden, wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, die Datensätze je nach Rolle in Vulnerability Manager Workspace oder IT Remediation Workspace geöffnet.

- Links werden in Vulnerability Manager Workspace für Benutzer mit der Rolle sn_vulc.admin geöffnet.
- Links werden in IT Remediation Workspace für Benutzer mit der Rolle „sn_vulc.remediation_owner“ geöffnet.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Benutzeroberfläche geöffnet.

## Konfigurieren Sie Genehmigungsregeln für Exception Management in Configuration Compliance

Verwenden Sie ab Configuration Compliance v13.0 den Flow Designer, um Ausnahmeanforderungen für die Ausnahmeverwaltung und Ausnahmeregeln zu genehmigen. Wenn Sie CC zum ersten Mal bereitstellen, ist der Flow Designer standardmäßig aktiviert.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie bereits ein Configuration Compliance -Benutzer sind, lautet die Standardoption workflow.

Wenn Sie Configuration Compliance v13.0 oder höher bereitgestellt haben, wird der Wert der Systemeigenschaft *`sn_vulc.flow_designer_activation`* auf „true“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie Configuration Compliance bereits vor v13.0 verwenden, wird der Wert dieser Systemeigenschaft auf „false“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in true ändern.

**Hinweis:**
Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer in Configuration Compliance.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmeverwaltungs-Workflows konfigurieren.

- Ausnahmegenehmigungsregeln für Testergebnisgruppen
- Genehmigungsregel für automatische Ausnahmeregeln



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Weitere Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management in Configuration Compliance.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Genehmigungsregeln** > **Ausnahmegenehmigungsregeln für Testergebnisgruppe**.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsregel“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Tabelle | Tabelle, auf die die Regel angewendet wird. |
| Anwendung | Der Standardwert ist Configuration Compliance. |
| Regeltyp | Gibt den Regeltyp an. Beispiel: Ausnahmeverwaltung oder Ausnahmeregel. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungsregeln. |
| Ablaufdatum der Genehmigung (Tage)<br>Ab v14.11 von Configuration Compliance | Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann. |
| Genehmiger benachrichtigen (Tage)<br>Ab v14.11 von Configuration Compliance | Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen. |

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte Genehmigungskonfigurationen sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel in Configuration Compliance.

**Hinweis:**
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management in Configuration Compliance.

**Example:**
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Testergebnisse in verschiedenen Testergebnisgruppen definieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erstellen Sie Konfigurationen für eine Genehmigungsregel in Configuration Compliance

Definieren Sie die Bedingungen, um übereinstimmende Testergebnisgruppen für eine Genehmigungsstufe herauszufiltern.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Im Modul „Genehmigungskonfigurationen“ können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

**Hinweis:**
Verwenden Sie das Modul „Genehmigungsregeln“, um Genehmigungsregeln für die Ausnahmeverwaltungs-Workflows zu konfigurieren. Weitere Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management in Configuration Compliance.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungskonfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungskonfiguration. |
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. |
| Bestellung | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird. |
| Beschreibung | Kurzbeschreibung der Genehmigungskonfigurationsebenen. |
| Bedingung | Identifiziert die übereinstimmenden Testergebnisgruppen. |

5. Wählen Sie **Aktualisieren**.
   Sie können Bedingungen mit mehreren Genehmigungsebenen innerhalb einer Regel definieren. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den entsprechenden Genehmigungs-Workflow. Weitere Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für Exception Management in Configuration Compliance.

### Example:

Sie können verschiedene Genehmigungspfade für verschiedene Arten von Testergebnisgruppen definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erstellen Sie Genehmigungsebenen für Exception Management in Configuration Compliance

Definieren Sie die Ebenen der Benutzer und Benutzergruppen, die die Ausnahmeanforderungen genehmigen.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Genehmigungsregeln**.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zur Registerkarte **Genehmigungskonfigurationen**.
3. Wählen Sie eine Konfiguration aus.
4. **Wählen Sie** im Abschnitt Genehmigerebenen eine Genehmigerebene aus.
5. Füllen Sie die Felder des Formulars aus.

#### Formular „Genehmigerebene“

| Feld | Beschreibung |
|---|---|
| Name | Name der Genehmigungsebene. |
| Erforderliche Genehmigung | Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind:<br>○ Ein Genehmiger erforderlich<br>○ Alle Anwender müssen genehmigen |
| Aktiv | Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird. |
| Bestellung | Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Reihenfolgeeintrag von 100 vor einer Konfiguration mit einem Reihenfolgeeintrag von 200 ausgeführt. |
| Freigaberegel | Enthält die Tabellen- und Typdetails für die Genehmigungsregel. Dieses Feld ist schreibgeschützt. |
| Genehmigungskonfiguration | Enthält die Genehmigungskonfigurationen Dieses Feld ist schreibgeschützt. |
| Zuweisen mit | Wählen Sie eine Option aus:<br>○ Anwender und Anwendergruppe<br>○ Genehmigungstabellenfeld<br>○ Skript |
| Gruppen | Genehmigerebenengruppe, die aus mehreren Benutzern besteht. Der Benutzer muss eine der folgenden Rollen für Ausnahmemanagement und Ausnahmeregeln haben: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ sn_vulc.exception_approver<br>○ sn_vulc.read<br>○ sn_vulc.read_auto_exception_rule |
| Anwender | Bearbeiten Sie die in den Gruppen aufgeführten Benutzer. |

6. Um die Änderungen zu speichern, wählen Sie **Aktualisieren**.

**Hinweis:**
Vor v13.0 funktionierte der Workflow-Prozess nur, wenn Benutzer nur auf Ausnahmeebene 1 vorhanden waren. Ab v13.0 muss jedoch mindestens ein Benutzer auf jeder Ebene vorhanden sein.

Vor v13.0 wurde im Workflow die Testergebnisgruppe zurückgestellt, wenn sich kein Benutzer auf der zweiten Ebene befand. Wenn jedoch ab v13.0 kein Benutzer auf der zweiten Ebene vorhanden ist, wird die Genehmigungsanforderung automatisch abgelehnt.

**Example:**
Für Testergebnisgruppen für Linux- und Windows-Server kann es unterschiedliche Genehmigungsebenen geben.

### Ausnahmeverwaltungs-Workflow im Vergleich zu Flow Designer in Configuration Compliance

Ab Configuration Compliance (CC) v13.0 ist bei der erstmaligen Bereitstellung von CC der Flow Designer für die Genehmigung von Ausnahmeanforderungen in der Ausnahmenverwaltung standardmäßig aktiviert. Wenn Sie bereits CC-Benutzer sind, lautet die Standardoption workflow.

#### Workflow und Flow Designer im Vergleich

| Überlegungen | Workflow | Flow Designer |
|---|---|---|
| Version | Vor Version 13.0 von CC | Ab v13.0 von CC. |
| Standardoption | Standardoption, wenn Sie ein vorhandener CC-Benutzer sind. | Standardoption für neue CC-Benutzer ab v13.0. |
| Festlegen des Genehmigungsprozesses | Die Ausnahmeverwaltung umfasst Ausnahmeanforderungen und Ausnahmeregeln. | Beinhaltet die Definition verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. Die Ausnahmeverwaltung umfasst Ausnahmeanforderungen und Ausnahmeregeln. |
| Upgrade auf Flow Designer | Sie können ein Upgrade von Workflow auf Flow Designer durchführen. Bestehende Anforderungen können jedoch nur mit dem Workflow genehmigt werden. | Flow Designer ist standardmäßig aktiviert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow und Flow Designer im Vergleich (Fortsetzung)**

| Überlegungen | Workflow | Flow Designer |
|---|---|---|
| Systemeigenschaft `sn_vulc.flow_designer_activation` | Wenn Sie den Workflow für die Änderungsverwaltung vor v13.0 verwendet haben, ist die Systemeigenschaft auf „false“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „true“ fest.<br>**Hinweis:** Sie können den Workflow nicht wiederherstellen, nachdem Sie den Flow Designer aktiviert haben. | Wenn Sie CC für v13.0 oder höher zum ersten Mal verwenden, wird der Wert der Systemeigenschaft standardmäßig auf „true“ festgelegt. |
| Modul „Genehmigungsregeln“ | Nach dem Festlegen der Systemeigenschaft auf „true“ wird die geplante Aufgabe „ **Modulfreigaberegeln aktivieren** “ innerhalb von 24 Stunden ausgeführt. Diese regelmäßige Aufgabe aktiviert das Modul „ **Genehmigungsregeln** “. Um dieses Modul sofort zu aktivieren, führen Sie diese Aufgabe manuell aus. | Wenn Sie CC zum ersten Mal aus CC v13.0 bereitgestellt haben, ist dieses Modul standardmäßig verfügbar. |
| Genehmigungsebenen | Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen. | Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel. |

## Configuration Compliance-Integrationen

Drittanbieterintegrationen importieren Konfigurationsbewertungsergebnisse, Richtlinien, Tests, Technologien, autoritative Quellen, Testergebnisse und andere Schwachstellendaten in die Anwendung Configuration Compliance.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die Anwendung Configuration Compliance unterstützt die folgenden Drittanbieterintegrationen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ab v14.11 können Sie die Behebung von Sicherheitslücken in Ihren Unternehmens-Assets, die von der Anwendung Security Posture Control identifiziert wurden, vorantreiben, indem Sie Ergebnisse als Testergebnisse in der Anwendung Configuration Compliance veröffentlichen. Die Anwendung Security Posture Control und ihre unterstützten Anwendungen sind mit separaten Abonnements über den ServiceNow® Storeverfügbar. Weitere Informationen finden Sie unter Sicherheitsstatus-Überwachung.
- Microsoft Defender for Cloud Integration für Security Operations
- Palo Alto Prisma Cloud Vulnerability Integration
- Integration von Configuration Compliance in Qualys
- Das Tenable.io -Produkt der Tenable Vulnerability-Integration

## Zusätzliche Hinweise für -Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 14.8.5 von Configuration Complianceregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

## Microsoft Defender for Cloud Integration für Security Operations

Das Produkt Microsoft Defender for Cloud Integration ist ein Sicherheitsmanagementsystem für Infrastrukturen, das die Sicherheitslage Ihrer Cloud-Umgebungen verbessert.

Microsoft Defender for Cloud Integration für Security Operations [] ist in die Anwendung Configuration Compliance integriert , um Tests Konfigurationselementen (CIs) zuzuordnen und so Testergebnisse zu erstellen. Er erkennt kontinuierlich neue Cloud-Ressourcen, die über Arbeitsauslastungen hinweg bereitgestellt werden, und bestimmt, ob sie gemäß Sicherheitsstandards wie dem Center for Internet Security (CIS) konfiguriert sind.

Ab Version 2.2 wird Microsoft Azure Security Center in Microsoft Defender for Cloud Integration für Security Operationsumbenannt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verfügbare Versionen

| Anwendung | Version |
|---|---|
| Microsoft Defender for Cloud Integration für Security Operations | 2.3 |
| Configuration Compliance | 14.3 |
| Security Support Common | 13.2 |
| Vulnerability Response | 16.2 |

## Mehrere Bereitstellungen der Microsoft Defender for Cloud -Plattform

Wenn Sie mehrere Bereitstellungen der Plattformanwendung Microsoft Defender for Cloud haben, können Sie für jede Bereitstellung eine Integration hinzufügen. Ressourcen, die von mehreren Drittanbieterbereitstellungen identifiziert werden, werden konsolidiert und mit Ihrem Configuration Management Database (CMDB)abgeglichen. Diese Konsolidierung findet auch dann statt, wenn sich Scan-Prozesse zwischen mehreren Bereitstellungen überschneiden.

## ServiceNow Microsoft Defender for Cloud Integrationen

Microsoft Defender for Cloud Integration für Security Operations erweitert die Compliance-Daten in Ihrer Instanz, indem Daten aus Microsoft Defender for Cloudabgerufen werden. Eine Reihe von regelmäßigen Aufgaben ruft die Integrationen automatisch auf. Sie können diese regelmäßigen Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Testergebniskorrektur, indem die Instanz mit Microsoft Defender for Cloudsynchronisiert wird.

Für jeden Integrationsdatensatz ist ein run-as-Benutzer mit dem Standardwert **VR.System konfiguriert**. Dieser Wert muss gleich bleiben.

**Hinweis:**
Wenn Sie keinen gültigen Run-as-Benutzer festlegen, werden für die Datenquellendatensätze doppelte oder mehrere Datenabrufanhänge erstellt. Die Anzahl der Anhänge erhöht sich jedes Mal, wenn die Integration ausgeführt wird. Dies erhöht die Verarbeitungszeit, was zu inkonsistenten Transformationsergebnissen führt.

Microsoft Defender for Cloud Plattformintegrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_asc.configure_integration: Möglichkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_asc.read_integration: Möglichkeit zum Lesen von Datensätzen.

## Microsoft Defender for Cloud Integrationen anzeigen

Zeigen Sie die Integrationen an, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem enthalten.

| Integration | Beschreibung |
|---|---|
| Integration der Richtliniendefinition | Ruft Richtlinien ab und erstellt Richtlinieneinträge in Ihrer Instanz. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Integration | Beschreibung |
|---|---|
| Bewertungsmetadaten-Integration | Ruft Bewertungsmetadaten ab und erstellt Tests in Ihrer Instanz. |
| Integration von Compliance-Standards und -Steuerungen | Ruft Standards und Steuerungen ab und erstellt die Autorisierungsquelle und die Bezugsvermerke. Anschließend werden sie mit den erstellten Tests verknüpft. |
| Bewertungsintegration | Ruft Bewertungen ab und verarbeitet sie in Ihrer Instanz. Die Ausgabe dieser Integration sind Testergebnisse. |

## Erstellen Sie CIs mit der Identification and Reconciliation Engine

Verwenden Sie die Identification and Reconciliation Engine (IRE), um CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Drittanbieter-Scanner importiert wurde.

Wenn ein CI in der CMDB nicht übereinstimmt, wird ein CI in der Klasse *cmdb_ci_cmp_resource* erstellt. Später, wenn eine Erkennung dasselbe CI findet, wird das CI erweitert oder ein anderes erstellt.

**Hinweis:**
Für Cloud-Ressourcen findet kein automatischer Abgleich statt.

### Microsoft Defender for Cloud Integration für Security Operationsinstallieren und konfigurieren

Installieren und konfigurieren Sie Microsoft Defender for Cloud Integration für Security Operations, damit Sie die aus Microsoft Defender for Cloud importierten Daten verwenden können, um Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

#### Vorbereitungen

Erstellen Sie eine neue App-Registrierung in Azure Active Directory. Um weitere Informationen zum Registrieren einer neuen Anwendung in Azure Active Directory zu erhalten, suchen Sie auf der Microsoft-Dokumentationswebsite nach Client-Anwendungen in Azure Active Directory registrieren. Weisen Sie die **Sicherheitsleser-** Rolle für die neu erstellte App-Registrierung im entsprechenden Bereich zu, mit dem Sie eine Verbindung zu ServiceNowherstellen möchten. Sie kann sich auf Verwaltungsgruppen- oder Abonnementebene befinden.

Erforderliche Rolle: sn_vulc.admin

#### Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
2. Suchen Sie in der Suchleiste nach Microsoft Defender for Cloud Integration for Security Operations.
3. Wählen Sie **Installieren** aus.

   Alle zu installierenden Abhängigkeiten werden angezeigt.
4. Navigieren zu **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Konfiguration** > **Microsoft Defender für Cloud-Konfiguration**.
5. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Microsoft Defender for Cloud Konfigurationsformular

| Feld | Beschreibung |
|---|---|
| API-URL | Ressourcen-URL der Instanz<br><br>Beispiel: https://management.azure.com (Azure Public Cloud) |
| Mandanten-ID | Mandantenidentität Ihrer Organisation. |
| Integrationsinstanz | Standardinstanz. Sie können auch eine Instanz erstellen, um die Daten aus mehreren Microsoft Defender -Mandanten oder -Abonnements zu übernehmen. |
| Client-ID | Clientidentität, die nach der Registrierung der Anwendung Microsoft Defender for Cloud Integration generiert wird. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel, der nach der Registrierung der Anwendung Microsoft Defender for Cloud Integration generiert wird. |
| Importieren Sie Ergebnisse aus | Ressourcen und Bewertungen, die den ausgewählten Verwaltungsgruppen-IDs und Abonnement-IDs entsprechen und abgerufen werden sollen. |
| Verwaltungsgruppen-IDs | Ressourcen und Bewertungen, die den abzurufenden Verwaltungsgruppen-IDs entsprechen.<br><br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn Sie im Feld Ergebnisse importieren aus die **OptionSpezifische Verwaltungsgruppen** auswählen. |
| Abonnement-IDs | Identifikationsnummern der Abonnements, für die die Ressourcen und Bewertungen abgerufen werden sollen.<br><br>**Hinweis:**<br>Dieses Feld wird nur angezeigt, wenn Sie **Spezifische Abonnements** im Feld **Ergebnisse** importieren aus auswählen. |
| Validierungsstatus | Gibt an, ob die angegebenen Anmeldeinformationen und Abonnement-ID gültig sind. |

6. Konfigurieren Sie die Integrationen, oder führen Sie sie aus, indem Sie **Speichern und testen**auswählen.

### Configuration Compliance importierte Daten für Microsoft Defender for Cloud Integration

Configuration Compliance importiert Richtlinien, Tests, autoritative Quellen und Testergebnisse aus Drittanbieterintegrationen und speichert sie in Modulen zur Ansicht.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Testgruppen

Eine Gruppe von Konfigurationstests bildet eine Testgruppe. Testgruppen beziehen sich auf autoritative Dokumente und Testdatensätze und können an die Anforderungen Ihrer Organisation angepasst werden. Ein Konfigurationstest kann mehreren Testgruppen angehören.

Wenn Microsoft Defender for Cloud Integration installiert ist, werden Testgruppen durch die regelmäßige Aufgabe **Policy Definitions Integration**abgerufen und ausgefüllt. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Integrationen** > **Integration von Richtliniendefinitionen**.

**Hinweis:**
Wenn Sie die Integration manuell ausführen möchten, führen Sie zuerst die Integration der **Richtliniendefinitionen** aus.

## Tests

Tests sind Bibliotheken von Datensätzen, die Scans von Computer-Assets organisieren. Konfigurationstests definieren, wie Assets gesteuert werden müssen.

Ein Configuration Compliance -Test ist der Mechanismus, den Integrationsanwendungen von Drittanbietern verwenden, um Assets nach Testergebnistyp zu gruppieren.

Wenn Microsoft Defender for Cloud Integration installiert ist, ruft die regelmäßige Aufgabe **Assessment Metadata Integration**die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Integration** > **Primäre Integrationen** > **Bewertungsmetadaten-Integration**.

**Hinweis:**
Wenn Sie die Integration manuell ausführen möchten, führen Sie die **Bewertungsmetadatenintegration nach der Integration** der **Richtliniendefinitionen**aus.

## Autorisierende Quellen

Configuration Compliance verwendet maßgebliche Quellen und Zitate, wenn Schwachstellenwarnungen für Tests generiert werden. Autorisierende Quellen beziehen sich normalerweise auf Abschnitte veröffentlichter Branchenstandards wie **ISO 27001** und **PCI DSS 3.2.1**.

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -verfahren.

Wenn Microsoft Defender for Cloud Integration installiert ist, ruft die regelmäßige Aufgabe **Compliance Standards & Controls**die autorisierenden Quellen und Bezugsvermerke ab. Sie können diese regelmäßige Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Integration von Compliance-Standards und -Steuerungen**.

**Hinweis:**
Wenn Sie die Integration manuell ausführen möchten, führen Sie die **Compliance Standards & Controls-Integration** nach der **Bewertungsmetadaten-Integration**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Assets

Die **Bewertungsintegration** stellt wichtige Informationen wie Ressourcen-Tags und Cloud-Attribute bereit. Diese Informationen werden im Formular „Erkanntes Element“ angezeigt. Sie wird hauptsächlich zum Filtern in Configuration Compliance Zuweisungs- und Gruppenregeln verwendet.

- Ressourcen-Tags: Alle Cloud-Ressourcen-Tags werden im Rahmen der **Bewertungsintegration**als Host-Tags importiert. Die Cloud-Tags für jeden Cloud-Ressourcentyp werden hier gespeichert, unabhängig davon, ob die Ressource ein Host ist oder nicht.
  - Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **Tokyo**-Tag erstellt wird, kann kein Tokyo-Tag in der Host-Tag-Tabelle gespeichert werden. **Tokyo** und **TOKIO** werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag hat den Vorzug.
  - Die Verwendung von Host-Tags als Gruppenschlüssel in einer Gruppenregel kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Cloud-Attribute für Assets: Im Folgenden sind die Cloud-Attribute aufgeführt, die die Integrationen aus Microsoft Defender for Cloudabrufen:
  - Cloud-Account
  - Cloud-Region
  - Cloud-Ressourcentyp
  - Cloud-Service-Provider

## Testergebnisse

Configuration Compliance berechnet die Testergebnisse nicht, sondern importiert sie als Teil einer Drittanbieterintegration. Sobald sie in Configuration Complianceangezeigt werden, werden sie mithilfe von **Testergebnisgruppen korrigiert**.

Wenn die Microsoft Defender for Cloud -Integration installiert ist, ruft die regelmäßige Aufgabe **Assessment Integration**die Testergebnisse ab. Sie können diese regelmäßige Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Bewertungsintegration**.

Der Import der **Bewertungsintegration** ist die einzige Integration, die den Parameter *`Start Time`* auf der Registerkarte „ **Integrationsdetails** “ verwendet. Alle anderen Configuration Compliance -Importe übernehmen alle verfügbaren Daten unabhängig von *`Start Time`*.

Wenn der Import der **Bewertungsintegration** abgeschlossen ist, wird ein Event gestartet, um Berechnungen für das Importende auszulösen.

Die **Bewertungsintegration** ruft die Datenbewertungen standardmäßig nur ab, wenn sich der Status seit der letzten erfolgreichen Integrationsausführung für den letzten Tag ändert. Wenn die Bewertung in den letzten Tagen kontinuierlich fehlgeschlagen ist, ruft die Integration die Bewertung nicht ab, da für die Bewertung keine Statusänderung erfolgt. Um die Testergebnisse mit den Bewertungen der Verteidigung auf dem neuesten Stand zu halten, wird eine neue **Comprehensive Assessment-Integration** hinzugefügt, die die Daten der letzten sieben Tage abruft. Er wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## CI-Suchregeln zum Identifizieren von CIs aus Microsoft Defender for Cloud -Integrationen

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Configuration Compliance automatisch Ressourcendaten, um mithilfe von CI-Suchregeln nach Übereinstimmungen in Configuration Management Database (CMDB)zu suchen. Diese Regeln werden verwendet, um die Konfigurationselemente (CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Fehlerkorrektur zu unterstützen. CI-Suchregeln des Basissystems sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu CI-Suchregeln finden Sie unter CI-Sperrregeln für Microsoft Defender for Cloud Integration for Security Operations.

## Vulnerability Response Integration with Palo Alto Prisma Cloud verstehen

Prisma Cloud ist eine API-basierte Sicherheitslösung für Cloud-Infrastrukturen. Er stellt eine Verbindung zu Ihrer Cloud-Umgebung her und überwacht die Ressourcen, die in öffentlichen Cloud-Umgebungen bereitgestellt werden, z. B. Amazon Web Services (AWS), Microsoft Azureusw. Sie erhalten vollständige Transparenz und Kontrolle über Risiken in Ihrer Public Cloud-Infrastruktur.

Die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud erleichtert die Erfassung von Richtlinien und Warnungen aus Prisma Cloud als Tests bzw. Testergebnisse in der Anwendung Configuration Compliance. Mit der richtigen Konfiguration können die Testergebnisse nahtlos verwaltet werden, indem entsprechende Risikopunktzahlen zugewiesen und sie gruppiert und relevanten Benutzern und Gruppen zugewiesen werden.

## Verfügbare Versionen

In der Tabelle werden die Anwendungen aufgelistet, von denen Vulnerability Response Integration with Palo Alto Prisma Cloud abhängig ist, zusammen mit der Version der Anwendung.

| Anwendung | Version |
|---|---|
| Prisma-Cloud-Integration für Security Operations | 2.3 |
| Configuration Compliance | 14.7 |
| Security Support Common | 13.5 |
| Vulnerability Response | 18.0 |

## ServiceNow Prisma-Cloud-Integrationen

Die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud hilft beim Importieren der Prisma-Daten in Ihre Instanz ServiceNow, um Ihre Instanz für eine bessere Verwaltung anzureichern. Eine Reihe von geplanten Aufgaben ruft die Integrationen automatisch auf. Sie können diese regelmäßigen Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Testergebniskorrektur, indem die Instanz auf dem neuesten Stand gehalten wird, indem regelmäßig Daten aus Prisma Cloud abgerufen werden.

Prisma Cloud-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_prismacloud.configure_integration: Möglichkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_prismacloud.read_integration: Möglichkeit zum Lesen von Datensätzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Anzeigen der Integrationen

Sie können die Integrationen anzeigen, die Teil von Vulnerability Response Integration with Palo Alto Prisma Cloud sind, indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**.

Die folgenden Integrationen sind im Basissystem verfügbar.

| Ausführungssequenz | Zeitplan | Integration | Beschreibung |
|---|---|---|---|
| 1 | Wöchentlich | Prisma-Richtlinienintegration | • Ruft Richtlinien aus Prisma Cloud ab und erstellt Testeinträge in Ihrer Instanz.<br>• Sie bietet keinen inkrementellen Support. Wenn Sie die Integration für die letzten 10 Tage ausführen, wird auch das Ergebnis für vorherige Integrationsausführungen angezeigt. |
| 2 | Täglich | Integration von Prisma-Warnungen | • Ruft Warnungen aus Prisma Cloud ab und erstellt Testergebniseinträge in Ihrer Instanz.<br>• Bietet inkrementellen Support. Die Integration wird täglich nach der letzten Integrationsausführungszeit ausgeführt. |

### Die Installation von wird vorbereitet Vulnerability Response Integration with Palo Alto Prisma Cloud

Bereiten Sie die Installation von Vulnerability Response Integration with Palo Alto Prisma Cloud vor, indem Sie Setup-Aufgaben ausführen.

## Bevor Sie beginnen

Um Vulnerability Response in Palo Alto Prisma Cloud zu integrieren, muss Ihnen in Prisma eine Berechtigungsgruppe zugewiesen werden, die schreibgeschützten Zugriff auf Richtlinien- und Warnungsdaten bietet. Weitere Informationen zu Berechtigungsgruppen finden Sie unter https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/prisma-cloud-administrator-roles#id437b5c4a-3dfa-4c70-8fc7-b6d074f5dffc .

Ausführliche Informationen zu den Rollen, die verschiedenen Berechtigungsgruppen zugewiesen sind, finden Sie auf der Seite https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/prisma-cloud-admin-permissions .

Darüber hinaus müssen Zugriffsschlüssel erstellt werden, um das Lesen der Warnungen zu ermöglichen. Weitere Informationen zum Erstellen von Zugriffsschlüsseln finden Sie unter https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/create-access-keys .

Verwenden Sie die folgende Prüfliste, um Vulnerability Response Integration with Palo Alto Prisma Cloudzu installieren und zu konfigurieren. Vergewissern Sie sich vor der Installation der Anwendung, dass die aufgeführten Elemente abgeschlossen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prüfliste zur Vorbereitung der Integration

| Aufgabe | Beschreibung |
|---|---|
| ☐ | Vergewissern Sie sich, dass Sie über die folgenden Informationen verfügen:<br>• API-Basis-URL<br>• Zugangsschlüssel-ID<br>• Geheimer Schlüssel<br>• Benutzername und Passwort für den Zugriff auf Prisma Cloud.<br><br>Diese Anmeldeinformationen werden verwendet, um von der Instanz Now Platform® aus eine Verbindung zur Prisma Cloud-Instanz herzustellen. Die Zugriffsschlüssel-ID und der geheime Schlüssel müssen nach der Registrierung im Prisma-Cloud-Portal generiert werden. |
| ☐ | Wenn noch nicht installiert und aktiviert, installieren Sie die Anwendung Vulnerability Response, bevor Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 15.2.0 von Vulnerability Response oder höher. |
| ☐ | Wenn Sie die Anwendung noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud in Ihre Instanz Now Platform® ] herunter.<br><br>Weitere Informationen finden Sie unter . |
| ☐ | Stellen Sie für eine reibungslose Integration sicher, dass Sie die folgenden Plugins installiert haben:<br>• Vulnerability Response<br>• Configuration Compliance<br>• Vulnerability Response Integration with Palo Alto Prisma Cloud<br><br>Die folgenden Plugins sind optional, können aber nützlich sein:<br>• Cloud Provisioning and Governance<br>• Muster für Discovery und Service-Mapping |
| ☐ | Schätzen Sie die Anzahl der Testergebnisse, die Sie importieren möchten.<br><br>Vergewissern Sie sich, dass Ihre Instanz die Anzahl der Testergebnisse akzeptieren kann, die Sie importieren möchten. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support von ServiceNow. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste zur Vorbereitung der Integration (Fortsetzung)**

| Aufgabe | Beschreibung |
|---|---|
| ☐ | Stellen Sie sicher, dass Sie einen Administrator haben, der die Integrationen verwaltet und die Testergebnisse korrigiert:<br><br>Der Administrator installiert die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud. Wenn sie nicht zugewiesen ist, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen zu. |

Sie sind bereit für Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud ..

### Installieren und konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud .

Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud, um die importierten Daten aus Prisma Cloud zu verwenden. Verwenden Sie diese Daten, um Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Systemdefinition** > **Plugins**.
2. Suchen Sie in der Suchleiste nach Vulnerability Response Integration with Palo Alto Prisma Cloud.
3. Klicken Sie auf **Installieren**.

   Alle zu installierenden Abhängigkeiten werden angezeigt.
4. Navigieren zu **Alle** > **Prisma-Cloud-Integration** > **Administration** > **Konfiguration** > **Prisma-Cloud-Konfiguration**.
5. Füllen Sie die Felder des Formulars aus.

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Name der neuen Integrationsinstanz.<br><br>Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen. |
| API-URL | URL für die Integration mit Prisma Cloud. |
| Zugangsschlüssel-ID | Eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung bei Prisma Cloud.<br><br>**Hinweis:**<br>Sie müssen den Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Geheimer Schlüssel | Privater Schlüssel zur Authentifizierung der Zugriffsanforderung bei Prisma Cloud.<br>**Hinweis:**<br>Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben. |

6. Klicken Sie auf **Speichern und testen**.

### Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation zu **Prisma-Cloud-Integration** > **Konfiguration** , um mit der Konfiguration fortzufahren.

## Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud .

Konfigurieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Prisma Cloud. Verwenden Sie die importierten Daten aus Prisma Cloud, um Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Prisma-Cloud-Integration** > **Konfiguration**.
2. Füllen Sie die Felder des Formulars aus.

#### Prisma-Cloud-Konfiguration

| Feld | Beschreibung |
|---|---|
| Integrationsinstanz | Name der neuen Integrationsinstanz.<br>Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen. |
| API-URL | URL für die Integration mit Prisma Cloud. |
| Zugangsschlüssel-ID | Ein eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung bei Prisma Cloud.<br>Sie müssen den Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben. |
| Geheimer Schlüssel | Ein privater Schlüssel zur Authentifizierung der Zugriffsanforderung bei Prisma Cloud. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben. |

3. Klicken Sie auf **Speichern und testen**.

### Nächste Maßnahme
Navigieren Sie nach Abschluss der Konfiguration zu **Prisma-Cloud-Integration** > **Integrationen** , um sicherzustellen, dass die Integration erfolgreich ausgeführt wurde.

## Überprüfen Sie den Importausführungsstatus Vulnerability Response Integration with Palo Alto Prisma Cloud .

Verwenden Sie den Importausführungsstatus Vulnerability Response Integration with Palo Alto Prisma Cloud, um den Erfolg Ihrer Integrationsausführungen zu überprüfen und Probleme zu identifizieren.

### Vorbereitungen
Erforderliche Rolle: admin

### Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 14.8.5 von Configuration Complianceregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur
1. Navigieren zu **Prisma-Cloud-Integration** > **Integrationen**.
2. Klicken Sie auf **Prisma-Richtlinienintegration**.
3. Klicken Sie auf **Jetzt ausführen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn diese Integration ausgeführt wird, werden die folgenden Tabellen in der folgenden Reihenfolge ausgefüllt:

**a.** sn_vulc_test.list (Konfigurationstests)

**b.** sn_vulc_auth_src (Authoritative Quelle).

**c.** sn_vulc_citation (Zitate)

4. **Zeigen** Sie auf der Registerkarte Elemente die Anzahl der neuen Tests an, die erstellt, aktualisiert und ignoriert wurden, indem Sie auf die Ausführung der Schwachstellenintegration klicken.

**Hinweis:**
Richtlinien werden in Prisma Cloud für die ausgewählte Cloud-Instanz definiert. Die Instanz wird basierend auf den definierten Richtlinien gescannt.

5. Klicken Sie **auf Prisma-Warnungsintegration**.

6. Klicken Sie auf **Jetzt ausführen**.
Die folgenden Tabellen werden basierend auf der Integration ausgefüllt:

   - Testergebnisse
   - Erkannte Elemente: Wenn die Konfigurationselemente im System nicht verfügbar sind, werden sie erstellt. Die Klasse ist immer Cloud-Ressource. Auf der Seite „Erkanntes Element“ werden drei neue Felder erstellt: **Cloud-Ressourcentyp**, **Cloud-Service-Provider**und **Asset-Kategorie**.

     **Klicken** Sie auf der Registerkarte Elemente auf die Ausführung der Schwachstellenintegration, um die Anzahl der neuen Testergebnisse anzuzeigen, die importiert, aktualisiert und ignoriert wurden. Die Registerkarte **Konfigurationselemente** wird auch basierend auf der Anzahl der erstellten Testergebnisse ausgefüllt.

### Datenzuordnung

Die Daten aus Prisma Cloud werden in das Modul ServiceNow der Instanz [ Configuration Compliance importiert.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die Daten aus Prisma Cloud werden mit einem anderen Namen in Configuration Compliance importiert, wie in der Tabelle angegeben.

#### Zuordnung von Prisma-Cloud-Daten in Configuration Compliance

| Prisma-Cloud | Configuration Compliance |
|---|---|
| Richtlinie | Test |
| Warnung | Testergebnis |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Zuordnung von Prisma-Cloud-Daten in Configuration Compliance (Fortsetzung)**

| Prisma-Cloud | Configuration Compliance |
|---|---|
| Compliance-Standard | Autorisierende Quelle |
| Abschnitte | Zitat |
| Asset | Discovery-Element/Konfigurationselement (CI) |

## Tests

Eine Richtlinie in Prisma Cloud wird als Test in Configuration Complianceimportiert. Richtlinien beziehen sich auf autoritative Dokumente und Testdatensätze und können an die Anforderungen Ihrer Organisation angepasst werden. Sie können die Tests anzeigen, indem Sie zu navigieren **Configuration Compliance** > **Tests**.

Wenn **Vulnerability Response Integration with Palo Alto Prisma Cloud** installiert ist, ruft der Integrationsauftrag *`Prisma Policy Integration`* die Tests ab. Sie können den Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integrationen** > **Prisma-Richtlinienintegration**.

## Testergebnisse

Eine Warnung in Prisma Cloud wird als Testergebnis in Configuration Complianceimportiert. Warnungen werden mithilfe von **Testergebnisgruppen**behoben. Sie können die Testergebnisse anzeigen, indem Sie zu navigieren **Configuration Compliance** > **Testergebnisse**.

Configuration Compliance importiert Testergebnisse als Teil einer Drittpartei-Integration. Nachdem sie in der Anwendung Configuration Compliance angezeigt werden können, werden sie mithilfe von Testergebnisgruppen korrigiert.

Wenn **Vulnerability Response Integration with Palo Alto Prisma Cloud** installiert ist, ruft der Integrationsauftrag **Prisma Alert Integration** die Testergebnisse ab. Sie können diesen Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integration** > **Integrationen** > **Prisma-Warnungsintegration**.

Die **Prisma-Warnungsintegration** ist ein Integrationsauftrag, der täglich ausgeführt wird und die Testergebnisse mit Statusänderung nach der im Feld **Startzeit** auf der Registerkarte „ **Integration** “ definierten Zeit abruft.

**Hinweis:**
Wenn Sie den Integrationsauftrag **Prisma-Warnungsintegration** manuell ausführen, führen Sie ihn aus, nachdem Sie den Integrationsauftrag **Prisma-Richtlinienintegration**ausgeführt haben.

Wenn die **Prisma-Warnungsintegration** den Import der Daten abschließt, wird ein Event gestartet, um Berechnungen für das Importende auszulösen. Wenn die Warnung in den letzten Tagen kontinuierlich fehlgeschlagen ist, werden die Warnungen von der Integration nicht abgerufen, da für die Warnung keine Statusänderung erfolgt. Um die Testergebnisdaten mit den Prisma-Warnungen auf dem neuesten Stand zu halten, wird ein neuer Integrationsauftrag, **Prisma Comprehensive alert Integration**, hinzugefügt, der die Warnungen abruft, die in den letzten sieben Tagen aktualisiert wurden. Er wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Autoritative Quellen

Configuration Compliance verwendet maßgebliche Quellen und Zitate, wenn Schwachstellenwarnungen für Tests generiert werden. Autorisierende Quellen beziehen sich normalerweise auf Abschnitte veröffentlichter Branchenstandards wie ISO 27001 und PCI DSS 3.2.1.

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardware-Konfigurationsproblemen von Experten auf dem Gebiet der Computersicherheit. Die Referenzen definieren Anforderungen für Sicherheitsrichtlinien und -verfahren. Navigieren zu **Configuration Compliance** > **Autoritative Quellen** , um die autorisierenden Quellen anzuzeigen.

## Assets

Wenn Vulnerability Response Integration with Palo Alto Prisma Cloud installiert ist, erfasst die regelmäßige Aufgabe `Prisma Alerts Integration` die Informationen im Zusammenhang mit Warnungen im Modul oder in der Tabelle „Erkannte Elemente“. Sie können diese regelmäßige Aufgabe anzeigen, indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**.

Die Integration von Prisma-Warnungen importiert zusätzliche Arten von Informationen, z. B. Ressourcen-Tags und Cloud-Attribute, die in Tabellen gespeichert sind. Diese Informationen werden im Formular „Erkannte Elemente“ angezeigt.

- Host-Tags: Eine Ressource kann mehrere Tags haben. Die Host-Tags sind im Schlüssel-Wert-Paar-Format verfügbar. Beispiel: Das Betriebssystem ist Windows 10 und die Java-Version ist 1.8.
- Cloud-Attribute für Assets: Die folgenden Cloud-Attribute sind verfügbar:
  - Cloud-Konto: Stellt die Konto-ID aus der Integration bereit. Die Informationen werden aus der Tabelle „Cloud-Konten“ [sn_sec_cmn_cloud_account.LIST] ausgefüllt.
  - Cloud-Region: Stellt den Standort bereit, an dem die Ressource gehostet wurde. Die Informationen werden aus der Tabelle „Cloud-Regionen“ [sn_sec_cmn_region.LIST] ausgefüllt.
  - Cloud-Ressourcentyp: Stellt Informationen zum Typ der Ressource bereit, z. B. ob es sich um einen virtuellen Computer oder eine Datenbankinstanz handelt. Die Informationen werden aus der Tabelle „Cloud-Ressourcentyp“ [sn_sec_cmn_cloud_resource_type.LIST] ausgefüllt.
  - Cloud-Service-Provider: Stellt Informationen zum Cloud-Service-Provider bereit, unabhängig davon, ob es sich um Amazon Web Services (AWS), Oracle Cloud usw. handelt. Die Informationen werden aus der Tabelle „Cloud Service Provider“ [sn_sec_cmn_cloud_service_provider.LIST] ausgefüllt.
  - Cloud-Kontogruppen: Stellt Informationen zu den Kontogruppen bereit. Die Informationen werden aus der Tabelle „Cloud-Kontogruppen“ [sn_vul_prismacloud_account_group.list] ausgefüllt.

**Hinweis:**
Das Attribut „Cloud-Kontogruppen“ ist nur für Prisma verfügbar.

## CI-Suchregeln

CI-Suchregeln des Basissystems sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu CI-Suchregeln finden Sie unter CI-Suchregeln für Microsoft Defender for Cloud Integration für Security Operations und Palo Alto Prisma Cloud.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prisma-Cloud-REST-Nachrichten

Prisma-REST-Nachrichten werden verwendet, um Aufrufe an die Prisma-API (Application Programming Interface) zu tätigen, um die Compliance-Daten abzurufen.

Die folgenden REST-Nachrichten werden mit dem Basissystem geliefert.

## Prisma Cloud-Integrationen

Alle Prisma Cloud-Integrationen verwenden das JSON Web Token (JWT) zur Authentifizierung und Autorisierung.

### REST-Nachricht bei Prisma-Anmeldung

| Endpunkt | Beschreibung | Methode | Textkörper | API-Dokumentationslink |
|---|---|---|---|---|
| /login | Ruft das JWT-Token zur Verwendung in allen nachfolgenden Integrationen ab. | *POST* | { "username": <<access key id >>, "password": <<secret access key>>} | https://pan.dev/prisma-cloud/api/cspm/app-login/ |

### REST-Nachricht „Prisma-Aktualisierungstoken“.

| Endpunkt | Beschreibung | Methode | Textkörper | API-Dokumentationslink |
|---|---|---|---|---|
| /auth_token/extend | Erneuert das JWT-Token bei Ablauf automatisch. Die Standarddauer für den Token-Ablauf beträgt 60 Minuten. | *GET* | NA | https://pan.dev/prisma-cloud/api/cspm/extend-session/ |

### REST-Nachricht für Prisma-Richtlinie

| Endpunkt | Beschreibung | Methode | Textkörper | API-Dokumentationslink |
|---|---|---|---|---|
| /v2/policy | Ruft alle Richtliniendaten aus Prisma ab. | *GET* | NA | https://pan.dev/prisma-cloud/api/cspm/get-policies/ |

### REST-Nachricht für Prisma-Warnung

| Endpunkt | Beschreibung | Methode | Textkörper | API-Dokumentationslink |
|---|---|---|---|---|
| /v2/alert | Ruft alle Warnungen von Prisma ab. | *POST* | { "detailed": "false", "filters": [ { "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" | https://pan.dev/prisma-cloud/api/cspm/post-alerts/ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**REST-Nachricht für Prisma-Warnung (Fortsetzung)**

| Endpunkt | Beschreibung | Methode | Textkörper | API-Dokumentationslink |
|---|---|---|---|---|
| | | | }<br>],<br>"sortBy": [<br>"resource.id"<br>],<br>"pageToken": "",<br>"offset": 0,<br>"limit": 2000,<br>"timeRange": {<br>"type": "absolute",<br>"value": {<br>"startTime": <<Import since at integration level>>,<br>"endTime": << Current integration run time>><br>}<br>}<br>} | |

Für die Integration von Prisma Comprehension Alert müssen die Filter im obigen POST-Text wie folgt ersetzt werden:

```
"filters": [
 {
                "name": "alert.status",
                "operator": "=",
                "value": "open"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "dismissed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "snoozed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "pending_resolution"
            },
            {
                "name": "timeRange.type",
                "operator": "=",
                "value": "ALERT_UPDATED"
            }

   ],
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Integration von Configuration Compliance in Qualys

Die Qualys Richtlinien-Compliance erfasst die Daten und sendet sie automatisch an die Anwendung Qualys, die die Informationen kontinuierlich analysiert und korreliert. Sie lässt sich problemlos als Qualys Integration for Security Operations integrieren, um Konfigurationsergebnisse CIs und Business Services zuzuordnen und die Auswirkungen und Priorität potenzieller Fehlkonfigurationen zu bestimmen.

Wenn Sie mehrere Bereitstellungen der Anwendung Qualys Cloud Platform haben, können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen und ihre Schwachstellen identifiziert wurden, werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scan-Prozesse zwischen mehreren Bereitstellungen überschneiden. Daten aus jeder Bereitstellung werden identifiziert und sind in einer einzigen Instanz von Vulnerability Responseverfügbar.

**Hinweis:**
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber Sie können sie deaktivieren. Integrationen, die aus inaktiven Vorlagen erstellt wurden, sind standardmäßig deaktiviert.

## Host-Tags

Alle Host-Tags werden als Teil der Qualys Hostlisten-Integration importiert. Host-Tags werden hauptsächlich zum Filtern in Vulnerability Response Zuweisungs- und Schwachstellengruppenregeln verwendet. Sie werden im Formular „Erkanntes Element“ angezeigt.

**Hinweis:**
Die Qualys -Hostlisten-Integration sollte vor dem Erstellen der Zuweisungs- oder Korrekturaufgabenregeln in Vulnerability Response ausgeführt werden, damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn ein **San Diego** -Tag erstellt wird, kann kein **SAN DIEGO** -Tag in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das zuerst importierte Tag hat den Vorzug.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft **sn_vul.import_host_tags gesteuert**. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt. Durch Deaktivieren von Tags werden sie in allen Instanzen deaktiviert.

Host-Tags (auch Asset-Tags genannt) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Host-Tags“ können Sie Host-Tag-Daten von Qualys nach Zeitplan in Ihre Instanz herunterladen.

## Integration von Qualys mit der Anwendung ServiceNow® Configuration Compliance .

Wenn Qualys Vulnerability Integration bereits auf Ihrem System installiert ist und sich Ihre API-Anmeldeinformationen von denen unterscheiden, die Sie für Configuration



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compliance verwenden möchten, rufen Sie den Setup-Assistenten auf (in Vulnerability Response), und weisen Sie sie jeder **Qualys PC-** Integration zu.

Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen** und bearbeiten Sie das Feld **Qualys-API-Anmeldeinformationen** auf der Registerkarte **Qualys-REST-Details**.

### Konfigurieren Sie die PCRS-Parameter

Ab v12.6.3 von Integration von Qualys für Security Operations können Sie die Qualys PCRS-Richtlinien-Host-Integration und die Qualys PCRS-Testergebnis-Integration für den Import von Testergebnissen mit neuen Sätzen von Qualys APIs verwenden. Diese Integrationen benötigen eine Gateway-URL, um Informationen aus Qualys abzurufen.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Integration von Qualys für Security Operations für Vulnerability Response installieren, können Sie „ **gateway_url“** für die neuen PCRS-Integrationen in Configuration Compliance konfigurieren. Weitere Informationen dazu, wie Sie die Gateway-URL für Ihre API-URL finden, finden Sie unter Qualys-Plattform identifizieren .

Die Gateway-URL muss in Ihrer ServiceNow -Instanz hinzugefügt werden.

#### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**.

   **Hinweis:**
   Vergewissern Sie sich, dass der Bereich, in dem Sie sich befinden, Qualys for Security Operations ist.

2. Öffnen Sie die Instanz, die von den PCRS-Integrationen verwendet wird.
3. Fügen Sie auf der Registerkarte „Integrationsinstanzparameter“ die Gateway-URL für die Konfiguration **„gateway_url“ hinzu**.

   **Hinweis:**
   Die Integration von Qualys PCRS-Testergebnissen ist von der Integration des Qualys PCRS-Richtlinienhosts abhängig. Wenn Sie also die Qualys PCRS-Testergebnisse der Integration zurückdatieren, müssen Sie sie möglicherweise erneut in derselben Reihenfolge ausführen.

### Mit Qualys Integration for Security Operations installierte Komponenten

Die folgenden Rollen, geplanten Aufgaben und Tabellen werden mit Qualys Integration for Security Operations installiert.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

## Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Anwendungsdateien-Tabelle, sodass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Sie diese Komponenten anzeigen möchten, muss so installiert sein, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Befolgen Sie diese Schritte, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im **Filternavigator sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, wählen Sie **UND**und dann **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

## Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| sn_vul_qualys.read | Hat Lesezugriff auf die Datensätze Qualys Vulnerability Integration. | |
| sn_vul_qualys.user | Benutzer für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben | sn_vul_qualys.read |
| sn_vul_qualys.admin | Administrator fürQualys Vulnerability Integration. Sie können beispielsweise die Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen. | • sn_vul_qualys.user<br>• sn_vul.vulnerability_analyst |
| sn_vul.configure_qualys_integration | Kann die konfigurieren Qualys Vulnerability Integration | sn_vul_qualys.admin |

## Integration Jobs Installiert

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| Qualys PC-Richtlinien | Ruft Richtlinien aus Qualysab. Die Ausgabe wird in der Tabelle sn_vulc_policy gespeichert. Die in dieser Integration verwendete API unterstützt keine Paginierung, daher werden alle Richtlinien auf einer einzigen Seite heruntergeladen. |
| Qualys PC-Richtliniendetail | Ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte. |
| Qualys PC-Steuerungen | Ruft Informationen zu Compliance-Kontrollen für verschiedene Kontroll-IDs aus Qualysab. |
| Qualys PC-Ergebnisse | Ruft Datensätze zur Compliance-Situation von Qualysab. Die Ausgabe dieser Integration |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| | ist Testergebnisse. Standardmäßig werden die Parameterdetails an den Import von Hostinformationen, Daten/Uhrzeiten der letzten Scans, Kontroll-ID und Nachweisinformationen übergeben. |
| Qualys PC Comprehensive Results | Ruft Datensätze zur Compliance-Situation von Qualys basierend auf dem letzten Bewertungsdatum für die Testergebnisse ab, die nicht bestanden wurden. Dieser Job wird einmal pro Woche ausgeführt.<br><br>Die Ausgabe dieser Integration sind Testergebnisse. Standardmäßig werden die Parameterdetails übergeben, um die Hostinformationen, die Daten/Uhrzeiten der letzten Scans, die Kontroll-ID und die Nachweisinformationen zu importieren. |
| Qualys PCRS-Richtlinien-Host-Integration | Ruft Hostdaten von Qualys ab und verarbeitet sie in Ihrer Instanz.<br><br>Die Ausgabe dieser Integration ist . Richtlinien-Host-IDs.<br><br>Die Qualys Host -[]- Daten werden in diese Integration importiert.<br><br>**Hinweis:**<br>• Diese regelmäßige Aufgabe wird nur angezeigt, wenn Configuration Compliance installiert ist.<br>• Konfigurieren Sie die Integrationsinstanzparameter „gateway_url“ und „pcrs_page_size“, bevor Sie diese Integration ausführen.<br><br>Diese beiden Integrationen sind inaktives OOB. Wenn Sie eine dieser Integrationen aktivieren, werden die PC-Ergebnisintegrationen deaktiviert. Diese beiden Integrationen werden basierend auf den neuen Streaming-APIs von Qualys hinzugefügt. |
| Qualys PCRS-Testergebnisintegration | Ruft die Testergebnisse für jede Host-ID ab. Diese Integration verwendet den Parameter Startzeit auf der Registerkarte „Integrationsdetails“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Regelmäßige Aufgabe | Beschreibung |
|---|---|
| | **Hinweis:**<br>• Diese regelmäßige Aufgabe wird nur angezeigt, wenn Configuration Compliance installiert ist.<br>• Konfigurieren Sie die Integrationsinstanzparameter „gateway_url“ und „pcrs_page_size“, bevor Sie diese Integration ausführen.<br>• Wenn Sie die Integration manuell ausführen möchten, führen Sie Qualys PCRS-Testergebnisintegration nach Qualys PC-Richtlinien, Qualys PC-Richtliniendetails und Qualys PCRS-Richtlinien-Hostintegration aus. |

**Hinweis:**
Die Integrationen Qualys PCRS-Richtlinienhost und Qualys PCRS-Testergebnisse sind standardmäßig inaktiv. Diese beiden Integrationen basieren auf den neuen Streaming-APIs von Qualys. Wenn Sie eine dieser Integrationen aktivieren, wird die PC-Ergebnisintegration deaktiviert und umgekehrt.

## Tabellen installiert

| Tabelle | Beschreibung |
|---|---|
| Qualys PC-Ergebnisimport<br><br>sn_vul_qualys_pc_result_import | Tabelle, die die Import Set-Zeile erweitert. Die Transformation von Feldzuordnungen wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |
| Richtlinien-Host-ID<br><br>sn_vul_qualys_policy_host_id | Tabelle, in der die Zuordnung zwischen der Richtlinie und dem Host gespeichert wird, für den diese Richtlinie gescannt wurde. Diese Tabelle wird in der neuen Qualys PCRS-Integration verwendet.<br><br>**Hinweis:**<br>Diese Tabelle wird nur angezeigt, wenn Configuration Compliance installiert ist. |
| Qualys PCRS-Richtlinienhostimport<br><br>sn_vul_qualys_pcrs_policy_host_import | Tabelle, die die Import Set-Zeile erweitert.<br>Die Transformation der Feldzuordnung wird übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet.<br><br>**Hinweis:**<br>Diese Tabelle wird nur angezeigt, wenn Configuration Compliance installiert ist. |
| Qualys PC-Richtlinienimport | Tabelle, die die Import Set-Zeile erweitert.<br>Die Transformation der Feldzuordnung wird |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| sn_vul_qualys_pc_policy_import | übersprungen, und der Antwortanhang wird direkt mit dem Skript „onComplete“ verarbeitet. |

### Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für die Qualys-Integration

Erstellen Sie eindeutige Konfigurationselemente (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Sie Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, sie werden jedoch als ein CI in Ihrer CMDB gespeichert.

Beispielsweise können, wie in den folgenden Tabellen gezeigt, mehrere Assets (CIs) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche als einzelnes CI (CI 1) identifiziert und gespeichert.

**Standardmäßige IP-Suche und CI-Erstellung**

| Quelle | IP-Adresse | NETWORK_ID | Konfigurationselement |
|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 |

| Quelle | IP-Adresse | REPOSITORY_ID | Konfigurationselement |
|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 |

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse haben, damit Sie sie als unterschiedliche Assets identifizieren können. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die regelmäßige Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.



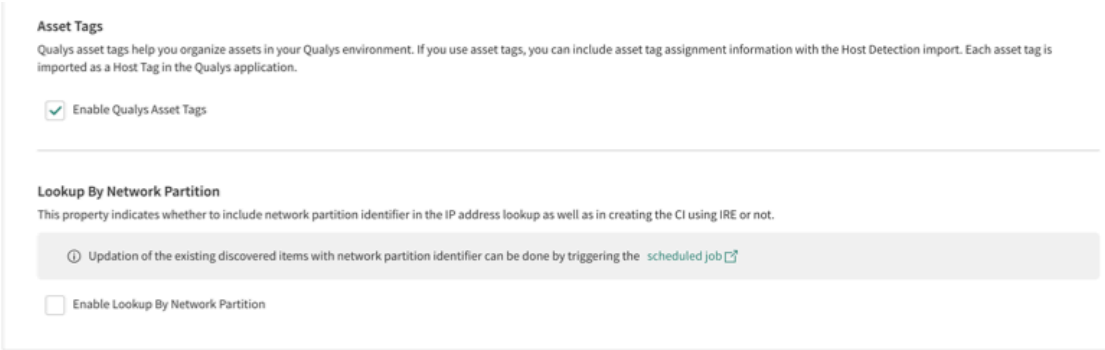
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] vorhandenen CI-Datensätzen aus importierten Daten hinzu. Vorhandene von der IRE erstellte CIs werden ebenfalls aktualisiert. Die regelmäßige Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie die Aufgabe bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Ab Version 14.0 von Vulnerability Response und Version 12.1 von Qualys Vulnerability Integration Vulnerability Integration wird CMDB CI Class Models (1.0.21.) unterstützt. Die Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

### Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Qualys Vulnerability Integration aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**.
5. Wählen **Suche nach Netzwerkpartition aktivieren** Checkbox aus dem **Suche nach Netzwerkpartition**




Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

#### Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID in IP-Suche und CI-Erstellung enthalten

| Quelle | IP-Adresse | NETWORK_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Qualys Vulnerability Integration: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 | CI 2 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quelle | IP-Adresse | REPOSITORY_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Qualys: Integrationen mit Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 | CI 2 |

Die Suchregeln IP-Adresse und unvollständige IP-Adresse für CI-Identifizierung enthalten das Attribut für den Netzwerkpartitionsbezeichner automatisch für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für Qualys Vulnerability Integration.

Nachdem Sie die regelmäßige Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie bei Bedarf regelmäßige Aufgaben starten. Die CIs in Ihren vorhandenen Datensätzen für erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden automatisch aktualisiert.

### Legen Sie zusätzliche Filterparameter für Qualys Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Qualys Vulnerability Integration an, damit Sie die Schwachstellendaten, die Sie mit den unterstützten Qualys -Integrationen importieren, weiter verfeinern können.

#### Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert werden. Oder Sie möchten nur Computer importieren, die sich in Ihrem Bereich befinden, z. B. nur Computer innerhalb Ihres Unternehmensnetzwerks, die keine externen Geräte sind.

Um die Erfassung dieser Daten zu erleichtern, können Sie Parameter Qualys hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Parametern Qualys in Ihrem Now Platformanpassen. Sie ändern oder fügen diese Werte in Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützten Qualys -Integrationen von Qualys Vulnerability Integrationhinzu.

Erforderliche Rolle: sn_vul.vulnerability_admin

#### Prozedur

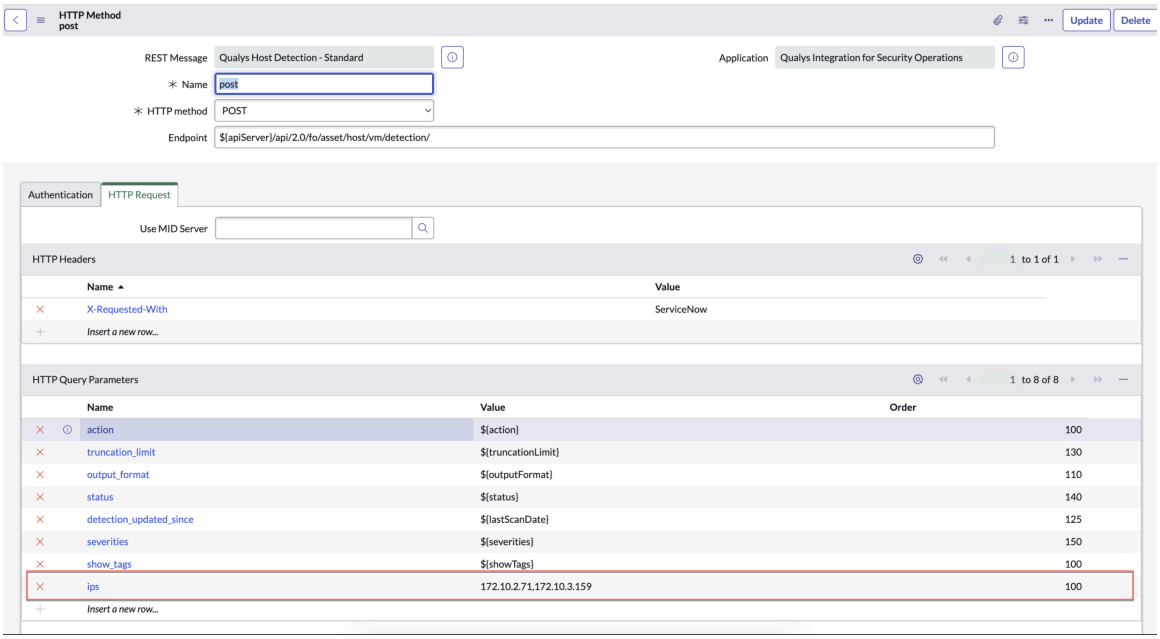
1. Suchen Sie die vom Produkt Qualys unterstützten Parameter auf der Entwickler-Website, die Sie zum Filtern verwenden möchten.
   Parameter und Werte, die Sie aus dem Produkt Qualys eingeben, werden nur auf der Ebene der Integrationsinstanz in Now Platformunterstützt. Alle Qualys -Integrationen unterstützen die Filterung mithilfe von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf der Listenseite Qualys Integrationen auf den Datensatz für die Integration, für die Sie den Datensatz öffnen möchten.
4. Suchen Sie auf der Registerkarte Qualys REST-Details das Informationssymbol (I) für die REST-Methode, gefolgt von **Datensatz** öffnen, um den HTTP-Methodendatensatz zu öffnen.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von der Entwickler-Website Qualys erhalten haben.

   In der folgenden Abbildung wurde beispielsweise der Parameter, der nur bestimmte IP-Adressen/Bereiche erfasst, `ips={value}` hinzugefügt. In diesem Fall ist der **Wert** eine oder mehrere von Ihnen angegebene IPs/Bereiche. Mehrere Einträge sind durch Kommas getrennt, 172.10.2.71, 172.10.3.159, und ein Bereich wird mit einem Bindestrich angegeben, 10.10.10.1-10.10.10.100. Weitere Informationen finden Sie auf der Entwickler-Website Qualys.




   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Qualys weitere Informationen zum Trennen der einzelnen Werte.

   **Hinweis:**
   Sie sollten Ihre API-Anforderungen kennen. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textinhalt hinzufügen.

   Einige andere Parameter, die Sie auf der Entwickler-Website Qualys nützlich finden könnten:

   - `ag_ids` Abzurufende Asset-Gruppenlisten-IDs. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich übernommen werden.
   - `qids` Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in Tabelle „Drittpartei-Eintrag“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überschwemmt wird.

7. Klicken Sie auf **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Qualys Probleme bei der Schwachstellenintegration werden gelöst

Einige häufig auftretende Probleme werden zusammen mit Problemumgehungen besprochen.

### Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge für Datenquellen oder bei einem Security Incident nach dem Import von Drittanbieterintegrationen nicht wie erwartet angezeigt werden, überprüfen Sie Ihre IP-Beschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge angezeigt werden, es sei denn, Sie sind über eine sichere IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies dazu führen, dass Sie Duplikate entfernen müssen.

Wenn Sie beispielsweise beim Ausführen einer Hostimportintegration einer Drittpartei keine Anhänge in Ihren Datenquellen sehen, überprüfen Sie Ihre IP-Beschränkungen, und fügen Sie der sicheren Liste Benutzer vor dem Import hinzu.

### Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und reichen in der Regel aus. Sie können Transformationszuordnungen entsprechend den Anforderungen Ihrer Organisation ändern.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + import_admin

#### Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** , um die REST-Nachrichten anzuzeigen.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf die Anwendung **Qualys Vulnerability Integration**.
3. Ändern Sie die Transformationszuordnungen gemäß den Kundenanforderungen.

   Weitere Informationen zu den von der Qualys-API bereitgestellten Daten finden Sie in der Qualys-API-Dokumentation .

### Überprüfen Sie die Größe der XML-Anhangeigenschaft

Überprüft, ob die XML-Anhangeigenschaft für große Dateien ausreichend ist.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**.
2. Scrollen Sie nach unten zu **Eigenschaften importieren** > **XML-Format** am Ende der Seite.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie ggf. den Wert in 250, und klicken Sie auf **Speichern**.

**Zugehörige Informationen**

Verfügbare Systemeigenschaften

### Einschränkungen beim Datenabruf

Standardmäßig gibt es keine Einschränkungen dafür, wie Daten aus Qualys abgerufen werden. Viele Datensätze können mit Schwachstellen mit geringem Schweregrad verknüpft werden, die ein Kunde nicht bereit ist, mit seinem Vulnerability Response-Prozess zu beheben. Durch Aktualisieren der entsprechenden REST-Nachrichten-/-Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/-Methode ist **Qualys Host Detection – Standard/post**. Um die Werte zu aktualisieren, fügen Sie der post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder welcher geeignete Schweregrad auch immer gewünscht wird)

### Qualys Knowledge Base-Integration schlägt fehl

Beheben Sie den Fehler bei der Knowledge Base-Integration von [ Qualys, indem Sie die von Qualys empfangene Nutzlast-Anhanggröße auf das angegebene Limit reduzieren.

## Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

## Prozedur

1. Stellen Sie sicher, dass die Größe des Nutzlastanhangs innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.
   b. Wechseln Sie zur Registerkarte „ **Integrationsinstanzparameter“**.
   c. Wählen **Sie max_delta_days aus,** und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**.
   b. Wählen Sie **Qualys Knowledge Base aus**.
   c. Wechseln Sie zur Registerkarte **Integrationsdetails**.
   d. Wählen Sie im Feld **Startzeit** das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wechseln Sie zur Registerkarte „ **Integrationsinstanzparameter“**.

g. Wählen **Sie kb_backfill_full_import aus,** und ändern Sie den Standardwert in true.

### Ergebnisse

Durch die Ausführung der Qualys Knowledge Base-Auffüllungsintegration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Während die Qualys-Hosterkennungsintegration einen Platzhaltereintrag erstellt, wird dieser durch die Qualys Knowledge Base-Auffüllungsintegration aktualisiert.

### Qualys Statusdiagramm der Integrationsausführung

Das Modul Qualys „ Integrationsausführungsstatus“ ist eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status der Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**.

Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

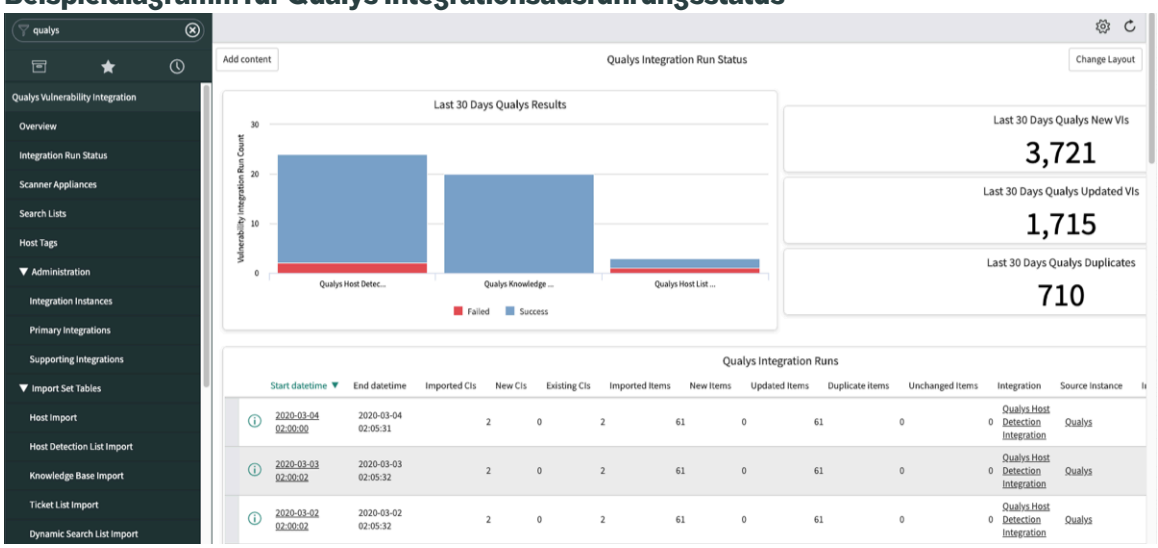
**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

Zeigen Sie im Diagramm auf einen beliebigen Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Der Integrationsausführungsstatus Qualys zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die von Qualys [qualys] aktualisierte VIs-Anzahl gibt die Anzahl für eindeutige Erkennungen im selben Asset an. Die VI wird dann mit der neuen Erkennung aktualisiert.

**Hinweis:**
Die Ausführungsanzahl der Schwachstellenintegrationen wird nur für die Integrationen angezeigt, die auf den Status „Aktiv“ gesetzt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** und legen Sie den Status auf „Aktiv“ fest.

### Beispieldiagramm für Qualys Integrationsausführungsstatus




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Werte in der Spalte „Importierte Elemente“ stellen die Gesamtzahl der Datensätze dar, die aus einer Integrationsausführung erstellt werden.
- Die Spalte Neue Elemente zeigt die Anzahl der Datensätze an, die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „Doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- Die Spalte Aktualisierte Elemente zeigt an, wie oft Datensätze während einer Integrationsausführung aktualisiert wurden. Dieser Wert ist nicht die Anzahl der eindeutigen Datensätze, die aktualisiert werden. Wenn beispielsweise ein Datensatz während der Integrationsausführung zweimal aktualisiert wird, wird er zweimal gezählt und als 2 aktualisierte Elemente angezeigt.
- Die Spalte Unveränderte Elemente zeigt Datensätze an, die während der Integrationsausführung gefunden wurden und bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hat.

**Hinweis:**
Die Integration wird mit null Ergebnissen für alle vier der folgenden Werte ausgeführt: **Neue CIs**, **vorhandene CIs**, **neue Elemente**und **aktualisierte Elemente** werden aus der Liste der **Qualys-Integrationsausführungen** herausgefiltert.

### Qualys Statusdiagrammberichte der Integrationsausführung

| Name | Beschreibung |
|---|---|
| Ergebnisse der letzten 30 Tage Qualys . | Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Führen Sie in einer visuellen Leiste aus. |
| Letzte 30 Tage Qualys Neue AEs | Die Anzahl der neuen Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Aktualisierte AEs der letzten 30 Tage Qualys . | Die Anzahl der aktualisierten Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Duplikate der letzten 30 Tage Qualys . | Die Anzahl der doppelten Datensätze, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Qualys Integrationsausführungen | Die Datensätze der Integrationsausführung werden in einer Liste angezeigt.<br>**Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |
| Angreifbares Element – Erfassungsleistungsmetriken der letzten 30 Tage Qualys . | Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich für die letzten 30 Tage. |



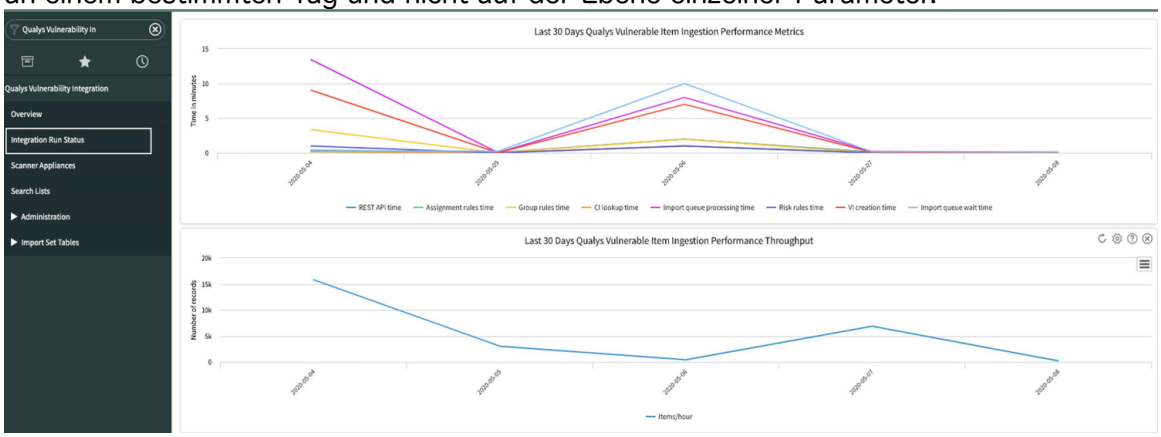
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Qualys Statusdiagrammberichte der Integrationsausführung (Fortsetzung)

| Name | Beschreibung |
|---|---|
| Angreifbares Element – Erfassungsleistungsdurchsatz der letzten 30 Tage Qualys . | Täglicher Durchsatz bei der Erfassung angreifbarer Elemente, gemessen für die Integration der Qualys -Hosterkennung in den letzten 30 Tagen. |

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

- Qualys Leistungsmetriken der Erfassung angreifbarer Elemente: Vergleichen Sie die täglichen Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit und andere Statistiken für angreifbare Elemente für die letzten 30 Tage, um die Ursache für Leistungsabweichungen zu ermitteln. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf der Ebene der Integrationsausführung berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.
- Qualys Leistungsdurchsatz bei der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Durchsatz bei der Erfassung angreifbarer Elemente für die Qualys Host-Erkennungsintegration. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf der Ebene einzelner Parameter.




### Qualys-REST-Nachrichten

Qualys-REST-Nachrichten werden verwendet, um Aufrufe an die Qualys-APIzu senden, um die Compliance-Daten abzurufen.

Die folgenden REST-Nachrichten werden mit dem Basissystem geliefert.

## Qualys PC-Richtlinien-REST-Nachricht

Die REST-Nachricht Qualys PC-Richtlinien ruft Richtliniendaten aus Qualys ab. Die Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys zum Abrufen von Richtlinieninformationen aus.

### Qualys PC-Richtlinien REST-Nachrichtenparameter

| Parametername | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Qualys PC-Richtlinien REST-Nachrichtenparameter (Fortsetzung)

| Parametername | Wert | Beschreibung |
|---|---|---|
| | | Erforderlicher Parameter. |
| details | Alle | Gibt die Detailebene an, die für abgerufene Richtlinien angezeigt wird.<br><br>Es ist sicher, gemäß Ihren Anforderungen zu ändern. |

## Qualys PC steuert die REST-Nachricht

Die REST-Nachricht von Qualys PC Controls ruft Compliance-Kontrollinformationen für verschiedene Kontroll-IDs aus Qualys ab.

### Qualys PC steuert REST-Nachrichtenparameter

| Parametername | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. |
| details | Alle | Gibt die Detailebene an, die für abgerufene Steuerungen angezeigt wird.<br><br>Es ist sicher, gemäß Ihren Anforderungen zu ändern. |

## Qualys PC-Richtliniendetail-REST-Nachricht

Die REST-Nachricht Qualys PC-Richtliniendetails ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte.

### Qualys PC-Richtliniendetail-REST-Nachrichtenparameter

| Parameter | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. |
| show_user_controls | Boolean | • Legen Sie den Wert auf 1 fest, um benutzerdefinierte Steuerungen (UDCs) in die XML-Ausgabe einzubeziehen.<br><br>• Wenn nicht angegeben, sind UDCs nicht enthalten.<br><br>Dies ist ein optionaler Parameter. Es ist sicher, gemäß Ihren Anforderungen zu ändern. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Qualys PC-Richtliniendetail-REST-Nachrichtenparameter (Fortsetzung)**

| Parameter | Wert | Beschreibung |
|---|---|---|
| show_appendix | Boolean | (Optional) Legen Sie den Wert auf 1 fest, um den Anhangabschnitt in der XML-Ausgabe anzuzeigen. Wenn nicht angegeben. |

## Qualys PC-Ergebnisse REST-Nachricht

Die REST-Nachricht Qualys PC-Ergebnisse ruft Datensätze zur Compliance-Situation aus Qualys ab.

**Qualys PC-Ergebnisse REST-Nachrichtenparameter**

| Quellfeld | Wert | Beschreibung |
|---|---|---|
| Aktion | Liste | Gibt die Art des angeforderten Vorgangs an.<br><br>Erforderlicher Parameter. Änderungen werden nicht empfohlen. |
| show_extended_evidence | Boolean | • Legen Sie den Wert auf 1 fest, um die erweiterten Nachweisinformationen in der Ausgabe anzuzeigen.<br>• Wenn der Wert auf 0 festgelegt ist oder nicht angegeben ist, werden die erweiterten Nachweisinformationen nicht in der Ausgabe angezeigt.<br><br>**Hinweis:**<br>• Sie können `show_extended_evidence=1` nicht in derselben Anforderung wie `hide_evidence=1` angeben. Dies führt zu einem Fehler. Der erweiterte Nachweis ist Teil der Nachweisdaten und wird nur angezeigt, wenn Nachweisdaten angezeigt werden.<br>• Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten. |
| „cause_of_failure“ | Boolean | Wenn Sie '1' übergeben, gibt Qualys die Fehlerursache zurück.<br><br>Wenn Sie '0' übergeben, gibt Qualys diese Attribute nicht zurück.<br><br>**Hinweis:**<br>Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten. |
| policy_id | | Zeigt Datensätze mit Informationen zur Compliance-Situation für eine angegebene Richtlinie an. Eine gültige Richtlinien-ID ist erforderlich. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Qualys PC-Ergebnisse REST-Nachrichtenparameter (Fortsetzung)**

| Quellfeld | Wert | Beschreibung |
|---|---|---|
| details | Alle | Gibt die Detailebene an, die für abgerufene Status angezeigt wird.<br><br>Es ist sicher, gemäß Ihren Anforderungen zu ändern. |
| show_remediation_info | | (Optional) Setzen Sie den Wert auf 1, um Korrekturinformationen in der XML- oder CSV-Ausgabe anzuzeigen. Standardmäßig enthält die Ausgabe keine Korrekturinformationen. Wenn nicht angegeben, sind die Korrekturinformationen nicht in der Ausgabe enthalten. |

## REST-Nachricht für Qualys PCRS-Richtlinienhostintegration

Die Qualys PCRS-Richtlinienhostintegration ruft Hostdaten aus Qualys ab und verarbeitet sie in Ihrer Instanz.

**Qualys PCRS-Richtlinienhostintegration REST-Nachrichtenparameter**

| Parametername | Wert | Beschreibung |
|---|---|---|
| policyId | ${lastRunDatetime} | Richtlinien-IDs für die Compliance-Auswertung. |

## Integration von Qualys PCRS-Testergebnissen

Die Tabelle zeigt die gesendeten Anforderungsparameter.

**Qualys PCRS-Testergebnisintegration REST-Nachrichtenparameter**

| Parametername | Wert | Beschreibung |
|---|---|---|
| NachweisErforderlich | ${lastRunDatetime} | • Der Standardwert ist 0. Dies gibt an, dass keine Nachweisdaten für die Hoststellung abgerufen werden.<br>• Legen Sie den Wert auf 1 fest, um die Nachweisdaten abzurufen.<br><br>**Hinweis:**<br>Wenn Sie den Wert auf 1 ändern, erhöht sich die Zeit, die zum Abrufen von Statusdaten erforderlich ist. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Qualys PCRS-Testergebnisintegration REST-Nachrichtenparameter (Fortsetzung)**

| Parametername | Wert | Beschreibung |
|---|---|---|
| komprimiertErforderlich | | • Der Standardwert ist 1, was angibt, dass die Ausgabe komprimiert wird.<br>• Legen Sie den Wert auf 0 fest, wenn die Daten nicht komprimiert werden sollen.<br>**Hinweis:** Wenn die Daten nicht komprimiert werden, erhöht sich die Zeit, die zum Abrufen von Statusdaten erforderlich ist. |

## Die Tenable Vulnerability-Integration verstehen

Die Anwendung Vulnerability Response Integration with Tenable, die von ServiceNow Engineering für die Integration von Tenable Vulnerability entwickelt wurde, verwendet Daten, die aus den Produkten Tenable.io und Tenable.sc importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement von ServiceNow® Storeverfügbar.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Die Tenable Vulnerability-Integration verwendet zwei Tenable-Integrationen, Tenable.io und Tenable.sc, um Scanner-Daten von Drittanbietern über Ihre Assets und Schwachstellen zu importieren. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.

- Tenable.io ist eine cloudbasierte Unternehmensintegration.
- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden.

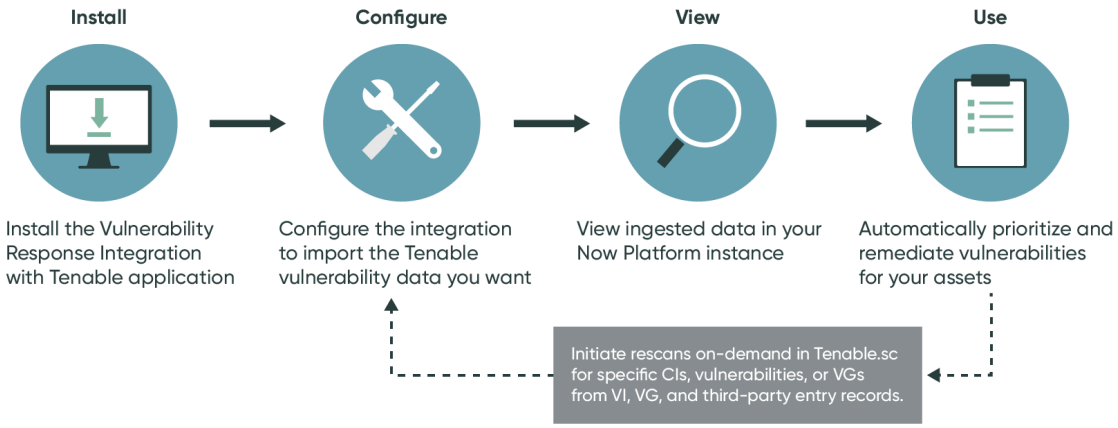
Die Anwendung Vulnerability Response Integration with Tenable ist im ServiceNow Store mit einem separaten Abonnement verfügbar.

Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integrationfinden Sie unter Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance . und Integrationen vonTenable.sc mit der Anwendung Vulnerability Response ..



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vertretbare Schwachstellenintegration




## Verfügbare Versionen für Washington DC

| Release-Version | Versionsinformationen |
|---|---|
| Vulnerability Response Integration with Tenable v3.5, v3.6 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

## Begriffe und Hauptfunktionen der Integrationen

### Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in Ihrer Instanz Now Platform erstellt, wenn:

- Eine importierte Schwachstelle aus einem Scanner einer Drittpartei wird mit einem vorhandenen Asset (einem Konfigurationselement in CMDB) abgeglichen. Das Tenable-Produkt bezeichnet diese Übereinstimmungen als **Schwachstellen**.
- Eine importierte Schwachstelle von einem Drittanbieter-Scanner stimmt nicht mit einem vorhandenen Asset in Ihrem CMDBüberein. In diesem Fall wird zusammen mit einem angreifbaren Element auch ein nicht abgeglichenes CI erstellt.

  Für nicht abgeglichene CIs können Sie auch die Identification and Reconciliation Engine (IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“..

### Schwachstelleneinträge und Plugins von Drittparteien

Schwachstelleneinträge von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in Ihrer Now Platform -Instanz aufgelistet. Drittpartei-Schwachstelleneinträge von Tenable werden in Vulnerability Response erfasst und mit vorhandenen Assets abgeglichen, die in Ihrem CMDBaufgeführt sind. Tenable bezieht sich auf Schwachstelleneinträge von Drittparteien als **Plugins**.

### Konfigurationselement (Configuration Item, CI)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationselemente sind die vorhandenen Assets, die in Ihrem CMDBaufgeführt sind.

**Erkanntes Element**

Assets, die aus dem Tenable-Asset-Import erfasst wurden, werden mit vorhandenen Konfigurationselementen in CMDBabgeglichen. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der CI-Klasse Nicht abgeglichen von CMDBerstellt. Wenn das Plugin „CMDB CI Class Models“ aktiviert ist, erstellt die Identification and Reconciliation Engine (IRE) neue CIs mit neuen Klassen. Weitere Informationen finden Sie unter Erstellen von CIs für Vulnerability Response mit der Engine „Identification and Reconciliation“.. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden die Datensätze der erkannten Elemente entsprechend dem Status aktualisiert. Erkannte Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in CMDBzugeordnet werden.

**CI-Suchregeln**

Wenn Daten aus einer Drittanbieterintegration importiert werden, verwendet Vulnerability Response automatisch Hostdaten (Asset-Daten), um nach Übereinstimmungen in der Configuration Management Database (CMDB) zu suchen. CI-Suchregeln werden verwendet, um CIs zu identifizieren und zu VI-Datensätzen hinzuzufügen, wenn VIs erstellt werden, um Sie bei der Korrektur zu unterstützen.

**Erneuter Scan und Korrekturscan**

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Schwachstellengruppe oder einen Drittanbietereintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Drittanbieter-Schwachstelleneinträge in Ihrer Now Platform -Instanz initiieren. Tenable bezeichnet diesen erneuten Scan als Korrektur **-Scan**.

**Ältere AEs automatisch schließen**

Mit dem Modul „Veraltete angreifbare Elemente automatisch schließen“ in Ihrem Now Platformkönnen Sie ältere, veraltete angreifbare Elemente (AEs) bereinigen, die von Ihren Drittanbieterintegrationen nicht kürzlich gefunden wurden. Wenn Sie diese AEs in den Status „ **Geschlossen** “ verschieben, können Sie die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben reduzieren und Assets in Ihrem CMDBabgleichen . Sie können alle Integrationen mit Vulnerability Response Integration with Tenable verwenden, um veraltete VIs automatisch zu schließen.

**Instanz**

Dieser Begriff bezieht sich auf ein eindeutiges Vorkommen Ihrer Now Platform® -Anwendung.

**Integration**

Eine Integration ist ein produktspezifischer Verweis auf eine Integration, z. B. die Tenable.io Assets-Integration oder die Tenable.sc Plugin-Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable Vulnerability-Integration in Ihrer Instanz gehören.

**Integrationsinstanz**

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach ihren Produkten Tenable.io und Tenable.sc aufgelistet sind.

**Bereitstellung**

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff wird verwendet, um sich auf die Integrationen und Produkte in Ihrer Umgebung zu beziehen. Beispielsweise können Sie mehrere Bereitstellungen verschiedener Integrationen der Produkte Tenable.io und Tenable.sc in Ihrer Umgebung haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integrationen Tenable.io und Tenable.sc umfassen auch die folgenden wichtigen Funktionen:

- Ergebnisse der Konfigurationsbewertung, d. h. Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit maßgeblichen Quellen, können mit dem Produkt Tenable.ioConfiguration Compliance in die Anwendung [] importiert werden. Weitere Informationen zur Funktionsweise dieser Integration mit der Anwendung Configuration Compliance ] finden Sie unter Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance . und Configuration Compliance erkunden.
- Erstellen Sie ab Version 2.1 von Tenable Vulnerability Integrationeindeutige Konfigurationselemente (CIs), die verschiedene Netzwerkpartitionsbezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.
- Sie können planen, wann die Aufträge für alle Tenable.io - und Tenable.sc -Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben bei Bedarf auch manuell ausführen.
- Für Asset-Importe mit Tenable.iokönnen Sie Asset-Tags aktivieren, um die in Ihrem CMDB in der Tenable.io -Umgebung aufgeführten Assets zu organisieren und nachzuverfolgen.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie CI-Suchregeln konfigurieren, um zu definieren, wie Asset-Daten aus Drittanbieterquellen zum Identifizieren von Konfigurationselementen (Configuration Items, CIs) in Now Platform CMDBverwendet werden.
- Mit den Integrationen Tenable.io und Tenable.sc können Sie Importfilter für den Import von Schwachstellen festlegen, sodass Sie nur die gewünschten Schwachstellen aus Tenable importieren. Für Tenable.iohaben Sie die Möglichkeit, mit dem Import von Schwachstellen behobene Schwachstellen aus **Tenable** zu importieren.
- Für Tenable.schaben Sie die Möglichkeit, erneute Scans bei Bedarf direkt aus Datensätzen für angreifbare Elemente, Korrekturaufgaben und Drittparteieinträgen in Ihrer Instanz Now Platform zu initiieren. Wenn AEs auf „ **Geschlossen"/** „Korrigiert" gesetzt wurden, aber in Ihrer Instanz noch nicht aktualisiert wurden, können Sie überprüfen, ob Schwachstellen in bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für die Tenable.sc -Integration.

In den folgenden Abschnitten werden weitere Details zu Tenable-Integrationen aufgeführt.

## Erforderliche Now Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrer Instanz Now Platform.

**Administrator**

Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.

**sn_vul.vulnerability_admin**

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und -Regeln für installierte Drittanbieterintegrationen.

**sn_vul_tenable.configure_integration**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Rolle enthält die granulare Rolle „sn_vul_tenable.read_integration“. Benutzer mit dieser Rolle können die Anwendung Vulnerability Response Integration with Tenable konfigurieren.

**sn_vul_tenable.read_integration**

Benutzer mit diesen Rollen können Datensätze der Anwendung Vulnerability Response Integration with Tenable anzeigen (lesen), aber nicht bearbeiten.

**Vulnerability Response-Gruppe**

Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.

## Angreifbare Elemente

Angreifbare Elemente werden gemäß Gruppenregeln in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln und Vulnerability Response Übersicht über Zuweisungsregeln.

## Konfigurationselement-Suchregeln (CI).

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Schwachstellenintegrationen von Drittparteien.

**Hinweis:**
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Die folgenden Suchregeln Tenable.io werden mit dem Basissystem geliefert.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Die folgenden Suchregeln Tenable.sc werden mit dem Basissystem geliefert.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

**Hinweis:**
Mehrere Werte für ip_address, mac_address, fqdns und network_interfaces werden für ein Asset verwendet. Alle Werte werden in den CI-Suchregeln für den Abgleich berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Konfigurieren der Kategorisierung nicht abgeglichener Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

## Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.iosind zwei Eigenschaften verfügbar, wenn Sie mehrere IP-Adressen oder mehrere MAC-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

**ignoreIPAddress**

Eine Liste der IP-Adressen, die für die CI-Suche und CI-Erstellung ignoriert werden sollen.

**ignoreMacAddress**

Eine Liste der MAC-Adressen, die für die CI-Suche oder CI-Erstellung ignoriert werden sollen.

## Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Integrationen von Tenable Vulnerable Items und Tenable Asset erkannt wurden.

**Hinweis:**
Der Standardfilter für diese Liste ist auf Nicht abgeglichenfestgelegt. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „Erkannte Elemente“ finden Sie unter Erkannte Elemente.

## Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den zu scannenden Assets zugeordnet sind. Mit dem Modul „Asset-Tags“ können Sie Asset-Tag-Daten aus Tenable.io nach Zeitplan in Ihre Instanz herunterladen. Asset-Daten, die Asset-Tags enthalten, werden aus Tenable.io abgerufen und mithilfe der Transformationszuordnungen der Tenable.io Asset Transform- Integration transformiert.

Alle Asset-Tags werden als Teil der Tenable.io Asset-Integration importiert. Asset-Tags werden im Allgemeinen zum Filtern in Vulnerability Response Zuweisungsregeln und Korrekturaufgabenregeln verwendet. Die Tags werden im Formular „Erkanntes Element“ angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Führen Sie die Tenable.io Asset-Integration aus, bevor Sie Vulnerability Response Zuweisungsregeln oder Regeln für Korrekturaufgaben in der Anwendung Vulnerability Response erstellen, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise ein Tag erstellen, um Assets an Ihrem Standort San Diego zu beschreiben, und Sie das San Diego -Tag erstellen, können Sie nicht auch ein SAN DIEGO -Tag erstellen und in der Asset-Tag-Tabelle speichern. San Diego und SAN DIEGO werden vom System als dasselbe Asset-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das in Zukunft gespeichert und erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.import_asset_tags gesteuert. Diese Eigenschaft ist standardmäßig auf „ true “ festgelegt. Durch das Deaktivieren von Tags werden sie in allen Now Platform® Instanzen deaktiviert.

## Datenabruffilter

Mit den Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in Ihre Now Platform® -Instanz importieren möchten. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable Vulnerability-Integration.

## Schwachstellenprioritätsbewertung (VPR)

Die Schwachstellenprioritätsbewertung (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in Vulnerability Responseverwendet wird. Die Tenable Risk-Regel wird mit der Anwendung Vulnerability Response Integration with Tenable als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Responseinstalliert.

Diese Risikoregel ist standardmäßig deaktiviert.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Die Aktivierung dieser Tenable Risk Calculator-Regel kann Auswirkungen auf die Leistung der Datenerfassung haben. Weitere Informationen zu Vulnerability Response -Rechnern und der Tenable-Risiko-Rechnerregel finden Sie unter Vulnerability Response -Rechner und Schwachstellen-Rechnerregeln.

## Installation und Konfiguration

Nachdem Sie Vulnerability Response Integration with Tenable aus dem ServiceNow® Storeheruntergeladen haben, werden Installation und Konfiguration durch den Setup-Assistenten in Vulnerability Responseunterstützt. Weitere Informationen finden Sie unter Vulnerability Response mit dem Setup-Assistenten konfigurieren.

### Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance .

Die Tenable.io -Integrationen in der Anwendung Vulnerability Response Integration with Tenable sind in den Anwendungen Vulnerability Response und Configuration Compliance verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Liste der Tenable.io Integrationen

Mehrere Quellen werden für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in Vulnerability Responsehinzufügen und bereitstellen. Sie installieren und konfigurieren die Anwendung Vulnerability Response Integration with Tenable auch über den Setup-Assistenten.

Tenable.io ist eine cloudbasierte Unternehmensintegration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für das Produkt Tenable.io.

Tenable.io Integration von Compliance-Ergebnissen und Tenable.io Integration von Compliance-Ergebnissen sind standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
2. Klicken Sie in der Liste Tenable Integrations (Vertretbare Integrationen) auf einen Integrationsnamen, um den Datensatz zu öffnen, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen können.

### Tenable.io-Integrationen

| Integration | Beschreibung |
|---|---|
| Tenable.io Assets-Integration | • Ruft alle Asset-Daten, einschließlich Asset-Tags, aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz.<br>• Ab v3.0 können Sie, wenn Tenable.io Compliance-Ergebnisse-Integration aktiviert ist, sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Asset-API.<br>• Die Ausgabe dieser Integration sind erkannte Elemente.<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br>• Ab v2.2 wird `Last Scan Time` nur für Assets mit Schwachstellen importiert und aktualisiert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| Tenable.io Integration von Compliance-Ergebnissen | • Ab v3.0 können Sie importierte sichere Konfigurationsbewertungsdaten aus der Compliance-Ergebnisintegration zusammen mit importierten Daten aus der Asset-Integration dabei unterstützen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.<br>• Wenn diese Option aktiviert ist, werden allgemeine sichere Konfigurationsbewertungsdaten abgerufen und in Ihrer Now Platform -Instanz verarbeitet. Importierte Daten umfassen Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen.<br>• Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert.<br>• Wenn ein Testergebnis importiert wird und das entsprechende Asset in Ihrer Instanz nicht abgeglichen werden kann, wird das Testergebnis ignoriert und die ID für das fehlende Asset in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_asset] gespeichert.<br>• Der Gesamtwert der ignorierten (fehlenden) Assets wird im Feld **Ignorierte CIs** auf der Registerkarte **Konfiguration** des Integrationsausführungsdatensatzes für diese Integration aufgelistet. |
| Tenable.io Integration von Compliance-Ergebnisauffüllung | • Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Assets-Integration im Rahmen einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration gleicht Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_tenable_missing_asset] aufgeführt sind.<br>• Importiert bis zu 200 Asset-IDs für fehlende Assets, die erkannt wurden oder in der Instanz vorhanden sind, nachdem der Import der Assets-Integration erfolgreich abgeschlossen wurde.<br>• Entfernt die temporären Datensätze aus der Tabelle [sn_vul_tenable_missing_asset], wenn Assets mit den entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können. |
| Tenable.io Integration von Scan-Anmeldeinformationen | • Diese Integration ruft die in Tenable.iokonfigurierten Scan-Anmeldeinformationen ab.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | • Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_tenable_scan_credential] ausgefüllt sind.<br>• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scan-Anforderungen von Now Platforminitiiert werden.<br>• Diese Integration ist so geplant, dass sie wöchentlich ausgeführt wird. |
| Tenable.io Vorlagenintegration | Während des erneuten Scannens wird ein Vorlagendatensatz an Tenable.io gesendet. Diese Integration ruft verfügbare Tenable.io Anmeldeinformationen ab, die für erneute Scans verwendet werden sollen. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und sicher vorübergehend in der Tabelle [sn_vul_tenable_io_template] gespeichert. |
| Tenable.io Plugin-Integration | • Ruft die Plugin-Daten aus dem Produkt Tenable.io ab. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt durch eine Tenable.io Integrationsausführung aktualisiert wurden.<br>• Dieser Import stellt sicher, dass die Tenable.io Bezeichner (10 IDs) aktuell sind.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API.<br>• Das Ergebnis dieser Integration sind Schwachstellen von Drittparteien. |
| Tenable.io Integration behobener Schwachstellen | • Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status „ **Offen** “ und **„Erneut geöffnet“** befinden, da diese Datensätze korrigiert werden müssen. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen **behoben**sind, aber angreifbare Elemente werden standardmäßig nicht für **feste** Erkennungen erstellt, da **Tenablefeste**Schwachstellen als verringert betrachtet.<br>• Wenn im Setup-Assistenten die Kennzeichnung **„Angreifbare Zeiten für Erkennungen von festen Schwachstellen erstellen** “ aktiviert ist, werden neue VIs im Status „ **Fest** “ erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann dies die Importleistung beeinträchtigen. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit bei **Erkennungen** mit Korrekturen nur die Status vorhandener angreifbarer Elemente aktualisiert werden.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **geschlossene/behobene** angreifbare Elemente (AEs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br><br>Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach dem erfolgreichen Abschluss einer Ausführung die unten beschriebene Integration offener Schwachstellen ausgelöst wird.<br><br>Ab Tenable v3.3 können Sie die folgenden Informationen für ausgeführte Schwachstellenintegrationen anzeigen:<br>• Blöcke**gesamt:** Gesamtzahl der von Tenable generierten Blöcke<br>• **Verfügbare Blöcke:** Anzahl der Blöcke, die für ServiceNow zum Download verfügbar sind. |
| Tenable.io Integration offener Schwachstellen | • Diese Integration wird nach erfolgreichem Abschluss der Tenable.io Integration behobener Schwachstellen ausgelöst.<br>• Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus dem Produkt Tenable.io ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **neue/erneut geöffnete** angreifbare Elemente (AEs). Außerdem werden |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind. Tenable betrachtet aktive Schwachstellen **kumulativ** (aktuell).<br>• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_chunk_status] gespeichert. Die Tabellenbereinigung entfernt gespeicherte Daten nach 30 Tagen automatisch aus dieser Tabelle.<br><br>Ab Tenable v3.3 können Sie die folgenden Informationen für ausgeführte Schwachstellenintegrationen anzeigen:<br>• Blöcke**gesamt:** Gesamtzahl der von Tenable generierten Blöcke<br>• **Verfügbare Blöcke:** Anzahl der Blöcke, die für ServiceNow zum Download verfügbar sind. |

### Integrationen vonTenable.sc mit der Anwendung Vulnerability Response .

Die Tenable.sc -Integrationen in der Anwendung Vulnerability Response Integration with Tenable.

Wenn ab Vulnerability Response v20.0 ein Asset von einem Agent gescannt wird, wird in der Spalte „Agent vorhanden“ der Wert „true“ in der Liste „Erkannte Elemente“ angezeigt, der angibt, dass es sich um einen echten Scan handelt.

## Liste der Tenable.sc Integrationen

Mehrere Quellen werden für alle Tenable.io - und Tenable.sc -Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in Vulnerability Responsehinzufügen und bereitstellen. Sie installieren und konfigurieren die Anwendung Vulnerability Response Integration with Tenable auch über den Setup-Assistenten.

- Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform in derselben Umgebung befinden.
- Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden.

**Tenable.sc-Integrationen**

| Integration | Beschreibung |
|---|---|
| Tenable.sc Assets-Integration | Um zu vermeiden, dass doppelte erkannte Elemente mit importierten Asset-Daten erstellt werden, besteht die Asset-Integration des Produkts Tenable.sc aus zwei Integrationen.<br>**Die Tenable.sc Open Assets-Integration**<br>Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **kumulativ** (aktuell) oder **offen**betrachtet. Die angreifbaren Elemente (VIs), die |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | in Ihrer Instanz mit diesen importierten Asset-Daten erstellt werden, gelten als offen, d. h. im Status „ **Offen** “. Diese angreifbaren Elemente müssen untersucht und möglicherweise korrigiert werden.<br>**Die Tenable.sc Integration von Anlagegütern**<br>Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable als **verringert** (nicht mehr angreifbar) oder **behoben**ansieht. Die angreifbaren Elemente für diese Assets gehen in Ihrer Instanz vom Status „ **Offen** “ in den Status **„Geschlossen/ Korrigiert** “ über, da die Ergebnisse von Scans zeigen, dass sie nicht mehr angreifbar sind.<br>• Ruft alle Asset-Daten aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Assets-API.<br>• Die Ausgabe dieser Integration sind erkannte Elemente.<br>• Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für die Tenable.sc Assets-Integration. Es werden nur die Assets mit den Schwachstellen importiert, die den Bedingungen des Abfragefilters entsprechen. |
| Tenable.sc Plugin-Integration | • Ruft die Plugin-Daten aus dem Produkt Tenable.sc ab. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt durch eine Tenable.sc Integrationsausführung aktualisiert wurden.<br>• Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (10 IDs) aktuell sind und nur aktive Schwachstellen importiert werden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API.<br>• Das Ergebnis dieser Integration sind Schwachstellen von Drittparteien. |
| Tenable.sc Integration behobener Schwachstellen | • Ruft Schwachstellendaten basierend auf Schweregradfiltern aus dem Produkt Tenable.sc ab und verarbeitet sie in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich im Status „ **Offen** “ und **„Erneut geöffnet“** befinden, da diese Datensätze korrigiert werden |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | müssen. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen **behoben**sind, aber angreifbare Elemente werden standardmäßig nicht für **feste** Erkennungen erstellt, da **Tenablefeste**Schwachstellen als verringert betrachtet.<br>• Wenn im Setup-Assistenten die Kennzeichnung **Schwachstellenzeiten für Erkennungen von festen Schwachstellen erstellen** aktiviert ist, werden neue VIs im Status „ **Fest** “ erstellt, sodass Sie Einblick in die Erkennungen haben, von denen sie erstellt wurden. Da VIs für **feste** Erkennungen erstellt werden, die in Ihrer Instanz noch nicht vorhanden sind, kann dies die Importleistung beeinträchtigen. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit bei **Erkennungen** mit Korrekturen nur die Status vorhandener angreifbarer Elemente aktualisiert werden.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration sind **geschlossene/ behobene** angreifbare Elemente (AEs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br><br>Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach einer erfolgreichen Ausführung die unten beschriebene Tenable.sc Integration offener Schwachstellen ausgelöst wird.<br><br>**Hinweis:**<br>Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen. |
| Tenable.sc Integration offener Schwachstellen | • Diese Integration wird nach erfolgreichem Abschluss der Tenable.sc Integration behobener Schwachstellen ausgelöst.<br>• Ruft Schwachstellendaten basierend auf den im Produkt Tenable.sc ausgewählten Abfragefiltern ab und verarbeitet sie in Ihrer Instanz.<br>• Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen.<br>• Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | „Netzwerkpartitionsbezeichner“ für Assets in Ihrer Umgebung, die dieselbe IP-Adresse verwenden.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.<br>• Die Ausgabe dieser Integration lautet **Aktualisieren/ Neue angreifbare Elemente erstellen**, sofern sie nicht bereits vorhanden sind. Außerdem werden Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>**Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen. |
| Tenable.sc Integration von Scan-Anmeldeinformationen | • Diese Integration ruft die in Tenable.sckonfigurierten Scan-Anmeldeinformationen ab.<br>• Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API.<br>• Die Ausgabe dieser Integration sind Scan-Anmeldeinformationen, die in die Tabelle [sn_vul_tenable_scan_credential] eingetragen werden.<br>• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scan-Anforderungen von Now Platforminitiiert werden.<br>• Diese Integration ist so geplant, dass sie wöchentlich ausgeführt wird. |
| Tenable.sc Integration von Auffüllung von Schwachstellen | • Diese Auffüllungsintegration importiert alle offenen und behobenen Schwachstellen, die während eines Imports möglicherweise übersehen wurden.<br>• Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren.<br>• Diese Integration kann sich auf Ihre Leistung auswirken.<br>• Diese Integration ist standardmäßig deaktiviert.<br>• Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, sollten Sie die Integrationen von Tenable.sc mit festen und offenen Schwachstellen so planen, dass sie ausgeführt werden, wenn keine anderen Scans ausgeführt werden.<br>• Die Ausgabe dieser Integration ist: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.sc-Integrationen (Fortsetzung)**

| Integration | Beschreibung |
|---|---|
| | ○ **Geschlossene/behobene** angreifbare Elemente (VIs). Außerdem werden Assets und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind.<br>○ zum **Aktualisieren/Erstellen neuer** angreifbarer Elemente (VIs), wenn sie noch nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittanbietereinträge erstellt, wenn sie nicht vorhanden sind. |

## Benutzerauthentifizierung und Tenable.sc

Die Benutzerauthentifizierung wird von Ihrer Now Platform® -Instanz und Version 5.13 des Tenable.sc -Produkts unterstützt. Die Benutzerauthentifizierung ist erforderlich, wenn Sie Version 5.12 und früher des Produkts Tenable.sc verwenden.

Wenn Sie die Benutzerauthentifizierung für die Tenable.sc -Integrationen auswählen, laufen Token möglicherweise ab und müssen während der Integrationsausführungen ersetzt werden. In der Spalte Notizen im Datensatz der Ausführung der Schwachstelle-Integration (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen. Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

### Vorbereitung auf die Tenable Vulnerability-Integration

Bereiten Sie sich auf die Integration von ServiceNow® Tenable Vulnerability vor, indem Sie die folgenden Setup-Aufgaben ausführen.

## Bevor Sie beginnen

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Für eine reibungslose Installation und Konfiguration der Anwendung Vulnerability Response Integration with Tenable sollten Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in Ihre Now Platform® -Instanz importieren.

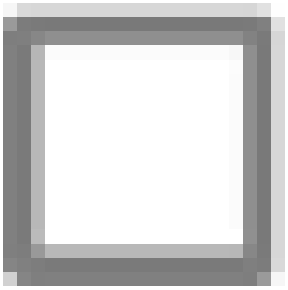
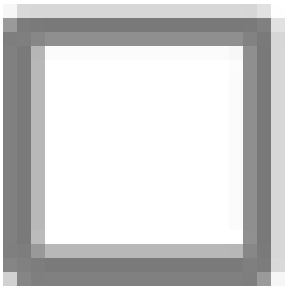
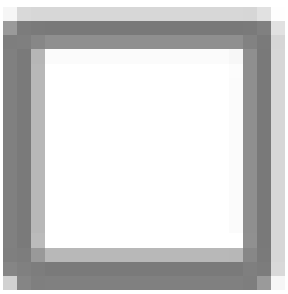
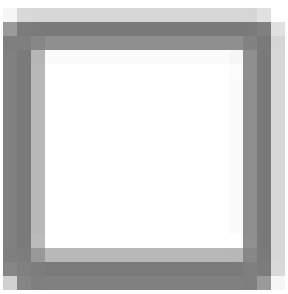
**Hinweis:**
Wenn Sie Daten mit der in Tenable erstellten Integration importiert haben und ServiceNow® Vulnerability Response Integration with Tenable verwenden möchten, finden Sie weitere Informationen unter

Aktuelle Informationen zur Datenbereinigung und Migration von der in Tenable erstellten Integration zur von ServiceNowerstellten Integration finden Sie im Artikel Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] .

Erforderliche Rolle: admin zum Herunterladen und Installieren der Anwendung.

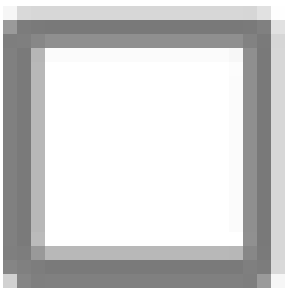
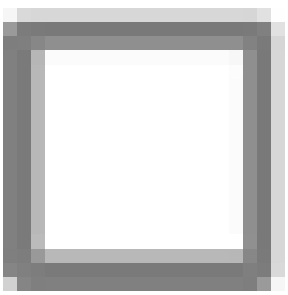


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
|  | (Optional) Wenn noch nicht installiert und aktiviert, ziehen Sie es möglicherweise vor, die Anwendung Vulnerability Response zu installieren, bevor Sie die Drittanbieteranwendung installieren.<br><br>Weitere Informationen zum Installieren und Aktivieren der Anwendung Vulnerability Response finden Sie unter Vulnerability Response installieren. Diese Integration erfordert Version 12.1 von Vulnerability Response oder höher. |
|  | Wenn Sie sie noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Integration with Tenable in Ihre Instanz Now Platform® ] herunter. Die Anwendung Vulnerability Response Integration with Tenable unterstützt das Produkt Tenable.sc ab Version 5.13.<br><br>Weitere Informationen finden Sie unter . |
|  | Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie voraussichtlich importieren werden.<br><br>Vergewissern Sie sich, dass Ihre Instanz die Anzahl der zu importierenden angreifbaren Elemente akzeptieren kann. Eine zu kleine Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an den technischen Support von ServiceNow®. |
|  | Vergewissern Sie sich, dass Sie über Gruppen oder Benutzer verfügen, die die Integrationen verwalten und angreifbare Elemente korrigieren.<br><br>**Administrator**<br><br>Der Systemadministrator verwendet den Setup-Assistenten, um die Anwendung Vulnerability Response Integration with Tenable zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.vulnerability_admin) und andere Rollen im Setup-Assistenten zu.<br><br>**sn_vul.vulnerability_admin**<br><br>Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittanbietern.<br><br>**sn_vul_tenable.configure_integration**<br><br>Kann die Tenable Vulnerability-Integration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_tenable.read_integration.<br><br>**sn_vul_tenable.read_integration** |

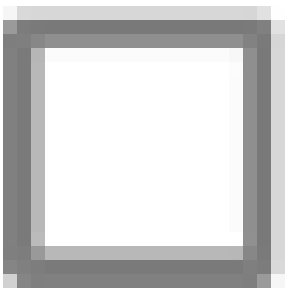


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | Kann Datensätze der Tenable Vulnerability-Integration anzeigen (lesen).<br>**Vulnerability Response-Gruppe**<br>Standardmäßig ist die Gruppe Vulnerability Response im Setup-Assistenten verfügbar. Benutzer, die der Vulnerability Response-Gruppe zugewiesen sind, erben automatisch die Rollen sn_vul.read_all und sn_vul.remediation_owner.<br>Der Systemadministrator führt die anfängliche Zuweisung von Rollen zu Benutzern und Gruppen im Setup-Assistenten für die -Integration durch. Standardmäßig ist die Gruppe Vulnerability Response verfügbar. Wenn dies noch nicht geschehen ist, ziehen Sie es möglicherweise vor, zusätzliche Gruppen zu erstellen und Benutzer mit dem Benutzerverwaltungsmodul in Ihrer Instanz hinzuzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Benutzergruppen erstellen .<br>Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu. |
|  | Um die Leistung beim ersten Import zu verbessern, sollten Sie bestimmte Funktionen, Regeln oder Aufgaben in Ihrer Instanz deaktivieren.<br>• Deaktivieren Sie Schwachstellenrechner, wenn Sie sie nicht verwenden. Diese und die von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Siehe Schwachstellenrechner deaktivieren.<br>• Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import möchten Sie möglicherweise benachrichtigungsbezogene Business Rules deaktivieren, wie in Importieren Sie Änderungen für die Integration von Tenable Vulnerabilitybeschrieben. |
|  | Vergewissern Sie sich, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Jobs in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind.<br>• Tenable.sc ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID Server zu verwenden, wenn sich das Produkt Vulnerability Response Integration with Tenable und Ihre Instanz Now Platform in derselben Umgebung befinden. Wenn sich das Produkt Tenable.sc und Ihre Instanz Now Platform nicht in derselben Umgebung befinden, müssen Sie einen MID Server verwenden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Aufgabe | Beschreibung |
| --- | --- |
| | Weitere Informationen zu MID Servern in Ihrer Instanz finden Sie unter MID Server .<br>• Vergewissern Sie sich, dass das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht Basissystemkomponenten den Aufruf externer Systeme mithilfe von Integrations-APIs und aktiviert Protokollschritte wie REST.<br>Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** und suchen Sie das Plugin. Wenn in Ihrer Instanz nicht installiert ist, installieren und aktivieren Sie es. |
|  | Rufen Sie Tenable-Anmeldeinformationen ab.<br>Vergewissern Sie sich, dass Sie über alle Kontonamen, Passwörter und andere Serviceinformationen verfügen, die für Ihre Tenable-Produkte erforderlich sind, damit Sie darauf zugreifen können.<br>Tenable.io erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64. Tenable.sc erfordert Sicherheitsanalysten oder Managerzugriff.<br>**Hinweis:**<br>Ab Version 3.8 von Vulnerability Response Integration with Tenablesind für den Zugriff auf Tenable.io keine Administratorrechte mehr erforderlich. Ein Basisbenutzer mit einem Berechtigungsattribut gleich 16 kann ebenfalls auf das Produkt zugreifen. |

Sie sind bereit für Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten.

### Installieren Sie die Anwendung Vulnerability Response Integration with Tenable mit dem Setup-Assistenten

Bevor Sie ServiceNow® Tenable Vulnerability Integration ausführen, müssen Sie die Anwendung Vulnerability Response Integration with Tenable aus dem ServiceNow Store herunterladen und mit dem Setup-Assistenten in der Anwendung Vulnerability Response ] installieren und konfigurieren.

#### Vorbereitungen

Vergewissern Sie sich vor der Installation der Tenable-Anwendung, dass Sie alle Elemente in der Prüfliste in Vorbereitung auf die Tenable Vulnerability-Integrationabgeschlossen haben.

**Hinweis:**
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Test- und Entwicklungsumgebungsinstanzen herunterladen, sind keine Berechtigungen erforderlich. Fahren Sie mit Aktivieren Sie eine Anwendung ServiceNow Store .fort.

Erforderliche Rollen: admin für die erstmalige Zuweisung der Rolle „sn_vul.vulnerability_admin“ und Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.vulnerability_admin oder sn_vul.admin (veraltet) zur Konfiguration der Anwendung im Setup-Assistenten nach der Installation.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**.

   Nach einiger Zeit werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie die Kachel **Tenable (Tenable-Plattform),** und klicken Sie auf **Installieren**.

   Mit dieser Aktion wird die Anwendung Vulnerability Response Integration with Tenable installiert, die Sie aus dem ServiceNow Storeheruntergeladen haben.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Sie Vulnerability Response Anwendungen von Drittanbietern mit dem Setup-Assistenten.

### Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie im Setup-Assistenten zu **Integrationskonfiguration > Scanner-Integrationen**, um mit der Konfiguration fortzufahren. Weitere Informationen zu den Eingabeaufforderungen im Setup-Assistenten finden Sie unter Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten.

#### Datenabrufeinstellungen für die Tenable Vulnerability-Integration

Mit den folgenden Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der ServiceNow® Tenable Vulnerability-Integration in Ihre Now Platform® ]-Instanz importieren möchten.

Mit den in den folgenden Abschnitten beschriebenen Einstellungen können Sie die Daten steuern, die Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter in Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Integrationsinstanzen** und klicken Sie auf Ihre Integration, Tenable.io oder Tenable.sc.

Klicken Sie auf der angezeigten Seite „Integrationsinstanz“ auf Integrationsinstanzparameter, um eine Liste von Parametern anzuzeigen, oder auf die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

### Allgemeine Schweregrad- und Abrufeinstellungen und Filter für Tenable.io und Tenable.sc in Ihrer Now Platform -Instanz

Die folgenden Einstellungen sind für die Integrationen Tenable.io und Tenable.sc in Ihrer Instanz Now Platform ] verfügbar. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ Ihrer Now Platform -Instanz angezeigt. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardwerten belassen.

Tenable.io

**insert_fixed**

Wenn Sie die **Kennzeichnung insert_fixed** im Setup-Assistenten für die Integration von Schwachstellenimport aktivieren, werden neue VIs für Erkennungen im Status „ **Fest** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

**Schweregrad_kritisch**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit kritischem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_hoch**

Dieser Filter ist standardmäßig aktiviert („true“), um Schwachstellen mit hohem Schweregrad aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_mittel**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad aus den Integrationen Tenable.io offene Schwachstellen und Tenable.io feste Schwachstellen zu erhalten.

**Schweregrad_info**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Infoebene aus den Integrationen Tenable.io Offene Schwachstellen und Tenable.io Feste Schwachstellen zu erhalten.

**Schweregrad_niedrig**

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad aus den Integrationen Tenable.io offene Schwachstellen und Tenable.io feste Schwachstellen zu erhalten.

**size**

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz aus der Tenable.io Plugin-Integration aufgenommen werden sollen. Muss im Format int32 vorliegen. Der Standardwert ist 1.000. Die maximale Größe beträgt 10.000.

**num_assets**

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus den Integrationen von Tenable.io Behobene Schwachstellen und Tenable.io Offene Schwachstellen. Der Standardwert ist 50.

**chunk_size**

Gibt die Anzahl der Assets pro exportiertem Block durch die Tenable.io Assets-Integration an. Der Standardwert ist 1.000.

Tenable.sc

**async_request**

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit Tenable.sc durchzuführen. Wenn bei synchronen Aufrufen eine Zeitüberschreitung bei 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box zu optimieren. Sobald dieser Parameter aktiviert ist, gilt er für alle Integrationen von Tenable.sc. Für bestehende Kunden, die asynchrone Aufrufe verwenden, ist ein Korrekturskript verfügbar, das den vorhandenen Tenable.sc -Integrationsinstanzen einen neuen async_request-Parameter hinzufügt. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**.

**insert_fixed**

Wenn Sie die **Kennzeichnung insert_fixed** im Setup-Assistenten für die Integration von Schwachstellenimport aktivieren, werden neue VIs für Erkennungen im Status „ **Fest** “ erstellt, die in Ihrer Instanz noch nicht vorhanden sind.

**Offset**

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Abfragefilter**

Abfragefilter werden in der Tenable-Konsole konfiguriert. Diese Abfragefilter haben IDs, die im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in Ihrer Now Platform -Instanz ausgewählt werden können. Diese Filter werden beim Abrufen der Daten aus den Tenable.sc -Integrationen angewendet.

### REST-Nachrichten für die Integration von Tenable Vulnerability

Die REST-Nachrichten ServiceNow® Tenable Vulnerability Integration werden für Aufrufe an die Tenable-API verwendet.

## Tenable.io REST-Nachricht für Assets

Die REST-Nachricht Tenable.io Assets ruft Assets-Informationen für die Tenable.io Asset-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Asset-Informationen aus. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „is_deleted“: falsch
- „is_licensed“: wahr

## Tenable.io Plugins-REST-Nachricht

Die REST-Nachricht Tenable.io Plugins ruft Plugin-Informationen für die Tenable.io Plugin-Integration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Plugin-Informationen aus.

## Tenable.io REST-Nachricht zu Schwachstellen

Die REST-Nachricht Tenable.io Schwachstellen ruft Schwachstelleninformationen für offene und geschlossene Schwachstellen aus der Schwachstellenintegration Tenable.io ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderungen an Tenable.io zum Abrufen von Informationen zu Schwachstellen aus.

## Tenable.sc Fragt die REST-Nachricht ab

Die REST-Nachricht „Tenable.sc-Abfragen“ ruft die Abfragefilterinformationen für die Tenable.sc-Asset-Integration und die Tenable.sc-Schwachstellenintegration ab, in der der Abfragefilter konfiguriert ist.

## Tenable.sc Plugins-REST-Nachricht

Die Tenable.sc Plugin-REST-Nachricht ruft Plugin-Informationen für die Tenable.sc Plugin-Integration ab. Änderungen am Methodendatensatz der REST-Nachricht „Plugins abrufen“ wirken sich auf die Anforderungen an Tenable.sc zum Abrufen von Plugin-Informationen aus.

| Parametername | Wert | Beschreibung |
|---|---|---|
| type | aktiv | Gibt an, aus welcher Quelle Tenable Daten abruft. Von Code verwendet. Änderungen werden nicht empfohlen. |
| Felder | ID, Beschreibung, cvssVector, cvssV3Vector, cvssV3TemporalVector, | Gibt die Liste der Felder an, die aus Tenable importiert wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Parametername | Wert | Beschreibung |
|---|---|---|
| | synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vpr, vprContext, PluginPubDate, PluginModDate, xrefs, Familie, RiskFactor, cpe, seeAlso, Lösung, ExploitFrameworkAvailable, ExploitFrameworkAvailable Typ, Copyright, Version, Quelldatei, Abhängigkeiten, erforderlichePorts, erforderlichUDPPorts, srcPort, dstPort,Protokoll, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifizierteZeit, md5 | |

## Tenable.sc REST-Nachricht zu Schwachstellen

Die REST-Nachricht Tenable.sc Schwachstellen ruft Schwachstelleninformationen aus der Tenable.sc -Integration ab. Änderungen an der REST-Nachricht „Schwachstellen abrufen“ oder „Gepatchte Schwachstellen abrufen“ oder, ab Version 14.0 Vulnerability Response und Version 2.2 der Tenable Vulnerability-Integration, am Datensatz „Schwachstellen für Auffüllung abrufen“ wirken sich auf die Anforderungen zum Abrufen von Informationen zu Schwachstellen an Tenable.sc aus.

## Tenable.sc REST-Nachricht „Anmeldeinformationen scannen“.

**Tenable.sc Richtlinien-REST-Nachricht**

Die POST-REST-Nachricht Tenable.sc policy fügt eine Richtlinie für angeforderte Plugins hinzu. Generierte Richtlinie wird in Tenable.sc Scan-Anforderungen verwendet.

**Tenable.sc REST-Nachricht scannen**

Die POST-REST-Nachricht Tenable.sc scan fügt einen Scan hinzu, der vom Zugriff und der Berechtigung abhängt, die im Anforderungstext der REST-Nachricht definiert sind. Im Anforderungstext für die Scan-Anforderung werden Richtlinie, Plugin-ID und IP(s) verwendet.

**Tenable.sc REST-Nachricht „Scan-Ergebnis“.**

Die GET-REST-Nachricht Tenable.sc Scan-Ergebnis enthält Scan-Details des Scans, der mit der Scan-REST-Nachricht generiert wurde. Er verwendet die scanResultId in der Antwort der Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

**Tenable.sc Anmeldeinformationen scannen**

Die REST-Nachricht Tenable.sc scan credentials ruft die Anmeldeinformationen aus Tenable.scab. Änderungen am Methodendatensatz der REST-Nachricht „Importieren“ wirken sich auf die Anforderungen an Tenable.sc zum Abrufen der Anmeldeinformationen aus.

| Parametername | Wert | Beschreibung |
|---|---|---|
| Felder | ID, Name, Beschreibung, Typ | Gibt die Liste der Felder an, die aus importiert wurden Tenable.sc |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Parametername | Wert | Beschreibung |
|---|---|---|
| filter | nutzbar | Gibt an, dass die Integration nur verwendbare Anmeldeinformationen von abruft Tenable.sc<br><br>Änderungen an einem der Parameter werden nicht empfohlen. |

### Datentransformation für die Integration von Tenable Vulnerability

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie aus dem Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „Normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen transformieren importierte Tenable-Schweregrade in Standardschweregrade für die Verarbeitung in Ihrer Instanz. Weitere Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Vulnerability Response-Schweregradzuordnungen erstellen in der Dokumentation Vulnerability Response.

## Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tenable.io-Asset-Importtabelle [sn_vul_tenable_io_asset_import] geladen.

Die Tenable.io Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach `Tenable.io Asset Transform`.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

### Tenable.io Asset-Transformationszuordnungsfelder

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | source_id | Tenable stellt eine eindeutige ID für Assets bereit, ordnet sie dem Datensatz des erkannten Elements zu und wird für die CI-Suche verwendet. |
| u_ipv4s | ip_address | Ordnet den ersten IP-Wert dem Feld ip_address im Datensatz des erkannten Elements zu. |
| u_mac_addresses | mac_address | Ordnet den ersten mac_address-Wert dem MAC-Adressfeld im Datensatz des erkannten Elements zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tenable.io Asset-Transformationszuordnungsfelder (Fortsetzung)**

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_fqdns | fqdn | Ordnet den ersten fqdn-Wert dem fqdn-Feld im Datensatz des erkannten Elements zu. |
| u_netBIOS_names | NetBIOS | Ordnet den ersten NetBIOS-Wert dem NetBIOS-Feld im Datensatz des erkannten Elements zu. |
| u_operating_systems | os | Ordnet den ersten BS-Wert dem BS-Feld im Datensatz des erkannten Elements zu. |
| (Vor Version 14.0 Vulnerability Response und Version 2.2 von Tenable Vulnerability Integration)u_last_scan_time | last_scan_date | Ordnet auf das Feld last_scan_date im Datensatz des erkannten Elements zu. |
| u_last_authenticated_scan_date | last_auth_scan_date | Ordnet auf das Feld last_auth_scan_date im Datensatz des erkannten Elements zu. |
| [Skript] | Name | Ordnet den Hostnamen mithilfe der Logik des Skripts zu. |
| u_tags | | Die Tags werden in sn_sec_cmn_host_tag gespeichert. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_tag gespeichert. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

## Timing und Zweck des Tenable.io Asset-Transformationszuordnungsskripts

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, die verwendet wird, um Werte auf dem Host zu aktualisieren und zu überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem import_set. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| | Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

## Integration von Tenable.io-Plugins

Die Transformationszuordnung für Tenable.io-Plugins wird verwendet, um aus Tenable.io importierte Plugins zu transformieren.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten verarbeitet werden, die von den Tenable-Plugins empfangen wurden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Tenable.io-Plugin-Transformation.

Die Nutzlast der Tenable.io-Plugins enthält alle Felder in der Spalte u_attributes der Tabelle sn_vul_tenable_io_plugin_import. Das Attributfeld wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| id | id | Ordnet die ID aus der Quelle zu und fügt das Präfix TEN hinzu. Beispiel: Wenn die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345. |
| Beschreibung | Zusammenfassung | Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu. |
| [Skript] | Quelle | Die Quelle für importierte TPE ist Tenable.io. |
| [Skript] | source_instance | Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert. |
| Familie | Kategorie | Ordnet die Familie des Plugins der Kategoriespalte zu |
| Plugin_Änderung_Datum | last_modified | Ordnet „plugin_modification_date“ dem Feld der letzten Änderung zu. |
| Plugin_Veröffentlichung_Datum | date_published | Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu. |
| has_patch | remediation_type | Ordnet den Korrekturtyp dem Wert has_patch zu. |
| synopsis | Bedrohung | Ordnet die Bedrohungsinformationen für diese Schwachstelle zu. |
| cvss_base__score | Punktzahl | Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| Lösung | Lösung | Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu. |
| Exploit_available | Exploit | Ordnet den vom Scanner bereitgestellten „ploit_available“ der Exploit-Spalte in der Drittpartei-Eintragstabelle zu |
| vpr.Punktzahl | source_risk_score | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| vpr.drivers.age_of_vuln | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.exploit_code_maturity | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.product_coverage | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.threat_sources_last28 | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittparteitabelle zu. |
| vpr.drivers.threat_intensity_last28 | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.threat_recency | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen von „scanner“ Threat_recency in der Drittpartei-Eintragstabelle zu. |
| vpr.drivers.cvss3_impact_score | v3_impact_subscore | Ordnet die cvss3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| cvss_temporal_score | cvss_temporal_score | Ordnet die temporäre Punktzahl für CVSS v2 zu. |
| cvss_v3_temporal_score | v3_temporal_score | Ordnet die temporäre Punktzahl für CVSS v3 zu. |
| risk_factor | source_severity | Ordnet auf den Quellschweregrad in der Drittpartei-Eintragstabelle zu. |
| Name | Name | Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu. |
| stig_severity | stig_severity | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| Plugin-Typ | check_type | Ordnet den Plugin-Typ check_type in der Drittpartei-Eintragstabelle zu. |
| unsupported_by_vendor | unsupported_by_vendor | Ordnet das Feld unsupported_by_vendor der Spalte unsupported_by_vendor zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve. |
| bid | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |
| see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| xrefs | Die X-REF-Liste wird als Referenz hinzugefügt. |
| [Skript] | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittparteieintrag. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

Die TenableIOPluginsImportProcessor-Skripteinbindung wird aus dem onBefore-Transformationsskript aufgerufen. Die Ausgabe der Tenable.io-Plugin-Integration wird in Now Platform Schwachstelleneinträge von Drittparteien umgewandelt. Alle Änderungen an dieser Skripteinbindung können die Transformation der Tenable.io-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

## Import von Tenable.io-Schwachstellen

Die Transformationszuordnung für angreifbare Tenable.io-Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

**Hinweis:**
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Tenable-Schwachstellenimport verarbeitet werden.

Dieselbe Transformationszuordnung wird sowohl für die Integration von Tenable.io mit festen Schwachstellen als auch für die Integration mit Tenable.io Open Vulnerabilities verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach der Transformationszuordnung für angreifbares Tenable.io-Element.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_asset.uuid | id | Uuid wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.ipv4 | ip_address | Das ipv4-Feld wird dem ip-Adressfeld des cmdb_ci-Datensatzes zugeordnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_asset .last_authenticated_results | last_auth_scan_date | Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Auth-Scans des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.mac_addess | mac_address | MAC-Adresse wird dem Host-MAC-Adressfeld des cmdb_ci-Datensatzes zugeordnet. |
| u_asset.netBIOS_name | NetBIOS | NetBIOS wird dem NetBIOS-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u._plugin.cvss3_base_score | v3_base_score | CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u._plugin.cvss3_temporal_score | v3_temporal_score | Die temporäre CVSS v3-Punktzahl wird der v3 temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u._plugin.cvss_base_score | Punktzahl | Die CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u._plugin.cvss_temporal_score | temporal_score | Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_plugin.description | Zusammenfassung | Die Beschreibung wird dem Zusammenfassungsfeld im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_plugin.familie | Kategorie | Ordnet die Plugin-Familie der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu. |
| u_plugin.modification_date | last_modified | Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittanbietereintrags zugeordnet. |
| u_plugin.publication_date | date_published | Das Veröffentlichungsdatum wird dem Feld |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | „Veröffentlichungsdatum“ des Datensatzes „Drittpartei-Eintrag“ zugeordnet. |
| u_plugin.risk_factor | source_severity | Der Risikofaktor wird dem Feld „source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_plugin.solution | Lösung | Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_plugin.synotsis | Bedrohung | Die Synopse wird dem Bedrohungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet. |
| u_severity_id | Priorität | Die Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5. |
| u_plugin.exploit_available | Exploit | Ordnet den vom Scanner bereitgestellten Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu. |
| vpr.Punktzahl | source_risk_score | Ordnet die vom Scanner bereitgestellte VPR-Punktzahl „source_risk_score“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_plugin.vpr.drivers.age_of_vuln | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.exploit_code_maturity | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_plugin.vpr.drivers.product_coverage | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_sources_last28 | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_intensity_last28 | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.threat_recency | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_plugin.vpr.drivers.cvss3_impact_score | v3_impact_subscore | Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte „v3_impact_subscore“ in der Drittpartei-Eintragstabelle zu. |
| u_plugin.type | check_type | Ordnet den Plugin-Typ check_type in der Drittpartei-Eintragstabelle zu. |
| u_plugin.unsupported_by_vendor | unsupported_by_vendor | Ordnet das Feld „unsupported_by_vendor“ im Plugin der Spalte „unsupported_by_vendor“ zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |
| u_plugin.family_id | Family_id | Ordnet die Familien-ID des Plugins der Spalte „family_id“ in der Drittpartei-Eintragstabelle zu. |
| port | port | Der Port wird dem Feld „Port“ des Datensatzes für angreifbare Elemente zugeordnet. |
| protocol | protocol | Das Protokoll wird dem Protokollfeld des Datensatzes |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | für angreifbare Elemente zugeordnet. |
| u_first_found | first_found | „Zuerst gefunden“ wird dem Feld „Zuerst gefunden“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_last_found | last_found | „Zuletzt gefunden“ wird dem Feld „Zuletzt gefunden“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_state | Status | Der Status wird dem Feld Status im Datensatz des angreifbaren Elements zugeordnet |
| [Skript] | Quelle | Die Quelle der Integration wird ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.io als Quelle. |
| [Skript] | integration_instance | integration_instance ist der Name der Instanz, aus der das angreifbare Element importiert wird. |
| u_plugin.name | Name | Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu. |
| u_plugin.stig_severity | stig_severity | Ordnet den STIG-Schweregrad des Plugins der Spalte „STIG-Schweregrad“ in der Drittpartei-Eintragstabelle zu |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve. |
| bid | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |
| see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| xrefs | Die X-REF-Liste wird als Referenz hinzugefügt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Beschreibung |
|---|---|
| [Skript] | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation löst TenableIOVulnerabilitiesProcessor aus, der Daten aus Tenable.io mithilfe des Importsatzes importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „Angreifbare Elemente“ und die Tabelle „Drittpartei-Schwachstelle“ lädt.Zur internen Verwendung. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Eine Funktion, um zu überprüfen, ob der Drittpartei-Eintrag und die Erkennungen bereits vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Anzahl der aus Tenable.io importierten CIs, VIs und Erkennungen zu aktualisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Tenable.sc-Asset-Import

Aus Tenable.sc importierte Asset-Daten werden zuerst in die Tenable.sc-Asset-Importtabelle (sn_vul_tenable_sc_asset_import) geladen. Die Tenable.sc Asset Integration-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Asset-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach `Tenable.sc Asset Transform`.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_uuid | id | Die UUID wird nicht über die Tenable-API ausgefüllt. Daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges UUID-Feld für Assets zu erstellen und dem cmdb_ci-Datensatz zuzuordnen. |
| u_ip | ip_address | Ordnet das IP-Feld der API dem Feld ip_address in einem cmdb_ci-Datensatz zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_macaddress | mac_address | Ordnet das Feld macaddress aus der API dem Adressfeld im cmdb_ci-Datensatz zu. |
| u_dnsname | fqdn | Ordnet das dnsname-Feld der API dem fqdn-Feld im cmdb_ci-Datensatz zu. |
| u_netBIOSName | NetBIOS | Ordnet das NetBIOS-Feld der API dem NetBIOS-Feld im cmdb_ci-Datensatz zu. |
| u_oscpe | os | Die BS-Informationen werden aus dem Attribut oscpe in der Nutzlast extrahiert und dem BS-Feld im cmdb_ci-Datensatz zugeordnet. |
| u_lastauthrun | last_auth_scan_date | Ordnet das Feld „lastauthrun“ der API dem Feld „last_auth_scan_date“ im Datensatz des erkannten Elements zu. |
| u_lastauthrun und u_lastunauthrun | last_scan_date | „lastauthrun“ wird aus der Tenable-API oder „lastunauthrun“ extrahiert. Basierend darauf, welcher Wert in der Nutzlast angezeigt wird, wird das Feld „last_scan_date“ im Datensatz des erkannten Elements ausgefüllt. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion zum Aktualisieren der Werte auf dem Host und Überprüfen, ob der Host bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem import_set. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten CIs sowie von CIs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Import von Tenable.sc-Plugins

Aus Tenable.sc importierte Plugin-Daten werden zuerst in die Tenable.sc-Plugin-Importtabelle (sn_vul_tenable_sc_plugin_import) geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**. Suchen Sie nach Tenable.sc Plugin Transform Map.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_id | id | Ordnet die ID der Quelle zu und fügt das Präfix TEN hinzu. Beispiel: Wenn die empfangene ID 12345 lautet, lautet die ID in der Zieltabelle TEN-12345. |
| u_description | Zusammenfassung | Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu. |
| [Skript] | Quelle | Importiertes TPE aus dieser Integration hat Tenable.sc als Quelle. |
| [Skript] | source_instance | Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert. |
| u_familie | Kategorie | Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu. |
| u_plugin_modification_date | last_modified | Ordnet „plugin_modification_date“ dem Feld der letzten Änderung zu. |
| u_plugin_publication_date | date_published | Ordnet „plugin_publication_date“ dem Veröffentlichungsdatum zu. |
| u_has_patch | remediation_type | Ordnet den Korrekturtyp dem Wert has_patch zu. |
| u_synosis | Bedrohung | Ordnet die Bedrohungsinformationen für diese Schwachstelle zu. |
| u_cvss_base_score | Punktzahl | Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu. |
| u_solution | Lösung | Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu. |
| u_cvss_temporal_score | cvss_temporal_score | Ordnet die temporäre Punktzahl für CVSS v2 zu. |
| u_cvss_v3_temporal_score | v3_temporal_score | Ordnet die temporäre Punktzahl für CVSS v3 zu. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_risk_factor | Quellschweregrad | Ordnet auf den Quellschweregrad in der Drittpartei-Eintragstabelle zu. |
| u_cvss_v3_base_score | v3_base_score | Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu. |
| u_exploit_available | Exploit | Ordnet das vom Scanner bereitgestellte ExploitAvailable der Exploit-Spalte in der Drittpartei-Eintragstabelle zu. |
| u_vpr_score | source_risk_score | Ordnet die VPR-Punktzahl vom Scanner der Quellrisikopunktzahl in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_vpr_context[id=age_of_vuln] | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = exploit_code_maturity] | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = product_coverage] | product_coverage | Ordnet die Produktabdeckung vom Scanner zu product_coverage in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = ”threat_sources_last_28] | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen von „scanner“ zu „thread_sources“ in der Drittparteitabelle zu. |
| u_vpr_context [id = ”threat_intensity_last_28] | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = „threat_recency“] | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = cvssV3_impactScore] | v3_impact_subscore | Ordnet die CVSS v3-Auswirkungspunktzahl des |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | Scanners v3_impact_subscore in der Drittpartei-Eintragstabelle zu. |
| u_name | Name | Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu. |
| u_stig_severity | stig_severity | Ordnet das Feld stig_severity im Plugin stig_severity in der Drittpartei-Eintragstabelle zu. |
| u_check_type | check_type | Ordnet den Prüfungstyp check_type in der Drittpartei-Eintragstabelle zu. |
| u_familie.id | familie_id | Ordnet das Plugin „family_id“ „family_id“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „exploit_attack_vector“ in der Drittpartei-Eintragstabelle wird basierend auf „exploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

Zusätzlich zu den direkten Feldern werden andere Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

| Quellenfeld | Beschreibung |
|---|---|
| u_cpe | Die Liste der CPEs wird als Referenz hinzugefügt. |
| u_see_also | Die Liste der URLs wird als Referenz hinzugefügt. |
| u_exploit_frameworks | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin in sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion zum Aktualisieren der Werte im Drittparteieintrag und zum Überprüfen, ob der Drittparteieintrag bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einem Drittparteieintrag. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte der erstellten und ignorierten Plugins festzulegen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

Die TenableSCPluginsImportProcessor-Skripteinbindung wird aus dem onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe der Tenable.sc-Plugin-Integration und wandelt sie in ServiceNow-Schwachstelleneinträge von Drittparteien um. Alle Änderungen an dieser Skripteinbindung können die Umwandlung von Tenable.sc-Plugin-Daten in der Drittpartei-Eintragstabelle ändern.

## Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung für Tenable.sc Open Vulnerabilities wird verwendet, um importierte Daten aus der Integration von Tenable.sc Open Vulnerabilities zu transformieren, und die Transformationszuordnung für Tenable.sc und feste Schwachstellen wird verwendet, um importierte Daten aus der Integration von Tenable.sc für feste Schwachstellen zu transformieren.

**Hinweis:**
Änderungen an diesen Transformationszuordnungen ändern, wie Daten aus dem Import von festen/offenen Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen für offene und feste Schwachstellen von Tenable.sc zuzugreifen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationsinstanzen** > **Tenable.sc – Integration von festen/offenen Schwachstellen** > **Datenquellen** > **Offene/behobene Schwachstellen von Tenable.sc** > **Transformationen**.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_pluginID | ID | Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_riskfactor | source_severity | Dieses Feld ist „source_severity“ im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_severity | Priorität | Das Prioritätsfeld wird dem Schweregrad zugeordnet. Der Standardwert ist 5. |
| u_hasbeenmitigated | Status | „Wurde verringert“ wird dem Statusfeld des Schwachstellendatensatzes zugeordnet. Bei der Integration behobener Schwachstellen befinden sich alle AEs im Status „Geschlossen“. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| u_ip | ip_address | Die IP-Adresse wird dem Host-IP-Feld der Tabelle „cmdb_ci“ zugeordnet. |
| u_port | port | Der Port wird dem Feld „Port“ des Datensatzes für angreifbare Elemente zugeordnet. |
| u_protocol | protocol | Das Protokoll wird dem Port-Feld des Datensatzes für angreifbare Elemente zugeordnet. |
| u_firstSeen | first_found | Der erste gefundene Wert wird dem ersten gefundenen Feld des VI-Datensatzes zugeordnet. |
| u_lastSeen | last_found | Der zuletzt angezeigte Wert wird dem zuletzt gefundenen Feld des VI-Datensatzes zugeordnet. |
| u_exploitVerfügbar | Exploit | ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_synosis | Bedrohung | Die Synopse wird dem Bedrohungsfeld im Datensatz des Drittpartei-Eintrags zugeordnet. |
| u_description | Zusammenfassung | Die Beschreibung wird dem Zusammenfassungsfeld im Datensatz „Drittpartei-Eintrag“ zugeordnet. |
| u_solution | Lösung | Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_basescore | Punktzahl | BaseScore wird dem Punktzahlfeld im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_temporalScore | temporal_score | Die temporäre Punktzahl wird der temporären Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet. |
| u_cvssv3basescore | v3_base_score | Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | Eintragsdatensatz zugeordnet. |
| u_cvsstemporalscore | v3_temporal_score | Cvssv3temporal score wird der zeitlichen v3-Punktzahl im Datensatz des Drittparteieintrags zugeordnet. |
| u_pluginpubdate | date_published | Das Plugin-Veröffentlichungsdatum wird dem Plugin-Veröffentlichungsdatum im Datensatz des Drittanbietereintrags zugeordnet. |
| u_pluginmoddate | last_modified | Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Datensatz des Drittanbietereintrags zugeordnet. |
| u_dnsname | fqdn | DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_macaddress | mac_address | MacAddress wird dem Feld mac_address des cmdb_ci-Datensatzes zugeordnet. |
| u_netBIOSName | NetBIOS | NetBIOSName wird dem NETBIOS-Feld des cmdb_ci-Datensatzes zugeordnet. |
| u_ip | ip | IP wird dem IP-Feld des cmdb_ci-Datensatzes zugeordnet. |
| hostUniqueness | uuid | Die Eindeutigkeit des Hosts wird keinem Feld zugeordnet, sondern verwendet, um die UUID für den Host zu bestimmen. |
| u_familie | Kategorie | Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu. |
| u_plugintext | Nachweis | Plugin-Text wird dem Nachweis im TPE-Datensatz zugeordnet. |
| [Skript] | Quelle | Die Quelle der Integration wird ausgefüllt. Die aus dieser Integration erstellten |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | angreifbaren Elemente haben Tenable.sc als Quelle. |
| [Skript] | integration_instance | integration_instance ist der Name der Instanz, aus der das angreifbare Element importiert wird. |
| u_vpr_score | source_risk_score | Ordnet die VPR-Punktzahl vom Scanner der Quellrisikopunktzahl in der Drittpartei-Eintragstabelle zu. |
| [Skript] | source_risk_rating | Ordnet die VPR-Punktzahl der Standardrisikobewertung basierend auf den Punktzahlbereichen zu:<br>• 9 – 10 – Kritisch<br>• 7 – 9 – Hoch<br>• 4 – 7 – Mittel<br>• 0–4: Niedrig |
| u_vpr_context[id=age_of_vuln] | „age_of_vuln“ | Ordnet das Alter der Schwachstelle vom Scanner „age_of_vuln“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = exploit_code_maturity] | Exploit_code_maturity | Ordnet die Reife des Exploit-Codes vom Scanner „ploit_code_maturity“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = product_coverage] | product_coverage | Ordnet die Produktabdeckung vom Scanner „product_coverage“ in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = ”threat_sources_last_28] | Bedrohungsquellen | Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner „thread_sources“ in der Drittparteitabelle zu. |
| u_vpr_context [id = ”threat_intensity_last_28] | Bedrohungsintensität | Ordnet die Bedrohungsintensität in den letzten 28 Tagen vom Scanner zu Threat_Intensity |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Zielfeld | Beschreibung |
|---|---|---|
| | | in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = „threat_recency“] | Threat_recency | Ordnet die Bedrohungsaktualitätsinformationen vom Scanner Threat_recency in der Drittpartei-Eintragstabelle zu. |
| u_vpr_context [id = cvssV3_impactScore] | v3_impact_subscore | Ordnet die CVSS v3-Auswirkungspunktzahl des Scanners v3_impact_subscore in der Drittpartei-Eintragstabelle zu. |
| u_pluginname | Name | Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu. |
| u_stigseverity | stig_severity | Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Drittpartei-Eintragstabelle zu. |
| u_checktype | check_type | Ordnet den Prüfungstyp check_type in der Drittpartei-Eintragstabelle zu. |
| u_familie.id | familie_id | Ordnet das Plugin „family.id“ „family_id“ in der Drittpartei-Eintragstabelle zu. |
| [Skript] | Exploit_Attack_Vector | Die Spalte „plot_attack_vector“ in der Tabelle „dritter_party_entry“ wird basierend auf „ploit_available“ und „v3_attack_vector“ der Spalten ausgefüllt. |

| Quellenfeld | Beschreibung |
|---|---|
| u_cve | Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung befindet sich in sn_vul_m2m_entry_cve. |
| u_BID | Die Liste der Fehlerverfolgungen wird als Referenz hinzugefügt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Quellenfeld | Beschreibung |
|---|---|
| u_cpe | Die Liste der CPEs wird als Referenz hinzugefügt. |
| u_seealso | Die Liste der URLs wird als Referenz hinzugefügt. |
| u_xrefs | Die Liste der X-REFs wird als Referenz hinzugefügt. |
| u_exploitframeworks | Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das entsprechende Exploit-Framework und Plugin zu sn_vul_m2m_framework_vul ein. |

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführungszeiten und der Zweck der einzelnen Skripts aufgelistet.

| Wann das Skript ausgeführt wird | Zweck |
|---|---|
| onStart (wenn die Transformation eines Importsatzes gestartet wurde) | Diese Transformation wird verwendet, um die Werte in import_set für den Integrationsprozess zu initialisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onBefore (bevor die Transformation eines Importsatzes abgeschlossen ist). | Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle bereits vorhanden ist. Basierend auf den Ergebnissen ändert die Werte in einer Tabelle mit angreifbaren Elementen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |
| onComplete (wenn die Transformation eines Importsatzes abgeschlossen ist). | Diese Transformation wird verwendet, um die Werte von neu erstellten AEs und AEs festzulegen, die aktualisiert und ignoriert wurden. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen. |

### Legen Sie zusätzliche Filterparameter für Tenable.io Importe fest

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit Tenable Vulnerability Integration an, um die mit dem Produkt Tenable.io importierten Schwachstellendaten weiter zu verfeinern.

#### Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach `cidr_range`, `num_assets`, `indexed_at`und `plugin_family`gefiltert werden. Angenommen, Sie möchten eine Tenable.io -Integration so ausführen, dass eine Ausführung nur kritische Schwachstellen alle vier Stunden importiert und eine andere alle 24 Stunden ausführt, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um die Erfassung dieser Daten zu erleichtern, können Sie von Tenable unterstützte Parameter hinzufügen, um die spezifischen Schwachstellendetails zu importieren, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in Ihrem Now Platformanpassen. Die folgenden Tenable.io -Integrationen unterstützen die Filterung durch Bereitstellung von JSON-Inhalten im Anforderungstext:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Assets-Integration
- Integration behobener Schwachstellen
- Integration offener Schwachstellen

Sie sollten wissen, wie JSON Zeichenfolgen für diese Funktion verwendet werden.

Erforderliche Rolle: sn_vul.vulnerability_admin

### Prozedur

1. Suchen Sie die vom Produkt Tenable.io unterstützten Parameter auf der Entwickler-Website, die Sie zum Filtern verwenden möchten.

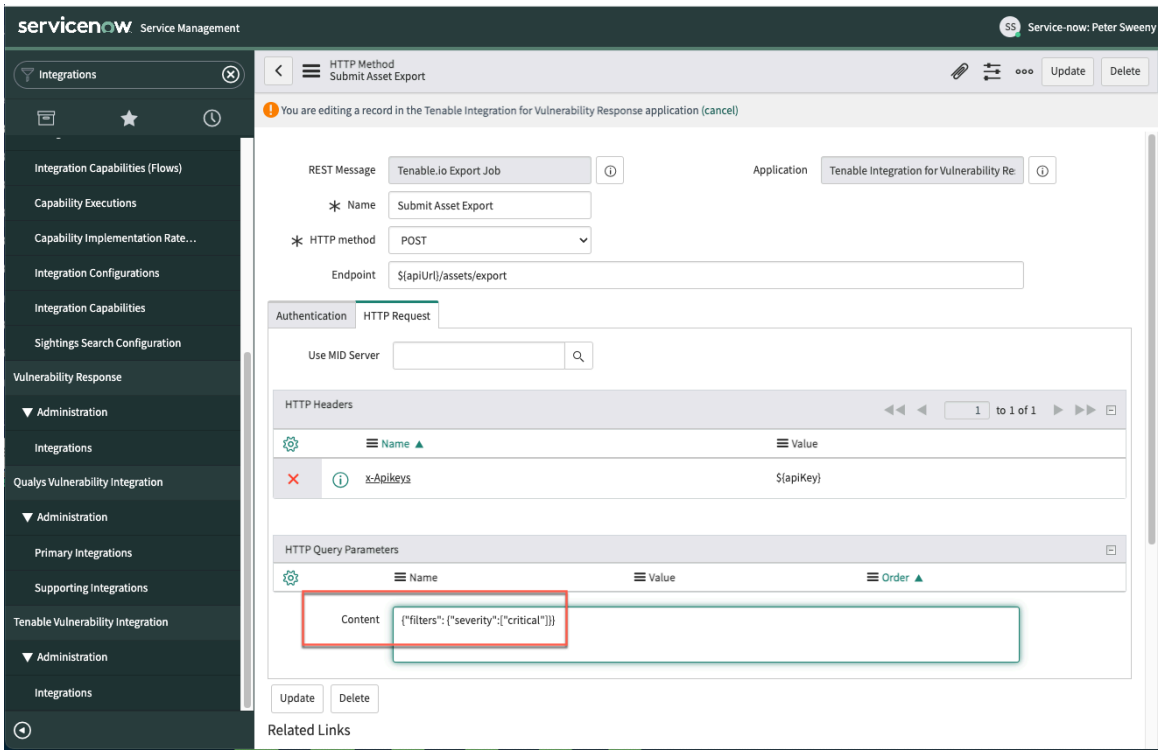
   Parameter und Werte, die Sie aus dem Produkt Tenable.io eingeben, werden nur auf der Ebene der Integrationsinstanz unterstützt.

2. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
3. Klicken Sie auf der Listenseite Tenable Integrations auf den Datensatz für die Tenable.io -Integration, die Sie öffnen möchten.
4. Klicken Sie bei ausgewählter Registerkarte Vertretbare REST-Methoden auf das Informationssymbol (I) für die REST-Methode, gefolgt von **Datensatz öffnen**.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in. Um den Datensatz zu bearbeiten, klicken Sie **hier**.
7. Geben Sie im Datensatz „REST-Methode“ im Feld Inhalt den JSON-Inhalt ein, den Sie als Teil des Anforderungstexts verwenden möchten.

   In der folgenden Abbildung wurde beispielsweise der Schweregradparameter für importierte Schwachstellen `{"filters": {"severity": ["critical"]}}` [] für die Asset-Integration von Tenable.io angepasst . Dieser Wert importiert nur kritische Schwachstellen (CVSS-Punktzahl 10,0).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie in der Dokumentation Tenable.io weitere Informationen zum Trennen der einzelnen Werte.

8. Klicken Sie auf **Aktualisieren**.

### Tenable Vulnerability Integration-Berichterstellung

Zeigen Sie Berichte über Schwachstellen und angreifbare Elemente in den Vulnerability Response -Dashboards an.

## Datenvisualisierungen in den Vulnerability Response -Arbeitsbereichen

Die Vulnerability Response -Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie den Fortschritt der -Korrektur überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation in dynamischen Datenvisualisierungen wichtig sind, die aktualisiert werden, wenn sich die Schwachstellendaten ändern. Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen finden Sie unter Vulnerability Response Arbeitsbereiche, Vulnerability Manager Workspace erkunden und IT Remediation Workspace erkunden.

## Vorherige Versionen von Vulnerability Response

Das Übersichts-Dashboard von Vulnerability Response (Vulnerability Management) bietet einen Überblick über Schwachstellen und angreifbare Elemente und hilft dem Schwachstellenadministrator, Problembereiche schnell zu erkennen. Das Vulnerability Response-Korrektur-Dashboard (Schwachstellenkorrektur) ermöglicht es einem Korrekturspezialisten, sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren, die er besitzt.

Weitere Informationen finden Sie unter Standardmäßige Dashboards Vulnerability Response werden verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Korrekturbesitzer.

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um das Dashboard anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Korrekturübersicht**.

### Statusdiagramm der Integrationsausführung für die Tenable Vulnerability-Integration

Das Modul Tenable Integration Run Status bietet Ihnen eine grafische Ansicht des Status von Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein beliebiges Teil im Balkendiagramm klicken, wird eine Liste mit detaillierteren Informationen geöffnet.

Erforderliche Rolle: Schwachstellenadministrator

Persona-Rollen und granulare Rollen sind verfügbar, um Sie bei der Verwaltung der Aktionen zu unterstützen, die Benutzer in der Anwendung Vulnerability Response ausführen und anzeigen können. Informationen zur erstmaligen Zuweisung von Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie die Persona-Rollen Vulnerability Response mit dem Setup-Assistenten zu.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Personas und granulare Rollen für Vulnerability Response.

Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Vertretbare Schwachstellenintegration** > **Status der Integrationsausführung**.

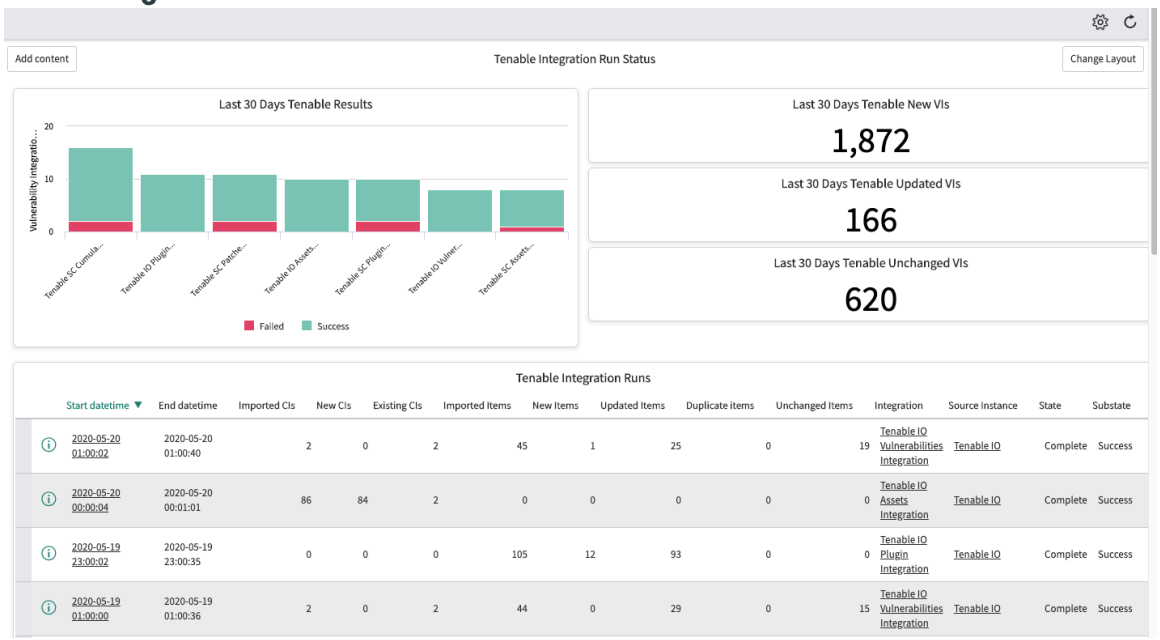
Ab Version 19.0 von Vulnerability Responseist dieses Dashboard in der New Experience-UI verfügbar.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausführungsstatus




## Berichte über den Ausführungsstatus der Tenable-Integration

| Name | Beschreibung |
|---|---|
| Tenable-Ergebnisse der letzten 30 Tage | Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt erfolgreiche und fehlgeschlagene Ausführungen an. Jede Ausführung wird im Diagramm als Balken angezeigt. |
| Neue Tenable-VIs der letzten 30 Tage | Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Aktualisierte Tenable-VIs der letzten 30 Tage | Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Nicht geänderte Tenable-VIs der letzten 30 Tage | Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt. |
| Tenable-Integrationsausführung | Die Datensätze der Integrationsausführung werden in einer Liste angezeigt.<br><br>**Hinweis:**<br>**V16.1:** Um Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit den Erkennungsdaten ServiceNow in der Tabelle `sn_vul_detection`.<br><br>Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennungen oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „Anzahl bis heute“ in der Instanz nach Abschluss der Integrationsausführung an. |

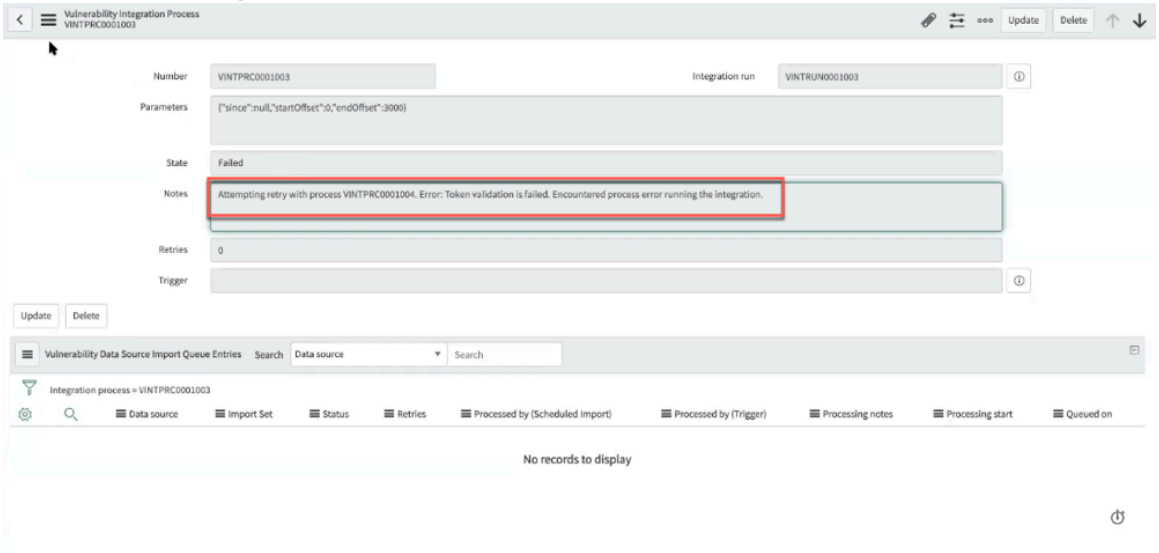


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ablauf der Tokenvalidierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und eine Nachricht wird im Datensatz des Integrationsprozesses für Schwachstellen angezeigt.

**Nachricht über abgelaufenes Token**




Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle fehlgeschlagenen und erfolgreichen Integrationsprozesse werden auf der Registerkarte „Schwachstellenintegrationsprozess“ im Datensatz „Schwachstellenintegrationsprozess“ angezeigt.

### Initiieren Sie einen erneuten Scan für die Tenable.sc -Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen geplanten Scan-Zyklen korrigiert wurden, indem Sie erneute Scans in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Tenable.sc aus Ihrer Instanz von Now Platform® initiieren.

#### Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

**Hinweis:**
Tenable.sc unterstützt das erneute Scannen auf Agent-basierten Computern nicht.

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

#### Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Initiieren eines erneuten Scans aus den Arbeitsbereichen finden Sie unter Scannen Sie Tenable.io und Tenable.sc angreifbare Elemente aus den Vulnerability Response -Arbeitsbereichen erneut.

Befolgen Sie die unten aufgeführten Schritte, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten oder Schwachstellenmanager bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselemente) in ihren Umgebungen initiieren. Sie können erneute Scans von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbaren Elementen (AEs), Korrekturaufgaben (RTs), Drittanbietereinträgen (TPE) oder Datensätzen erkannter Elemente aus Ihrer Now Platform -Instanz initiieren.

Mit erneuten Scans können Ihre Korrekturbesitzer und Schwachstellenanalysten überprüfen, ob durch Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Beispiel: Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde, erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformTenable.sc auf angreifbare Elemente von [] initiieren.

**Hinweis:**
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen von Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.sc Scan Credential Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.sc -Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen wird automatisch im Setup-Assistenten in Ihrer Instanz aktiviert (Aktiv), wenn Sie die Integrationen von Tenable.sc Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen) konfigurieren.

Notieren Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf in Ihrer Now Platform -Instanz anzeigen können:

- Mit der Administratorbenutzerrolle Tenable.sc erstellte Anmeldeinformationen stehen Benutzern in allen Ihren Organisationen zur Verfügung.
- Mit der Benutzerrolle der Organisation Tenable.sc erstellte Anmeldeinformationen sind nur für Benutzer innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in Now Platform importiert, es sei denn, sie werden mit dem Konto des Benutzers geteilt, der für die Verbindung mit der Instanz verwendet wird.

Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.sc.

Weitere Informationen zum Konfigurieren der Anwendung Tenable.scKonfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-Assistenten finden Sie unter []. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Vertretbare Schwachstellenintegration** > **Integrationen** > **Tenable.sc-Integration von Scan-Anmeldeinformationen**.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats)



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   **Hinweis:**
   Sie können erneute Scans nur für AEs mit Tenable.sc als Quelle initiieren. Vergewissern Sie sich, dass Tenable.sc in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle nicht in der VI-Listenansicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol „ **Liste personalisieren** “ (Zahnradsymbol), und verwenden Sie den Slushbucket, um **Quelle** von **Verfügbar** zu **Ausgewählt**zu verschieben.

3. Navigieren Sie alternativ zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Korrekturaufgabe bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss die VI aus dem Produkt Tenable.sc stammen und sich in einem anderen Status als **Geschlossen**befinden. Für mehrere VI-Datensätze müssen alle VIs aus dem Tenable.sc-Produkt stammen und sich in einem anderen Status als **Geschlossen**befinden.
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als **Geschlossen**befinden, und alle zugehörigen AEs müssen aus dem Produkt Tenable.sc stammen.
   - In einem TPE-Datensatz muss mindestens ein zugeordneter VI-Datensatz aus dem Produkt Tenable.sc einen anderen Status als **Geschlossen**aufweisen.

4. Klicken Sie oben rechts im Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Scanner-Anmeldeinformationen für den Zugriff auf den Scanner auszuwählen. Dies sind die Anmeldeinformationen, die von der Tenable.sc Scan Credential Integration importiert werden.
5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie **auf Scan anfordern**.

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Details** anzeigen, um den Status des erneuten Scans anzuzeigen und alle anderen erneuten Scans anzuzeigen, die von einem bestimmten Datensatz aus gestartet wurden.

   Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Die untergeordneten Scans importieren Daten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

   Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt. Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens. Alle VIs, die in den Status „ **Geschlossen/** Behoben“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.sc-Integration mit festen Schwachstellen importiert.

### Initiieren Sie einen erneuten Scan für die Tenable.io -Integration

Vergewissern Sie sich, dass Ihre angreifbaren Elemente zwischen den geplanten Scan-Zyklen korrigiert wurden, indem Sie erneute Scans in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für das Produkt Tenable.io aus Ihrer Instanz von Now Platform® initiieren.

#### Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Stellen Sie sicher, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**.

#### Warum und wann dieser Vorgang ausgeführt wird

- Informationen zum Initiieren eines erneuten Scans in den Vulnerability Response-Arbeitsbereichen finden Sie unter und Scannen Sie Datensätze und Korrekturaufgaben im Arbeitsbereich des Schwachstellenmanagers erneut und Scannen Sie angreifbare Elemente und Korrekturaufgaben im erneut IT Remediation Workspace.
- Befolgen Sie die unten aufgeführten Schritte, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

**Hinweis:**
Tenable.io unterstützt das erneute Scannen auf Agent-basierten Computern nicht.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Korrekturbesitzer, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. können Sie nach bestimmten Schwachstellen in Assets (Konfigurationselementen) in Ihren Umgebungen suchen. Sie können erneute Scans aus Datensätzen für angreifbare Elemente (AEs), Korrekturaufgaben (VUL), Drittanbietereinträgen (TPE) oder erkannten Elementen (SDI) aus Ihrer Now Platform -Instanz initiieren. Mit erneuten Scans können Sie überprüfen, ob mit Ihren Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn Sie einen erneuten Scan von Ihrer Instanz Now Platform® anfordern, ist die Auswahl der Anmeldeinformationen von Vulnerability Response Integration with Tenable optional. Die ServiceNow® Tenable.io Scan Credential Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.io -Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Die folgenden Informationen beschreiben die Anmeldeinformationen, die Sie importieren, damit Ihre Benutzer sie bei Bedarf in Ihrer Now Platform -Instanz anzeigen können:

- Mit der Administratorbenutzerrolle Tenable.io erstellte Anmeldeinformationen stehen Benutzern in allen Ihren Organisationen zur Verfügung.
- Mit der Benutzerrolle der Organisation Tenable.io erstellte Anmeldeinformationen sind nur für Benutzer innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden für Benutzer außerhalb der Organisation des Erstellers nicht in Now Platform importiert, es sei denn, sie werden mit dem Konto des Benutzers geteilt, der für die Verbindung mit der Instanz verwendet wird.

  Weitere Informationen finden Sie auf der Dokumentationswebsite Tenable.io.

- Die Tenable.io Template Integration und die Tenable.io Scan Credential Integration müssen vor dem Initiieren von erneuten Scans aktiviert werden. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Vertretbare Schwachstellenintegration** > **Integrationen** > **Tenable.io-Integration von Scan-Anmeldeinformationen**.

  Standardmäßig sind die Integrationen von Vorlagen und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für Tenable.ioeingeben, werden alle Tenable.io -Integrationen automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
  2. Suchen Sie in der angezeigten Liste die gewünschten Tenable.io Integrationsdatensätze.
  3. Öffnen Sie jeden Datensatz, und aktivieren Sie das Kontrollkästchen **Aktiv**, um die Integration zu aktivieren.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit der Konfiguration für Tenable Vulnerability Integration mit Vulnerability Responsefortzufahren.

Weitere Informationen zum Konfigurieren der Produkte Konfigurieren Sie die Integration von Tenable Vulnerability mit dem Setup-AssistentenTenable.io und Tenable.sc finden Sie unter [].

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, Sie haben jedoch gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass die Schwachstelle behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle, die während eines früheren Scans erkannt wurde,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erfolgreich behoben hat, können Sie einen gezielten erneuten Scan von Now PlatformTenable.io auf angreifbare Elemente von [] initiieren.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von festen Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten in Seiten enthalten. Diese Einträge müssen die Daten innerhalb der einstündigen Frist verarbeiten. Wenn die Nutzlast jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Zeitüberschreitungsfehler bei der Integration führt. Die Integration verarbeitet die Daten trotz der Zeitüberschreitung weiter. Um diese Fehlkommunikation zu vermeiden, werden ab Version 18.2.4 von Vulnerability Responseregelmäßig Zeitstempel (Heartbeats) gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Das Feld **Zuletzt verarbeiteter Datensatz** auf der Seite „Eintrag der Importwarteschlange“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag das Zeitlimit von einer Stunde überschreitet, überprüft das System das Feld **Zuletzt verarbeiteter Datensatz**, um festzustellen, ob er auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag hängen bleibt und eine Zeitüberschreitung vorliegt, um weitere Verzögerungen bei der Verarbeitung zu verhindern.

**Hinweis:**
Das Feld **Zuletzt verarbeiteter Datensatz** wird basierend auf der Definition in den folgenden Systemeigenschaften aktualisiert:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Takt (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag überschritten werden muss.

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**.
2. Suchen Sie den Datensatz des angreifbaren Elements, für den Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   **Hinweis:**
   Wenn Sie den Scanner Tenable.io verwenden, können Sie erneute Scans für VIs nur mit Tenable.io als Quelle initiieren. Vergewissern Sie sich, dass Tenable.io in der Spalte „ **Quelle** “ in den VI-Listenansichten oder in den Feldern „ **Quelle** “ in einzelnen Datensätzen angezeigt wird. Sie können den Bedingungsgenerator verwenden, um AEs nach Quelle zu gruppieren. Oder, wenn die Spalte Quelle nicht in der VI-Listenansicht angezeigt wird, klicken Sie oben links in der Liste auf das Symbol „ **Liste personalisieren** “ (Zahnradsymbol), und verwenden Sie den Slushbucket, um **Quelle** von **Verfügbar** zu **Ausgewählt**zu verschieben.

3. Navigieren Sie alternativ zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl ist die **Schaltfläche Erneut scannen** für die folgenden Datensätze verfügbar:



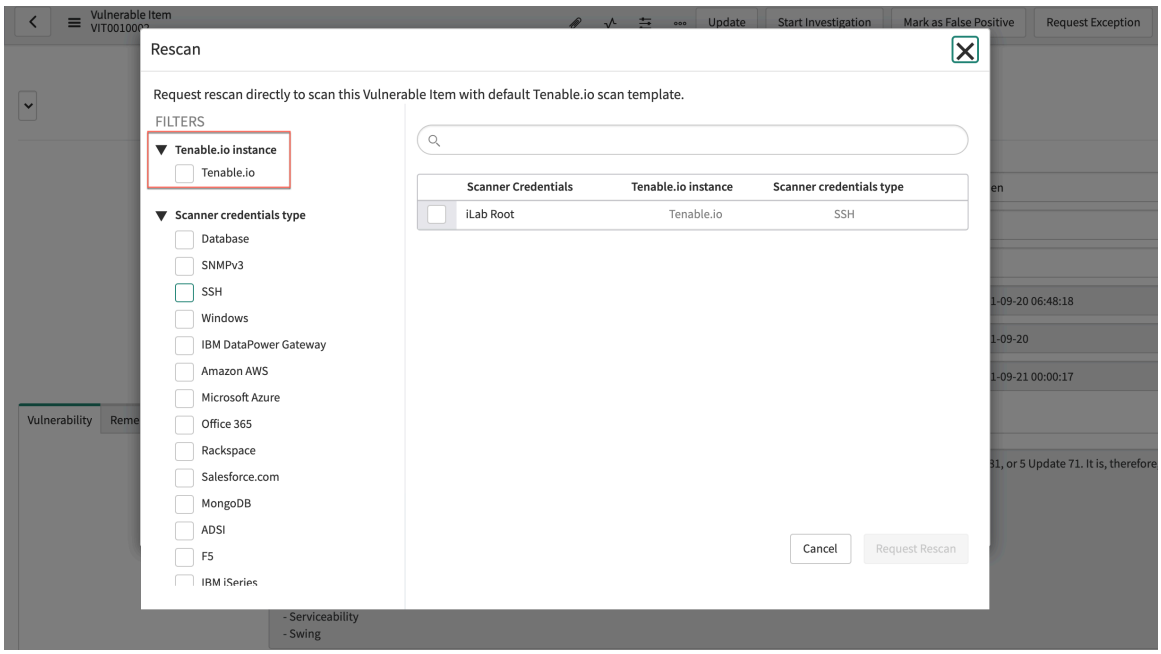
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In einem einzelnen VI-Datensatz muss sich die VI in einem anderen Status als **Geschlossen**befinden. Für mehrere VI-Datensätze müssen alle VIs aus dem Produkt Tenable.io stammen und sich in einem anderen Status als **Geschlossen**befinden.
- Für Korrekturaufgabendatensätze werden nur Korrekturaufgaben in einem anderen Status als **„Geschlossen"** unterstützt. Alle zugeordneten AEs müssen sich in einem anderen Status als „ **Geschlossen** " befinden und Tenable.io als Quelle verwenden.
- In einem TPE-Datensatz muss mindestens ein zugeordneter VI-Datensatz aus dem Produkt Tenable.io einen anderen Status als **Geschlossen**aufweisen.
- Bei Datensätzen für erkannte Elemente muss der Datensatz mindestens einen zugeordneten VI-Datensatz aus dem Produkt Tenable.io in einem anderen Status als **Geschlossen**haben.
- In der Liste „Angreifbare Elemente" können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen links unten auf dem Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz auf **Erneut scannen**.
   Sie werden aufgefordert, die Instanz(en) für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind die, die von der Tenable.io Scan Credential Integration importiert wurden.

5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   In der folgenden Abbildung wird eine Integrationsinstanz, Tenable.io, angezeigt. Wenn Sie mehr als eine Instanz Tenable.io haben, werden sie alle im Abschnitt Tenable.io im Formular angezeigt.




6. Klicken Sie **auf Erneutes Scannen anfordern**.

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird, und ein übergeordneter Scan-Datensatz wird erstellt. Der Status für alle untergeordneten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgaben-,



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Details** anzeigen, um den Status des erneuten Scans anzuzeigen und alle anderen erneuten Scans anzuzeigen, die von einem bestimmten Datensatz aus gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Die untergeordneten Scans importieren Daten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden mehrere untergeordnete Scans in einem übergeordneten Scan-Datensatz angezeigt. Zum Beispiel beträgt die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, 1000. Wenn 1002 IPs für ein angreifbares Element vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

Ihre Instanz Now Platform® verfolgt den Status des erneuten Scannens bis zum erfolgreichen Abschluss oder bis zum Ablauf des festgelegten Nachverfolgungszeitraums, je nachdem, was zuerst eintritt. Die Zeitüberschreitung stoppt den Scan nicht. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, zu dem Now Platform® die Nachverfolgung Ihres Status des erneuten Scannens beendet hat, nicht auf das Ende des tatsächlichen erneuten Scannens. Alle VIs, die in den Status „ **Geschlossen/** Behoben“ überführt wurden oder werden, werden mit dem nächsten geplanten Import der Tenable.io Integration behobener Schwachstellen importiert.

Bei Scans, bei denen ein Fehler auftritt, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

Sie können aktualisierte Ergebnisse für die Datensätze anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von festen Schwachstellen initiiert haben.

### Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartitionsbezeichner für den Tenable Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (CIs) für Assets in Ihrer Umgebung, die IP-Adressen gemeinsam nutzen. Identifizieren Sie die unterschiedlichen Assets in Ihrer Umgebung, und aktualisieren Sie automatisch die CIs für Ihr vorhandenes erkanntes Element, angreifbares Element und Ihre Erkennungsdatensätze, um weitere Details zu Ihren Schwachstellen zu erhalten.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Sie Assets in der Anwendung Vulnerability Response anhand der IP-Adresse identifizieren. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, sie werden jedoch als ein CI in Ihrer CMDB gespeichert.

Beispielsweise können, wie in den folgenden Tabellen gezeigt, mehrere Assets (CIs) in Ihrer Umgebung IP-Adressen gemeinsam nutzen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch während der IP-Adresssuche als einzelnes CI (CI 1) identifiziert und gespeichert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Standardmäßige IP-Suche und CI-Erstellung**

| Quelle | IP-Adresse | Netzwerk-ID | Konfigurationselement |
|---|---|---|---|
| Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 |

| Quelle | IP-Adresse | Repository_id | Konfigurationselement |
|---|---|---|---|
| Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 |

Sie können einzelne CIs für Assets erstellen, die dieselbe IP-Adresse haben, damit Sie sie als unterschiedliche Assets identifizieren können. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartitionsbezeichners [network_partition_identifier], indem Sie die regelmäßige Aufgabe *`Update existing discovered items with network partition identifier`*ausführen.

Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese regelmäßige Aufgabe aktiviert ist, fügt sie den Netzwerkpartitionsbezeichner [network_partition_identifier] vorhandenen CI-Datensätzen aus importierten Daten hinzu. Vorhandene von der IRE erstellte CIs werden ebenfalls aktualisiert. Die regelmäßige Aufgabe erstellt ab dem nächsten Import auch CIs, die den Netzwerkpartitionsbezeichner enthalten. Alternativ können Sie die Aufgabe bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

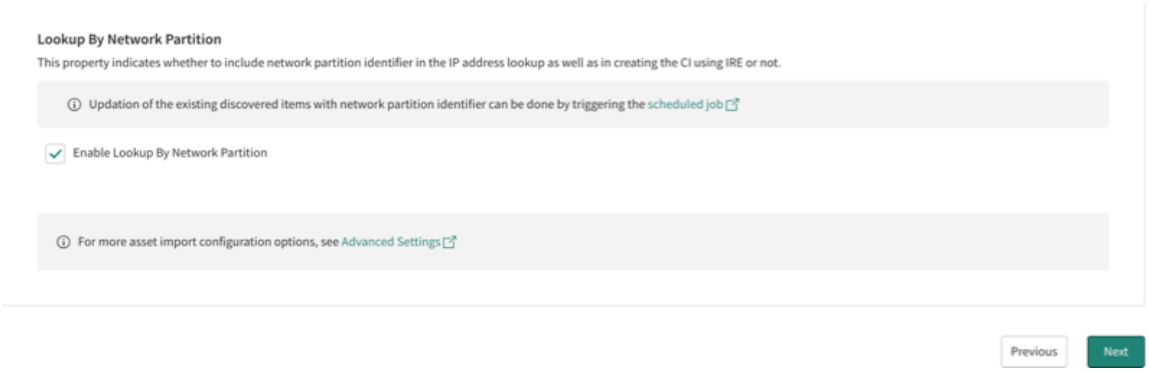
Wenn Sie ein Upgrade ab Version 14.0 von Vulnerability Response und Version 2.2 von Tenable Vulnerability Integration durchführen, wird CMDB CI Class Models (1.0.21.) unterstützt. Die Klassenmodelle haben den Netzwerkpartitionsbezeichner [network_partition_identifier] in den Identifizierungsregeln von Identification and Reconciliation (IRE).

### Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**.
2. Wählen Sie Tenable.io Integrationen oder Tenable.sc Integrationen aus.
3. **Bearbeiten Sie** die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Checkbox aus dem **Suche nach Netzwerkpartition aktivieren** Abschnitt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Klicken Sie auf **Next (Weiter)**.

Die Netzwerkpartitionsbezeichner NETWORK_ID und REPOSITORY _ID sind enthalten und aktualisieren vorhandene CIs oder erstellen CIs mit der nächsten geplanten Aufgabe.

**Attribut für Netzwerkpartitionsbezeichner, das in die IP-Suche und CI-Erstellung einbezogen wird**

| Quelle | IP-Adresse | NETWORK_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Tenable.io: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 03712 | CI 1 | CI 1 |
| | 123.12.12.141 | 03713 | CI 1 | CI 2 |

| Quelle | IP-Adresse | REPOSITORY_ID | CI für Assets ohne Netzwerkpartitions | CIs-Assets mit Netzwerkpartitions |
|---|---|---|---|---|
| Tenable.sc: Integrationen von Assets und festen und offenen Schwachstellen | 123.12.12.141 | 12 | CI 1 | CI 1 |
| | 123.12.12.141 | 13 | CI 1 | CI 2 |

Mit der nächsten geplanten Aufgabe beziehen die Suchregeln für IP-Adresse und unvollständige IP-Adressen-CI-Identifizierung das Attribut „Netzwerkpartitionsbezeichner“ automatisch für einen Datenimport aus den Integrationen von Assets und festen und offenen Schwachstellen für die Produkte Tenable.io und Tenable.sc ein.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartitionsbezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

### Importieren Sie Änderungen für die Integration von Tenable Vulnerability

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration von Tenable-Schwachstellen in der ServiceNow® Integration von Tenable-Schwachstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Aufgabensatz erfordert Codierung und fortgeschrittene Kenntnisse über Now Platform.

Befolgen Sie diese Schritte, um domänengetrennte Importe für die Integrationen von Tenable Vulnerabilities zu erstellen. Das folgende Beispiel bezieht sich auf die Tenable.io Open Vulnerabilities-Integration, aber dieser Inhalt gilt auch für die anderen Tenable-Integrationen.

### Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede Domäne, die Sie erstellen, einen Benutzer, und weisen Sie den Benutzer dieser Domäne zu.

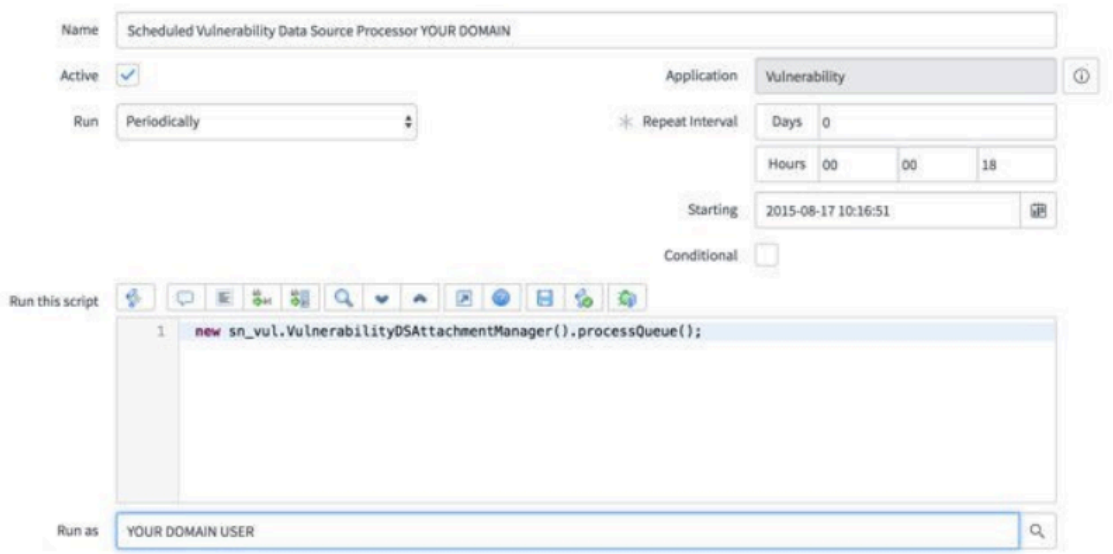
   Stellen Sie sich diesen Benutzer als run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration offener Schwachstellen
   Der Benutzer entspricht dem VR.System-Benutzer in der globalen Domäne und muss die folgenden Rollen haben: sn_vul.tenable_configure_integration, import_admin und sn_vul.vulnerability_write. Dieser Benutzer benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   **Hinweis:**
   Betrachten Sie diesen Benutzer als spezifisch für diese Rolle. Der Benutzer sollte keinen anderen Zweck haben
4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den Datenquellenprozessor für geplante Schwachstellen kopieren, der sich unter befindet **Systemdefinition** > **Geplante Aufgaben**.
5. Hängen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Benutzer run_as in den Benutzer, den Sie im vorherigen Schritt erstellt haben.

   **Hinweis:**
   Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




7. Bearbeiten Sie die UI-Aktion Jetzt ausführen in der Tenable.io Open Vulnerabilities-Integration, um diesen Codeblock am Anfang der Datei hinzuzufügen.
   `//sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }`

   **Hinweis:**
   Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Benutzerdomäne „run_as“ ausgeführt wird.

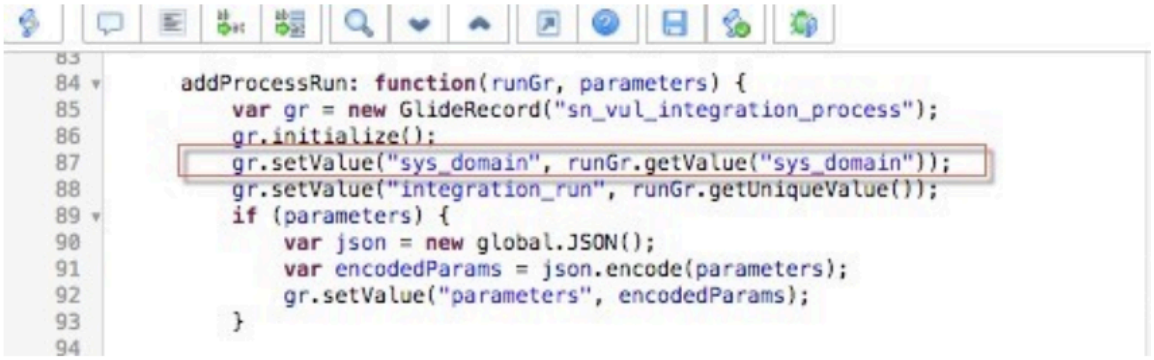
8. Bearbeiten Sie die VulnerabilityIntegrationUtils-Skripteinbindungsmethode addIntegrationRun, um den hervorgehobenen Code hinzuzufügen.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Bearbeiten Sie die VulnerabilityIntegrationUtils-Skripteinbindungsmethode addProcessRun, um den hervorgehobenen Code hinzuzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um den ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in Bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die VulnerabilityDSAttachmentManager-Skripteinbindungsmethode queueItem, um die folgenden hervorgehobenen Codeblöcke hinzuzufügen queueItem, _getNext, _processQueueEntry-Funktion.

Sie sind bereit für domänengetrennte Hosterkennungsimporte.

Deaktivieren Sie Rechner vor dem Import

Befolgen Sie diese Schritte, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellenrechner verwenden, deaktivieren Sie am besten die Standardrechner zusätzlich zu den anderen, die Sie definiert haben. Schwachstellenrechner werden bei jedem Zugriff auf einen Datensatz eines angreifbaren Elements ausgeführt und können sich auf die Instanzleistung auswirken.

Erforderliche Rolle: sn_vul.vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Sicherheitsrisiko-Rechner**.
13. Öffnen Sie die Gruppe Schwachstellenauswirkung.
14. Öffnen Sie den Rechner für Punktzahl und servicebasierte Auswirkung.
15. Deaktivieren Sie das Feld Aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie vor dem ersten Import benachrichtigungsbasierte Business Rules

Befolgen Sie diese Schritte, um Benachrichtigungsbezogene Geschäftsregeln deaktivieren vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Business Rules viele Benachrichtigungen generieren, was sich auf die Leistung auswirkt. Diese Geschäftsregeln müssen geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**.
18. Suchen Sie nach Benachrichtigungen über betroffene CIs.
19. Öffnen Sie die Geschäftsregel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie dieses Verfahren für die folgenden Geschäftsregeln:
    - Betroffene Kostenstellenbenachrichtigungen
    - Betroffene Gruppenbenachrichtigungen
    - Betroffene Standortbenachrichtigungen

**Hinweis:**
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Geschäftsregeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und die Leistung Ihrer Instanz beeinträchtigen.

Ändern Sie ein anfängliches Startdatum

Befolgen Sie diese Schritte, um ein anfängliches Startdatum zu ändern. Während der Installation mit dem Setup-Assistenten legen Sie ein anfängliches Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Vertretbare Schwachstellenintegration** > **Administration** > **Integrationen**.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle gescannten und erkannten Schwachstellen seit diesem Zeitpunkt erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, ist das Feld Startzeit vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass eine große Datenmenge die Ratenbeschränkungen der Tenable-API überschreitet und Ausführungszeitüberschreitungen auslöst.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie auf **Jetzt** ausführen, um den Vorgang sofort auszuführen.

## Configuration Compliance Fehlerkorrektur

Configuration Compliance Die Fehlerkorrektur ist in erster Linie ein manueller Prozess, der durch geplante Aufgaben (Integrationen), Testergebnisgruppenaufgaben, Workflows und Change-Anforderungen ergänzt wird.

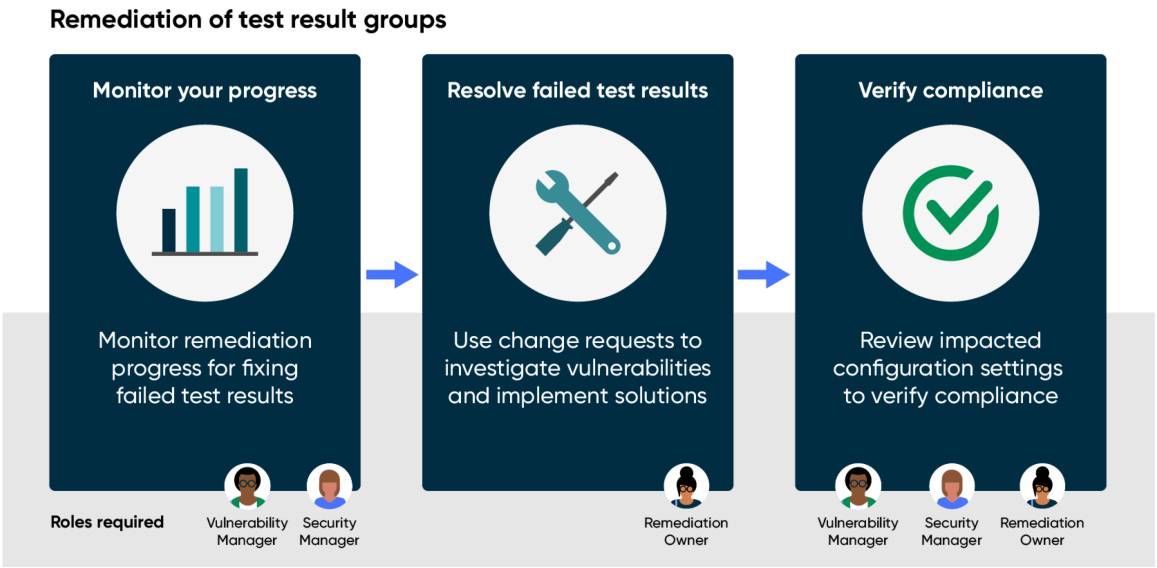
**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Separate SCA-Plugins von Drittanbietern erfassen und transformieren Daten in Configuration Compliance. Bevor Sie Configuration Compliance zur Korrektur von Konfigurationselementen verwenden können, müssen Sie eine Scanner-Integration einer Drittpartei installieren und mindestens einen Netzwerk-Scan durchführen.

Verwenden Sie Change-Anforderungen, um einzelne Testfehler aus Testergebnisgruppen zu beheben.

Die Status von Testergebnisgruppen werden automatisch geändert, wenn zugehörige Change-Anforderungen ihre Lebenszyklen mit Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgabendurchlaufen. Benutzer mit der Rolle „itil“ können Change-Anforderungen direkt aus Testergebnisgruppen erstellen und verwalten.

## Erstellen Sie manuell eine Korrekturaufgabe Configuration Compliance .

Sie können eine Korrekturaufgabe manuell aus dem Modul „ **Testergebnisgruppen“** erstellen und die Korrektur durchführen.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Durch die Verwendung von Testergebnisgruppenregeln wird die Registerkarte „ **Testergebnisse** “ automatisch ausgefüllt. Die manuelle Erstellung ist für eine Gruppe nützlich, die keine Regel benötigt oder wiederholt werden muss.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

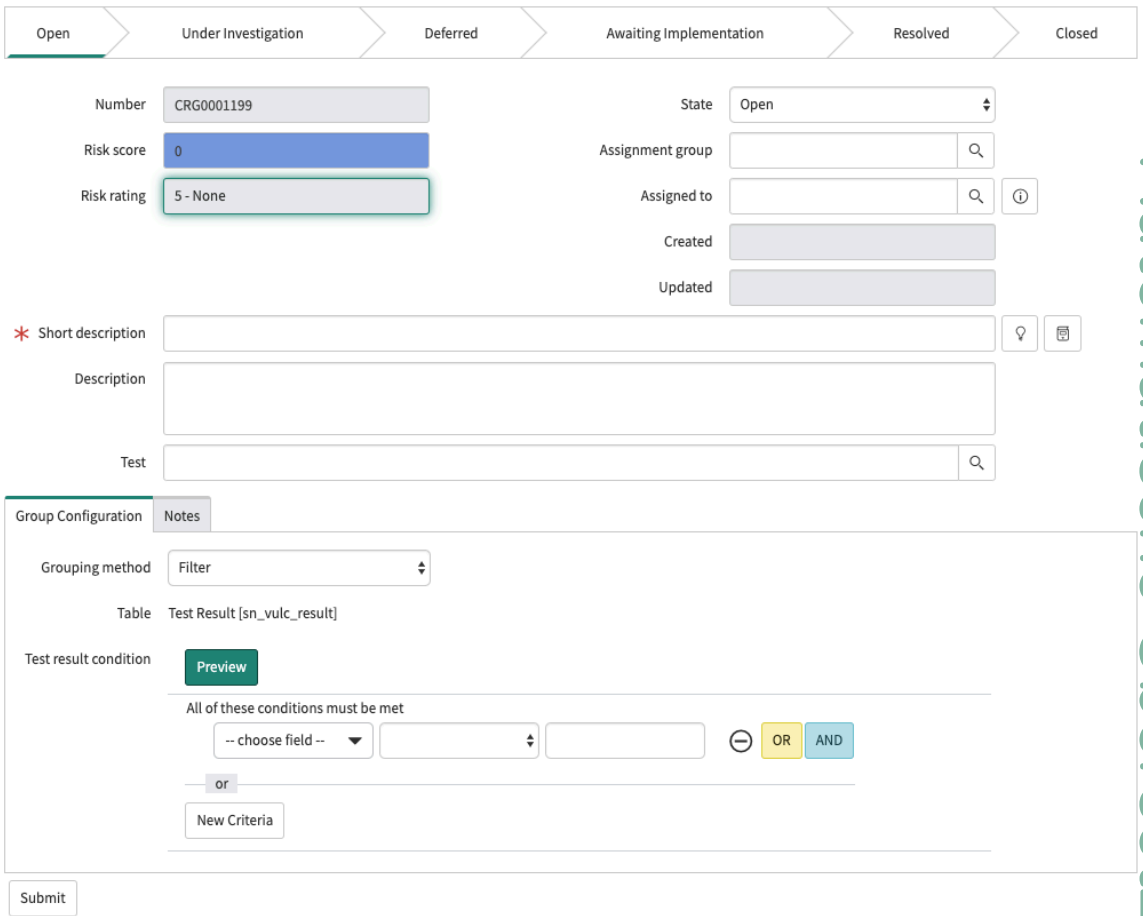
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Korrekturaufgaben**.
2. Klicken Sie im Navigationsbereich auf **Meine offenen Aufgaben** oder **Alle offenen Aufgaben**, um die Liste anzuzeigen.
3. Klicken Sie auf **Neu**.

**Formular „Testergebnisgruppe“.**




4. Füllen Sie die entsprechenden Felder im Formular „Korrekturaufgabe“ aus.

**Formular „Korrekturaufgabe“.**

| Feld | Beschreibung |
|---|---|
| Nummer | Automatisch zugewiesene ID im System. |
| Risikopunktzahl | Wird automatisch vom Risikopunktzahl-Rechner ausgefüllt.<br><br>Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl ist gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht geschlossenen Testergebnisse (Offen, Wird untersucht, Warten auf Implementierung, Zurückgestellt, Gelöst) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind. |
| Risikobewertung | Wird automatisch vom Risikopunktzahl-Rechner ausgefüllt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

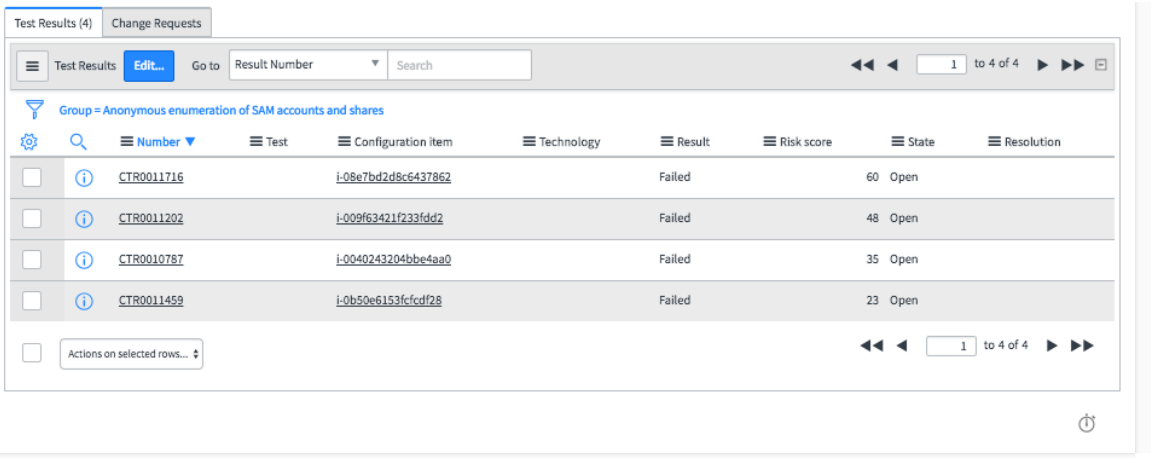
| Feld | Beschreibung |
|---|---|
| | Basierend auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen von 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen. |
| Status | „Anfänglich **Offen**“ ist der Korrekturstatus der Gruppe. Weitere Informationen finden Sie unter Configuration Compliance Status. |
| Zuweisungsgruppe | Weisen Sie die Testergebnisgruppe einer Korrekturgruppe zu. |
| Zugewiesen an | Weisen Sie Personal zu, um die Testergebnisgruppe zu korrigieren. |
| Erstellt | Datum, an dem Sie diese Gruppe erstellt haben. |
| Aktualisiert | Datum, an dem Sie diese Gruppe aktualisiert haben. |
| Kurzbeschreibung | Name der Testergebnisgruppe. |
| Beschreibung | Beschreibung dieser Testergebnisgruppe. |
| Test | Wählen Sie einen Konfigurationstest für diese Testergebnisgruppe aus. |
| **Zugehörige Registerkarten** | |
| Gruppenkonfiguration | Zu verwendende Gruppierungsmethoden:<br>○ Manuell (Standard):<br>○ Filter- oder Gruppenregel:<br>Tabelle: vorausgewählt als Testergebnis [sn_vulc_result]<br>Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus.<br>**Hinweis:**<br>Der Link Datensätze entsprechen Bedingung über den Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an.<br>Klicken Sie auf **Vorschau**, um zu sehen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Gruppe speichern.<br>Die zugehörige Liste „Testergebnisse“ muss manuell erstellt werden, indem Sie auf der zugehörigen Registerkarte „ **Testergebnisse** “ auf die Schaltfläche **Bearbeiten** klicken. |
| Notizen | Arbeitsnotizen in Bezug auf diese Testergebnisgruppe. |

5. Klicken Sie mit der rechten Maustaste in den Header, um **Speichern**, oder klicken Sie auf **Absenden**, um zu speichern und zur Liste der Testergebnisgruppen zurückzukehren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt die zugehörigen Listen „ **Testergebnisse“** und **„Change-Anforderung** “ an.




## Erstellen Sie manuell eine Testergebnisgruppe Configuration Compliance aus der Liste der Testergebnisse

Sie können eine **Testergebnisgruppe** manuell aus der Liste „Testergebnis“ erstellen und anhand der resultierenden Testergebnisgruppe eine Fehlerkorrektur durchführen.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

### Warum und wann dieser Vorgang ausgeführt wird

Diese Methode erfordert die Auswahl der einzubeziehenden Testergebnisse und die Erstellung der Gruppe im Menü **Aktionen für ausgewählte Zeilen...** Diese Methode eignet sich für Ergebnisse, die nicht einfach gefiltert werden können, oder für Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

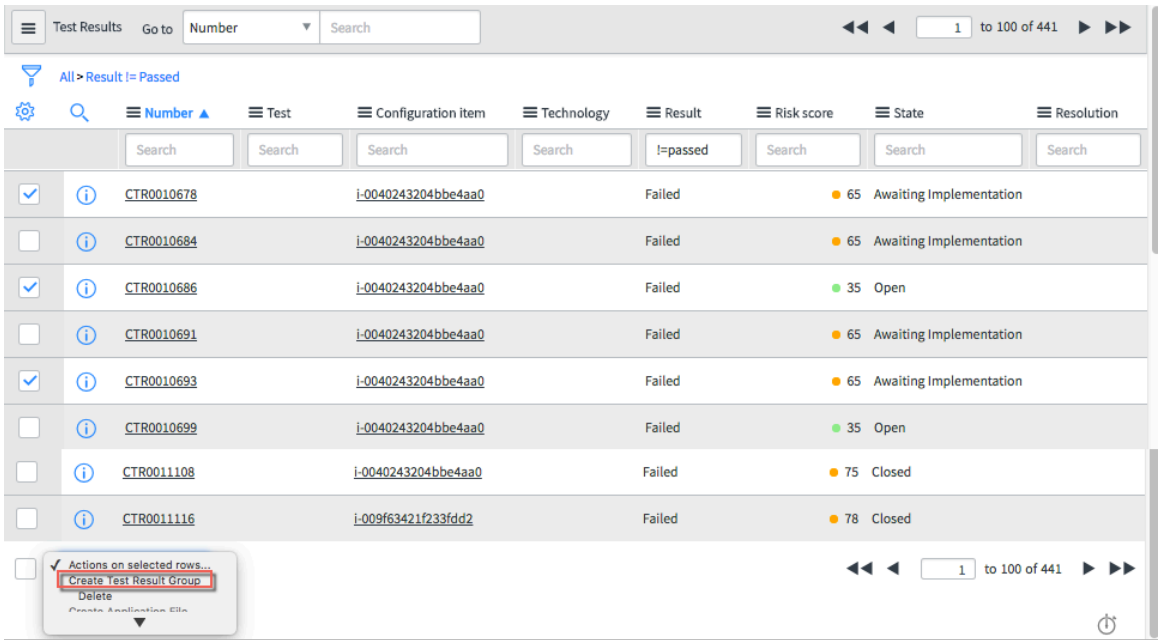
| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisse**.
2. Wählen Sie im Navigationsbereich ein Testergebnismodul aus, um eine Liste zu öffnen.
3. Wählen Sie die Testergebnisse aus, die in die Gruppe aufgenommen werden sollen, indem Sie das Kontrollkästchen neben jedem Ergebnis aktivieren.
4. Öffnen Sie das Menü **Aktionen für ausgewählte Zeilen...** am Ende der Liste.

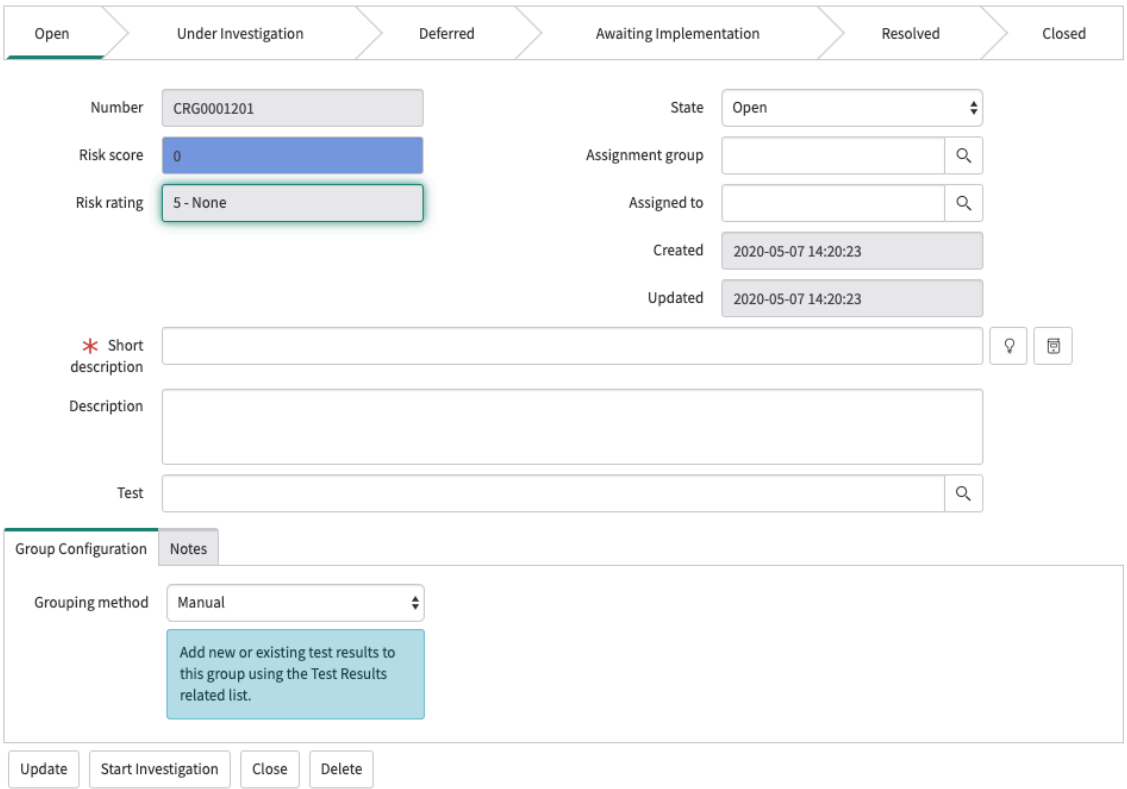
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**5.** Wählen **Sie Testergebnisgruppe erstellen**.
Die Testergebnisgruppe wird erstellt und geöffnet.

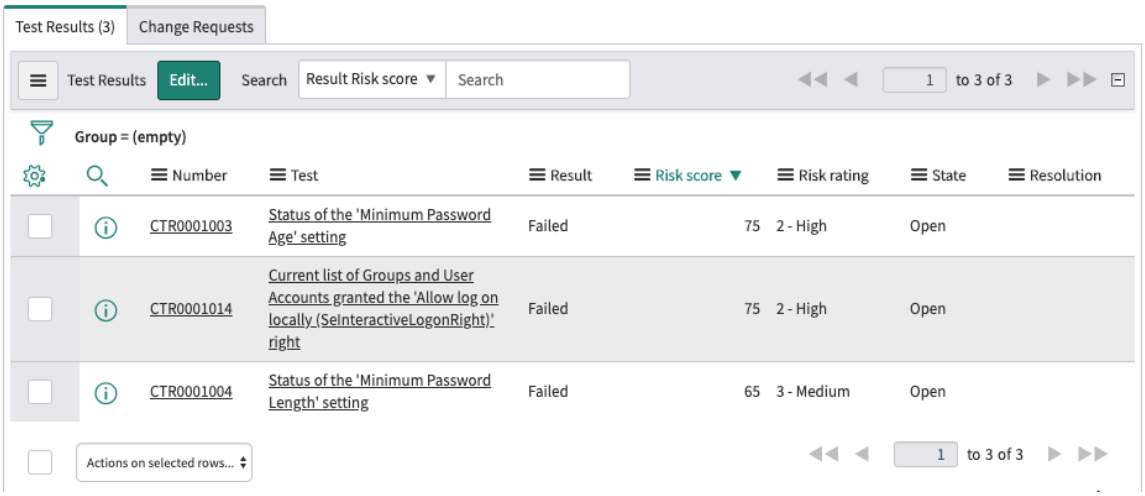
**Formular „Testergebnisgruppe“.**




Die Testergebnisse, die Sie für die Gruppe ausgewählt haben, werden in der zugehörigen Liste „Testergebnisse“ zusammen mit den zugehörigen Change-Anforderungen angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**6.** Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Nummer | Automatisch zugewiesene ID im System. |
| Punktzahl | Wird automatisch durch den Rollup-Rechner der Risikopunktzahl ausgefüllt.<br><br>Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl ist gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht geschlossenen Testergebnisse (Offen, Wird untersucht, Warten auf Implementierung, Zurückgestellt, Gelöst) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind. |
| Bewertung | Wird automatisch durch den Rollup-Rechner der Risikopunktzahl ausgefüllt.<br><br>Basierend auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen von 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen. |
| Historische Risikopunktzahl | Wird automatisch durch den Rollup-Rechner der Risikopunktzahl ausgefüllt.<br><br>Die inhärente Risikopunktzahl für alle bestandenen Testergebnisse in einer Testergebnisgruppe. Dieses Feld zeigt die Höhe des Risikos an, das von einer Testgruppe behoben wurde. Es wird nur angezeigt, wenn sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl 0 ist. |
| Status | „Anfänglich **Offen**“ ist der Korrekturstatus der Gruppe. Weitere Informationen finden Sie unter Configuration Compliance Status. |
| | |
| Zuweisungsgruppe | Weisen Sie die Testergebnisgruppe einer Korrekturgruppe zu. |
| Zugewiesen an | Weisen Sie Mitarbeiter zu, die die Gruppe korrigieren sollen. |
| Erstellt | Datum, an dem Sie diese Gruppe erstellt haben. |
| Aktualisiert | Datum, an dem Sie diese Gruppe aktualisiert haben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Kurzbeschreibung | Name der Testergebnisgruppe. |
| Beschreibung | Textbeschreibung dieser Testergebnisgruppe. |
| | Wählen Sie einen Konfigurationstest für diese Testergebnisgruppe aus. |
| **Zugehörige Registerkarten** | |
| Gruppenkonfiguration | Zu verwendende Gruppierungsmethoden:<br>○ Manuell (Standard)<br>○ Filter<br>Tabelle: als Testergebnis vorausgewählt<br>Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus.<br>**Hinweis:**<br>Der Link Datensätze entsprechen Bedingung über den Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an.<br>Klicken Sie auf **Vorschau**, um zu sehen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Gruppe speichern. |
| Notizen | Arbeitsnotizen in Bezug auf diese Testergebnisgruppe. |
| **Zugehörige Listen** | |
| Testergebnisse | In dieser Gruppe enthaltene Testergebnisse. |
| Change-Anforderungen | Change-Anforderungen, die dieser Gruppe zugeordnet sind. |

7. Klicken Sie mit der rechten Maustaste auf den Header, um zu **speichern**, oder klicken Sie auf **Absenden**, um zu speichern und zur Liste der Testergebnisgruppen zurückzukehren.

## Change-Anforderung in Configuration Compliance erstellen

Sie können eine Change-Anforderung aus einer Testergebnisgruppe (TRG) in der Anwendung Configuration Compliance erstellen.

### Vorbereitungen

Erforderliche Rolle: Benutzer mit der Rolle itil

### Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie als IT- oder Fehlerkorrekturspezialist eine Change-Anforderung (CHG) direkt aus einer Testergebnisgruppe für alle Testergebnisse in der Gruppe. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung von Schwachstellen zu beschleunigen, die ein manuelles Eingreifen erfordern.

Sie können Change-Anforderungen direkt aus Testergebnisgruppen, die Ihnen zugewiesen sind, erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Testergebnisgruppe erstellen:

**Standard**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.

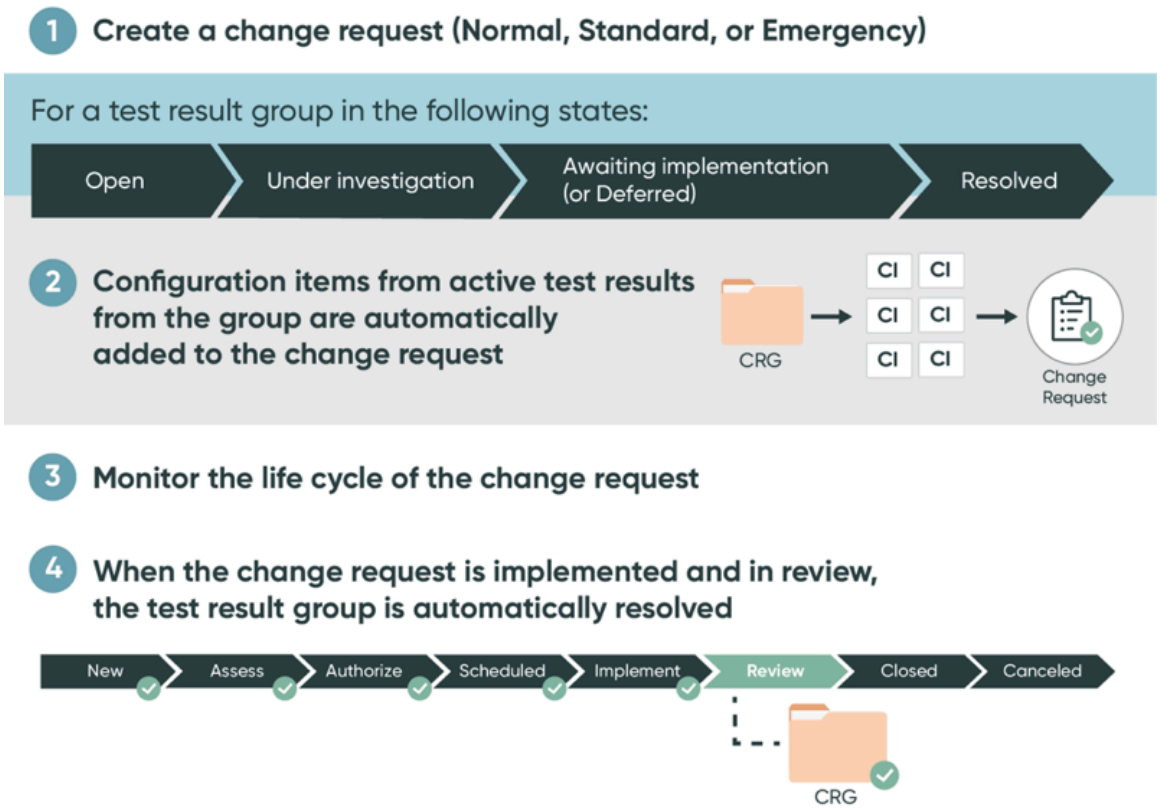
**Normal**

Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.

**Notfall**

Eine Änderung zur Lösung eines schwerwiegenden Incident.

Die folgende Abbildung zeigt den grundlegenden Ablauf zum Erstellen einer Change-Anforderung aus einer Testergebnisgruppe. Die detaillierten Schritte für diesen Flow folgen der Abbildung.




Ab Version 19.0 von Vulnerability Responsekönnen Sie Change-Anforderungen für Testergebnisgruppen (TRGs) aus dem IT-Korrekturarbeitsbereich erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung in IT Remediation Workspace.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisgruppen** > **Meine offenen Gruppen**.
   Die Liste der Testergebnisgruppen, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Testergebnisgruppe, für die Sie eine Change-Anforderung erstellen möchten.
   Sie können Change-Anforderungen aus Testergebnisgruppen in einem anderen Status als **Geschlossen** oder **Wird überprüft**erstellen.

   Der Datensatz der Testergebnisgruppe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz auf **Change erstellen**.
   Das Change Request-Formular wird angezeigt.
4. Füllen Sie die Felder aus.
   a. Wählen Sie aus der Liste des Felds Betrifft eine **Option** aus, um fortzufahren.
5. Wählen Sie für das Kontrollkästchen **CIs zu CA hinzufügen eine Option** aus, um fortzufahren.
6. Wählen Sie in der Liste für das Feld **Change-Typ** einen aus, um fortzufahren.

   Die Funktion liest automatisch die Typen von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von Standard in Vorab genehmigtändern, wird Ihr neuer Name automatisch in der Liste Change-Typ im Formular „Change-Anforderung erstellen“ angezeigt.
7. Die Felder im Abschnitt „Change Request-Vorschau“ des Formulars sind vorab mit Informationen aus der Testergebnisgruppe ausgefüllt.
   Bearbeiten Sie bei Bedarf diese Felder.
8. Klicken **Sie auf Change erstellen**.
   Die Change-Anforderung wird angezeigt. In der zugehörigen Liste „Betroffene CIs“ werden die CIs aus den Testergebnissen angezeigt, die Ihren Kriterien entsprechen. Wenn die Change-Anforderung eine Genehmigung erfordert, wird die Schaltfläche Genehmigung **anfordern** angezeigt.

   Nachdem die Change-Anforderung erstellt wurde, wird die Testergebnisgruppe in den Status „ **Warten auf Implementierung** “ verschoben. Nachdem die Change-Anforderung für diese Testergebnisgruppe gelöst wurde und dieser Testergebnisgruppe keine weiteren offenen Change-Anforderungen zugeordnet sind, wird die Testergebnisgruppe ebenfalls in den Status **Gelöst** verschoben.

   Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

**Hinweis:**
Sie können Change-Anforderungen und Testergebnisgruppen weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung seinen Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder entfernen aus einer Testergebnisgruppe kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben die Testergebnisgruppe jedoch nicht automatisch aus den Status „ Geschlossen “ oder „ Zurückgestellt “.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ordnen Sie eine Testergebnisgruppe einer vorhandenen Change-Anforderung zu

Ordnen Sie eine Testergebnisgruppe in der Anwendung Configuration Compliance einer vorhandenen Change-Anforderung zu.

### Vorbereitungen

Erforderliche Rolle: ein Benutzer mit der itil-Rolle

### Warum und wann dieser Vorgang ausgeführt wird

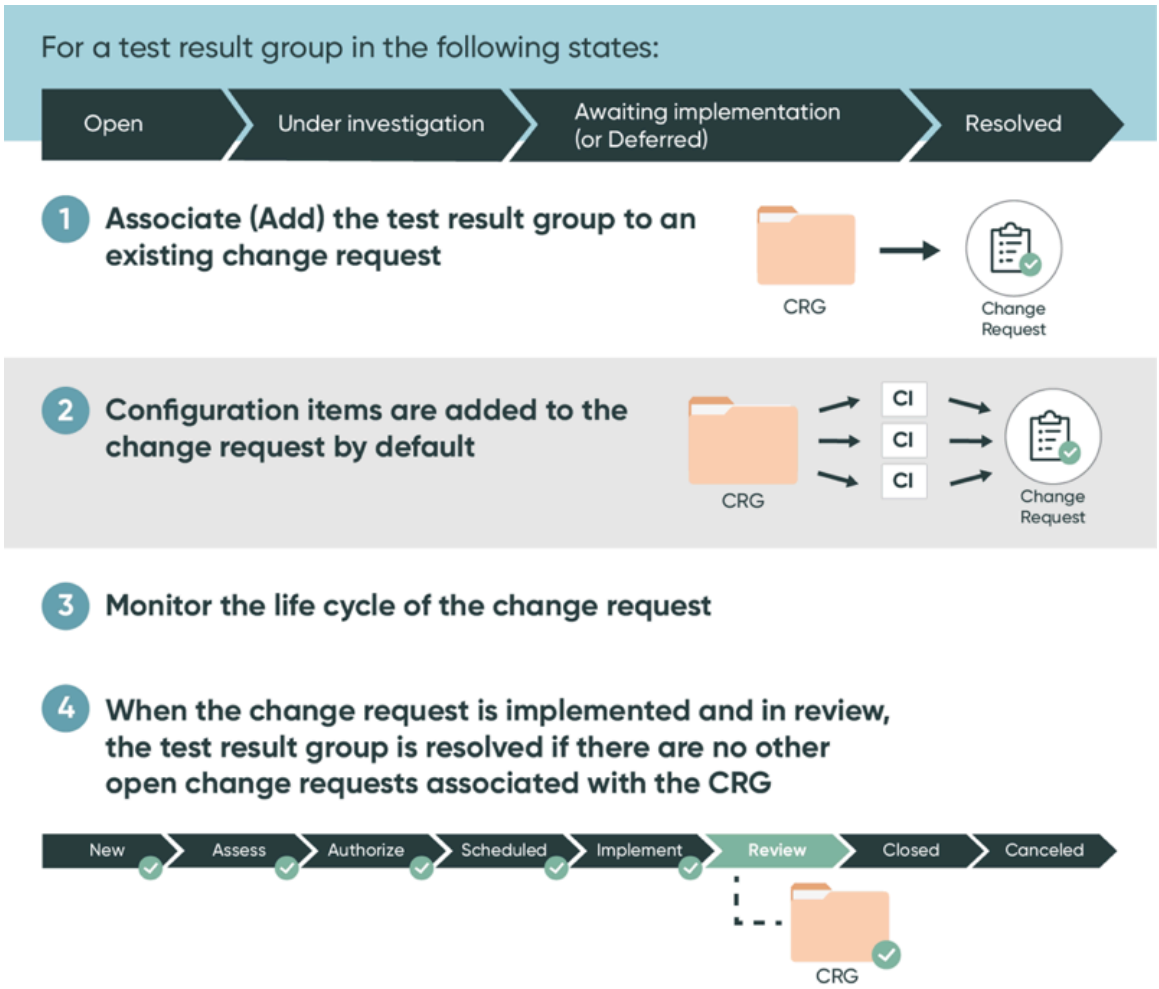
Vermeiden Sie als IT- oder Fehlerkorrekturspezialist die Erstellung doppelter Change-Anforderungen (CHG), wenn Sie an der Lösung Ihrer Testergebnisgruppen arbeiten, indem Sie eine Testergebnisgruppe (TRG) einer Change-Anforderung zuordnen, die bereits in Ihrer Instanz verfügbar ist.

Sie können Testergebnisgruppen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Datensätzen der Testergebnisgruppe zuordnen. Die folgende Abbildung zeigt den grundlegenden Ablauf für die Zuordnung einer vorhandenen Change-Anforderung zu einer TRG. Die detaillierten Schritte für diesen Flow folgen der Abbildung.

**Hinweis:**
Sie können eine vorhandene Change-Anforderung einer TRG in einem anderen Status als „ **Abgebrochen** “ zuordnen (**Offen**, Wird **untersucht**, **Implementierung ausstehend**, **Geschlossen**und **Zurückgestellt**). Change-Anforderungen, einschließlich der innerhalb der letzten 90 Tage geschlossenen, können über das Formular zugeordnet werden. Wenn Sie eine Change-Anforderung einer vorhandenen TRG zuordnen, werden nur die aktiven Testergebnisse und ihre Konfigurationselemente der Change-Anforderung hinzugefügt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisgruppen** > **Meine offenen Gruppen**.
   Die Liste der Testergebnisgruppen, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Testergebnisgruppe, für die Sie eine Change-Anforderung erstellen möchten.

   Der Datensatz der Testergebnisgruppe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz auf **Change erstellen**.
   Das Change Request-Formular wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Scrollen Sie zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle mit der TRG verknüpften Change-Anforderungen werden zusammen mit der Schaltfläche **Hinzufügen** angezeigt.
5. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld „Bestehende Change-Anforderung zu Testergebnisgruppe hinzufügen“ wird angezeigt.
6. Klicken Sie auf das Suchsymbol, und wählen Sie ein Element aus der Liste aus.
   Sie können die angezeigte Liste filtern, um Ihre Suche einzugrenzen.
7. Klicken Sie auf **Absenden**.
   Die TRG wird zusammen mit einer Meldung angezeigt, die angibt, dass die Change-Anforderung erfolgreich der Testergebnisgruppe zugeordnet wurde. Unter der zugehörigen Liste der Change-Anforderungen wird die neue Change-Anforderung angezeigt. Die CIs aus der Testergebnisgruppe werden dem Change Request standardmäßig hinzugefügt und in der zugehörigen Liste Betroffene CIs angezeigt. Sie können dem Change Request auch CIs aus dieser zugehörigen Liste hinzufügen. Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Gruppe verschoben wurden, und die neue TRG wird angezeigt.

**Hinweis:**
Bei weniger als 200 Testergebnissen wird der Aufteilungsvorgang synchron ausgeführt, und die Testergebnisse werden in der neuen Gruppe angezeigt.

Bei mehr als 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Gruppe angezeigt werden. Die folgende Nachricht wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxxx in die neue Testergebnisgruppe GRCxxxxx verschoben.

Sie können der TRG beliebige Change-Anforderungen zuordnen, mit den folgenden Ausnahmen:

- Change-Anforderungen im Status **„Abgebrochen“**
- Change-Anforderungen im Status „ **Geschlossen** “, die älter als 90 Tage sind
- Change-Anforderungen sind bereits der TRG zugeordnet. Das System lässt nicht zu, dass Sie eine Change-Anforderung zuordnen, die bereits der TRG zugeordnet ist.

Nachdem die Change-Anforderung für diese Testergebnisgruppe gelöst wurde und dieser Testergebnisgruppe keine weiteren offenen Change-Anforderungen zugeordnet sind, wird die Testergebnisgruppe ebenfalls in den Status**Gelöst** verschoben.

**Hinweis:**
Sie können Change-Anforderungen und Testergebnisgruppen weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung seinen Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder entfernen aus einer Testergebnisgruppe kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben die Testergebnisgruppe jedoch nicht automatisch aus den Status „ Geschlossen “ oder „ Zurückgestellt “.

Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

## Teilen Sie eine Testergebnisgruppe auf

Identifizieren Sie aus einer vorhandenen Testergebnisgruppe (TRG) in der Anwendung Configuration Compliance eine Teilmenge der Testergebnisse, die Sie in eine neue Testergebnisgruppe verschieben möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

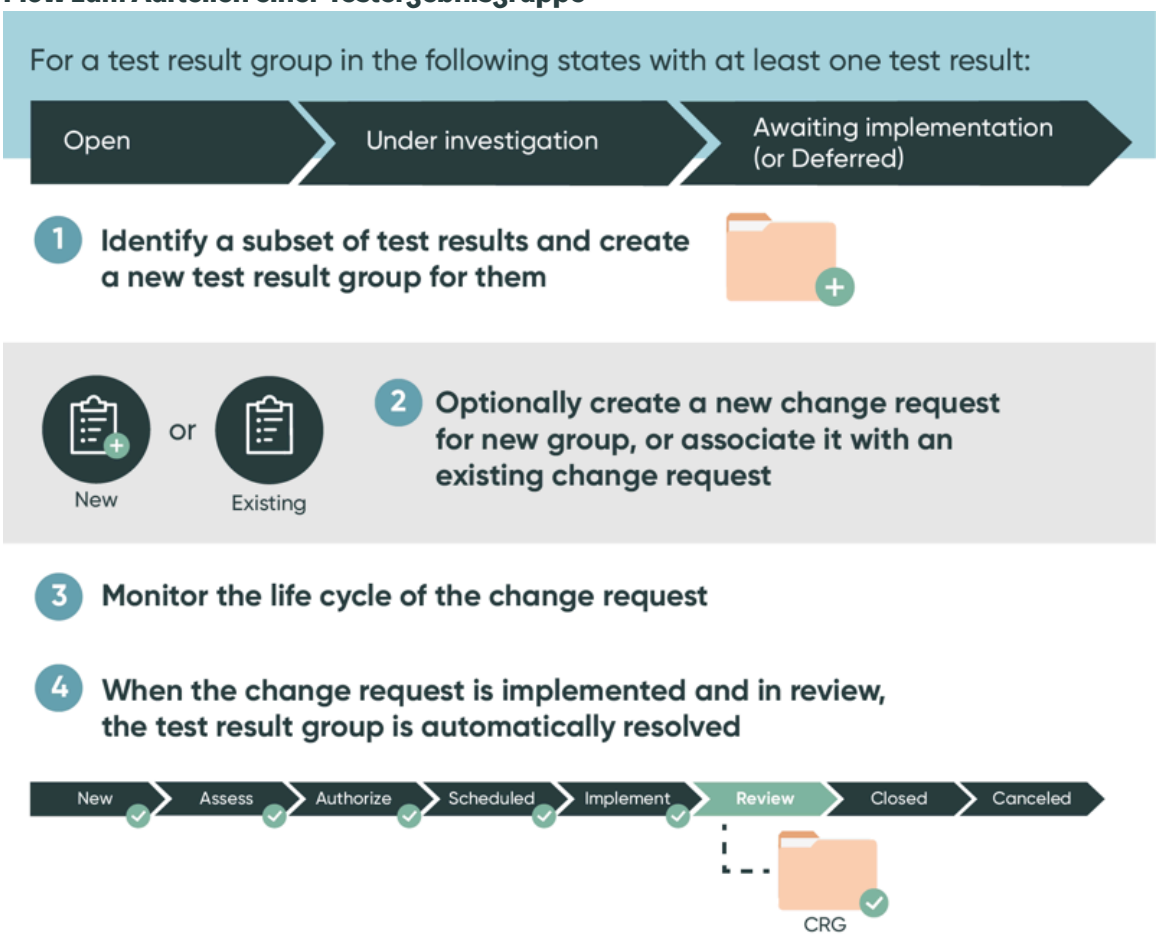
**Vorbereitungen**
Erforderliche Rolle: ein Benutzer mit der itil-Rolle

**Warum und wann dieser Vorgang ausgeführt wird**
Als IT- oder Fehlerkorrekturspezialist können Sie vorhandene Testergebnisgruppen in den Status „ **Offen**“, „ **Wird untersucht**“ oder **„Warten auf Implementierung“** mit mehr als einem Testergebnis aufteilen. Durch die Erstellung einer neuen TRG mit Testergebnissen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Gruppe zu beeinträchtigen.

Wenn Sie die Bedingungen für die Testergebnisse angeben, die Sie mit dem Bedingungsgenerator in eine neue Testergebnisgruppe verschieben möchten, werden nur die aktiven Testergebnisse, die Ihren Kriterien entsprechen, in die neue Gruppe verschoben. Sie müssen keine Change-Anforderungen (CHGs) erstellen, wenn Sie eine TRG aufteilen. Sie haben die Möglichkeit, eine TRG aufzuteilen, während Sie eine Change-Anforderung erstellen, oder Sie können eine TRG aufteilen, ohne eine Change-Anforderung zu erstellen.

Die folgende Abbildung zeigt den grundlegenden Ablauf für die Aufteilung einer Testergebnisgruppe. Die detaillierten Schritte für diesen Flow folgen der Abbildung.

**Flow zum Aufteilen einer Testergebnisgruppe**




Anwendungsfälle für die Aufteilung von Testergebnissen aus vorhandenen TRGs in neue Gruppen können die folgenden Beispiele umfassen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine oder mehrere Change-Anforderungen für eine Split-Gruppe erstellen möchten.
- Wenn Sie eine Split-Gruppe einem anderen Benutzer in Ihrer Zuweisungsgruppe neu zuweisen.
- Wenn Sie eine Zurückstellung oder Ausnahme für eine Split-Gruppe anfordern, da Sie wissen, dass einige Testergebnisse für bestimmte Konfigurationselemente (CI) nicht in einem bestimmten Zeitrahmen korrigiert werden können.

[store-future: BEGIN review]Ab Version 19.0 von Vulnerability Responsekönnen Sie Aufgaben für Testergebnisgruppen aus dem IT-Korrekturarbeitsbereich aufteilen.[End]

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Tests** > **Testergebnisgruppen** > **Meine offenen Gruppen**.
   Die Liste der Testergebnisgruppen, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Testergebnisgruppe, die Sie aufteilen möchten.

   Der Datensatz der Testergebnisgruppe wird angezeigt.
3. Führen Sie die folgenden Schritte aus, um eine Teilmenge der Testergebnisse für eine neue Gruppe zu erstellen, die bestimmten Kriterien entspricht.

   Klicken Sie oben rechts im Datensatz auf **Gruppe aufteilen**.

   Möglicherweise bevorzugen Sie diese Methode zum Erstellen einer neuen Gruppe, wenn Sie in einer großen Gruppe mit mehreren Testergebnissen arbeiten.

   Das Formular „Testergebnisgruppe aufteilen“ wird angezeigt.
4. Geben Sie bei angezeigtem Bedingungsgenerator die Bedingungen für die Testergebnisse an, die Sie in eine neue Testergebnisgruppe verschieben möchten.

   Beispielsweise können Sie nur Testergebnisse herausfiltern, die den folgenden Bedingungen entsprechen:

   - Im Status **„Offen** “.
   - Risikopunktzahlen größer als 75.
   - Ergebnis ist **„Fehlgeschlagen“**.

   Wenn Testergebnisse Ihrem Filter entsprechen, nachdem Sie die Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der übereinstimmenden Testergebnisse angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Meldung angezeigt wird, dass keine Testergebnisse Ihrem Filter entsprechen oder dass alle Testergebnisse Ihren Kriterien entsprechen, passen Sie die Bedingungen so an, dass mindestens ein Testergebnis Ihren Filterkriterien entspricht.

5. Klicken Sie auf **Elemente in der Vorschau** anzeigen, um die übereinstimmenden Testergebnisse anzuzeigen.
   In einem neuen Fenster, Testergebnisgruppen, werden die Elemente angezeigt.
6. Um eine Vorschau der Details zu den Testergebnissen anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie diese Schritte aus, bevor Sie auf **Gruppe** aufteilen klicken, um die neue Gruppe zu erstellen. Diese Details umfassen die Zuweisungsgruppe und die Person, der das Testergebnis zugewiesen wurde. Wenn Sie diese Informationen in der Vorschau anzeigen, können Sie sicherstellen, dass die neue Gruppe ordnungsgemäß zugewiesen wird.

   a. Wenn die Liste der Testergebnisgruppen in der Vorschau angezeigt wird, klicken Sie auf ein Element in der Spalte Ergebnis.
      Der Testergebnis-Datensatz wird angezeigt.

   b. Vergewissern Sie sich, dass die Felder **Zuweisungsgruppe** und **Zugewiesen an** korrekt sind.

   c. Klicken Sie auf **Aktualisieren**.

7. Wenn Sie bereit sind, die neue Gruppe zu erstellen, klicken Sie auf **Gruppe**aufteilen.
   Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Gruppe verschoben wurden, und die neue TRG wird angezeigt. Um die neue Gruppe leichter zu identifizieren, sollten Sie den Text im Feld **Kurzbeschreibung** bearbeiten und die Felder Zuweisungsgruppe oder Zugewiesen an bei Bedarf erneut bearbeiten.

   **Hinweis:**
   Bei weniger als 200 Testergebnissen wird der Aufteilungsvorgang synchron ausgeführt, und die Testergebnisse werden in der neuen Gruppe angezeigt.

   Bei mehr als 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Gruppe angezeigt werden. Die folgende Nachricht wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxxx in die neue Testergebnisgruppe GRCxxxxx verschoben.

8. Alternativ können Sie eine neue Testergebnisgruppe erstellen, indem Sie Testergebnisse direkt aus der zugehörigen Liste „Testergebnisse“ in einer Testergebnisgruppe auswählen.

   Möglicherweise bevorzugen Sie diese Methode, wenn Sie nur wenige Testergebnisse in einer Gruppe haben oder genau wissen, welche Tests Sie in eine neue Gruppe verschieben möchten.

   a. Scrollen Sie bei angezeigtem Datensatz der Testergebnisgruppe zur zugehörigen Liste „Testergebnisse“.

   b. Aktivieren Sie in der Spalte ganz links die Kontrollkästchen für die Testergebnisse, für die Sie eine neue TRG erstellen möchten.

   c. Klicken Sie in der Liste Aktionen für ausgewählte Zeilen unten links im Datensatz auf **Gruppe aufteilen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Im angezeigten Formular „Testergebnisgruppe aufteilen“ können Sie den Text im Feld **Kurzbeschreibung** bearbeiten, damit Sie die neue Gruppe leichter identifizieren können.

**e.** Klicken Sie **auf Gruppe**teilen.
Eine Nachricht gibt die Anzahl der Testergebnisse an, die in die neue Gruppe verschoben wurden, und die neue TRG wird angezeigt.

Nachdem die Change-Anforderung für diese Testergebnisgruppe gelöst wurde und dieser Testergebnisgruppe keine weiteren offenen Change-Anforderungen zugeordnet sind, wird die Testergebnisgruppe ebenfalls in den Status **Gelöst** verschoben.

**Hinweis:**
Sie können Change-Anforderungen und Testergebnisgruppen weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung seinen Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder entfernen aus einer Testergebnisgruppe kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Die Status von Change-Anforderungen verschieben die Testergebnisgruppe jedoch nicht automatisch aus den Status „ Geschlossen “ oder „ Zurückgestellt “.

Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

### Nächste Maßnahme
Sie können Change-Anforderungen für Ihre neuen Testergebnisgruppen erstellen oder zuordnen. Weitere Informationen finden Sie unter Ordnen Sie eine Testergebnisgruppe einer vorhandenen Change-Anforderung zu und Change-Anforderung in Configuration Compliance erstellen.

## Entfernen Sie Zuweisungen aus Testergebnisgruppen für sich oder Ihre Gruppen

Weisen Sie die Testergebnisdatensätze in der Anwendung Configuration Compliance neu zu, wenn die Datensätze Ihnen oder Ihrer Gruppe fälschlicherweise zugewiesen wurden.

### Vorbereitungen
Erforderliche Rolle: sn_vulc.remediation_owner

### Warum und wann dieser Vorgang ausgeführt wird
Ab Version 14.3 der Anwendung Configuration Compliance Wenn Sie feststellen, dass Testergebnisgruppen (TRG) und die zugehörigen Testergebnisse nicht in Ihrem Bereich der Korrektur liegen, oder wenn Sie der Meinung sind, dass Ihnen oder Ihren Gruppen Datensätze fälschlicherweise zugewiesen wurden, sollten Sie sich selbst oder Ihre Gruppen entfernen aus den Feldern Zugewiesen an und Zuweisungsgruppe in TRG-Datensätzen.

Die **Schaltfläche Zuweisung** aufheben wird in TRG-Datensätzen in einem anderen Status als „Geschlossen“ oder „Gelöst“ angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren Sie zu einem Ihnen zugewiesenen Testergebnis-Gruppendatensatz, der sich in einem anderen Status als Geschlossen oder Gelöst befindet.
2. Um die Felder **Zugewiesen an** und **Zuweisungsgruppe** zu löschen, wählen Sie oben im Datensatz die Option Zuweisung **aufheben**aus.
3. **Geben** Sie im Dialogfeld „Zuweisung aufheben“ Arbeitsnotizen an, und wählen Sie **Absenden**.
   - Die von Ihnen angegebenen Arbeitsnotizen werden im Abschnitt „Notizen“ angezeigt.
   - Auf der Registerkarte **Statusänderungsgenehmigung** zeigt der Statusänderungsgenehmigungsdatensatz (CA#) den Status Wird überprüft an, was Ihnen hilft, den Genehmigungs-Workflow nachzuverfolgen.
   - Auf der Registerkarte „ **Angeforderte Genehmigungen** “ wird Ihre Anforderung zur Entfernung von Ihnen oder Ihrer Zuweisungsgruppe als Status „Angefordert“ angezeigt.

## Ergebnisse

Die Anforderung wird mithilfe eines standardmäßigen einstufigen Genehmigungsworkflows genehmigt. Weitere Informationen finden Sie unter Anforderung zur Aufhebung der Zuweisung in Configuration Compliance genehmigen.

- Wenn Ihre Anforderung genehmigt wird, gehen der Statusänderungsgenehmigungsdatensatz und der Anforderungsgenehmigungsdatensatz in **Genehmigt**über. Sie und Ihre Gruppen werden aus den Feldern **Zugewiesen an** und **Zuweisungsgruppe** entfernt. „Nicht zugewiesen “ wird im Feld **Zuweisungstyp** angezeigt, und die Testergebnisgruppe wird in der Liste des Moduls „Nicht zugewiesen“ für die Anwendung Configuration Compliance angezeigt.

  Benachrichtigungen, dass Datensätze nicht zugewiesen sind, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Weitere Informationen zu den Benachrichtigungen und Eigenschaften für diese Funktion finden Sie unter Zuweisungen aus Configuration Compliance-Testergebnisgruppen entfernen.

- Wenn Ihre Anforderung abgelehnt wird, gehen der Statusänderungsgenehmigungsdatensatz und der angeforderte Genehmigungsdatensatz in „Abgelehnt“ über.

**Hinweis:**
Als Schwachstellenadministrator können Sie die Systemeigenschaft `sn_vulc.unassign_test_result_group.approval_required` auf „ **false** “ setzen, um den Genehmigungsprozess zu deaktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Navigieren Sie zum Modul „Nicht zugewiesen“ für die Anwendung Configuration ComplianceContainer Vulnerability Response].

## Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Configuration Compliance

Genehmigen Sie Anforderungen zum Entfernen von Testergebnisgruppen aus einer Zuweisungsgruppe oder einem einzelnen Benutzer in der Anwendung Configuration Compliance.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.unassign_approver

### Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt. Um die Zuweisung von Genehmigungen aufzuheben, ist ein Genehmiger in der Genehmigungsgruppe „Genehmiger – Ebene 1“ erforderlich. Standardmäßig wird die Genehmigungsgruppe „Zuweisung aufheben“ (Zuweisung des Genehmigersaufheben – CC – Ebene 1) erstellt, und Benutzer, die Teil dieser Gruppe sind, können die Anforderung genehmigen. Standardmäßig enthält diese Gruppe die Rolle „Zuweisung aufheben“ des Genehmigers, sn_vulc.unassign_approver. Sie können eine Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren, indem Sie zu navigieren **Alle** > **Configuration Compliance** > **Meine Freigaben** > **Genehmigungsregeln** > **Change-Anforderung für Testergebnis-Gruppenfeld** > **Heben Sie die Zuweisung der Testergebnisgruppe auf**.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung ab, indem Sie die entsprechenden Kommentare hinzufügen.

## Automatisches Schließen von Testergebnissen

Sie können Testergebnisse (TRs), die stillgelegten Konfigurationselementen (CIs) zugeordnet sind, automatisch schließen.

Um die Option zum automatischen Schließen zu konfigurieren, navigieren Sie zur Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** und legen Sie sie auf true fest. Informationen zum automatischen Schließen von TRs im Zusammenhang mit stillgelegten CIs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Weitere Informationen zum Arbeiten mit deaktivierten Konfigurationselementen finden Sie unter Arbeiten mit deaktivierten Konfigurationselementen in Configuration Compliance.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Arbeiten mit deaktivierten Konfigurationselementen in Configuration Compliance

Außer Betrieb genommene Konfigurationselemente (CIs) werden in den Status „Stillgelegt“, „Archiviert“ oder „Gelöscht“ in Configuration Management Database (CMDB)verschoben. Configuration Compliance enthält Testergebnisse (TRs), die aus CIs bestehen. Wenn der Status eines CI auf „Deaktiviert“ aktualisiert wird, werden die zugehörigen TRs mit dem Substatus „CI außer Betrieb genommen“ geschlossen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „Deaktiviert“ ändert, können Sie die zugehörigen TRs automatisch schließen. Weitere Informationen zum automatischen Schließen der zugeordneten TRs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Das stillgelegte CI wird schließlich archiviert oder dauerhaft aus dem CMDBgelöscht.

Auswirkung der Außerkraftsetzung der CIs:

- **Auswirkung auf erkannte Elemente:** Wenn das CI stillgelegt wird, wird der zugehörige DI als „CI außer Betrieb genommen“ markiert.
- **Auswirkung auf Testergebnisse:** Wenn der Status eines DI auf „CI außer Betrieb genommen“ aktualisiert wird, wird die zugehörige TR geschlossen und der Abschnitt „Notizen“ wird automatisch aktualisiert.

**Hinweis:**
Der Status eines DI wird automatisch auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Dagegen wird der Status einer TR nur dann auf Geschlossen aktualisiert, wenn die Eigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** auf true gesetzt ist. Weitere Informationen zum automatischen Schließen der zugeordneten TRs finden Sie unter Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen.

Die regelmäßige Aufgabe `Close Test Results for decommissioned CIs` wird täglich für die aktualisierten DIs ausgeführt. Wenn die Konfigurationsoption für das automatische



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließen für stillgelegte CIs aktiviert ist, wird der DI identifiziert, der ein stillgelegtes CI enthält, und die zugehörige TR wird mit dem Substatus „CI stillgelegt“ geschlossen. Wenn alle TRs in einer Testergebnisgruppe geschlossen sind und ihr Substatus „CI außer Betrieb genommen“ ist, wird die Testergebnisgruppe ebenfalls mit dem Substatus „Abgebrochen“ geschlossen.

**Hinweis:**
Wenn ein CI aus dem Status „Deaktiviert“ in den ursprünglichen Status zurückversetzt wird, wird auch der Eintrag „Erkannte Elemente“ aktualisiert. TRs werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

### Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch schließen

Wenn Configuration Management Database (CMDB) den Lebenszyklusphasenstatus eines Konfigurationselements (CI) in „Deaktiviert“ ändert, können Sie die zugehörigen Testergebnisse (TRs) automatisch schließen.

#### Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Um die zugeordneten TRs automatisch zu schließen, müssen Sie die Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** aktivieren, um TRs, die stillgelegten CIs zugeordnet sind, automatisch zu schließen. Wenn diese Option aktiviert ist, werden neue und vorhandene TRs, die für dasselbe CI gemeldet werden, automatisch erstellt oder im Status „Geschlossen“ aktualisiert. Diese basieren auf der Asset-ID in der Scanner-Nutzlast und dem Eintragsstatus „Erkannte Elemente“. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit deaktivierten Konfigurationselementen in Configuration Compliance.

**Hinweis:**
Der Status eines DI wird auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Dagegen wird der Status einer TR nur dann auf „Geschlossen“ aktualisiert, wenn die Systemeigenschaft „ **sn_vulc.auto_close_test_results_linked_to_retired_CIs** “ aktiviert ist.

#### Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** und filtern Sie nach `sn_vulc.auto_close_test_results_linked_to_retired_CIs` in der Spalte Name.
2. Wählen Sie die Eigenschaft aus.
3. Um Testergebnisse, die den stillgelegten CIs zugeordnet sind, automatisch zu schließen, legen Sie den Wert der Eigenschaft auf true fest.

## Veraltete Testergebnisse in werden automatisch geschlossen Configuration Compliance

Sie können die Funktion „Veraltete Testergebnisse automatisch schließen“ aktivieren, um ältere Testergebnisse, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden, automatisch zu schließen. Wenn Sie diese Testergebnisse in den Status „ **Geschlossen – Veraltet“ verschieben**, wird die Anzahl der aktiven Testergebnisse und Testergebnisgruppen in Ihrer Instanz reduziert, und Sie können Assets in Configuration Management Database (CMDB)abgleichen .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Übersicht

Das Modul „Veraltete Testergebnisse automatisch schließen“ hilft Ihnen, ältere, veraltete Testergebnisse, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden, automatisch zu schließen. Testergebnisse werden basierend auf den Bedingungen, die Sie im Bedingungsgenerator festgelegt haben, in den Status „ **Geschlossen – Veraltet** “ verschoben.

## Wichtige Begriffe

**Testergebnis**

Testergebnisse sind importierte Ergebnisse aus Bibliotheken von Konfigurationstests, die Frameworks, Richtlinien und autoritativen Quellen zugeordnet sind, die definieren, wie eine Klasse von Technologie-Assets verwaltet werden soll. Die Anwendung Configuration Compliance berechnet die Testergebnisse nicht, sondern importiert sie mit Integrationen von Drittanbietern.

**Datum des letzten Scans des Assets**

Bezieht sich auf den Wert in der Spalte „Datum des Compliance-Scans der letzten Konfiguration“ der Tabelle „Erkanntes Element“, der sich auf das Testergebnis bezieht. Dieses Datum bezieht sich auf das aktuelle Datum und die aktuelle Uhrzeit, zu der ein Asset zuletzt von einem Drittanbieter-Scanner gescannt wurde.

**Datum des letzten Fehlers**

Bezieht sich auf das Datum der Spalte „Zuletzt angezeigt“ der Tabelle „Testergebnisse“, wenn der **Feldwert Ergebnis** [failed] ist.

**Veraltete Testergebnisse**

Bezieht sich auf Testergebnisse in Ihrer Instanz, die veraltet sind und seit längerer Zeit nicht mehr gefunden, aktualisiert oder von Integrationsscans von Drittanbietern erkannt wurden.

**Zuletzt gefundene Testergebnisse**

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner einer Drittpartei bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuelle oder letzte Datum (vor Tagen), an dem Testergebnisse erneut vom Scanner gefunden wurden. Dieser Parameter kann konfiguriert werden.

## Anwendungsfall

Manchmal werden Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Scannern von Drittanbietern gelöscht. In diesem Fall werden die den Assets zugeordneten Konfigurationstestergebnisse in der Anwendung Configuration Compliance nicht durch importierte Erkennungen aktualisiert und inaktiv (veraltet).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Anzahl der aktiven Testergebnisse (TRs) und Testergebnisgruppen (TRGs) in Ihrer Instanz zu reduzieren, aktivieren Sie die Funktion Veraltete Testergebnisse automatisch schließen. Diese Funktion schließt veraltete Testergebnisse automatisch, die unveränderte Status haben oder kürzlich nicht von Ihren Integrationen importiert wurden.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) verfügt über mehrere Asset-IDs, und eine dieser IDs wurde in den letzten 90 Tagen nicht bei Erkennungen von einem Drittanbieter-Scanner importiert. Wenn Sie den Bedingungsgenerator im Modul Veraltete Testergebnisse automatisch schließen so einstellen, dass Testergebnisse geschlossen werden, die in den letzten 90 Tagen oder mehr nicht gefunden oder aktualisiert wurden, schließt diese Funktion automatisch alle Testergebnisse, die dieser Filterung entsprechen.

**Hinweis:**
Diese Funktion schließt Testergebniserkennungen nur basierend auf den Filterbedingungen, die Sie im Bedingungsgenerator festgelegt haben und die von Ihren Scanner-Integrationen einer Drittpartei erkannt werden.

## Das Feld Auflösung

Um zwischen den Erkennungen zu unterscheiden, die von Scannern von Drittanbietern wie den Produkten Qualys und Tenable.io und der Funktion „Veraltete Testergebnisse automatisch schließen“ in Ihrer Instanz geschlossen werden, wurde der neue Wert für das Feld **Auflösung**, [Closed-Stale], hinzugefügt wurde hinzugefügt. **Geschlossen – Veraltet** gibt an, dass eine TR durch die Funktion zum automatischen Schließen geschlossen wurde. „**Geschlossen** “ oder „ **Fest geschlossen** “ gibt an, dass ein TR von einem Scanner geschlossen wurde.

## Rollup von TR-Status zu TRGs mit der Funktion „Automatisch schließen“.

Der Statusverlauf und die Rangfolge für Testergebnisse sind: **Offen** > **Geschlossen** > **Fest – Geschlossen** > **Geschlossen – Veraltet**.

1. Wenn TRs in einer TRG **Offen**sind, wird der TRG-Status nicht geändert.
2. Wenn mindestens eine TR „ **Geschlossen – Repariert“** und die restlichen **„Geschlossen – Veraltet“**sind, geht der TRG-Status in „ **Geschlossen – Repariert“**über.
3. Wenn alle TRs in einer TRG **Geschlossen – Veraltet**sind, geht der TRG-Status in **Geschlossen – Abgebrochen**über.

## Unterstützte Integrationen

Weitere Informationen zu den Integrationen von Drittanbietern, die diese Funktion unterstützen, finden Sie unter Qualys Vulnerability Integration verstehen und Tenable.io Integrationen mit den Anwendungen Vulnerability Response und Configuration Compliance ..

### Verwenden Sie Veraltete Testergebnisse automatisch schließen in Configuration Compliance

Aktivieren Sie Veraltete Testergebnisse (TRs) automatisch schließen, um ältere Testergebnisse basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

**Vorbereitungen**
Weitere Informationen zu dieser Funktion, zu wichtigen Begriffen und zu allen Setups, die möglicherweise für Ihre Drittanbieterintegrationen erforderlich sind, die Testergebnisdaten importieren, finden Sie unter Veraltete Testergebnisse in werden automatisch geschlossen Configuration Compliance.

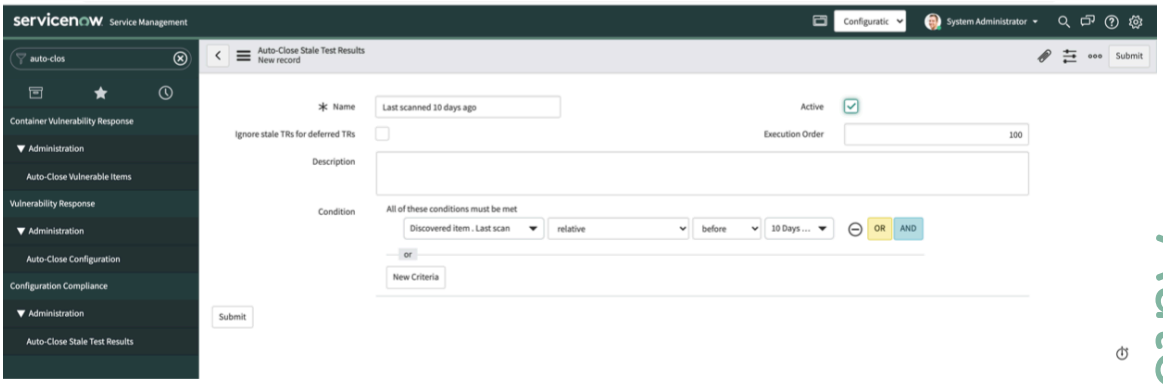


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vulc.admin

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Administration** > **Veraltete Testergebnisse automatisch schließen**.
2. Füllen Sie die Felder des Formulars aus.




| Feld | Wert |
|---|---|
| Name | Name für diesen Konfigurationsdatensatz. |
| Aktiv | Wenn diese Option ausgewählt ist, ist dieser Datensatz aktiv und es werden automatisch alle Testergebnisse geschlossen, die den Filterkriterien entsprechen. |
| Veraltete TRs für zurückgestellte TRs ignorieren | Wenn diese Option ausgewählt ist, werden alle **TRs**, die den Status „Wird **überprüft“** oder „Zurückgestellt“ zugeordnet sind, ignoriert und nicht geschlossen. Wenn Sie diese Option deaktivieren, werden alle TRs, die Ihren Kriterien entsprechen, geschlossen. |
| Ausführungsbefehl | 100 ist der Standardwert. Dieser Wert bestimmt die Ausführungsreihenfolge in aufsteigender Reihenfolge für jeden Konfigurationsdatensatz, der zum Suchen und Markieren von veralteten Testergebnissen verwendet wird. |
| Beschreibung | Eine Beschreibung für diesen Datensatz. Dieser Text kann Ihnen helfen, sie leicht wiederzufinden, wenn Sie eine größere Anzahl von Datensätzen erstellen. |
| Bedingung | Die Filterbedingungen, die für die Suche nach TRs verwendet werden, die geschlossen werden sollen. Der Standardfilter ist **Erkanntes Element** > **Zuletzt gescannt** > . |

3. Klicken Sie auf **Absenden**.

Die regelmäßige Aufgabe *`Auto-Close Stale Test Results`*wird täglich ausgeführt. Dieser Auftrag identifiziert die TRs basierend auf den von Ihnen angegebenen Bedingungen und überführt diejenigen, die übereinstimmen, in **Geschlossen – Veraltet**.

Nachdem TRs als **Closed-Stale**markiert wurden und der Scanner diese TRs erneut findet, werden die Testergebnisse erneut geöffnet, und die Status gehen in**Open**über.

Wenn eine TR als **Geschlossen – Veraltet**markiert ist und der Scanner feststellt, dass sie repariert wurde, wechselt die TR zu**Geschlossen – Repariert**. Für Status wird auch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein Rollup zu Testergebnisgruppen (TRGs) durchgeführt, wie in der folgenden Liste beschrieben:

a. Wenn TRs in einer TRG **Offen**sind, wird der TRG-Status nicht geändert.

b. Wenn mindestens eine TR „ **Geschlossen – Repariert“** und die restlichen **„Geschlossen – Veraltet“**sind, geht der TRG-Status in „ **Geschlossen – Repariert“**über.

c. Wenn alle TRs in einer TRG **Geschlossen – Veraltet**sind, geht der TRG-Status in **Geschlossen – Abgebrochen**über.

## Schließen Sie eine Testergebnisgruppe

Wenn Sie der Meinung sind, dass das einer Testergebnisgruppe zugeordnete Problem sofort ohne weitere Analyse geschlossen werden kann, können Sie die Funktion **Schließen** verwenden.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin
- sn_vulc.remediation_owner

**Hinweis:**
Mit der Rolle „sn_vulc.remediation_owner“ können Sie Testergebnisgruppen, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind, neu zuweisen oder schließen.

### Prozedur

1. Öffnen Sie den Datensatz der Testergebnisgruppe.
2. Klicken Sie auf die Schaltfläche **Schließen**.
3. Beschreiben Sie, warum das Problem im Popup-Fenster geschlossen wird.
4. Klicken Sie auf **Schließen**.

#### Zugehörige Informationen

Configuration Compliance Status

## Eine Ausnahme für eine Testergebnisgruppe anfordern und genehmigen

Sie können anfordern, dass die Korrektur einer Testergebnisgruppe für einen bestimmten Zeitraum zurückgestellt wird. Benutzer, die Teil der Genehmigergruppe sind, können Ausnahmeanforderungen genehmigen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Anfordern oder Genehmigen von Ausnahmeanforderungen finden Sie unter:

- Fordern Sie eine Ausnahme für eine Testergebnisgruppe in an Configuration Compliance
- Genehmigen Sie eine Ausnahmeanforderung in Configuration Compliance

**Hinweis:**

E-Mail-Benachrichtigungen werden in jeder Phase der Ausnahmeverwaltung gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, in der bestätigt wird, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, dass eine Ausnahme angefordert wurde.

Ab v14.11 von Configuration Compliancekönnen Sie die Zeitrahmen für die Genehmigung von Ausnahmen zusammen mit E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer bestimmten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das Testergebnis in den Status Wird überprüft, und ein Status-Change-Datensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das Testergebnis auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird im Feld **„backup_state“** gespeichert. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für Exception Management.

### Fordern Sie eine Ausnahme für eine Testergebnisgruppe in an Configuration Compliance

Fordern Sie eine Ausnahme an, um die Korrektur einer Testergebnisgruppe für einen bestimmten Zeitraum zurückzustellen, wenn sie nicht sofort korrigiert werden kann.

#### Vorbereitungen

Erforderliche Rolle: sn_vulc.remediation_owner

#### Warum und wann dieser Vorgang ausgeführt wird

Ab Version 19.0 von Vulnerability Responsekönnen Sie Ausnahmen für Testergebnisgruppen im IT-Korrekturarbeitsbereich anfordern. Weitere Informationen zum Anfordern von Ausnahmen für Testergebnisse im IT-Korrekturarbeitsbereich finden Sie unter Fordern Sie eine Ausnahme in an IT Remediation Workspace.

**Hinweis:**

Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

#### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisgruppen** > **Alle Gruppen**.
2. Wählen Sie die Testergebnisgruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Klicken Sie im Formular „Testergebnisgruppe“ auf **Ausnahme anfordern**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Abhängig davon, ob Vulnerability Response oder GRC: Policy and Compliance Management im ausgewählt ist **Configuration Compliance** > **Ausnahmenverwaltung** Im Bildschirm „“ ändert sich das Formular „Ausnahme anfordern“. Siehe Konfigurieren Sie Exception Management für Configuration Compliance

4. Wenn Vulnerability Response im Bildschirm „Exception Management“ ausgewählt ist, gehen Sie wie folgt vor:

   a. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Bis | Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der im ausgewählten Zeitraum liegen **Alle** > **Configuration Compliance** > **Administration** > **Ausnahmenverwaltung** -Bildschirm.<br><br>Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „Offen“ zurück.<br><br>**Hinweis:**<br>Wenn ab Version 14.7 von Configuration Compliance (CC) eine zurückgestellte Testergebnisgruppe von einem Scanner erneut geöffnet wird, bevor das Ausnahmefenster abläuft, ändert sich der Status der Testergebnisgruppe von Offen in Zurückgestellt. Diese Funktionalität ist standardmäßig deaktiviert. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft `sn_vulc.auto_defer_test_result_in_active_exc` auf „true“ fest. Außerdem bleibt das Datum für „Zurückgestellt bis“ erhalten, auch nachdem die Testergebnisgruppe nach dem Ablaufdatum erneut geöffnet wurde. |
| Grund | Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt:<br>▪ Risiko akzeptiert<br>▪ Warten auf Wartungsfenster<br>▪ Behebung nicht verfügbar<br>▪ Ausgleichende Steuerung vorhanden<br>▪ Sonstige<br><br>Informationen zum Hinzufügen neuer Grundoptionen finden Sie unter Definieren Sie Richtliniengrundzuordnungen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zusätzliche Informationen | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden. |

**b.** Senden Sie die Ausnahmeanforderung, indem Sie auf **Genehmigung**anfordern klicken.

### Ergebnisse
Der Status der Testergebnisgruppe ändert sich in Wird überprüft. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

## Fordern Sie eine Verlängerung für eine Testergebnisgruppe an

Fordern Sie eine Verlängerung für eine zurückgestellte Testergebnisgruppe an, bevor das Fälligkeitsdatum erreicht ist. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

### Vorbereitungen
Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.admin (veraltet)

### Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Prozedur
1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisgruppe**.
2. Öffnen Sie eine zurückgestellte Testergebnisgruppe.
3. Wählen Sie **Verlängerung anfordern aus**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Testergebnisgruppe erneut aktiviert wird. |
| Grund | Geben Sie den Grund für das Zurückstellen des Problems ein. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Zur Auswahl stehen:<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Risiko akzeptiert<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Die Schaltfläche Verlängerung anfordern ist für Testergebnisgruppen, die als Teil einer Ausnahmeregel erstellt werden, nicht verfügbar.
- Wenn eine zurückgestellte Testergebnisgruppe erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Configuration Compliance

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie ihr Fälligkeitsdatum erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.exception_approver

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Verlängerung auch über die Vulnerability Response Arbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Arbeitsbereich von Vulnerability Manager an.

**Hinweis:**

Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

#### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Ausnahmeregeln**.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie **Verlängerung anfordern aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Verlängern bis | Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel verlängert werden muss. |
| Grund | Geben Sie den Grund für das Zurückstellen der Ausnahmeregel ein.<br>Zur Auswahl stehen:<br>○ Risiko akzeptiert<br>○ Warten auf Wartungsfenster<br>○ Korrektur nicht verfügbar<br>○ Ausgleichende Kontrolle vorhanden<br>○ Sonstige |
| Zusätzliche Informationen | Geben Sie andere relevante Informationen ein. |

5. Wählen Sie **Genehmigung anfordern**.
Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und Zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Testergebnisgruppen aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion des Genehmigers ausgelöst.

**Hinweis:**

- Die Anforderung durchläuft zwei Genehmigungsstufen.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Erweiterungszurückstellungen im Back-End.

### Fordern Sie mit eine Ausnahme für Testergebnisgruppen an GRC: Policy and Compliance Management

Fordern Sie Richtlinienausnahmen mit der Funktion GRC zur Verwaltung von Richtlinienausnahmen in der Anwendung Policy and Compliance Management aus Configuration Complianceanan.

### Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen zum Anfordern von Richtlinienausnahmen verwenden können, müssen Sie die Anwendung GRC: Policy and Compliance Management aus dem ServiceNow Storeherunterladen.

Erforderliche Rolle: sn_vulc.remediation_owner

Sie können Ausnahmen auch in der klassischen Benutzeroberfläche anfordern.

### Warum und wann dieser Vorgang ausgeführt wird

Ab Version 19.0 von Vulnerability Responsekönnen Sie Richtlinienausnahmen für Testergebnisgruppen (TRGs) im IT-Korrekturarbeitsbereich anfordern. Weitere Informationen finden Sie unter Ausnahme mit GRC: Policy and Compliance Management in IT Remediation Workspaceanfordern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (oder **Korrekturaufgaben**)>**Alle**, und öffnen Sie das Element oder die Gruppe, für die Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „Wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme anfordern**.
3. Wenn GRC: Policy and Compliance Management im Bildschirm „Exception Management“ ausgewählt ist, gehen Sie wie folgt vor.

   a. Füllen Sie die Felder des Formulars aus.

**Formular „Ausnahme anfordern“.**

| Feld | Beschreibung |
|---|---|
| Richtlinie | Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern. |
| Kontrollziel | Kontrollziele, die der ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet. |
| Gültig ab | Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen. |
| Gültig bis | Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von „Zurückgestellt“ in „Offen“ geändert wird<br>**Hinweis:**<br>Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf die **maximale Ausnahmedauer (Tage)** nicht überschreiten, die Sie für die Richtlinie in Policy and Compliance festgelegt haben. Weitere Informationen finden Sie unter Richtlinie erstellen. |
| Grund | Grund für die Anforderung einer Ausnahme. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Begründung | Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden. |

**b.** Senden Sie die Ausnahmeanforderung, indem Sie auf **Genehmigung**anfordern klicken.
Der Status der Testergebnisgruppe ändert sich in Wird überprüft, und eine Richtlinienausnahme wird erstellt. Verwenden Sie die Registerkarte Statusänderungsgenehmigung, um den Status der Ausnahmeanforderung **nachzuverfolgen**.

**c.** Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

**d.** Klicken Sie auf die Nummer der Richtlinienausnahme.

**e. Wählen Sie** im Feld Genehmiger den Namen des Genehmigers aus.

**f.** Klicken Sie auf die Registerkarte Quelle, und wählen Sie im Feld **Kontrollziel** ein Kontrollziel aus.

**g.** Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie im Feld Risikobewertung die **Risikobewertung** aus.

**h.** Speichern Sie das Formular.

**i.** Klicken Sie auf die Registerkarte **Betroffene Steuerungen**.

**j.** Fügen Sie die Steuerungen hinzu, indem Sie auf **Hinzufügen**klicken.

**k.** Speichern Sie das Formular.

**Hinweis:**
Sie können eine Compliance-Überprüfung durchführen, indem Sie auf **Compliance-Überprüfung anfordern**klicken.

Das Genehmigungsformular wird an den Genehmiger gesendet.

Der Genehmiger kann die Anforderung entweder genehmigen, indem er auf **Genehmigen klickt**, oder eine zusätzliche Genehmigung anfordern, indem er auf **Zusätzliche Genehmigung**anfordern klickt.

Der Datensatzstatus ändert sich in „Zurückgestellt“. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte **Zurückstellung** enthält zusätzliche Hinweise zum Datensatz.

**Hinweis:**
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

**4.** Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Verantwortlichen für die Fehlerkorrektur und dem Compliance-Manager finden Sie unter Optionales Setup für Policy and Compliance Management .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Genehmigen Sie eine Ausnahmeanforderung in Configuration Compliance

Genehmigen Sie Ausnahmeanforderungen für Testergebnisgruppen, die nicht sofort korrigiert werden können. Sie müssen diese Anforderungen auf Risiken bewerten und sie dann zur Zurückstellung genehmigen, bis sie korrigiert werden können.

#### Vorbereitungen

Erforderliche Rolle: sn_vulc.exception_approver

#### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Meine Freigaben**.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit den entsprechenden Kommentaren ab.

**Hinweis:**
Bei einem zweistufigen Genehmigungsworkflow wird die Anforderung nach der Genehmigung auf der ersten Ebene zur weiteren Genehmigung an die zweite Ebene übermittelt. Wenn sich keine Benutzer auf der zweiten Ebene befinden, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

Nachdem die Anforderung genehmigt wurde, wird die Testergebnisgruppe in den Status „Zurückgestellt“ verschoben. Im Falle einer Ablehnung wird die Testergebnisgruppe in ihren vorherigen Status zurückgesetzt.

### Definieren Sie Richtliniengrundzuordnungen

Sie können die Grundoptionen so definieren, dass sie jedem Benutzer zur Verfügung stehen, der eine Ausnahme anfordert.

#### Vorbereitungen

Erforderliche Rolle: sn_vul.compliance.manager und sn_vulc.admin

#### Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**.

**Hinweis:**
Sie können entweder einen Grund aus den in der Tabelle „Grundauswahlmöglichkeiten“ verfügbaren Gründen auswählen oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung „Container Vulnerability Response – CVIT“.
3. Führen Sie die folgenden Schritte aus, um eine vorhandene Grundauswahl hinzuzufügen:
   a. Klicken Sie in der Liste Grundauswahl auf **Neu**.
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Führen Sie die folgenden Schritte aus, um der Tabelle „Grundauswahlmöglichkeiten“ neue Gründe hinzuzufügen:
   a. Klicken Sie in der Liste Grundauswahl auf **Neu**.
   b. Klicken Sie auf das Lupensymbol.
   c. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**d.** Füllen Sie die Felder des Formulars aus.

**Formular „Grundauswahlliste“**

| Feld | Beschreibung |
|---|---|
| Bezeichnung | Eindeutige Bezeichnung für diese Auswahl. |
| Wert | Eindeutiger Wert für diese Auswahl.<br><br>Dieser Wert wird in der Tabelle „Richtlinienausnahme – Grundzuordnungen“ für die entsprechenden Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie im Filternavigator sn_sec_cmn_policy_reason_mapping.LIST ein. |
| Bestellung | Reihenfolge für diese Auswahl. Die Gründe werden basierend auf dieser Nummer sortiert. |
| Standard | Option, um anzugeben, dass diese Grundauswahl immer dann verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, sind alle Grundoptionen verfügbar, für die das Feld **Standard** ausgewählt ist. |
| Aktiv | Option zum Anzeigen der Auswahl in der Liste der Grundoptionen. |

**5.** Klicken Sie auf **Absenden**.

## Berichterstellung und Analytics für Configuration Compliance

Die folgenden Berichte werden für die Überwachung bereitgestellt.

Zeigen Sie Richtlinien, CIs, Tests und Testergebnisse in den Übersichtsberichten von Configuration Compliance an.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Configuration Compliance Berichterstellung

Die Configuration Compliance -Homepage bietet einen Überblick über Richtlinien, CIs, Tests und Testergebnisse, sodass Sicherheitsmitarbeiter Problembereiche schnell erkennen können. Configuration Compliance Signifikanzdiagramme können nach Bedarf hinzugefügt werden. Sie können auch Configuration Compliance -bezogene Informationen über die globale Suchfunktion zurückgeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

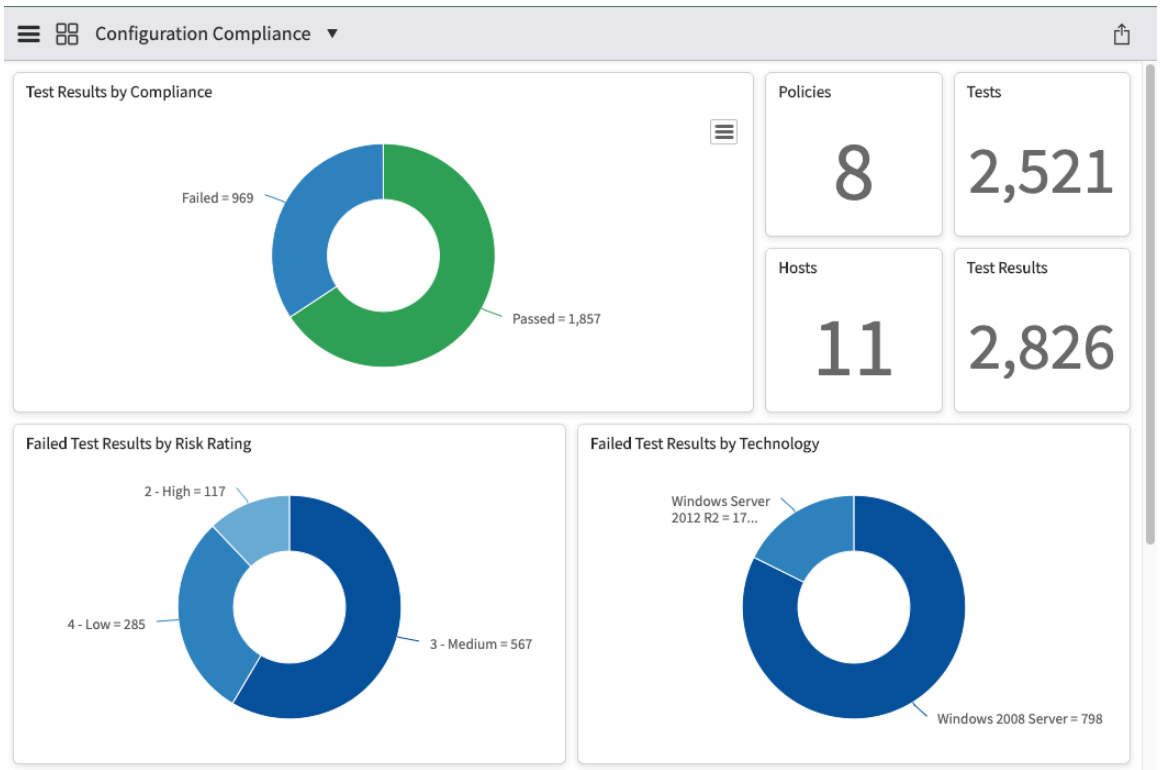
### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt) zeigen, um allgemeine Daten anzuzeigen, die für diesen Teil des Diagramms spezifisch sind. Wenn Sie auf einen beliebigen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

**Hinweis:**
Jeder mit der Rolle „sn_vulc.read“ kann das Dashboard anzeigen. Jeder mit der Rolle „sn_vulc.write“ oder „sn_vulc.admin“ kann ein Dashboard erstellen und bearbeiten. Nur sn_vulc.admin kann ein Dashboard löschen.

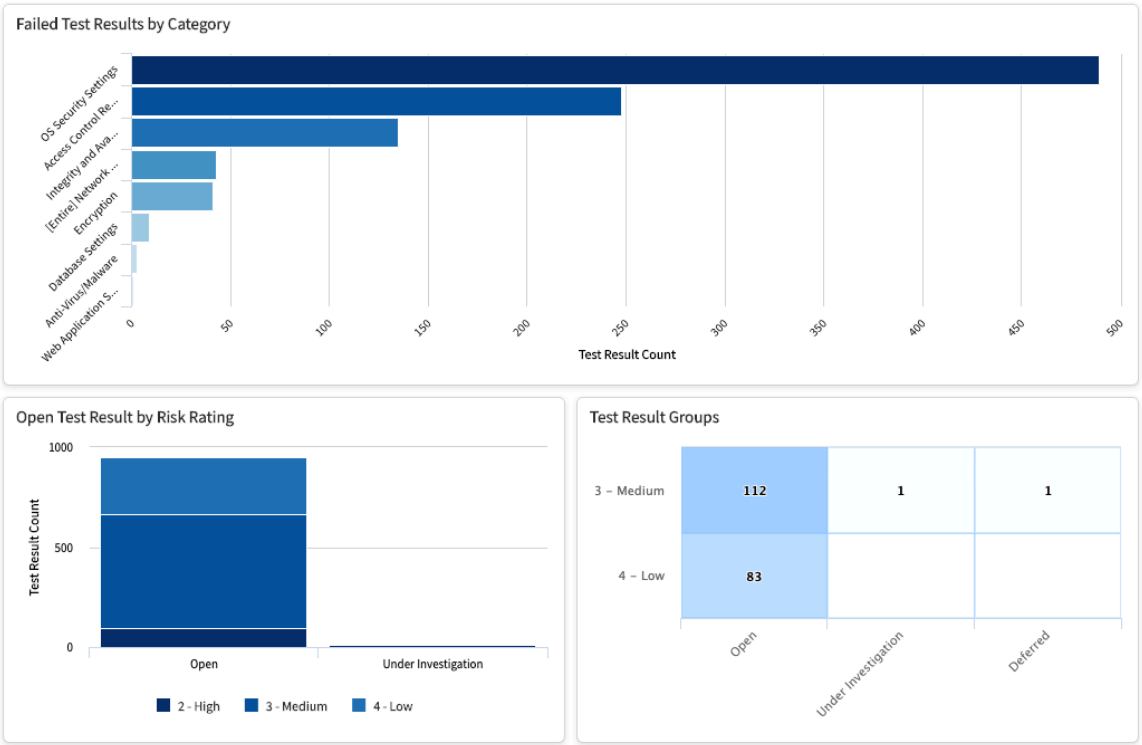
### Schwachstellenübersichtsberichte






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Configuration Compliance-Bericht




## Schwachstellenübersichtsberichte

| Name | Visuell | Beschreibung |
|---|---|---|
| Testergebnisse nach Compliance | Ring | Zeigt die Anzahl der offenen Tests an, die bestanden wurden oder fehlgeschlagen sind. |
| Richtlinien | Nummer | Anzahl der Richtlinien mit fehlgeschlagenen Testergebnissen. |
| Tests | Nummer | Anzahl der Tests mit fehlgeschlagenen Testergebnissen. |
| Hosts | Nummer | Anzahl der Hosts mit fehlgeschlagenen Testergebnissen. |
| Testergebnisse | Nummer | Zeigt die Anzahl der Testergebnisse an. |
| Ergebnisse fehlgeschlagener Tests nach Risikobewertung | Ring | Zeigt die Anzahl der fehlgeschlagenen Tests nach Risikobewertung an. |
| Ergebnisse fehlgeschlagener Tests nach Technologie | Ring | Zeigt Modelle mit fehlgeschlagenen Tests an. |
| Ergebnisse fehlgeschlagener Tests nach Kategorie | Balkendiagramm | Zeigt Kategorien mit den meisten fehlgeschlagenen Testergebnissen an. |
| Offenes Testergebnis nach Risikobewertung | Balkendiagramm | Zeigt die Anzahl der offenen Testergebnisse nach Risikobewertung an. |
| Testergebnisgruppen | Diagramm | Zeigt Testergebnisgruppen nach Status und Risikobewertung an. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Configuration Compliance -Dashboard

Dieser Platform Analytics-Lösung enthält vorverpackte Performance Analytics - und Reporting -Inhalte zur Verwendung mit anderen Now Platform -Produkten. Dieser Platform Analytics-Lösung bietet Einblick in nicht konforme Konfigurationen auf Hostebene und Cloud-Steuerungsebene.

Diese Platform Analytics-Lösung enthält vorgefertigte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Diese Platform Analytics-Lösung bietet Einblick in nicht konforme Konfigurationen auf Hostebene und Cloud-Steuerungsebene.

Das Dashboard „Performance Analytics für Konfigurations-Compliance“ enthält mehrere Widgets, die Daten für verschiedene Dimensionen darstellen. Sie bietet einen umfassenden Überblick über Compliance-Trends, Konfigurationsprobleme, Korrekturtrends und Ausnahmemanagement.

**Hinweis:**
Das Plugin Performance Analytics für Configuration Compliance muss installiert sein, um das Dashboard Next ExperienceConfiguration Compliance [PA] im Framework [] anzuzeigen. Wenn nicht installiert ist, können Sie das vorhandene Dashboard anzeigen, das mit dem Reporting-Framework erstellt wurde.

### Performance Analytics für Configuration Compliance aktivieren

Aktivieren Sie die Inhaltspaketanwendung ServiceNow Store für Platform Analytics-Lösung.

#### Vorbereitungen

Aktivieren Sie die vollständige Abonnementversion von Performance Analytics für die Instanz, auf der Sie diese Now Intelligence-Lösung aktivieren. Sie können Performance Analytics in einer Instanz außerhalb der Produktion aktivieren, ohne ein Abonnement zu erwerben. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Sie benötigen einen Now Support -Account und die Berechtigung, um Anwendungen für die betreffenden Instanzen anzufordern. Das Konto Now Support und die Instanz müssen zum selben Unternehmen gehören. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.

Erforderliche Rolle: admin

#### Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Performance Analytics für das Dashboard Configuration Compliance, um Berichte über die Testergebnisgruppen, den Compliance-Status, die Korrekturaktionen und die Ausnahmeanforderungen zu generieren.

#### Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**.
2. Suchen Sie Performance Analytics nach Configuration Compliance und vergewissern Sie sich, dass Sie über die gültigen Berechtigungen verfügen.
3. Suchen Sie nach Performance Analytics für Configuration Compliance.
4. Installieren Sie die Anwendung.

   Wenn Sie diese Anwendung installieren, aktivieren Sie auch die Anwendung Configuration Compliance.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Anzeigen des Dashboards Performance Analytics für Configuration Compliance .

Sie können Ihre wichtigsten Konfigurationsprobleme verwalten und schnell beheben, indem Sie die Berichte im Dashboard Configuration Compliance Performance Analytics (PA) anzeigen.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Erforderliche Now Platform-Rollen

Die folgenden Rollen sind für das Dashboard Configuration Compliance Performance Analytics erforderlich:

- admin: Ein Administrator kann Performance Analytics für Configuration Compliance installieren und aktivieren und Änderungen an den Systemeigenschaften vornehmen.
- pa_admin: Ein Performance Analytics-Administrator kann Hintergrundaufträge, Indikatoren, Aufgliederungen, Widgets und Dashboards erstellen und überprüfen. Dieser Administrator kann auch die Datenerfassung einrichten und starten.
- sn_vulc.read: Ein Benutzer mit der Leserolle kann die Dashboard-Daten überprüfen.

## Greifen Sie auf das Dashboard Configuration Compliance zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Configuration Compliance** > **Übersicht**.

Ab Version 14.9 von Configuration Compliancekann dieses Dashboard auch in der New Experience-UI angezeigt werden. Um das Dashboard in der neuen Benutzeroberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** und klicken Sie auf das**Dashboard-** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboardübersicht und Dashboardübersicht.

**Hinweis:**
Wenn Sie Tokyoverwenden, können Sie die Dashboards in der Next Experience-UI anzeigen, jedoch mit einigen Funktionsverlusten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Configuration Compliance [PA] Dashboard-Registerkarten

### Registerkarte „Übersicht“

Die Registerkarte **Übersicht** enthält fünf Filter. Diese Filter sind Asset-Kategorie, Cloud-Ressourcentyp, Cloud-Service-Provider, Cloud-Konto und Cloud-Region, die Sie anwenden können, um die Berichte für die angewendeten Filter zu visualisieren. Wenn Sie eine Kategorie auswählen und die Änderungen anwenden, werden alle Widgets aktualisiert, die die Kategorie unterstützen. Jedes Widget zeigt unten den angewendeten Filter und die Anzahl der angewendeten Filter auf dem Filtersymbol des Widget an. Klicken Sie in einem Widget auf den Bericht, um die zusätzlichen Informationen auf der Registerkarte **KPI-Details** anzuzeigen. Auf der Registerkarte „ **KPI-Details** “ können Sie:

- Zeigen Sie die Datensätze an.
- Vergleichen Sie die Datensätze.
- Ändern Sie den Diagrammtyp.
- Wählen Sie den Datumsbereich aus.
- Zeigen Sie die Trends an, die auf der Dauer basieren.
- Wenden Sie die zusätzlichen Filter an, einschließlich der Filter, die auf der Registerkarte **Übersicht** nicht verfügbar sind. Ein Beispiel ist das Host-Tag.

Das folgende Beispiel zeigt, wie Sie die Filter auf der Registerkarte „ **Übersicht** “ anwenden und die Aktionen auf der Registerkarte „ **KPI-Details** “ ausführen können.

Registerkarte „Übersicht“ im Dashboard „Configuration Compliance“

### Registerkarte „Compliance“.

Auf der Registerkarte **Compliance** wird der Compliance-Prozentsatz für die verschiedenen maßgeblichen Quellen angezeigt, z. B. Health Insurance Portability and Accountability Act (HIPAA) und Data Interchange Standards Association (DISA). Sie können diese Liste verfeinern, indem Sie die Spaltenheaderfilter verwenden und eine Kategorie auswählen.

Das folgende Beispiel zeigt, wie Sie die Daten auf der Registerkarte „ **Compliance** “ filtern können.

Registerkarte „Compliance“ im Dashboard „Configuration Compliance“

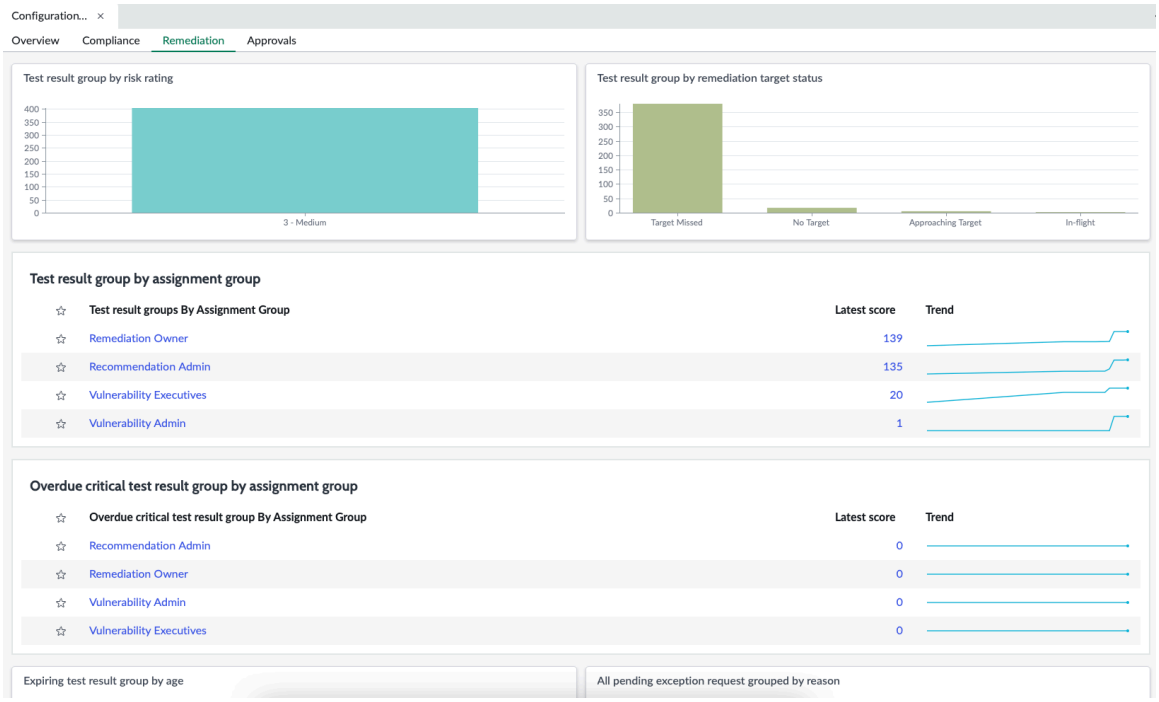


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Registerkarte „Remediation“

Auf der Registerkarte **Fehlerkorrektur** werden Informationen zum Fortschritt der Fehlerkorrektur angezeigt. Sie können diese Registerkarte verwenden, um sich die Hygiene der Korrektur von Fehlkonfigurationen anzusehen.

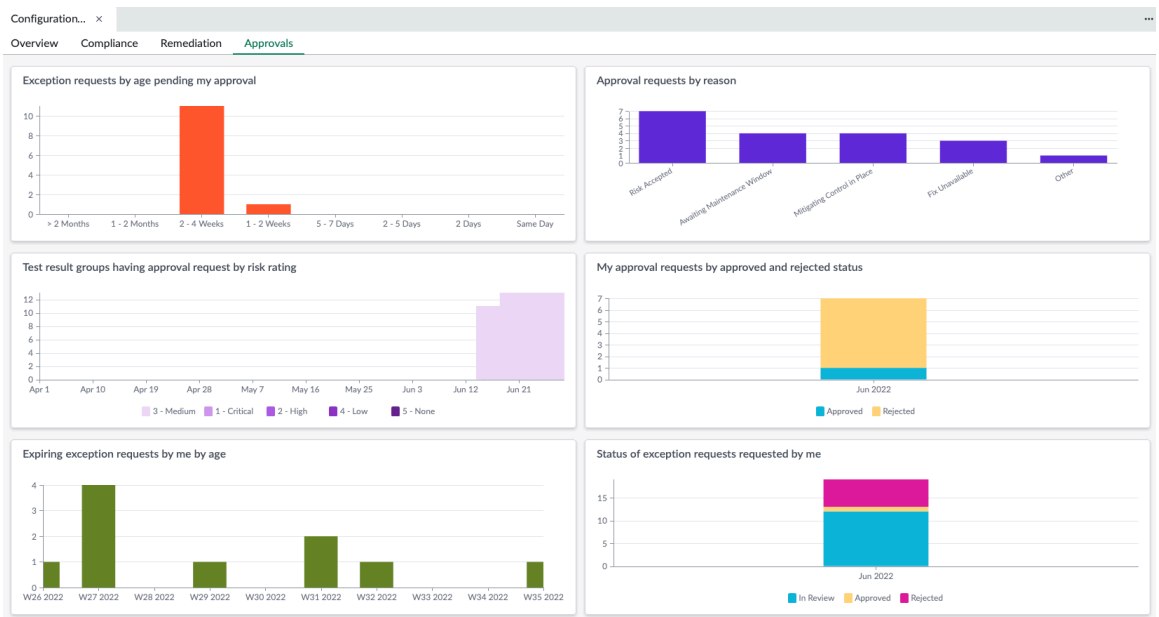
Das folgende Beispiel zeigt die Registerkarte **Fehlerkorrektur**.




## Registerkarte Genehmigungen

Die Berichte auf der Registerkarte **Genehmigungen** zeigen die Informationen zu den Ausnahmeanforderungen und deren Genehmigungsstatus an.

Das folgende Beispiel zeigt die Registerkarte **Genehmigungen**.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### BreakdownsAufgliederungen

Die folgenden Aufgliederungen werden von den Indikatoren verwendet:

- Grund für Zurückstellung
- Alter
- Zuweisungsgruppe
- Korrekturstatus
- Ergebnis
- Risikobewertung
- Asset-Kategorie
- Host-Tag
- Konfigurationstest
- Cloud-Service-Provider
- Cloud-Region
- Cloud-Account
- Cloud-Ressourcentyp

### Filter

Auf der Registerkarte **Übersicht** können Sie die folgenden Filter auf die Widgets anwenden, um die gefilterten Daten zu visualisieren.

| Name | Typ | Beschreibung |
|---|---|---|
| Asset-Kategorie | Auswahl | Art des Assets.<br>Die vier Optionen sind:<br>• Cloud<br>• Behälter<br>• Infra<br>• OT |
| Cloud-Ressourcentyp | Auswahl | Typ der Ressource. Ein Beispiel ist ein virtueller Computer.<br>Die Daten im Filter werden ausgefüllt, wenn Sie die Integration ausführen. |
| Cloud-Service-Provider | Auswahl | Service Provider für die Cloud.<br>Die drei Optionen sind: |



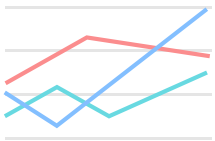
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Name | Typ | Beschreibung |
|---|---|---|
| | | • Amazon Web Services (AWS<br>• Microsoft Azure<br>• Google Cloud Platform (GCP) |
| Cloud-Account | Auswahl | Konto-ID, die erstellt wird, wenn ein Konto in einem Cloud-Service erstellt wird. Beispiel: AWS Die Konto-ID-Daten werden in den Filter eingetragen, wenn Sie die Integration ausführen. |
| Cloud-Region | Auswahl | Standort, an dem die Ressource gehostet wird |

**Hinweis:**
Sie können mehrere Optionen aus den Filtern auswählen und **Anwenden**auswählen. Jedes Widget zeigt die angewendeten Filter und die nicht angewendeten Filter an. Abhängig von den verfügbaren Daten wird der Bericht generiert. Das Widget zeigt auch die Anzahl der unterstützten Filter an.

## Datenvisualisierungen

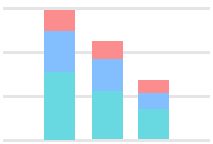
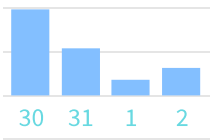
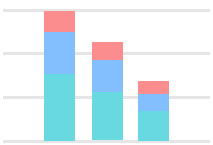
### Visualisierungen auf der Registerkarte „Übersicht“.

| Berichtname | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Compliance-Trend | Liniendiagramm  | Testergebnisse | Informationen zum Compliance-Trend:<br>• Ressourcen: Gesamtzahl der im System verfügbaren Ressourcen.<br>• Fehler: Anzahl der Ressourcen mit mindestens einem fehlgeschlagenen Testergebnis.<br>• Bestanden: Anzahl der Ressourcen, bei denen sich alle Testergebnisse im Status „Bestanden“ befinden. |
| Testergebnisgruppe | Einzelne Punktzahl | Testergebnisse | Anzahl der Testergebnisgruppen, die im System vorhanden sind und sich in einem aktiven Status befinden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Visualisierungen auf der Registerkarte „Übersicht“. (Fortsetzung)**

| Berichtname | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| | | | |
| In Kürze fällige kritische Testergebnisgruppen | Einzelne Punktzahl | Testergebnisse | Anzahl der Testergebnisgruppen, bei denen die Risikobewertung „Kritisch“ und der Korrekturstatus „Ziel erreicht“ ist. |
| Testergebnisse nach Risikobewertung | Balkendiagramm  | Testergebnisse | Testergebnisse im Status „Fehlgeschlagen“, gruppiert nach Risikobewertung. |
| Testergebnisse nach Alter | Balkendiagramm   | Testergebnisse | Testergebnisse im Status „Fehlgeschlagen“, gruppiert nach dem Zeitpunkt, zu dem die Testergebnisse erstellt wurden. |
| Geschlossene Testergebnisse nach Einhaltung des Korrekturziels | Balkendiagramm  | Testergebnisse | Testergebnisse im Status „Bestanden“, was darauf hinweist, dass dieser Test geschlossen ist. |
| Überfällige kritische Testergebnisse nach Zuweisungsgruppe | Liste und Punktzahl | Testergebnisse | Anzahl der Testergebnisse, bei denen die Risikobewertung „Kritisch“ und der Korrekturstatus „Ziel verfehlt“ ist. Der Bericht gibt an, dass sich die Testergebnisse im Status |

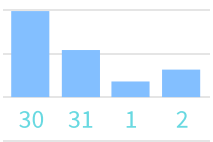


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Visualisierungen auf der Registerkarte „Übersicht“. (Fortsetzung)

| Berichtname | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| | | | „Offen“ befinden. Wenn die Testergebnisse das Korrekturzieldatum überschreiten, gilt dies als überfällig. |
| Überfällige Testergebnisse – Services | Liste, Punktzahl und Trend | PA-Dashboards-Datenbankansicht für Services | Anzahl der Testergebnisse für Services, bei denen der Korrekturstatus „Ziel verfehlt“ lautet. In diesem Bericht werden auch die Namen der Services oder Abteilungen mit den höchsten Testergebnissen angezeigt. |
| Überfällige Testergebnisse – Serviceverantwortliche | Liste, Punktzahl und Trend | PA-Dashboards-Datenbankansicht für Services | Anzahl der Testergebnisse für Serviceverantwortliche, deren Korrekturstatus „Ziel verfehlt“ ist. In diesem Bericht werden auch die Namen der Services oder Abteilungen mit den höchsten Testergebnissen angezeigt. |

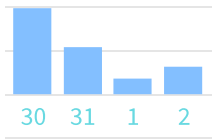
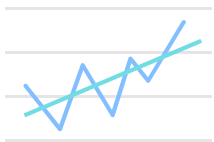
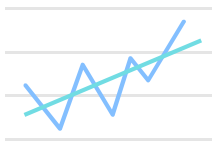
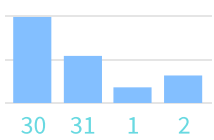
### Visualisierungen auf der Registerkarte „Korrektur“.

| Titel | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Testergebnisgruppe nach Risikobewertung | Balkendiagramm   | Testergebnisgruppe | Aufgliederung der Risikobewertungen aller Testergebnisgruppen, die sich im aktiven Status befinden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

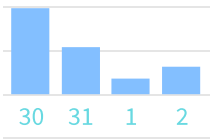
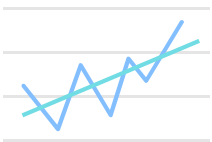
### Visualisierungen auf der Registerkarte „Korrektur“. (Fortsetzung)

| Titel | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Testergebnisgruppe nach Status des Korrekturziels | Balkendiagramm   | Testergebnisgruppe | Aufgliederung der Korrekturziele aller Testergebnisgruppen, die das Ziel verfehlt haben, kein Ziel haben und sich dem Ziel nähern. |
| Testergebnisgruppen nach Zuweisungsgruppe | Liste, Punktzahl und Trend  | Testergebnisgruppe | Aufgliederung der Testergebnisgruppen, die auf einer Zuweisungsgruppe basieren. |
| Überfällige kritische Testergebnisgruppen nach Zuweisungsgruppe | Liste, Punktzahl und Trend  | Testergebnisgruppe | Aufgliederung der Testergebnisgruppen, die auf einer Zuweisungsgruppe basieren. Diese Testergebnisgruppen haben die Risikobewertung „Kritisch“, und ihr Korrekturziel wurde nicht erreicht. |
| Ablaufende Testergebnisgruppen nach Alter | Balkendiagramm   | Testergebnisgruppe | Testergebnisgruppen, die innerhalb einer bestimmten Dauer ablaufen. Es können maximal 10 Dauer-Buckets erstellt werden. |

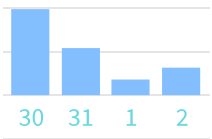
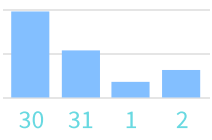
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Visualisierungen auf der Registerkarte „Korrektur“. (Fortsetzung)

| Titel | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Alle ausstehenden Ausnahmeanforderungen gruppiert nach Grund | Balkendiagramm   | Genehmigung der Statusänderung | Statusänderungs-Genehmigungsanforderungen, die nach dem Grund für die Ausnahme gruppiert sind. |
| Kritische Ausnahmen bei Testergebnissen nach Zuweisungsgruppe | Liste, Punktzahl und Trend  | Testergebnisse | Testergebnisse, die sich im Status „Zurückgestellt“ und „Kritisch“ befinden und basierend auf der Zuweisungsgruppe gruppiert sind. |

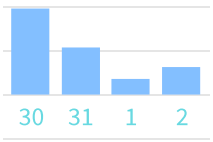
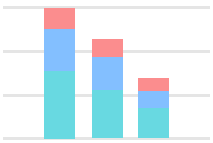
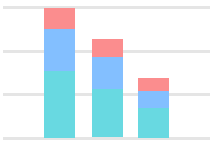
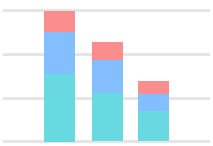
### Visualisierungen auf der Registerkarte „Genehmigungen“.

| Berichte | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| Ausnahmeanforderungen nach Alter, für die meine Genehmigung aussteht | Balkendiagramm   | Freigabe | Ausnahmeanforderungen, die von Ihnen erstellt werden und deren Genehmigung aussteht. Die Anforderungen werden nach der Dauer der Anforderung gruppiert. |
| Genehmigungsanforderungen nach Grund | Balkendiagramm   | Genehmigung der Statusänderung | Statusänderungsgenehmigungsanforderungen zum Erstellen einer Ausnahme, einschließlich des Grunds für die Ausnahme. |
| Testergebnisgruppen mit Genehmigungsanforderung nach Risikobewertung | Balkendiagramm | Testergebnisgruppe | Testergebnisgruppen mit einer Genehmigungsanforderung, |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Visualisierungen auf der Registerkarte „Genehmigungen“. (Fortsetzung)**

| Berichte | Typ | Quelltabelle | Beschreibung |
|---|---|---|---|
| |  | | die auf der Relevanz basiert. |
| Meine Genehmigungsanforderungen nach Status „Genehmigt“ und „Abgelehnt“ | Balkendiagramm  | Genehmigung der Statusänderung | Ausnahmeanforderungen, die nach den Status „Genehmigt“ und „Abgelehnt“ gruppiert sind. |
| Ablaufende Ausnahmeanforderungen von mir nach Alter | Balkendiagramm  | Genehmigung der Statusänderung | Ausnahmeanforderungen, die in den kommenden Wochen ablaufen. Die Ausnahmeanforderungen werden nach Wochen gruppiert.<br>Immer wenn eine Ausnahmeanforderung erstellt wird, wird ein Datum für die Gültigkeit der Ausnahmeanforderung ausgewählt. Die Berechnung des Alters der Anforderung basiert auf diesem Datum. |
| Status der von mir angeforderten Ausnahmeanforderungen | Balkendiagramm  | Genehmigung der Statusänderung | Von Ihnen erstellte Ausnahmeanforderungen, die nach den folgenden Status gruppiert sind:<br>• Wird überprüft<br>• Genehmigt<br>• Abgelehnt |

## Configuration Compliance Referenzinformationen

Bei der Aktivierung der Anwendung Configuration Compliance werden verschiedene Arten von Komponenten installiert, z. B. Tabellen, regelmäßige Aufgaben und Benutzerrollen.

Die folgenden Themen enthalten Referenzinformationen, Fehlerbehebung sowie Felddaten in den Formularen und Datensätzen in Configuration Compliance.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit Configuration Compliance installierte Komponenten
- Testergebnisfelder
- Configuration Compliance Importprobleme werden gelöst
- Ändern Sie das Startdatum der Qualys PC-Ergebnisse

## Zeigen Sie Configuration Compliance Richtlinien an

Nachdem Sie die Ergebnisse eines Drittanbieter-Scans in Ihre Instanz importiert haben, können Sie Ihre Test-Compliance auf Richtlinienebene anzeigen. Verwenden Sie diese Ansicht vor einem Audit dieser Richtlinie und der zugehörigen Testdatensätze.

### Vorbereitungen

Erforderliche Rolle: sn_vulc.read und sn_vulc.remediation_owner zum Anzeigen

### Warum und wann dieser Vorgang ausgeführt wird

Richtlinien sind importierte Datensätze und können in Configuration Compliancenicht bearbeitet werden.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Richtlinien**.
2. Klicken Sie auf die **Kurzbeschreibung** der Richtlinie, die Sie anzeigen möchten.

**Felder des Configuration Compliance-Formulars „Richtlinie“**

| Feld | Beschreibung |
|---|---|
| Quelle | Systemname des Drittanbieter-Scanners oder der im ServiceNow -Plugin eingegebene Name für die API, die zur Kommunikation mit Configuration Complianceverwendet wird. |
| Technologien | Liste der Technologien, die der Richtlinie in der Scanner-Anwendung einer Drittpartei zugeordnet sind. |
| Quellen ID | Bezeichner, der dieser Richtlinie vom Drittanbieter-Scanner zugewiesen wird. |
| Quelle erstellt | Datum und Uhrzeit, zu der die Richtlinie in der Scanner-Anwendung einer Drittpartei definiert wurde. |
| Quelle aktualisiert | Datum und Uhrzeit der letzten Änderung der Richtlinie in der Drittpartei-Richtlinien-Scanner-Anwendung. |
| Kurzbeschreibung | Zusammenfassungsbeschreibung oder Titel, die der Richtlinie in der Scanner-Anwendung einer Drittpartei zugewiesen ist. |
| Beschreibung | Detaillierte Beschreibung der Richtlinie, wie in der Scanner-Anwendung einer Drittpartei definiert. |
| Tests | Liste der Tests, die auf diese Richtlinie verweisen. Aus dem Scanner einer Drittpartei importiert. Bei Bedarf können Sie in der Liste zu detaillierten Informationen zu einem bestimmten Test navigieren. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| **Korrekturstatus (Version 12.0)** | |
| Zurückgestellte sind ausgeschlossen | Diese Werte enthalten keine CIs aus zurückgestellten Testergebnissen.<br>○ **Verbleibende CIs**: Die Anzahl (Anzahl) der Konfigurationselemente (CIs) mit aktiven Testergebnissen (anderer Status als **Geschlossen**) für diese Richtlinie.<br>○ **Behobene CIs**in Prozent: Prozentsatz der konformen CIs für diese Richtlinie. Diese Zahl schließt CIs mit zurückgestellten Testergebnissen aus.<br>○ **CIs gesamt**: Die Gesamtzahl der von dieser Richtlinie betroffenen CIs. Diese Anzahl enthält nicht die zurückgestellten Testergebnisse. |
| Beinhaltet Zurückgestellte | Die Werte stellen CIs aus allen aktiven Testergebnissen dar (jeder andere Status als **Geschlossen**).<br>○ **Verbleibende CIs**: Die Anzahl der eindeutigen CIs, die einem oder mehreren nicht geschlossenen Testergebnissen zugeordnet sind, auf die diese Richtlinie angewendet wurde.<br>○ **Behobene CIs**in Prozent: Der Prozentsatz der konformen CIs für diese Richtlinie.<br>○ **CIs**gesamt: Gesamtzahl der von dieser Richtlinie betroffenen CIs. |

Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte Korrekturstatus auf den zugehörigen Link **Status** aktualisieren. Eine Meldung wird angezeigt, die angibt, dass die Daten aktualisiert werden. Klicken Sie auf den Link **Status** anzeigen, um den Fortschritt der Aktualisierung anzuzeigen. Nach einigen Minuten werden alle Daten, die seit der letzten geplanten Aufgabe geändert oder aktualisiert wurden, im Datensatz aktualisiert. Aktualisierte Feldwerte werden aktualisiert.

## Zeigen Sie Configuration Compliance autoritative Quellen an

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu jeder autoritativen Quelle anzuzeigen und die Quellveröffentlichungen zu recherchieren, die zum Erstellen des Datensatzes verwendet wurden.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Unterstützungsdaten** > **Autoritative Quellen**.
2. Klicken Sie auf die **Kurzbeschreibung** der autoritativen Quelle, die Sie anzeigen möchten.

#### Configuration Compliance Autorisierende Quellen Formularfelder

| Feld | Beschreibung |
|---|---|
| Nummer | ID-Nummer, die der autorisierenden Quelle von Ihrer Instanz während des Importvorgangs zugewiesen wurde. |
| Quelle | Systemname der Scanner-Anwendung einer Drittpartei oder der im Scanner-Plugin eingegebene Name für die API, die mit Configuration Compliancekommuniziert. |
| Quellen ID | Bezeichner, der der autorisierenden Quelle vom Drittanbieter-Scanner zugewiesen wurde. |
| Kurzbeschreibung | Name, der dieser autorisierenden Quelle im Scanner einer Drittpartei zugewiesen wurde. |
| Herausgeber | Name der Organisation oder Veröffentlichung, die die ursprüngliche Informationsquelle für diese autoritative Quelle war. |
| Bezugsvermerke | Liste der angegebenen Informationen zu den Testergebnissen. Aus dem Scanner einer Drittpartei importiert. Sie können in dieser Liste bei Bedarf zu detaillierten Informationen zu einem bestimmten Test navigieren. |

3. **Wahlweise:** Fügen Sie einen **Herausgeber**hinzu.
4. Klicken Sie auf **Aktualisieren**.
5. Sie können diesen Datensatz löschen, indem Sie auf **Löschen**klicken.
   Entfernt den Datensatz aus Ihrer Instanz. Wenn sie in Ihrer Drittanbieterintegration noch verwendet wird, wird sie beim nächsten Import zurückgegeben

## Zeigen Sie die Technologien von Configuration Compliance an

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu allen maßgeblichen Quellen und Zitaten anzuzeigen (in Qualys auch als Framework bezeichnet). Sie können die Quellveröffentlichungen durchsuchen, die zum Erstellen des Datensatzes verwendet wurden.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Unterstützungsdaten** > **Technologien**.
2. Klicken Sie auf die **Kurzbeschreibung** der autoritativen Quelle, die Sie anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Configuration Compliance Autorisierende Quellen Formularfelder**

| Feld | Beschreibung |
|---|---|
| Nummer | ID-Nummer, die der autorisierenden Quelle von Ihrer Instanz während des Importvorgangs zugewiesen wurde. |
| Quelle | Systemname des Drittanbieter-Scanners oder der Name, der im Drittanbieter-Scanner-Plugin für die API eingegeben wurde, die mit Configuration Compliancekommuniziert. |
| Quellen ID | Bezeichner, der der autorisierenden Quelle vom Drittanbieter-Scanner zugewiesen wurde. |

3. Sie können diesen Datensatz löschen, indem Sie auf **Löschen**klicken.
   Entfernt den Datensatz aus Ihrer Instanz. Wenn sie in Ihrer Drittanbieterintegration noch verwendet wird, wird sie beim nächsten Import zurückgegeben

## Zeigen Sie Configuration Compliance Tests an

Verwenden Sie dieses Modul, um detaillierte Informationen zu diesen Tests zu recherchieren. Enthalten sind die Bezugsvermerke der Expertenquelle, die bei der Erstellung verwendet wurden, die Konfigurationsrichtlinien von Drittanbietern, in denen sie verwendet werden, und die Ergebnisse des Scans.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zu aktualisieren
- sn_vulc.remediation_owner zum Anzeigen

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Steuerungen**.
2. Navigieren zu **Alle** > **Configuration Compliance** > **Tests**
3. Öffnen Sie in der Liste die Kontrolle (Compliance-Test), die Sie anzeigen möchten.

   Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte Korrekturstatus auf den zugehörigen Link **Status** aktualisieren. Eine Meldung wird angezeigt, die angibt, dass die Daten aktualisiert werden. Klicken Sie auf den Link **Status** anzeigen, um den Fortschritt der Aktualisierung anzuzeigen. Nach



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einigen Minuten werden alle Daten, die seit der letzten geplanten Aufgabe geändert oder aktualisiert wurden, im Datensatz aktualisiert. **Feldwerte**wie**Risikopunktzahl**, **Risikobewertung**, **Korrekturzieldatum**, **Status** und die Felder auf der Registerkarte Korrekturstatus werden aktualisiert.

### Configuration Compliance Testformularfelder

| Feld | Beschreibung |
|---|---|
| Nummer | Nummer, die der Kontrolle während des Importvorgangs zugewiesen wurde. |
| Ergebnis | Status des Scans. Bestanden oder nicht bestanden. Wenn dieser Test zu mehreren Korrekturaufgaben gehört, wird sein Status anhand einer Rangfolgebestimmt. |
| Quelle | Systemname der Integrationsanwendung einer Drittpartei oder der im Plugin eingegebene Name für die API, die zur Kommunikation mit Configuration Complianceverwendet wird. |
| Relevanz | Schweregrad des Konfigurationsproblems oder der Konfigurationsprobleme, die mit der Steuerung verbunden sind, wie in der Drittpartei-Integration definiert. Die Relevanzstufe wird an die Granularität ähnlicher Schwachstellenindikatoren angepasst, die in Vulnerability Responseverfügbar sind. Mögliche Ebenen:<br>**Kritisch**<br>Das mit der Steuerung verbundene Konfigurationsproblem verursacht eine Unterbrechung eines oder mehrerer geschäftskritischer CIs.<br>**Hoch**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung dar, verursacht jedoch nicht das Herunterfahren wichtiger Netzwerkressourcen.<br>**Mittel**<br>Das mit der Kontrolle verbundene Konfigurationsproblem ist ein Risiko, aber keine unmittelbare Bedrohung.<br>**Niedrig**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt eine Bedrohung auf niedriger Ebene dar und kann für CIs mit höherem Risiko ignoriert werden.<br>**Kleiner**<br>Das mit der Steuerung verbundene Konfigurationsproblem stellt ein |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | geringes Risiko dar und kann bei Bedarf ignoriert werden. |
| Quellen ID | Bezeichner, der der Kontrolle durch die Drittpartei-Integration zugewiesen wurde. |
| Kategorie | Hauptklassifizierungskategorie, die für diesen Steuerungstyp vom Drittanbieter vergeben wird. |
| Risikopunktzahl | Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl ist gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht geschlossenen Testergebnisse (Offen, Wird untersucht, Warten auf Implementierung, Zurückgestellt, Gelöst) und 15 % der Punktzahl aus der Anzahl der Tests stammen Ergebnisse, die nicht „Geschlossen“ sind.Von Risikopunktzahlrechnern berechneter Wert, der auf den Geschäftsrelevanz- und Testrelevanzwerten der Testergebnisse basiert. |
| Unterkategorie | Unterkategorie, die dieser Testklasse vom Drittanbieter zugewiesen wurde. |
| Risikobewertung | Basierend auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen von 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen. |
| Technologien | Liste der von diesem Test abgedeckten Technologien. |
| Quelle erstellt | Datum, an dem der Test erstmals in der Drittpartei-Integration definiert wurde. |
| Quelle aktualisiert | Datum, an dem der Test zuletzt in der Drittpartei-Integration aktualisiert wurde. |
| Kurzbeschreibung | Zusammenfassungsbeschreibung oder Titel, die dem Test in der Drittpartei-Integration eingegeben oder zugewiesen wurde. |
| **Korrekturstatus (v 12.0)** | |
| Zurückgestellte sind ausgeschlossen | Diese Werte enthalten keine zurückgestellten Testergebnisse.<br>○ **Offene Testergebnisse**: Die Anzahl (Anzahl) aktiver Testergebnisse (anderer Status als „ **Geschlossen**“) für diesen Konfigurationstest.<br>○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten Testergebnisse für diese Korrekturaufgabe.<br>○ **Testergebnisse**gesamt: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Beinhaltet Zurückgestellte | Diese Werte enthalten zurückgestellte Testergebnisse.<br>○ **Offene Testergebnisse**: Die Anzahl (Anzahl) aller aktiven Testergebnisse (anderer Status als „ **Geschlossen**“) für diese Korrekturaufgabe.<br>○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten Testergebnisse für diese Korrekturaufgabe.<br>○ **Testergebnisse**gesamt: Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe. |
| Beschreibung | Ausführliche Beschreibung des Tests. Für die Qualys Vulnerability-Integration wird in diesem Feld standardmäßig der Inhalt der Qualys Cloud Platform -Deckblattseite verwendet. |
| Korrektur | Schrittanweisungen, die beschreiben, wie die Nichteinhaltung behoben werden kann. |
| **Zugehörige Registerkarten** | |
| Bezugsvermerke | Liste der Bezugsvermerke, die für jede dem Test zugeordnete autoritative Quelle eingegeben wurden. |
| Richtlinien | Liste von Configuration Compliance Richtlinien, die diesen Test verwenden. |
| Testergebnisse | Liste der CIs, die von dem Konfigurationsproblem oder den mit diesem Test verbundenen Problemen betroffen sind. Sie können bei Bedarf auf einzelne Tests, ServiceNow Konfigurationselemente oder die Liste der betroffenen Technologien zugreifen. |
| GRC-Richtlinienanweisungen | Wenn das Plugin GRC Policy and Compliance Management installiert ist, enthält diese Registerkarte die zugehörige Richtlinie GRC. Sie können diese Liste bearbeiten, um Richtlinienanweisungen hinzuzufügen oder zu entfernen. |



## Zeigen Sie Configuration Compliance Testergebnisse an

Zeigen Sie Configuration Compliance Testergebnisse für Audits und Korrekturen an.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.read zum Anzeigen
- sn_vulc.remediation_owner zum Anzeigen und Aktualisieren
- sn_vulc.admin zum Löschen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisse**.
2. Öffnen Sie das Steuerelement, das Sie anzeigen möchten.

**Configuration Compliance Felder des Formulars „Testergebnisse“.**

| Feld | Beschreibung |
|---|---|
| Nummer | Die dem Test während des Importvorgangs zugewiesene Nummer. |
| Quelle | Der Systemname der SCA-Anwendung einer Drittpartei oder der im Anwendungs-Plugin für die API eingegebene Name, der für die Kommunikation mit Configuration Complianceverwendet wird. |
| Quellen ID | Der Bezeichner, der dem Steuerelement von der SCA-Anwendung zugewiesen wurde. |
| Ergebnis | Bestanden, Fehlgeschlagen, Fehler oder Unbekannt. Aus Qualys importiert. |
| Risikopunktzahl | Rechnerergebnis für diesen Test. |
| Risikobewertung | Basierend auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen von 1 – Kritisch bis 5 – Keine bewertet. Dieses Feld ersetzt das Feld Priorität in früheren Versionen. |
| Status | Berechnet aus den Testergebnisgruppen, zu denen das Testergebnis gehört. Wenn das Testergebnis zu mehreren Gruppen gehört, wird eine Rangfolge angewendet, um den Status zu bestimmen. |
| Lösung | Berechnet aus den Testergebnisgruppen, zu denen das Testergebnis gehört. Wenn das Testergebnis zu mehreren Gruppen gehört, wird eine Rangfolge angewendet, um die Auflösung zu bestimmen. |
| Zuerst gesehen | Datum des ersten Imports in Configuration Compliance.<br><br>Ab v13.1.1 wird im Feld „ **Zuerst gesehen** “ das vom Scanner bereitgestellte Datum angezeigt. Andernfalls wird das Datum |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | angezeigt, an dem zuerst in Configuration Complianceimportiert wurde. |
| Zuletzt gesehen | Datum des letzten Imports in Configuration Compliance.<br><br>Ab v13.1.1 wird im Feld **Zuletzt gesehen** das vom Scanner bereitgestellte Datum angezeigt. Andernfalls wird das Datum des letzten Imports in Configuration Complianceangezeigt. |
| Letzte Übergabe | Spätestes Datum, an dem das Testergebnis bestanden wird. |
| Test | Name des Tests. |
| Konfigurationselement | Name des an den Test angehängten CI. |
| Technologie | Softwareversion, die auf dem CI ausgeführt wird. |
| Beschreibung | Beschreibung des Tests |
| Erwartete Werte | Erwartete Werte, die in Qualys konfiguriert und von Configuration Complianceimportiert wurden. Dieser Wert ist ein boolescher Ausdruck, der bei einer Auswertung mit „true“ das Testergebnis zu **Bestanden**macht. Der Ausdruck kann eine Kombination aus logischen Operatoren, festgelegten Operatoren oder regulären Ausdrucksoperatoren sein. |
| Tatsächliche Werte | Vom Test zurückgegebene Werte. Diese Werte werden in den booleschen Ausdruck für erwartete Werte eingefügt, um zu bestimmen, ob das Ergebnis erfolgreich sein oder fehlschlagen soll. Sie werden aus Qualys importiert.<br><br>Ab Version 14.9 von Configuration Compliancewerden die Werte für „Erweiterter Nachweis“ und „Fehlerursache“ in der Spalte „Tatsächliche Werte“ hinzugefügt. |
| Korrektur | Korrekturanweisungen. |
| **Zugehörige Registerkarten** | |
| Testergebnisgruppen | Testergebnisgruppen, die diesem Testergebnis zugeordnet sind. |
| Testergebnisverlauf | Zugehörige Liste von Testergebnissen, die den Verlauf der Bestanden/Fehlgeschlagen-Ergebnisse für dasselbe CI/Technologie/Test anzeigen. |

## Zeigen Sie eine Testergebnisgruppe an

Sie können eine Testergebnisgruppe anzeigen oder alternativ erstellen und die Fehlerkorrektur durchführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren oder Erstellen
- sn_vulc.remediation_owner zum Anzeigen

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

#### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

### Prozedur

1. Navigieren zu **Alle** > **Configuration Compliance** > **Testergebnisgruppen**.
2. Klicken Sie in der Liste auf den Datensatz, den Sie anzeigen möchten.
3. Klicken Sie alternativ auf **Neu**, um eine neue Testergebnisgruppe zu erstellen und die Felder auszufüllen.

#### Felder des Formulars „Configuration Compliance Test-Ergebnisgruppe“.

| Feld | Beschreibung |
|---|---|
| Nummer | Die automatisch generierte Nummer für diesen Datensatz. |
| Status | Fortschrittsstatus der Gruppe.<br>○ Offen<br>○ Wird untersucht<br>○ Warten auf Implementierung<br>○ Zurückgestellt<br>○ Gelöst<br>○ Geschlossen |
| Risikopunktzahl | Diese Punktzahl ist der zusammengefasste Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Testergebnisgruppe. Diese Punktzahl ändert sich, wenn Testergebnisse in der Testergebnisgruppe korrigiert werden. |
| Zuweisungsgruppe | Gruppe, die für die Bearbeitung dieser Testergebnisgruppe ausgewählt wurde. |
| Risikobewertung | Das Risiko, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einem Bereich von Risikopunktzahlen auf einer Skala von 1 bis 5, der Risiken als „Kritisch“ (1) bis „Keine“ (5) bewertet. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem Aufgabensatz arbeitet. |
| Korrekturziel | Datum, bis zu dem die Testergebnisse seit der ersten Identifizierung korrigiert werden sollen. |
| Erstellt | Datum und Uhrzeit der Erstellung dieser Testergebnisgruppe. |
| Korrekturstatus | Status der Fehlerkorrektur für die Gruppe. Sie wird durch das Testergebnis mit dem nächsten Fälligkeitsdatum bestimmt.<br>Zu den Status offener Gruppen gehören „In Ausführung“, „Ziel erreicht“ und „Ziel verfehlt“. Für geschlossene Gruppen sind dies „Kein Ziel“, „Ziel erfüllt“ und „Ziel verfehlt“.<br>Wenn für berechnete Korrekturzieldaten die Testergebnisgruppe geschlossen ist, wird der allgemeine Korrekturstatus aller geschlossenen Testergebnisse in der Testergebnisgruppe angezeigt. Diese bestimmen, ob die Gruppe ihr Datum erreicht hat oder nicht.<br>Der Status einer geschlossenen Testergebnisgruppe ist „ **Kein Ziel** “, wenn keines der geschlossenen Ergebnisse ein Korrekturzieldatum hatte. Er lautet **„Ziel verfehlt“**, wenn eines der geschlossenen Ergebnisse sein Zieldatum verfehlt hat. **Ziel** ist erfüllt, wenn mindestens ein geschlossenes Ergebnis sein Ziel erreicht hat und keines der anderen es verfehlt hat. |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung dieses Datensatzes. |
| Kurzbeschreibung | Kurze Beschreibung dieser Testergebnisgruppe. |
| Beschreibung | Ausführliche Beschreibung der Testergebnisgruppe, die die Liste der Software enthält, die dieser Testergebnisgruppe zugeordnet ist. |
| Test | Der dieser Testergebnisgruppe zugeordnete Konfigurationstest. |
| **Korrekturstatus (Version 12.0)** | |
| Zurückgestellte sind ausgeschlossen | Diese Werte enthalten keine zurückgestellten Testergebnisse. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ **Offene Testergebnisse**: Die Anzahl (Anzahl) aktiver Testergebnisse (anderer Status als „ **Geschlossen**“) für diese Testergebnisgruppe.<br>○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Testergebnisgruppe.<br>○ **Testergebnisse**gesamt: Die Gesamtzahl der Testergebnisse für diese Testergebnisgruppe. |
| Beinhaltet Zurückgestellte | Die Werte stellen alle aktiven Testergebnisse dar (jeder andere Status als **Geschlossen**).<br>○ **Offene Testergebnisse**: Die Anzahl (Anzahl) aktiver Testergebnisse (anderer Status als „ **Geschlossen**“) für diese Testergebnisgruppe.<br>○ **% der korrigierten Testergebnisse**: Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Testergebnisgruppe.<br>○ **Testergebnisse**gesamt: Die Gesamtzahl der Testergebnisse für diese Testergebnisgruppe. |
| **Gruppenkonfiguration** | Die Art der Filterung, die zum Auswählen der Testergebnisse für die Testergebnisgruppe verwendet wird. |
| Gruppierungsmethode | Name der verwendeten Methode. |
| Gruppenregel | Name der verwendeten Gruppenregel. |
| **Notizen** | Systemhinweise, die dem Datensatz zugeordnet sind. |
| **Zugehörige Links** | **Version 12.0: Link zum Aktualisierungsstatus**. Aktualisieren Sie die Werte im Testergebnisdatensatz bei Bedarf. Zeigen Sie alle Daten an, die seit der letzten geplanten Aufgabe geändert oder aktualisiert wurden. |
| Testergebnisse | Die Testergebnisse in dieser Testergebnisgruppe. |
| **Change-Anforderungen (v 12.0)** | Die Liste der Change-Anforderungen, die dieser Testergebnisgruppe zugeordnet sind. |
| **Statusänderungsgenehmigungen (v 12.0)** | Status und Status der Change-Anforderungsgenehmigungen, die dieser Testergebnisgruppe zugeordnet sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

In der Anwendung Configuration Compliance besteht eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben und den Statusfeldern von Change-Anforderungen (CHGs).

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Während eine Change-Anforderung ihren Lebenszyklus durchläuft, wird auch der Status der zugehörigen Korrekturaufgaben automatisch verschoben. Die Statussynchronisierung wird durch eine Systemeigenschaft standardmäßig in Ihrer Instanz aktiviert, wenn Sie die Anwendung Configuration Compliance aus dem ServiceNow Store ab v12.0 herunterladen.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG-Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn eine neue Change-Anforderung für eine Korrekturaufgabe erstellt wird und sich diese nicht in **„Warten auf Implementierung“**befindet, wird der Status der Korrekturaufgabe in **„Warten auf Implementierung“ verschoben**.
- Wenn eine vorhandene Change-Anforderung einer Korrekturaufgabe zugeordnet ist und sich nicht in **„Warten auf Implementierung**“ befindet, wird der Status der Korrekturaufgabe in **„Warten auf Implementierung“ verschoben**.
- Nachdem die Aufgaben für eine Change-Anforderung abgeschlossen (Implementiert) sind und die CHG in den Status **Überprüfen** verschoben wurde, wird die Korrekturaufgabe in den Status **Gelöst**verschoben.

Weitere Informationen und Beispiele für die Statussynchronisierung finden Sie in den folgenden Abschnitten.

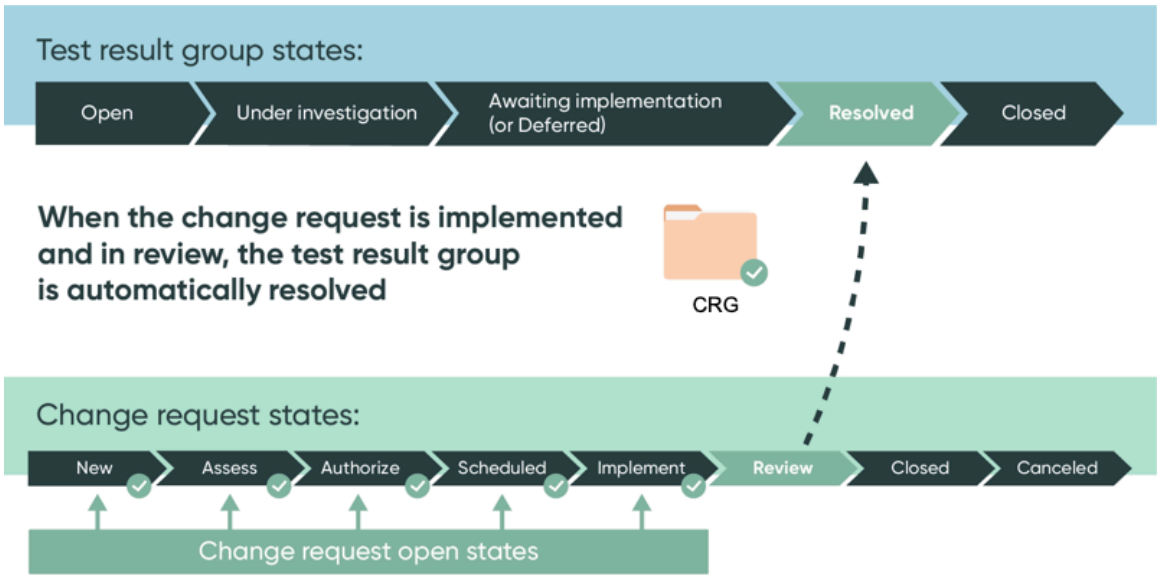
**Hinweis:**
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die Status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist, aber wenn das System registriert, dass eine Change-Anforderung seinen Status geändert hat, oder Sie eine Change-Anforderung hinzufügen oder aus entfernen Bei einer Korrekturaufgabe kann die Statussynchronisierung möglicherweise Ihren manuellen Eingriff überschreiben. Change Request-Status verschieben die Korrekturaufgabe jedoch nicht automatisch aus **Geschlossen**.

## Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-Status die Status von Korrekturaufgaben in einem Vorwärtslebenszyklus automatisch verschieben, d. h. von „ **Offen** “ zu **„Gelöst“**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als **Gelöst** oder **Geschlossen**erstellen. Die Statussynchronisierung verschiebt die TRG automatisch bidirektional durch die Status „ **Offen**“, „ **Wird untersucht**“, **„Warten auf Implementierung“**und **„Gelöst“**. Diese Verschiebung basiert auf bestimmten Werten des Statusfelds im Change Request. Die Statussynchronisierung zwischen Change-Anforderung und Korrekturaufgabe wird automatisch aufgerufen, es sei denn, das Kontrollkästchen (**CIs zu CR hinzufügen**) wird in einem Formular angezeigt, und Sie deaktivieren das Kontrollkästchen.

Die Korrekturaufgabe wird nicht in den Status „ **Gelöst** “ verschoben, wenn sich ein CHG im Status „Offen“ befindet. Alle **CHGs**, die sich in ihrem Lebenszyklus in einem Status vor der **Überprüfung**befinden, z. B. „ **Neu**“, „Bewerten“, „ **Autorisieren**“, „ **Geplant** “ oder „ **Implementieren**“, wie in der vorherigen Abbildung dargestellt, gelten als offene Status für die CHG. Offene Status verschieben das Statusfeld in der Korrekturaufgabe nicht, da Untersuchungen oder Aufgaben im CHG noch nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn ein CHG für die Korrekturaufgabe erstellt oder ihr zugeordnet wird oder wenn sich der Status einer vorhandenen Beziehung im CHG ändert. Die abgeschlossenen CHG-Status sind **Überprüfen** und erfolgreich **Geschlossen**. Wenn ein CHG erfolgreich geschlossen wird, lauten seine Abschlusscodes: **Erfolgreich**oder **Erfolgreich mit Problemen**. In diesem Fall wird die Korrekturaufgabe zu **Gelöst verschoben**.

## Statussynchronisierung rückwärts

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann er irgendwann abgebrochen werden. In diesem Fall wird die Korrekturaufgabe automatisch zurück in den Status „Wird **untersucht**“ verschoben, wenn CHG **Abgebrochen** oder **Geschlossen**ist (mit dem Abschlusscode **Nicht erfolgreich**). Die Korrekturaufgabe wird zurück in den Status „ **Wird untersucht**“ verschoben, da kein aktiver Plan zur Korrektur der Schwachstelle vorhanden ist.

Wenn sich eine Korrekturaufgabe im Status **Gelöst** befindet und Sie eine neue CHG erstellen oder sie einer vorhandenen CHG in einem der anfänglichen offenen Status zuordnen, wird die Korrekturaufgabe automatisch in den Status „ **Warten auf Implementierung“**zurückgesetzt. Die Korrekturaufgabe wird in diesen Status zurückgesetzt, da dem CHG jetzt mehr Arbeit zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Korrekturaufgaben mit mehr als einem CHG

Wenn einer Korrekturaufgabe in **„Warten auf Implementierung** “ mehr als ein CHG zugeordnet ist, basiert die Statussynchronisierung auf dem Status des CHG im frühesten Status seines Lebenszyklus. Angenommen, einer Korrekturaufgabe sind vier CHGs zugeordnet: CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle dargestellt.

| CHG-Nummer | CHG-Status |
|---|---|
| 1 | **Implementieren** |
| 2 | **Abgebrochen** |
| 3 | Geschlossen (Abschlusscode von **Nicht erfolgreich**) |
| 4 | Geschlossen (Abschlusscode nicht **erfolgreich**) |

Die Statussynchronisierung zwischen CHG und Korrekturaufgabe basiert in diesem Fall auf CHG1, das sich im frühesten Status der vier CHGs befindet (**Implementieren**). In diesem Fall bleibt die Korrekturaufgabe in **Warten auf Implementierung**.

In einem anderen Beispiel wird die Korrekturaufgabe von „ **Gelöst** “ zurück zu **„Warten auf Implementierung** “ verschoben, wenn sich eine Korrekturaufgabe im Status „ **Gelöst** “ befindet und eine vorhandene CHG vorhanden ist, die implementiert wurde und sich im Status „ **Überprüfung**“ befindet, und eine neue CHG erstellt wird. Die Statussynchronisierung basiert auf dem CHG im Status **Neu**, dem CHG im frühesten Status.

| CHG-Nummer | CHG-Status |
|---|---|
| 1 | Prüfung |
| 2 | Neu |

Wenn Korrekturaufgaben mehr als eine CHG haben, ändert sich der Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn ein CHG in den Status **Überprüfen**übergeht und sich alle anderen CHGs, die der Korrekturaufgabe zugeordnet sind, im Status „ **Überprüfen** “ oder „ **Geschlossen** “ befinden (mit einem erfolgreichen Abschlusscode), wird die Korrekturaufgabe automatisch in **„Gelöst**“ geändert. Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn eine CHG in den Status „ **Abgebrochen** “ oder „**Geschlossen** “ (Abschlusscode von **Nicht erfolgreich**) verschoben wird und sich alle anderen mit der Korrekturaufgabe verknüpften CHGs im selben Status befinden, wird die Korrekturaufgabe automatisch in den Status „Wird untersucht“ zurückgesetzt **.**

Weitere Informationen zu den Status von Korrekturaufgaben und den Möglichkeiten, die Sie in den einzelnen Status haben, finden Sie unter Configuration Compliance Status.

## Domain Separation und Configuration Compliance

Die Domänentrennung wird in Configuration Compliance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

**Änderungen in der Terminologie**

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

## So funktioniert Domain Separation in Configuration Compliance

Mit der Domänentrennung können Sie (Configuration Compliance) Verfahren für den gesamten Kundenstamm standardisieren, den Sie bedienen, mit geringeren Betriebskosten und einer höheren Servicequalität.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt und niemals für andere Clients verfügbar sind.

**Unterstützung der Domänentrennung in Configuration Compliance nach Versionsveröffentlichungen**

| Release | Support-Stufe | Notizen |
|---|---|---|
| Orlando | Standard | |
| Paris | Standard | |
| Quebec | Standard | |
| Rome | Standard | |
| San Diego | Standard | |
| Tokio | Standard | |
| Utah | Standard | |
| Vancouver | Standard | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Domänentrennung für die Anwendung Configuration Compliance umfasst die folgenden Produktfunktionen:

- Erfasst die Testergebnisse von Drittanbieter-Scannern (Qualys) in der richtigen Domäne.

  Die Daten werden in derselben Domäne wie der Integrationsbenutzer erfasst, dessen Anmeldeinformationen für die Integration verwendet werden.

- Scannt bestimmte Hosts von Configuration Compliance in der Domäne, von der er angefordert wurde, erneut.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen von den Scannern mit den CIs in der CMDB der Domäne des Integrationsanwenders übereinstimmen.
- Berechnet Risikopunktzahlen auf Testergebnisebene gemäß dem Risikopunktzahl-Rechner, der in derselben Domäne wie die des Integrationsbenutzers definiert ist.
- Testergebnis-Gruppenregeln können in derselben Domäne wie die Domäne des Integrationsbenutzers definiert und zugewiesen werden.
- Korrekturaufgaben, die mithilfe der Gruppenregeln für Dokumenttestergebnisse erstellt wurden, bleiben in derselben Domäne wie die, in der die Gruppenregeln erstellt werden.
- Der Zurückstellungs-Workflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.
- Berichte und Dashboards zeigen die Testergebnisstatus an, z. B. Alter der Testergebnisse, offene Testergebnisse nach CI, Testergebnisse nach Auswirkung in der Domäne, zu der sie gehören.
- Wissen von Scannern von Drittanbietern (Qualys) kann in der globalen Domäne erfasst werden, und Daten können über mehrere Clients hinweg gemeinsam genutzt werden.

**Hinweis:**
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz bei der Trennung getrennter Domänen in der NOW-Plattform.

## Anwendungsfälle

Die Anwendung Configuration Compliance verwaltet den Lebenszyklus eines Testergebnisses End-to-End. Die folgenden Anwendungsfälle sind für die Domänentrennung geeignet:

- **Testergebnisse** aus Qualyserfassen
  - Daten aus mehreren Instanzen erfassen
  - Deduplizieren Sie die Testergebnisse
  - Mit CMDB-CI abgleichen
- **Anreicherung** von Testergebnissen mit Risikopunktzahlen
  - Asset-Ergänzung (CMDB)
  - Risikopunktzahl
- **Gruppieren** Sie die Testergebnisse, und weisen Sie die Korrekturaufgabe zu
  - Testergebnisse automatisch gruppieren
  - Weisen Sie die Korrekturaufgabe automatisch zu
- **Beheben**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Korrekturaufgabe als Korrekturaufgabe zugewiesen
- Umfassender Lebenszyklus der Korrektur
- Zurückstellungs-Workflow

- **Messen Sie** die Sicherheitslage der Organisation und des Compliance-Management-Programms
  - Ergebnistrend nach Compliance, Kategorie, Relevanz und Technologie
  - Status und Verteilung von Richtlinien, Tests, Hosts, Testergebnissen und Risikopunktzahlen

## Setup

Das Einrichten der Domänentrennung für Configuration Compliance erfordert keine zusätzlichen Schritte. Alle Configuration Compliance -Tabellen erfassen die Domänenspalte, nachdem die Instanz domänengetrennt wurde. Sie können die Importdaten der Testergebnisintegration in bestimmte Domänen leiten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration. Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für die Domänentrennung.

## Domänengetrennte Daten

Daten können domänengetrennt sein, was bedeutet:

- Von Scannern von Drittanbietern erfasste Testergebnisse verbleiben in derselben Domäne wie die Domäne des Integrationsbenutzers und sind von keiner anderen Domäne aus zugänglich.
- Testergebnisse oder Hosts in einer Domäne können nicht von anderen Domänen aus angezeigt werden.
- Der Risikobewertungsalgorithmus und die Gruppenregeln für Testergebnisse können von niemandem außerhalb der Domäne angezeigt werden.
- Zurückstellungs-Workflows, die in einer Domäne erstellt wurden, sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen sind in der Domäne enthalten, zu der sie gehören.

## Wie Compliance-Analysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen ihre eigene Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen und CI-Suchregeln.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können ihre eigenen Zurückstellungs- und Change-Management-Workflows erstellen.
- Analysten können ihre eigenen Testergebnisgruppenregeln und Risikobewertungslogik erstellen, um die Ergebnisse genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und sie der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenbenutzer erstellen eine manuelle Korrekturaufgabe und schließen sie.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Geschäftslogik und Prozesse, die nach Instanzbesitzern domänengetrennt werden können

- Configuration Compliance -Benutzer und -Gruppen
- Configuration Compliance -Integrationen (ab Madrid-Release)
- Vollständige Setup-Konfiguration (Benutzer- und Gruppenverwaltung, Anwendungsinstallation, Anwendungsverwaltung mit mehreren Quellen, CI-Suchregeln, Testergebnis-Gruppenregeln, Risikorechner usw.)
- Vollständiger Korrekturlebenszyklus einschließlich Zurückstellung

**Zugehörige Informationen**

Domänentrennung für Service Provider

## Testergebnisfelder

Testergebnisse werden während des Imports von Drittpartei-Schwachstellenintegrationen automatisch erstellt.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

Configuration Compliance erstellt oder aktualisiert die Testergebnisse nicht, sondern importiert sie als Teil einer Drittanbieterintegration. Sobald sie in Configuration Complianceangezeigt werden, werden sie mithilfe von **Testergebnisgruppen korrigiert**.

## Testergebnisfelder

| Feld | Beschreibung |
|---|---|
| Nummer | Nummer, die dem Testergebnis während des Importvorgangs zugewiesen wurde. |
| Quelle | Systemname der Integrationsanwendung einer Drittpartei oder der in der Anwendung für die API eingegebene Name, die für die Kommunikation mit Configuration Complianceverwendet wird. |
| Quellen ID | Bezeichner, der dem Testergebnis von der Drittpartei-Integration zugewiesen wurde. |
| Risikopunktzahl | Punktzahl basierend auf dem Wert `Criticality` des Tests. Wenn Sie nicht installiert und konfiguriert haben, wird ein Mittelwert von 50 verwendet. |
| Lösung | Auflösung des Testergebnisses, berechnet aus zugeordneten Gruppen. |
| Ergebnis | Status des Scans. Bestanden oder nicht bestanden. Wenn dieser Test zu mehreren Korrekturaufgaben gehört, wird sein Status anhand einer Rangfolgebestimmt. |
| Status | Status des Testergebnisses, berechnet aus zugeordneten Gruppen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Zuweisungsgruppe | Gruppe, die ausgewählt wurde, um an diesem Testergebnis zu arbeiten. |
| Zugewiesen an | Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem Testergebnis arbeiten soll. |
| Zuweisungstyp | Der Typ der Zuweisung. Die Auswahlmöglichkeiten lauten wie folgt:<br>• Regel<br>• Manuell<br>• Keine |
| Zuweisungsregel | Welche Zuweisungsregel mit diesem Testergebnis verwendet wurde, falls zutreffend. |
| Zuerst gesehen | Uhrzeit und Datum, an dem das Testergebnis zuerst angezeigt wurde. |
| Zuletzt gesehen | Uhrzeit und Datum, an dem das Testergebnis zuletzt angezeigt wurde. |
| Test | Die Kontrolle, zu der dieses Ergebnis gehört. |
| Konfigurationselement | Konfigurationselement, das diesem Testergebnis zugeordnet ist. |
| Technologie | Technologie, die diesem Testergebnis zugeordnet ist. |
| **Beschreibung** | |
| Beschreibung | Detaillierte Beschreibung des Testergebnisses, wie in der Scanner-Anwendung einer Drittpartei definiert. |
| **Erwartete Werte** | |
| Erwartete Werte | Beschreibung und erwartete Werte, wie in der Scanner-Anwendung einer Drittpartei definiert. |
| **Tatsächliche Werte** | |
| Tatsächliche Werte | Beschreibung und tatsächliche Werte, wie in der Scanner-Anwendung einer Drittpartei definiert. |
| **Fehlerkorrektur** | |
| Korrektur | Korrekturaktion, wie in der Scanner-Anwendung einer Drittpartei definiert. |

Im Folgenden finden Sie die zugehörigen Listen angreifbarer Elemente.

| Zugehörige Liste | Beschreibung |
|---|---|
| Testergebnisgruppen | Testergebnisgruppen, die diesem Testergebnis zugeordnet sind. |
| Testergebnisverlauf | Liste der früheren Datensätze mit unterschiedlichen Ergebnissen. |

## Configuration Compliance Relevanzzuordnungen

DieConfiguration Compliance -Relevanzzuordnung transformiert Relevanzfelder aus der Quelle in Felder in Configuration Compliance.

Das Configuration Compliance Basissystem wird mit einer Zuordnung von Standard Qualys Cloud Platform zu Standard ServiceNow geliefert. Das Erstellen oder Bearbeiten einer Relevanzzuordnung ist nur für benutzerdefinierte oder nicht standardmäßige Drittparteizuordnungen in Ihrer Umgebung vorgesehen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Configuration Compliance Status

Mit Configuration Compliancekönnen Sie ein Statusmodell anzeigen, um zu erfahren, wie der Status der Testergebnisgruppe zu einem bestimmten Zeitpunkt ist. Die Testergebnisgruppenstatus steuern die Testergebnisstatus nach Rang.

**Hinweis:**
Ab Version 14.9 von Configuration Compliancewurden die folgenden Begriffe umbenannt:

### Änderungen in der Terminologie

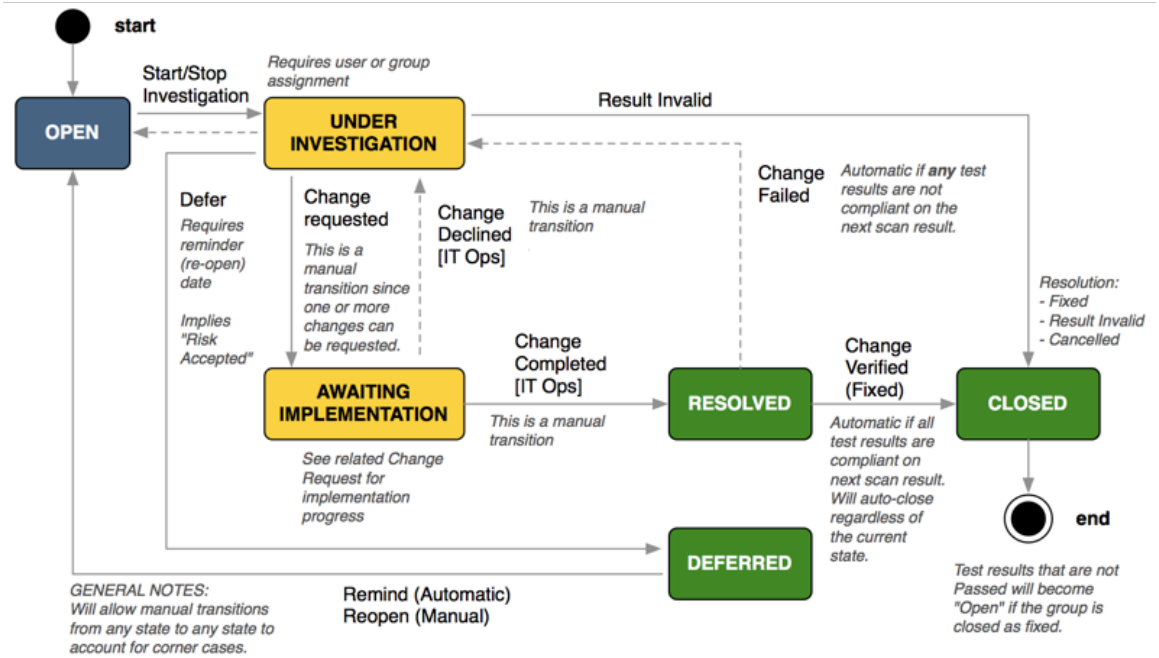
| Terminologie vor v14.9 | Terminologie v14.9 und höher |
|---|---|
| Testergebnisgruppe | Korrekturaufgabe |
| Gruppenregeln | Regeln für Korrekturaufgaben |
| Richtlinie | Testgruppe |

## Status der Korrekturaufgabe

Korrekturaufgaben haben viele mögliche Status. Der automatische Übergang ist ab dem Status Gelöst basierend auf den nächsten Scan-Ergebnissen verfügbar. Wenn alle Testergebnisse beim nächsten Scan übergeben werden, wird die Gruppe geschlossen. Andernfalls geht er in den Status Wird untersucht über. Das System überprüft diesen geschlossenen Status, wertet den Gruppenstatus jedoch erneut aus, wenn ein Testergebnis der Gruppe hinzugefügt oder daraus gelöscht wird. Arbeitsnotizen werden entsprechend dem Übergang aktualisiert.

Die folgende Abbildung zeigt, wie der Status einer Korrekturaufgabe vom Status „Offen“ in den Status „Geschlossen“ übergeht.

### Konfigurations-Compliance-Status-Flow




**Hinweis:**
Jedes Gruppenformular enthält die Schaltflächen **Folgen** und **Aktualisieren**, die für ServiceNow -Aufgaben Standard sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle sind die Status Configuration Compliance aufgelistet.

### Konfigurations-Compliance-Status

| Status | Beschreibung |
|---|---|
| Offen | Status bei Erstellung. |
| Wird untersucht | Wird durch die Schaltfläche **„Untersuchung starten“** ausgelöst. In diesem Status können Sie:<br>**Erstellen Sie eine Change-Anforderung**<br>Weitere Informationen finden Sie unter Change-Anforderung in Configuration Compliance erstellen.<br>**Zurückstellen**<br>Geben Sie einen Grund an, und wählen Sie ein Datum für die Wiedereröffnung aus.<br>**Schließen**<br>Geben Sie eine Lösung und Notizen an. Schließt die Gruppe.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. |
| Zurückgestellt | Ausgelöst durch die Schaltfläche **Zurückstellen**. In diesem Status können Sie:<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Schließen**<br>Geben Sie eine Lösung und Notizen an. Schließt die Gruppe.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe.<br>Informationen zum Aufschub werden auf der zugehörigen Registerkarte **Zurückstellen/Schließen** angezeigt. Am Zurückstellungsdatum wird die Gruppe erneut zur Korrektur geöffnet. |
| Warten auf Implementierung | Ausgelöst durch die Schaltfläche **„Warten auf Implementierung** “. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Erstellen Sie eine Change-Anforderung**<br>Weitere Informationen finden Sie unter Change-Anforderung in Configuration Compliance erstellen.<br>**Lösen**<br>Wählen Sie eine **Lösung aus**, und fügen Sie Notizen hinzu. Die Auswahlmöglichkeiten lauten wie folgt:<br>• Ergebnis ungültig<br>• Abgebrochen<br>• Repariert |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Konfigurations-Compliance-Status (Fortsetzung)**

| Status | Beschreibung |
|---|---|
| | Der Status wird zu Gelöst. Notizen werden auf der zugehörigen Registerkarte **Auflösung** angezeigt.<br>**Schließen**<br>Wählen Sie eine **Lösung aus**, und fügen Sie Notizen hinzu. Die Auswahlmöglichkeiten lauten wie folgt:<br>• Ergebnis ungültig<br>• Abgebrochen<br>• Repariert<br>Der Status wird zu Geschlossen. Notizen werden auf der zugehörigen Registerkarte **Auflösung** angezeigt.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. |
| Gelöst | Wird über die **Schaltfläche „Lösen** “ ausgelöst. In diesem Status können Sie:<br>**Security Incident**<br>Weitere Informationen finden Sie unter Security Incidents erstellen.<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Schließen**<br>Wählen Sie eine **Lösung aus**, und fügen Sie Notizen hinzu. Die Auswahlmöglichkeiten lauten wie folgt:<br>• Ergebnis ungültig<br>• Abgebrochen<br>• Repariert<br>Der Status wird zu **Geschlossen**. Notizen werden auf der zugehörigen Registerkarte **Auflösung** angezeigt.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe.<br>Notizen werden auf der zugehörigen Registerkarte **Notizen** angezeigt. Lösungsinformationen werden auf der zugehörigen Registerkarte **Auflösung** angezeigt. |
| Geschlossen | Ausgelöst durch die Schaltfläche **Schließen**. In diesem Status können Sie:<br>**Erneut öffnen**<br>Gehen Sie zurück in den Status „Offen“.<br>**Löschen**<br>Bestätigen Sie den Löschvorgang. Entfernt die Gruppe.<br>Abschlussinformationen werden auf der zugehörigen Registerkarte **Zurückstellen/Schließen** angezeigt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Korrekturaufgabe als Geschlossen markiert ist und einen nicht festen Substatus aufweist (z. B. „Risiko akzeptiert“ oder „Irrelevant“), wird der Status von Testergebnissen, die der Gruppe hinzugefügt werden, entsprechend der Korrekturaufgabe aktualisiert.
- Wenn die Korrekturaufgabe als „Geschlossen“ oder „Behoben“ markiert ist und das hinzugefügte Testergebnis nicht selbst „Geschlossen“ oder „Behoben“ ist, ändert sich der Status des Testergebnisses nicht, und der Status der Korrekturaufgabe wird in „Offen“ geändert.
- Wenn Sie feststellen, dass die Ergebnisse eine niedrige Priorität haben, können Sie ihre Gruppe für eine bestimmte Zeit in den Status „Zurückgestellt“ ändern oder sie sofort schließen.

**Hinweis:**
Wenn Korrekturaufgaben zurückgestellt oder geschlossen werden, können Sie Substatus angeben, um die Gründe dafür weiter zu definieren. Arbeitsnotizen werden entsprechend dem Übergang aktualisiert.

- Wenn Sie eine neue Korrekturaufgabe erstellen oder eine Korrekturaufgabe aufteilen, werden die Felder **Grund**und **Bis** für neue und alte Testergebnisgruppen neu ausgewertet. Wenn der Status aller Testergebnisse Zurückgestellt ist, wird der Wert in den Feldern **Grund** und **Bis** zur Testergebnisgruppe zusammengefasst.
  - Wenn alle Testergebnisse in einer Testergebnisgruppe zurückgestellt werden und denselben **Grund**haben, wird der Testergebnisgruppe derselbe **Grund**zugewiesen. Andernfalls wird das Feld **Grund** in **Keine**geändert.
  - Das Datum im Feld **Bis** wird mit dem nächsten Bis-Datum aller Testergebnisgruppen aktualisiert, zu denen die Testergebnisse gehören.

**Hinweis:**
Diese Auswertung erfolgt durch die geplante Aufgabe *`Rollup test result values to test result group and configuration test`*, die stündlich ausgeführt wird.

## Testergebnisstatus

Der Status einer Korrekturaufgabe ändert auch den Status der zugehörigen Testergebnisse. Dieser Mechanismus hat zwei Fälle.

**Testergebnisse, die nur zu einer Gruppe gehören**

Die Ergebnisse stimmen mit drei Ausnahmen mit dem Status der Korrekturaufgabe überein:

- Wenn der Status der Korrekturaufgabe in „Geschlossen“ und ihre Auflösung (Substatus) in „Festgelegt“ geändert wird, ignoriert das Element diese Änderung und fällt dann in den Status „Offen“ zurück.
- Wenn die Korrekturaufgabe ihren Status in „Geschlossen“ und ihre Auflösung (Substatus) in „Abgebrochen“ ändert, ignoriert das Element diese Änderung und fällt dann in den Status „Offen“ zurück.
- Wenn der Status der Testergebnisquelle „Korrigiert“ lautet (aktualisiert durch einen Scan oder Import), ändert sich der Status der Korrekturaufgabe in „Geschlossen (Korrigiert)“ des Testergebnisses, unabhängig davon, in welchem Status sich die Korrekturaufgabe befindet .

**Testergebnisse, die mehreren Gruppen angehören**

Testergebnisse stimmen nicht automatisch mit dem Status der Korrekturaufgabe überein. Stattdessen wird in allen zugeordneten Gruppen nach dem Status mit der höchsten anzuwendenden Rangfolge gesucht. Dies ist der Status der Rangfolge:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Geschlossen (Substatus: Ergebnis ungültig)** > **Zurückgestellt** > **Gelöst** > **Warten auf Implementierung** > Wird **untersucht** > **Offen**

**Hinweis:**
**Geschlossen (Substatus: Fest)** und **Geschlossen (Substatus: Abgebrochen)** sind zwei Sonderfälle.

## Beispiele für Korrekturaufgabenstatus

Beispiel:

| Status der Korrekturaufgaben | Status des Testergebnisses |
|---|---|
| Gruppe A: **Offen** > **Wird untersucht**<br><br>Gruppe B: **Offen** | **Wird untersucht**<br><br>Wenn Gruppe A „Wird untersucht“ und Gruppe B „Offen“ ist, ändert sich das Testergebnis in „Wird untersucht“, da nach der Suche Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat. |
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Offen** > **Wird untersucht** | **Wird untersucht**<br><br>Wenn Gruppe B „Wird untersucht“ und Gruppe A „Wird untersucht“ ist, bleibt das Testergebnis „Wird untersucht“, da nach der Suche zwischen Gruppe A und Gruppe B beide den Status mit derselben Rangfolge haben. |
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Wird untersucht** > **Warten auf Implementierung** | **Warten auf Implementierung**<br><br>Wenn Gruppe B „Warten auf Implementierung“ und Gruppe A „Wird untersucht“ lautet, ändert sich das Testergebnis in „Warten auf Implementierung“, da nach der Suche zwischen Gruppe A und Gruppe B Gruppe B den Status mit der höchsten Priorität hat |
| Gruppe A: **Wird untersucht** > **Zurückgestellt**<br><br>Gruppe B: **Warten auf Implementierung** | **Zurückgestellt**<br><br>Wenn Gruppe A „Zurückgestellt“ und Gruppe B „Warten auf Implementierung“ ist, ändert sich das Testergebnis in „Zurückgestellt“, da Element 1 nach der Suche herausgefunden hat, dass Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat |
| Gruppe A: **Zurückgestellt**<br><br>Gruppe B: **Warten auf Implementierung** > **Geschlossen (Ergebnis ungültig)** | **Geschlossen (Ergebnis ungültig)** > **Zurückgestellt**<br><br>Wenn Gruppe B Geschlossen ist und die Auflösung (Substatus) Ergebnis ungültig ist und Gruppe A Zurückgestellt ist, ändert sich das Testergebnis in Geschlossen (Ergebnis ungültig), da nach der Suche Gruppe B zwischen Gruppe A und Gruppe B den Status mit hat die höchste Rangfolge. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Status der Korrekturaufgaben | Status des Testergebnisses |
|---|---|
| Gruppe A: **Zurückgestellt**<br><br>Gruppe B: **Geschlossen (Ergebnis ungültig)** > **Öffnen (über Erneut öffnen)** | **Zurückgestellt**<br><br>Wenn Gruppe B erneut geöffnet wird und sich ihr Status in „Offen“ ändert und Gruppe A „Zurückgestellt“ ist, ändert sich das Testergebnis in „Zurückgestellt“, da nach der Suche Gruppe A zwischen Gruppe A und Gruppe B den Status mit der höchsten Priorität hat. |

### Sonderfälle für Testergebnisstatus

| Status der Korrekturaufgabe | Testergebnisstatus |
|---|---|
| Gruppe A: **Wird untersucht**<br><br>Gruppe B: **Warten auf Implementierung** > **Geschlossen (repariert oder storniert)** | **Wird untersucht**<br><br>Wenn Gruppe B „Geschlossen“ ist (Substatus „Festgelegt“ oder Substatus „Abgebrochen“) und Gruppe A „Wird untersucht“ ist, ändert sich das Testergebnis von „Warten auf Implementierung“ (bisher die höchste Rangfolge) zu „Wird untersucht“ (derzeit die höchste Rangfolge). |
| Gruppe A: beliebiger Status<br><br>Gruppe B: beliebiger Status | Wenn der Status der Testergebnisquelle „Korrigiert“ lautet (aktualisiert durch einen Scan oder Import), ändert sich der Status der Korrekturaufgabe in „Geschlossen (Korrigiert)“, unabhängig vom Status der anderen zugeordneten Korrekturaufgaben. sind in. Die Testergebnissuche für den Status der Korrekturaufgabe tritt nicht auf. |

## Configuration Compliance Importprobleme werden gelöst

Beheben Sie Probleme mit dem Import von Drittanbieterintegrationen.

### Problemlösung importieren

| Vorfall | Lösung |
|---|---|
| Testergebnisse fehlen | Überprüfen Sie `Start Time` für die Integration von **Qualys PC-Ergebnissen**.<br><br>Er ist möglicherweise nicht weit genug zurückgesetzt. Weitere Informationen finden Sie unter Ändern Sie das Startdatum der Qualys PC-Ergebnisse. |
| Die Integration ist fehlgeschlagen | Überprüfen Sie den Ausführungsstatus der **Schwachstellenintegration**.<br><br>Einzelne Integrationsprozesseinträge enthalten die importierte XML, die auf unerwartete Informationen untersucht werden kann.<br><br>Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **QualysPC-Ergebnisse** > **Integrationsausführungen für Schwachstellen** Zugehörige Registerkarte.<br><br>Wählen Sie die letzte Ausführung aus. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Problemlösung importieren (Fortsetzung)**

| Vorfall | Lösung |
|---|---|
| | Überprüfen Sie den Status und die Notizen der Einträge in der zugehörigen Liste **Integrationsprozess für Schwachstellen** auf Anomalien.<br>. |

### Ändern Sie das Startdatum der Qualys PC-Ergebnisse

Wenn Daten für das Startdatum im Qualys PC-Ergebnisimport fehlen, können sie geändert werden.

#### Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin

#### Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**.
2. Klicken Sie **auf Qualys PC-Ergebnisse** Integration.
3. Klicken Sie auf **Integrationsdetails**.
4. Legen Sie das Feld **Startzeit** auf einen Wert in der Vergangenheit fest, damit alle gescannten und erkannten Testergebnisse seit diesem Zeitpunkt erkannt werden.

   **Hinweis:**
   Wenn das Datum leer gelassen wird, werden bei der ersten Ausführung keine Daten zurückgegeben. Legen Sie den Wert auf maximal einen Monat in der Vergangenheit fest. Diese Einstellung verhindert, dass eine große Datenmenge die Ratenbeschränkungen der Qualys-API überschreitet und Ausführungszeitüberschreitungen auslöst.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie auf **Jetzt** ausführen, um den Vorgang sofort auszuführen.

## CI-Suchregeln für Microsoft Defender for Cloud Integration für Security Operations und Palo Alto Prisma Cloud

Sie können die Suchregeln für Configuration Items (CIs) für die Integrationen Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud verwenden, um eine korrekte Übereinstimmung mit häufig verwendeten Ressourcentypen in Configuration Management Database (CMDB)zu finden.

### Übersicht

Das Modul „CI-Suchregeln“ enthält die Regeln, die Sie beim Definieren der Felder mit den übereinstimmenden Daten in Configuration Management Database (CMDB)unterstützen. Sie können die folgenden Regeln verwenden, um die Anwendungen und Anwendungsveröffentlichungen zu identifizieren. Alle Microsoft Defender for Cloud Integration - und Palo Alto Prisma Cloud -Assets werden eindeutig durch die Kombination von Objekt-ID, Cloud-Konto und logischem Rechenzentrum in der ServiceNow -Plattformidentifiziert. Die Erkennung [ ServiceNow füllt die Ressourcen-ID in der Spalte `Object_id` von CMDB in verschiedenen Formaten für die verschiedenen Ressourcentypen aus. Die folgende Tabelle zeigt die Objekt-ID-Formate häufig verwendeter Ressourcentypen, die vom Discovery-Service zum Ausfüllen der Spalte `Object_id` des CI verwendet werden. Jeder Scanner, der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein Asset eines bestimmten Ressourcentyps suchen möchte, muss im richtigen Objekt-ID-Format suchen. Sie können das richtige Objekt-ID-Format erhalten, indem Sie in die Objekt-ID-Spalte der entsprechenden CMDB CI-Klasse schauen und dann versuchen, die Objekt-ID mit den vom Scanner empfangenen Werten zu erstellen.

**Objekt-ID-Format für verschiedene Ressourcentypen**

| Ressourcentyp | Format |
|---|---|
| AWS::EC2::Instance | Objekt-ID |
| AWS::ElasticLoadBalancing::LoadBalancer | Name des Lastenausgleichsmoduls |
| AWS::S3::Bucket | arn:aws:s3:::<Bucket Name> |

Die CI-Übereinstimmung für ein Testergebnis wird in Configuration Management Database (CMDB) möglicherweise nicht genau gefunden, es sei denn, in der Suchregel wird dasselbe Format der `object_id` verwendet. Meistens finden die OOB-CI-Suchregeln eine Übereinstimmung mit den am häufigsten verwendeten Ressourcentypen für Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud. Wenn die folgenden CI-Suchregeln die CIs in CMDB für Ihre Testergebnisse nicht finden, können Sie eine CI-Suchregel für einen Ressourcentyp erstellen. Weitere Informationen zum Erstellen einer CI-Suchregel finden Sie unter CI-Suchregeln erstellen.

## CI-Suchregeln

Die folgenden CI-Suchregeln gelten spezifisch für Microsoft Defender for Cloud Integration und Palo Alto Prisma Cloud.

### S3-Bucket

Diese Suchregel versucht, das CI in CMDB anhand des Werts zu finden, der durch Verkettung von `arn:aws:s3:::` und Ressourcenname erhalten wurde. Der erhaltene Wert wird in der Spalte `object_id` der Tabelle `cmdb_ci_cloud_object_storage` gesucht. Diese Suchregel gilt nur, wenn der Ressourcentyp `AWS::S3::Bucket`lautet

### Name

Diese Suchregel versucht, das CI in CMDB anhand des Namens zu finden. Der Name, der in der Spalte `Object_id` der CI-Klasse gesucht wird, entspricht einem Ressourcentyp in der Tabelle `sn_capi_resource_type`.

**Hinweis:**
Für die Anwendung Palo Alto Prisma Cloud wird diese CI-Suchregel nur für die `Ressourcentypen AWS::RDS::DBInstance`, `AWS::ElasticLoadBalancing::LoadBalancer`und `AWS::CloudTrail::Trail` `ausgeführt`. Sie können die Ressourcentypen hinzufügen, für die Sie diese CI-Suchregel ausführen möchten.

### Ressourcen-ID

Diese Suchregel versucht, das CI in CMDB anhand der Ressourcen-ID zu finden. Die Ressourcen-ID, die in der Spalte `Object_id` der CI-Klasse gesucht wird, entspricht einem Ressourcentyp in der Tabelle `sn_capi_resource_type`.

**Hinweis:**
Sie können die Priorität für eine CI-Suchregel im Feld **Reihenfolge** festlegen. Die CI-Suchregel mit dem geringsten Reihenfolgewert wird zuerst ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Vulnerability Response – Allgemein

Das Plugin „Vulnerability Response Common“ wird installiert, wenn Sie die Anwendung Vulnerability Response installieren.

Ab Version 20.0 von Vulnerability Response können Sie das Framework für zusammengefasste Berichte in Vulnerability Response Common verwenden, um Berichte für Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Fehlkonfigurationen zu erstellen.

## Framework für zusammengefasste Berichte

Mit dem Framework für zusammengefasste Berichte können Sie Berichte für die Daten erstellen, die komplexe On-the-fly-Abfragen mit langer Ausführungszeit umfassen, um die Leistung zu verbessern.

Das Framework für zusammengefasste Berichte verbessert die Leistung durch:

- weniger Ressourcen verbrauchen und Berichte schneller erstellen,
- Zusammenfassen der Daten und Wiederverwenden von Zusammenfassungen und Aufgliederungen (Gruppieren nach) und
- Reduzieren der Abfragen an die Datenbank

Wenn Sie mehr als eine Million angreifbarer Elemente haben, verwenden Sie das in Vulnerability Response Common bereitgestellte Framework neben Standardberichten.

### Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics -Administrator (pa_admin): Zusammenfassungen, Widgets und Dashboards überprüfen Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in den Zusammenfassungen und den zusammengefassten Ergebnissen.
- VR-Leser (sn_vul_cmn.read): Überprüfen Sie die Daten in den Zusammenfassungen und den zusammengefassten Ergebnissen.
- Schwachstellenanalyst (sn_vul.vulnerability_analyst): Überprüfen Sie die zusammengefassten Ergebnisse.

**Zugehörige Informationen**

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Konfigurieren Sie eine Zusammenfassung für Quelldaten

Um die Leistung eines bestimmten Aspekts in einem Geschäftsprozess zu analysieren, der in einer Tabelle ServiceNow aufgezeichnet wird, erstellen Sie eine für den Aspekt spezifische Zusammenfassung und erstellen einen Bericht für diese Zusammenfassung.

### Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin

### Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zusammenfassungsdefinitionen** > **Alle** und klicken Sie auf **Neu**.
2. Geben Sie der Zusammenfassung im Feld **Name** einen beschreibenden Namen.
3. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der Zusammenfassung ein.
4. Füllen Sie die Felder auf der Registerkarte **Quelle** aus.

**Felder auf der Registerkarte „Quelle“**

| Feld | Beschreibung |
|---|---|
| Tabelle | Tabelle, aus der Sie die Daten für den Bericht abrufen möchten. Diese Dropdown-Liste enthält nur die Tabellen „App Sec Common“, „App-Vul“, „App-Vulc“, „App-Vul-Container“ und „Anwendungsschwachstelle“. |
| Aggregatfunktion | Funktion, die auf die in **Feld**ausgewählte Spalte angewendet werden soll.<br>○ **Anzahl**: Anzahl der Datensätze.<br>○ **Summe**: Gesamtsumme der Werte in der in **Feld**ausgewählten Spalte.<br>○ **Durchschnitt**: Durchschnitt aller Werte in einer in **Feld**ausgewählten Spalte.<br>○ **Maximum**: Höchstwert in der unter **Feld**ausgewählten Spalte.<br>○ **Minimum**: Mindestwert der in **Feld**ausgewählten Spalte.<br>○ **Count Distinct**: Eindeutige Werte in der in **Feld**ausgewählten Spalte. |
| Feld | Spalte, auf die Sie die Funktion anwenden möchten.<br>**Hinweis:** Dieses Feld wird nicht angezeigt, wenn Sie im Feld **Funktion aggregieren** die Option Anzahl **auswählen**. |

5. Geben Sie auf der Registerkarte **Zusätzliche Bedingungen** die **Bedingung** im Feld Bedingungen an, um eine bestimmte Gruppe von Datensätzen auszuwählen, für die Sie die zusammengefassten Ergebnisse abrufen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. **Wählen** Sie auf der Registerkarte Gruppieren nach die Spalten der Tabelle aus, nach denen Sie die Daten gruppieren oder stapeln möchten.
   Sie können bis zu zwei Aufgliederungen auswählen.

   Wenn Sie die **Datumsspalte** in einem Gruppieren nach-Feld auswählen, wird das Feld **Trend nach** angezeigt. Sie können die nach Woche, Tag, Minuten usw. kategorisierten Zusammenfassungsergebnisse abrufen, indem Sie die Optionen im Feld **Trend nach** auswählen.

7. Wählen oder erstellen Sie auf der Registerkarte **Zeitplan** einen Zusammenfassungszeitplan, der die Häufigkeit definiert, mit der Sie die Zusammenfassung zum Abrufen der Daten ausführen können.
   Informationen zum Erstellen eines Zusammenfassungszeitplans finden Sie unter Führen Sie mehrere Zusammenfassungen gleichzeitig aus.

   **Hinweis:**
   Sie können die Zusammenfassungsausführung nicht für eine inaktive Zusammenfassungsdefinition planen.

8. Klicken Sie auf **Absenden**, um die Zusammenfassung zu erstellen.
   Die Zusammenfassung wird in der Zusammenfassungsliste angezeigt. Mit der vordefinierten Häufigkeit wird die Zusammenfassung ausgeführt, und in der zugehörigen Liste „Geplante Ausführungen“ wird für jede Ausführung ein Datensatz zusammen mit einem Ausführungsdatum und einer Ausführungszeit erstellt.
9. Navigieren zu **Alle** > **Zusammengefasste Ergebnisse** und öffnen Sie Ihre Zusammenfassung, um die zusammengefassten Ergebnisse und geplanten Ausführungen anzuzeigen.
   Die zusammengefassten Ergebnisse werden in der **zugehörigen** Liste „Zusammengefasste Ergebnisse“ aufgelistet. Wenn die Zusammenfassungsausführung fehlschlägt, finden Sie weitere Informationen in der Spalte „ **Notizen** “ in der zugehörigen Liste **„Geplante** Ausführungen“.
10. **Wahlweise:** Wählen Sie **Jetzt ausführen** aus, um die Zusammenfassungsergebnisse unabhängig vom Zusammenfassungszeitplan zu erfassen.
    Wenn Sie die geplante Ausführung beenden, während sie ausgeführt wird, werden an den zusammengefassten Ergebnissen keine Änderungen vorgenommen. Sie können eine Zusammenfassung auch löschen oder deaktivieren.

### Nächste Maßnahme

Erstellen Sie einen Bericht mit Ihrer Zusammenfassung. Weitere Informationen zum Erstellen eines Berichts mithilfe einer Zusammenfassung finden Sie unter Erstellen Sie einen Bericht mithilfe einer Zusammenfassung.

#### Zugehörige Informationen

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

## Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Sie können die Ausführung mehrerer Zusammenfassungen mit einem einzigen Zusammenfassungszeitplan planen.

### Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Sie möchten sechs Zusammenfassungen gleichzeitig ausführen. Erstellen Sie einen Zusammenfassungszeitplan, und fügen Sie ihm alle Zusammenfassungen hinzu. Diese Zusammenfassungen werden mit der definierten Häufigkeit und Uhrzeit ausgeführt.

### Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zeitplan**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Zusammenfassungszeitplan“ aus.

| Feld | Beschreibung |
|---|---|
| Zeitplanname | Name des Zusammenfassungszeitplans. |
| Regelmäßige Aufgabe | Geplante Skriptausführung, die die Häufigkeit definiert, mit der die Zusammenfassungen ausgeführt werden müssen. Sie können eine regelmäßige Aufgabe erstellen, indem Sie auf die Schaltfläche **Neu** klicken. |

4. Wählen Sie **Absenden**.
   Der Zusammenfassungszeitplan wird in der Liste Zusammenfassungszeitplan angezeigt.
5. Öffnen Sie Ihren Zusammenfassungszeitplan.
6. Wählen Sie **Bearbeiten**aus, fügen Sie der Zusammenfassungsliste die Zusammenfassungen **hinzu**, und wählen **Sie Speichern**aus.
   Die ausgewählten Zusammenfassungen werden in der zugehörigen Liste „Zusammenfassungen“ angezeigt.

   **Hinweis:**
   Wenn Sie einem Zeitplan eine inaktive Zusammenfassung hinzufügen, wird die geplante Ausführung nicht gestartet.

7. Wählen Sie **Aktualisieren**.
   Diese Zusammenfassungen werden mit der im Zusammenfassungszeitplan definierten Häufigkeit ausgeführt.

#### Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

## Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Ein neuer Prozessor oder ein Hintergrundauftrag, Prozessor für zusammengefasste Berichte, wird mit dem Basissystem geliefert, das die geplanten Aufgaben ausführt, die sich auf die Tabelle „Framework für zusammengefasste Berichte“ beziehen. Dadurch kann das gesamte Subsystem im Hintergrund ausgeführt werden, und die Systemressourcen werden besser genutzt, wenn sie verfügbar sind.

### Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Hintergrundauftragskonfiguration – Vulnerability Response Common – Zusammenfassungsergebnisrechner**.
2. Definieren Sie die Anzahl der Zusammenfassungen, die Sie gleichzeitig ausführen möchten, im Feld **Max. gleichzeitige Threads**, und wählen **Sie Speichern**aus.
   Standardmäßig werden vier Zusammenfassungen gleichzeitig ausgeführt.
3. Navigieren Sie zur Liste Hintergrundauftrags-Prozessorpools.
   **sn_sec_cmn_background_job_processor_pool.list**, und wählen Sie **Neu**, um einen Hintergrundauftrags-Prozessor für das Framework für zusammengefasste Berichte zu erstellen.
   Weitere Informationen zum Erstellen eines Prozessorpools für Hintergrundaufgaben finden Sie unter Erweiterte parallele Verarbeitung für Hintergrundaufgaben in Vulnerability Response .

**Hinweis:**
Die Anzahl der Hintergrundauftragsprozessoren muss der Anzahl der maximalen gleichzeitigen Threads entsprechen, die im Formular „ **Hintergrundauftragskonfiguration – Vulnerability Response Common – Aggregation Result Calculator“ angegeben** sind. Siehe Schritt 2.

#### Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

## Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Um die für eine von Ihnen erstellte Zusammenfassung spezifischen Daten zu visualisieren und zu analysieren, generieren Sie einen Bericht, indem Sie im Bedingungsgenerator eine Bedingung für die Zusammenfassung angeben.

### Vorbereitungen

Erforderliche Rolle: pa_admin

### Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Neu erstellen**.
2. Füllen Sie die Felder auf der Registerkarte **Daten** aus.

**Felder der Registerkarte „Daten“.**

| Feld | Beschreibung |
|---|---|
| Berichtname | Name des Berichts. |
| Quelltyp | Typ der Quelle, aus der Daten abgerufen werden. Wählen Sie **Tabelle** aus. |
| Tabelle | Name der Tabelle, für die die Zusammenfassung erstellt wird. Wählen Sie die Tabelle der zusammengefassten Ergebnisse, Zusammengefasstes **Ergebnis [sn_vul_cmn_aggregate_result] aus**. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Legen Sie im Bedingungsgenerator die Bedingung für Ihre Zusammenfassung fest, für die Sie einen Bericht generieren möchten.

**Bedingung im Bedingungsgenerator**

| Teil | Beschreibung |
|---|---|
| Feld | **Wählen**Sie Zusammenfassung aus. |
| Operator | Wählen Sie **ist**aus. |
| Wert | Name der Zusammenfassung. |

4. Klicken Sie auf der Registerkarte **Daten** auf **Weiter**.
5. Wählen Sie auf der Registerkarte **Typen** aus, wie Sie die Daten visualisieren möchten, und klicken Sie auf **Weiter**.
Weitere Informationen zu Berichtstypen finden Sie unter Berichte erstellen.

   Die unterstützten Visualisierungen sind Balkendiagramme, Kreisdiagramme und Heatmaps. Sie können die Liniendiagramme und andere Trendvisualisierungen ändern, um die unterstützten Visualisierungen mit aggregiertem Ergebnis zur Darstellung derselben Daten zu verwenden. Die Listenansicht wird nicht unterstützt.

6. Füllen Sie die Felder auf der Registerkarte **Konfigurieren** aus.

| Feld | Beschreibung |
|---|---|
| Gruppieren nach | Wählen **Sie Gruppiert nach 1** aus, die Sie auf der **Registerkarte** Gruppieren nach für die Zusammenfassung ausgewählt haben. |
| Stapeln nach | Wählen **Sie Gruppiert nach 2** aus, die Sie auf der **Registerkarte** Gruppieren nach für die Zusammenfassung ausgewählt haben. |
| Zusammenfassung | Wenden Sie die **Minimum-** oder **Maximum-**Funktion auf **den Wert**an. |

7. Füllen Sie auf der Registerkarte **Stil** die entsprechenden Felder aus, und klicken Sie auf **Ausführen**.
Weitere Informationen zu den Feldern auf den Registerkarten „ **Konfigurieren** “ und „ **Stil** “ finden Sie im Video „Bericht erstellen“ .
8. Legen Sie im Bedingungsgenerator die Bedingung für Ihre Zusammenfassung fest, für die Sie einen Bericht generieren möchten, und klicken Sie auf **Ausführen**.

   Der Bericht wird angezeigt.

9. Um die Werte auf der X-Achse zu sortieren, wählen **Sie Sortierung hinzufügen**aus.

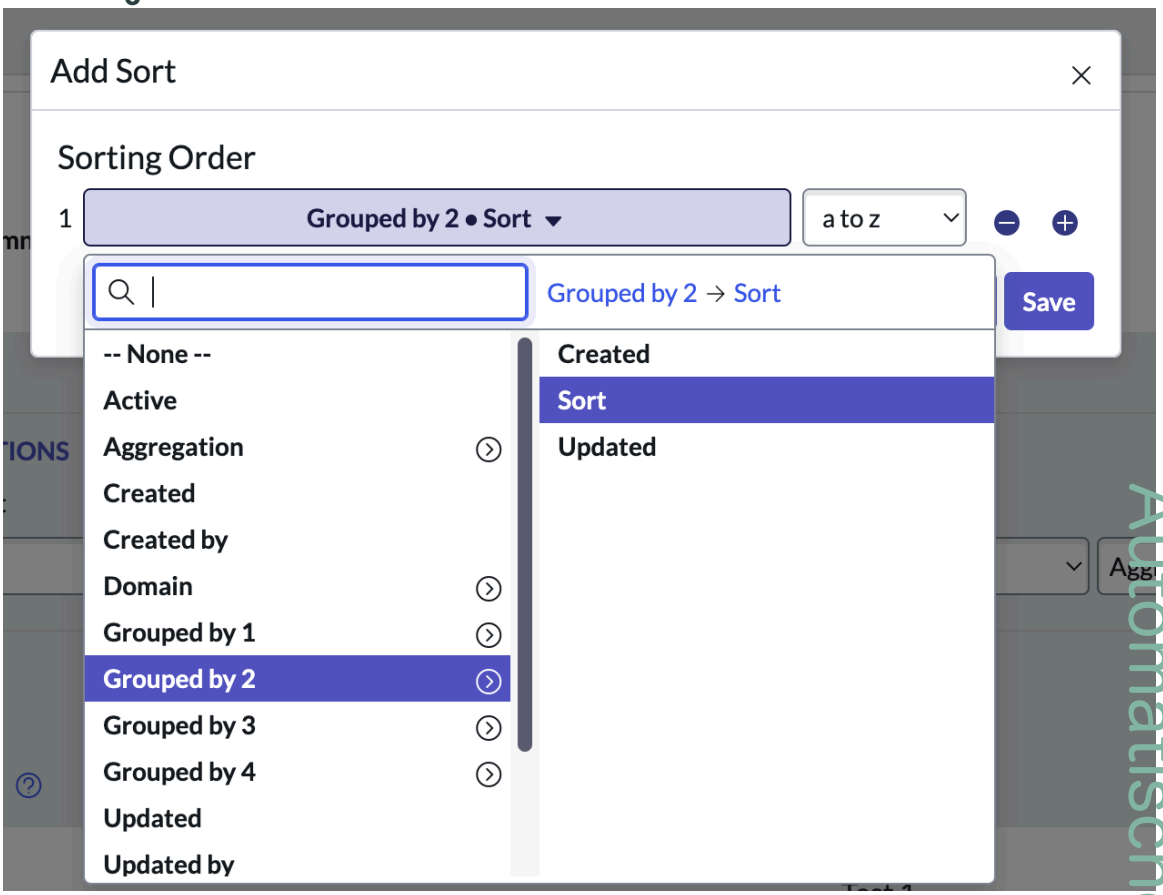
   a. Geben Sie für Zeichenfolgen die Bedingung **Gruppiert nach > az oder za** an, um die Zeichenfolgen in alphabetischer Reihenfolge zu sortieren.

   b. Geben Sie für Werte vom Datentyp Ganzzahl und Datum die Bedingung **Gruppiert nach.Sortieren > az oder za** an, um die Werte in aufsteigender bzw. absteigender Reihenfolge zu sortieren.

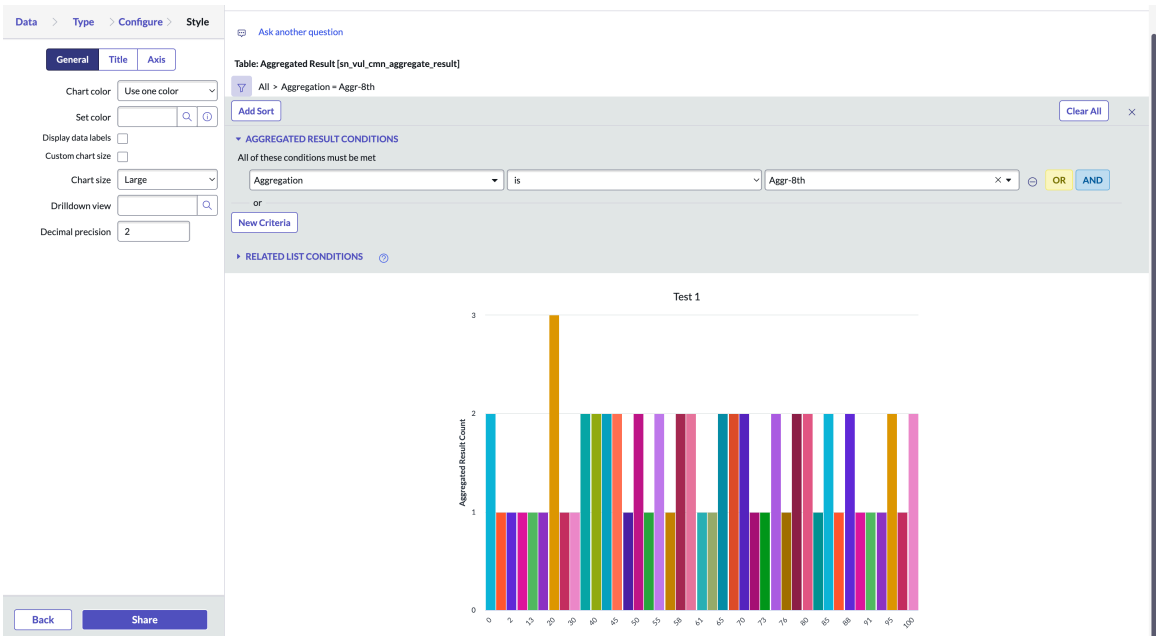
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Sortierung von Ganzzahlen auf der X-Achse**




**c.** Wählen Sie **Ausführen**.
Die Ganzzahl- und Datumswerte werden auf der X-Achse sortiert.




**10.** Klicken Sie auf **Speichern**, um Ihren Bericht zu speichern.
Der Bericht, der für eine Zusammenfassung generiert wird, wird auf der Registerkarte **Ergebnisse** des entsprechenden Zusammenfassungsformulars **angezeigt**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. **Wahlweise:** Fügen Sie Ihren Bericht einem Dashboard hinzu.
    Weitere Informationen zum Hinzufügen eines Berichts zu einem Dashboard finden Sie unter Berichte zu einem interaktiven Dashboard hinzufügen.

    Das Dashboard **„Schwachstellenmanagement [Aggregiert]“**, das aus Berichten besteht, die mit dem zwischengespeicherten Berichts-Framework erstellt wurden, ist im Lieferumfang des Basissystems enthalten. Um dieses Dashboard anzuzeigen, navigieren Sie zu **Alle** > **Performance Analytics** > **Dashboards** > **Alle** > **Schwachstellenmanagement [Aggregiert]**. Die aktiven Zusammenfassungen, die den Berichten in diesem Dashboard entsprechen, werden mit dem Basissystem geliefert.

12. Geben Sie Ihren Bericht für andere Benutzer frei.
    Weitere Informationen zum Freigeben von Berichten finden Sie unter Berichte verteilen .

**Zugehörige Informationen**

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

# Threat Intelligence

Mit der Anwendung ServiceNow® Threat Intelligence können Sie Kompromittierungsindikatoren (IoC) finden und Security Incidents mit Threat Intelligence-Daten anreichern.

| | | |
|---|---|---|
| Erkunden<br>• Threat Intelligence verstehen<br>• Domain Separation und Threat Intelligence<br>• Washington DC<br>• Orchestration für Threat Intelligence<br>• Videos zu Security Operations | Einrichten<br>• Threat Intelligence installieren<br>• Definieren Sie eine Bedrohungsquelle | Verwalten<br>Legen Sie Threat Intelligence Eigenschaften fest |
| Verwenden | Entwickeln | Integrieren |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | | |
|---|---|---|
| • Angriffsmodi und -methoden<br>• Kompromittierungsindikatoren<br>• Erkennbare Elemente<br>• Security Case Management | • Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden | • Threat Intelligence-Integrationen<br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen |
| Problembehandlung und Hilfe<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | | |

## Threat Intelligence verstehen

Mit der Anwendung Threat Intelligence können Sie auf dieSTIX™-Daten Ihres Unternehmens zugreifen und einen Bezugspunkt dafür bereitstellen. In Threat Intelligence ist die Anwendung Security Case Management enthalten, die eine Möglichkeit zur Analyse von Bedrohungen für Ihre Organisation bietet, die von gezielten Kampagnen oder staatlichen Akteuren ausgehen.

STIX ist eine Sprache zur Beschreibung von Cyberbedrohungsinformationen auf standardisierte und strukturierte Weise. Mithilfe von STIX-Daten undTAXII-™Profilen (Trusted Automated Exchange of Indicator Information) können Bedrohungsexperten freigegebene Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und aus anderen Quellen identifiziert wurden. TAXII ermöglicht einen weit verbreiteten automatisierten Austausch von Informationen über Cyberbedrohungen.

Threat Intelligence unterstützt die STIX-Versionen 1.1, 2.0 und 2.1.

STIX™ und TAXII™ sind Markenzeichen von MITRE.

### Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Domain Separation und Threat Intelligence

Domänentrennung wird im Modul Threat Intelligence unterstützt, das als Teil von Security Incident Response verfügbar ist. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

## Support-Stufe: Basis

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für Domänentrennung .

## Übersicht

Im Threat Intelligence-Modul (als Teil der Security Incident Response-Anwendung) ermöglicht die Domänentrennung Service Providern (SPs), das Threat Intelligence-Repository wie folgt zu erstellen und zu verwalten:

- Bedrohungsquellen und TAXII-Profile (Trusted Automated Exchange of Indicator Information).
- Erkennbare Elemente
- Kompromittierungsindikatoren
- Bedrohungsangriffsmodi/-methoden und Fallmanagement im gesamten Kundenstamm mit geringeren Betriebskosten und höherer Servicequalität

Durch separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. wird sichergestellt, dass Kundendaten getrennt und niemals für andere Clients verfügbar sind.

## Unterstützung der Domänentrennung in Threat Intelligence nach Versions-Release

Die Domänentrennung für das Threat Intelligence-Modul (als Teil der Anwendung Security Incident Response ) umfasst die folgenden Produktfunktionen:

- Erkennbare Security Incident-Elemente werden an die entsprechende Domäne des Benutzers weitergeleitet, dessen ID/Anmeldeinformationen/Umfang den Incident generiert. Die aus dem Incident extrahierten erkennbaren Elemente werden in der Domäne des Security Incident gespeichert.
- Einrichten von TAXII-Serviceprofilen zum Herunterladen einer oder mehrerer TAXII-Sammlungen, die Informations-Feeds zu Cyberbedrohungen anbieten. Die Konfiguration wird in der Domäne gespeichert, unter der das Profil eingerichtet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Richten Sie den Download von Bedrohungs-Feeds in das IoC-Repository in der Domäne ein, in der die Konfiguration ausgeführt wird.
- Erstellung von Angriffsmodus/-methoden in der Domäne der Threat Intelligence-Quelle, die die Informationen automatisch bereitstellt, oder der Domäne, in der ein neuer Angriffsmodus/eine neue Angriffsmethode manuell vom Benutzer hinzugefügt wird
- Erstellung von Fällen für die langfristige Untersuchung von Incidents, erkennbaren Elementen, CIs, Benutzern und Gefährdungsindikatoren (IoC), die dem Fall zugeordnet sind. Der Fall wird in der vom Benutzer erstellten Domäne gespeichert.

**Hinweis:**
In allen oben genannten Fällen gelten die übergeordneten Prinzipien der Transparenz in getrennten Domänen in der NOW-Plattform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

## Funktionsweise der Domänentrennung in Threat Intelligence (als Teil von Security Incident Response)

Threat Intelligence ist Teil von Security Incident Response in den Stufen „Professional“ und „Enterprise“, nicht jedoch in der Stufe „Standard“. Daher ist ein separates Plugin erforderlich. Das Threat Intelligence-Modul (als Teil der Anwendung Security Incident Response ) erstellt und verwaltet die Threat Intelligence-Informationen, die Security Incidents in einer Organisation zugeordnet sind. Die folgenden Anwendungsfälle sind für die Domänentrennung geeignet:

- Erstellung von erkennbaren Security Incident-Elementen zum Zeitpunkt der Incident-Erstellung
  - Von E-Mail-Parsern (plattformbasiert, von Benutzern gemeldetes Phishing, benutzerdefiniert)
  - Aus Anwendungen in SIEM-Speichern (Security Information and Event Management) von Drittanbietern
  - Manuell vom SOC-Analysten eingegeben
- Sammlung von erkennbaren Elementen aus Bedrohungs-Feed-Quellen: Threat Intelligence-Quellen aus TAXII-Sammlungen
- Erkennbare Security Incident-Elemente verwalten
  - Ordnen Sie erkennbare Elemente zugehörigen Indikatoren zu
  - Verknüpfen Sie erkennbare Elemente mit Security Incidents
  - Ordnen Sie erkennbare Elemente untergeordneten erkennbaren Elementen zu
  - Ordnen Sie das erkennbare Element der Bedrohungs-Feed-Quelle zu
  - Fügen Sie Sicherheitsanmerkungen zu erkennbaren Elementen hinzu
- Gefährdungsindikatoren verwalten
  - Verknüpfen Sie Indikatoren mit zugehörigen erkennbaren Elementen
  - Ordnen Sie Indikatoren dem Angriffsmodus/der Angriffsmethode zu
  - Ordnen Sie Indikatoren Indikatortypen zu
  - Ordnen Sie Indikatoren der Bedrohungs-Feed-Quelle zu
  - Fügen Sie Indikatoren Sicherheitsanmerkungen hinzu
- Fälle verwalten



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fall erstellen (manuell oder aus einem Incident)
- Neuen Fall bearbeiten, um Details hinzuzufügen (Falltyp und Schweregrad auswählen, Incidents, erkennbare Elemente, Konfigurationselemente, Benutzer, Indikatoren hinzufügen)
- Löschen Sie einen Fall

## Domänentrennung – Einrichtung

Das Einrichten der Domänentrennung für Threat Intelligence erfordert keine zusätzlichen Schritte. Alle Threat Intelligence-Tabellen erfassen die Domänenspalte, nachdem die Instanz domänengetrennt wurde.

## Domänengetrennte Daten

Daten können domänengetrennt sein, was bedeutet:

- Erkennbare Security Incident-Elemente in einer Domäne können nicht im Umfang anderer Domänen angezeigt werden.
- Kompromittierungsindikatoren in einer Domäne können nicht im Umfang anderer Domänen angezeigt werden.
- Angriffsmodi/-methoden, die einer Domäne zugeordnet sind, können nicht aus dem Bereich anderer Domänen angezeigt werden.
- TAXII-Serviceprofile, die einer Domäne zugeordnet sind, können nicht aus dem Bereich anderer Domänen angezeigt werden.
- Einer Domäne zugeordnete Threat Intelligence-Quellen können nicht im Umfang anderer Domänen angezeigt werden.
- Fälle, die einer Domäne zugeordnet sind, können nicht im Bereich anderer Domänen angezeigt werden.

Threat Intelligence-Eigenschaften werden auf globaler Ebene festgelegt und sind daher nicht domänengetrennt. Die Einstellungen umfassen:

- Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs
- Der API-Schlüssel, der für den Abruf verwendet werden soll
- Sucht nach lokalen IoC-Tabellen, bevor sie an den Remote-Scanner gesendet wird
- Anzahl der Tage, an denen lokale erkennbare Elemente berücksichtigt werden
- Markieren eines Angriffsmodus/einer Angriffsmethode als inaktiv, wenn er nicht aus Bedrohungsinformationsquellen empfangen wird
- Markieren eines Indikators als inaktiv, wenn er für eine bestimmte Anzahl von Tagen nicht von einer Quelle empfangen wurde

## Konfiguration

Alle Aspekte der Konfiguration der Threat Intelligence-Funktionalität sind in einer domänengetrennten Umgebung in sich abgeschlossen.

Die folgenden Aufgaben können pro Domäne konfiguriert werden:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Erstellung von TAXII-Serviceprofilen
   - Wählen Sie eine Discovery-Servicekonfiguration aus
   - Wählen Sie eine Sammlungsservice-Konfiguration aus: Weisen Sie Benutzern und Benutzergruppen Rollen zu
2. Erstellung von Threat Intelligence-Quellen
   - Konfigurieren Sie den REST-Service, der die Bedrohungsinformationen bereitstellt
   - Planen Sie den Download von Informationen zu Bedrohungen
   - Wählen Sie Bedrohungsdetailinformationen aus, die der Quelle zugewiesen werden sollen
3. Erstellung von Angriffsmodus/-methoden (manuell)
   - Quelle, Malware-Typ, Angriffsmechanismus, Typ des Bedrohungsakteurs, Beschreibung, Handhabung, beabsichtigte Wirkung, zuerst gesehen, zuletzt gesehen
   - Zugehörige Indikatoren, untergeordneter Angriffsmodus/-methode, zugehörige Security Incidents

   **Hinweis:**
   Angriffsmodi/-methoden werden auch automatisch aus den Bedrohungs-Feed-Quellen erstellt.

4. Standardlisten für die folgenden Bedrohungsinformationskategorien festlegen:
   - Angriffsmechanismen
   - Discovery-Methoden
   - Feeds
   - Indikatortypen
   - Beabsichtigte Wirkungen
   - Benachrichtigungen
   - Erkennbare Typen
   - Quotengrenzdefinitionen
   - Bedrohungsakteurtypen
   - Angriffsmotivationen
   - Infrastrukturtypen
   - Malware-Fähigkeiten
   - Schadsoftwaretypen
   - Berichtstypen
   - Rollen des Bedrohungsakteurs
   - Tooltypen

## Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Mandantendomänenbesitzer können ihre eigenen TAXII-Serviceprofile erstellen.
- Mandantendomänenbesitzer können ihre eigenen Threat Intelligence-Quellen erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mandantendomänenbesitzer können ihre eigenen Angriffsmodi/-methoden erstellen.
- Mandantendomänenbesitzer können ihre eigenen Standardlisten für Bedrohungsinformationskategorien erstellen.

**Hinweis:**
Geschäftslogik und Prozesse ermöglichen die Domänentrennung nach Instanzbesitzern für die Download-Zeitpläne für Threat Intelligence-Quellen.

**Zugehörige Informationen**

Domänentrennung für Service Provider

## Threat Intelligence einrichten

Bevor Sie Threat Intelligence in Ihrer Instanz ausführen, müssen Sie es aus dem ServiceNow Storeherunterladen. Sie können auch Eigenschaften einrichten und eine Bedrohungsquelle definieren.

### Threat Intelligence installieren

Bevor Sie Threat Intelligence in Ihrer Instanz ausführen, müssen Sie es aus dem ServiceNow Storeherunterladen.

**Vorbereitungen**
Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

| Setupaufgaben | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie über die erforderlichen Rollen ServiceNow für Ihre Instanz verfügen. | Die folgenden Rollen sind für die Installation, Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Wenn noch nicht zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Bedrohungsadministrator“ [sn_ti.admin] zu.<br>• Der Bedrohungsadministrator [sn_ti.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. |

Erforderliche Rolle: admin

**Prozedur**

Befolgen Sie die Anweisungen für Herunterladen einer Anwendung aus dem ServiceNow Store.

**Nächste Maßnahme**
Legen Sie Threat Intelligence Eigenschaften fest.

#### Mit Threat Intelligence installierte Komponenten

Bei der Aktivierung des Threat Intelligence-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

## Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| Bedrohungsadministrator<br><br>[sn_ti.admin] | Hat die vollständige Kontrolle über alle Bedrohungseigenschaften, SLAs und Benachrichtigungen. | sn_ti.write |
| Bedrohungsleser<br><br>[sn_ti.read] | Hat Lesezugriff auf Bedrohungsinformationen. | sn.sec_cmn.int_read |
| Bedrohungsautor<br><br>[sn_ti.write] | Hat Schreibzugriff auf Bedrohungsinformationen.<br><br>Angriffsmodi, Indikatoren oder erkennbare Elemente können nicht gelöscht werden. Nur ein Bedrohungsadministrator kann sie löschen. | • sn_sec_cmn.int_write<br>• sn_ti.read |
| MITRE-Analyst<br><br>[sn_ti.mitre_analyst] | Diese Rolle ermöglicht den Lesezugriff auf die Module [ MITRE-ATT&CK in Threat Intelligence und auf das Modul SIR. | • sn_ti.read<br>• sn_si.read |

## Installierte Tabellen

| Tabelle | Beschreibung |
|---|---|
| Angriffsmechanismus<br><br>[sn_ti_attack_mechanismus] | Organisiert Angriffsmuster hierarchisch basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle verwendet werden. Die Kategorien, die Mitglieder dieser Ansicht sind, stellen die verschiedenen Techniken dar, die für Angriffe auf ein System verwendet werden. |
| Angriffsmodus/-methode<br><br>[sn_ti_attack_mode] | Angriffsmodi und -methoden sind Darstellungen des Verhaltens von Cyberangreifern. Sie beschreiben in zunehmendem Detailgrad, was ein Angreifer tut und wie er es tut. |
| Discovery-Methode<br><br>[sn_ti_discovery_method] | Ein Ausdruck dafür, wie ein Incident erkannt wurde. |
| Feed-Gruppe<br><br>[sn_ti_feed] | Wird für die Konfiguration des Bedrohungs-Feeds (RSS) in der Bedrohungsübersicht verwendet. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Indikatorangriffsmodus/-methode<br><br>[sn_ti_m2m_indicator_attack_mode] | Wird verwendet, um Angriffsmodi/-methoden Indikatoren zuzuordnen. |
| Indikator für Gefährdung<br><br>[sn_ti_indicator] | Wird verwendet, um bestimmte erkennbare Muster in Kombination mit kontextbezogenen Informationen zu vermitteln, die Artefakte und/oder Verhaltensweisen von Interesse in einem Cybersicherheitskontext darstellen sollen. |
| Indikator für Gefährdungsmetadaten<br><br>[sn_ti_indicator_metadata] | Wird verwendet, um TAXII-Datensätze auszufüllen. |
| Indikatorquelle<br><br>[sn_ti_m2m_indicator_source] | Wird verwendet, um alle Quellen zu erfassen, die den spezifischen Indikator melden. |
| Indikatortyp<br><br>[sn_ti_indicator_type] | Kennzeichnet einen Cyberbedrohungsindikator, der aus einem Muster besteht, das bestimmte erkennbare Bedingungen identifiziert, sowie aus kontextbezogenen Informationen über die Bedeutung der Muster, wie und wann darauf reagiert wird usw. |
| Zugehöriger Indikatortyp<br><br>[sn_ti_m2m_indicator_indicator_type] | Verknüpft Indikatoren mit den entsprechenden Typen |
| Incident-Anzahl<br><br>[sn_ti_observable] | Anzahl der Security Incidents, die einem erkennbaren Element zugeordnet sind |
| Beabsichtigte Wirkung<br><br>[sn_ti_intended_effect] | Wird verwendet, um die beabsichtigte Auswirkung eines Bedrohungsakteurs auszudrücken. |
| Ergebnis des IP-Scans<br><br>[sn_ti_ip_result] | Wird verwendet, um die Ergebnisse einer IP-Suche anzuzeigen. |
| Grenzwert für Malware-Quoten<br><br>[sn_ti_rate_limit] | Definiert eine Quotengrenze, die für eine Suchquelle verwendet werden soll. |
| Malware-Scan<br><br>[sn_ti_scan] | Eine Suche. Enthält die zu suchenden Elemente, die Suchquelle und eine Zusammenfassung der Suchergebnisse. |
| Malware-Scan-Warteschlangeneintrag<br><br>[sn_ti_scan_q_entry] | Ein Suchdatensatz, der zur Suche oder Verarbeitung in die Warteschlange gestellt wurde. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen. |
| Ergebnis des Malware-Scans | Zeigt das Ergebnis einer Suche an. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| [sn_ti_scan_result] | |
| Malware-Scanner<br>[sn_ti_scanner] | Definiert Suchquellen von Drittparteien, die bei Suchvorgängen verwendet werden sollen. |
| Ratenbegrenzung für Malware-Scanner<br>[sn_ti_scanner_rate_limit] | Ordnet eine Suchquelle einer Quotengrenze zu. |
| Malware-Typ<br>[sn_ti_malware_type] | Wird verwendet, um die Typen von Malware-Instanzen auszudrücken. |
| Erkennbares Element<br>[sn_ti_observable] | Erkennbare Elemente in STIX stellen zustandsbehaftete Eigenschaften oder messbare Ereignisse dar, die für den Betrieb von Computern und Netzwerken relevant sind. |
| Kontexttyp des erkennbaren Elements<br>[sn_ti_observable_context_type] | Speichert den Kontext (Quelle, Ziel einer IP-Adresse usw.) für ein erkennbares Element |
| Indikator für erkennbares Element<br>[sn_ti_m2m_observable_indicator] | Wird verwendet, um erkennbare Elemente mit Indikatoren zu verknüpfen. |
| Quelle erkennbares Element<br>[sn_ti_observable_source] | Wird verwendet, um erkennbare Elemente mit Bedrohungsquellen zu verknüpfen. |
| Erkennbarer Typ<br>[sn_ti_observable_type] | Listet die verschiedenen Arten von erkennbaren Elementen auf, z. B. IP-Adressen. |
| Typkategorie des erkennbaren Elements<br>[sn_ti_observable_type_category] | Speichert die erste Kategorisierung von erkennbaren Elementen (z. B. IP-Adressen und URLs). Es wird verwendet, um erkennbare Typen genauer zu bestimmen. |
| Zugehöriger Angriffsmodus/-methode<br>[sn_ti_m2m_attack_mode_attack_mode] | Wird verwendet, um Angriffsmodi miteinander zu verknüpfen. |
| Zugehörige erkennbare Elemente<br>[sn_ti_m2m_observables] | Wird verwendet, um erkennbare Elemente miteinander zu verknüpfen. |
| Überprüfungstyp<br>[sn_ti_scan_type] | Die Definition eines Suchtyps mit anfänglichen Datensätzen für Datei, URL und IP. |
| Sicherheitsfall<br>[sn_ti_case] | Speichert Sicherheitsfalldatensätze, die mit Case Management erstellt wurden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Sicherheitsfall-IoC<br>[sn_ti_case_ioc] | Wird verwendet, um die Beziehung zwischen erkennbaren Elementen und Fällen zu verwalten. |
| Zugehörige Aufgabe für Sicherheitsfall<br>[sn_ti_m2m_case_task] | Wird verwendet, um die Beziehung zwischen Aufgaben (Security Incidents, Change-Anforderungen usw.) mit Sicherheitsfällen zu verwalten. |
| Sicherheitsfall-Beziehungsausschluss<br>[sn_ti_case_relationship_exclusion] | Stellt die Definition des Einschlusses und Ausschlusses zugehöriger Datensätze in Sicherheitsfällen bereit. |
| Sichtung<br>[sn_ti_sighting] | Die m2m-Verknüpfung zwischen dem erkennbaren Element und dem Detailergebnis der Sichtungssuche, die bei der Ausführung einer Sichtungssuchanforderung verwendet wird. |
| Konfigurationselemente der Sichtung<br>[sn_ti_m2m_sighting_ci] | Ordnet Konfigurationselemente einer Sichtungssuche zu. |
| Sichtungssuchdetails<br>[sn_ti_sighting_search_detail] | Details einer Sichtungssuche, z. B. die Anzahl der gefundenen internen externen Elemente. |
| Sichtungssuchergebnis<br>[sn_ti_sighting_search] | Der Header für die Ausführung einer Sichtungssuche. |
| Unterstützte erkennbare Typen<br>[sn_ti_m2m_ind_type_obs_type] | Verknüpft Indikatortypen mit gültigen erkennbaren Typen. |
| Unterstützter Scan-Typ<br>[sn_ti_supported_scan_type] | Ordnet den Suchtyp einer Suchquellen-/Lieferanten-spezifischen Implementierung zu. Gibt an, dass eine bestimmte Suchquelle den Typ unterstützt. |
| Modus/Methode des Aufgabenangriffs<br>[sn_ti_m2m_task_attack_mode] | Verknüpft Angriffsmodi mit Aufgaben. |
| Aufgabenindikator<br>[sn_ti_m2m_task_indicator] | Verknüpft Indikatoren mit Aufgaben. |
| Aufgabe – erkennbares Element<br>[sn_ti_m2m_task_observable] | Verknüpft erkennbare Elemente mit Aufgaben. |
| Aufgabensichtung<br>[sn_ti_m2m_task_sighting] | Speichert Aufgabendatensätze (Security Incidents und Fälle), die sich auf einen Sichtungsdatensatz beziehen. |
| TAXII-Sammlung | Definiert einen Cyber-Risk Intelligence-Feed, der von einem TAXII-Server importiert werden kann. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| [sn_ti_taxii_collection] | |
| TAXII-Profil<br>[sn_ti_taxii_profile] | Definiert ein Repository für die Freigabe von Cyber Risk Intelligence. Enthält TAXII-Sammlungen |
| Typ des Bedrohungsakteurs<br>[sn_ti_threat_actor_type] | Stellt Merkmale böswilliger Akteure (oder Angreifer) bereit, die eine Cyberangriffsbedrohung darstellen, einschließlich vermuteter Absichten und bisher beobachtetem Verhalten. |
| Threat Intelligence-Quelle<br>[sn_ti_source] | Definiert eine Quelle für den Import von Bedrohungsdaten. |
| Zugehörige Angriffsmotivation<br>[sn_ti_stix2_m2m_object_attack_motivation] | Erfasst alle Angriffsmotivationen, die einem STIX-Objekt zugeordnet sind. |
| Zugeordneter Infrastrukturtyp<br>[sn_ti_stix2_m2m_infra_type] | Verknüpft Infrastruktur mit ihren Typen. |
| Zugehörige Kill Chain-Phase<br>[sn_ti_stix2_m2m_indicator_kill_kette_phase] | Verknüpft Phasen der Kill Chain mit Indikatoren. |
| Zugehörige Kill Chain-Phase<br>[sn_ti_stix2_m2m_object_kill_Chain_phase] | Verknüpft Phasen der Kill Chain mit STIX-Objekten. |
| Zugehörige Malware-Fähigkeit<br>[sn_ti_stix2_m2m_malware_capability] | Verknüpft Malware mit ihren Fähigkeiten. |
| Zugeordneter Malware-Typ<br>[sn_ti_stix2_m2m_malware_malware_type] | Verknüpft Malware mit ihren Typen. |
| Zugeordnetes erkennbares Element<br>[sn_ti_stix2_m2m_malware_observable] | Sammelt alle erkennbaren Elemente, die einer Malware zugeordnet sind |
| Zugeordnetes erkennbares Element<br>[sn_ti_stix2_m2m_observed_data_observable] | Sammelt alle erkennbaren Elemente, die Beobachtungsdaten zugeordnet sind |
| Zugeordneter Berichtstyp<br>[sn_ti_stix2_m2m_report_report_type] | Verknüpft Bedrohungsberichte mit ihren Typen. |
| Zugeordnete Rolle des Bedrohungsakteurs<br>[sn_ti_stix2_m2m_threat_actor_threat_actor_role] | Verknüpft Bedrohungsakteure mit ihren Rollen. |
| Zugeordneter Bedrohungsakteurtyp | Verknüpft Bedrohungsakteure mit ihren Typen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| [sn_ti_stix2_m2m_threat_actor_threat_actor_type] | |
| Zugeordneter Tooltyp<br>[sn_ti_stix2_m2m_tool_tool_type] | Verknüpft Tools mit ihren Typen. |
| Angriffsmotivation<br>[sn_ti_stix2_attack_motivation] | Angriffsmotivation bestimmt die Stärke und Dauer eines Angriffs. Bedrohungsakteure und Angriffssätze verhalten sich normalerweise in einer Weise, die ihre zugrunde liegenden Emotionen oder Situationen widerspiegelt, und dies informiert die Abwehrkräfte über die Art des Angriffs. |
| Angriffsmuster<br>[sn_ti_stix2_attack_pattern] | Ein TTP-Typ, der Methoden beschreibt, mit denen Angreifer versuchen, Ziele zu gefährden. |
| Kampagne<br>[sn_ti_stix2_campaign] | Eine Gruppierung von gegnerischem Verhalten, die eine Reihe von böswilligen Aktivitäten oder Angriffen (manchmal als „Waves“ bezeichnet) beschreibt, die über einen Zeitraum für eine bestimmte Reihe von Zielen auftreten. |
| Vorgehensweise<br>[sn_ti_stix2_course_of_action] | Eine Empfehlung eines Erstellers von Informationen an einen Verbraucher zu den Aktionen, die er als Reaktion auf Informationen unternehmen könnte. |
| Externe Referenz<br>[sn_ti_stix2_external_reference] | Verweist auf Informationen, die außerhalb von STIX dargestellt werden. |
| Identitätssichtung<br>[sn_ti_stix2_m2m_sighting_identity] | Sammelt alle Identitäten, die einer Sichtung zugeordnet sind |
| Identität<br>[sn_ti_stix2_identität] | Tatsächliche Personen, Organisationen oder Gruppen (z. B. ACME, Inc.) sowie Klassen von Personen, Organisationen, Systemen oder Gruppen (z. B. Finanzbranche). |
| Externe Indikatorreferenz<br>[sn_ti_stix2_indicator_external_reference] | Stellt externe Referenzen dar, die Indikatoren zugeordnet sind. |
| Indikator Sichtung<br>[sn_ti_stix2_indicator_sighting] | Stellt Sichtungen von Indikatoren dar. |
| Infrastrukturtyp<br>[sn_ti_stix2_infrastructure_type] | Stellt die verschiedenen Infrastrukturtypen dar. |
| Infrastruktur<br>[sn_ti_stix2_infrastructure] | Ein TTP-Typ, der alle Systeme, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen beschreibt, die |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| | einen bestimmten Zweck erfüllen sollen (z. B. C2-Server, die als Teil eines Angriffs verwendet werden, Geräte oder Server, die Teil der Verteidigung sind, Datenbankserver, die Ziel eines sind). -Angriff usw.). |
| Installierte Software<br>[sn_ti_stix2_m2m_malware_analysis_sw] | Erfasst die gesamte Software (SCO-Softwaretypen), die einer Malware-Analyse zugeordnet ist. |
| Angriffssatz<br>[sn_ti_stix2_intrus_set] | Ein gruppierter Satz gegnerischer Verhaltensweisen und Ressourcen mit gemeinsamen Eigenschaften, von dem angenommen wird, dass er von einer einzelnen Organisation orchestriert wird. |
| Kill Chain-Phase<br>[sn_ti_stix2_kill_kette_phase] | Stellt Kill Chain-Phasen dar, die einer Kill Chain zugeordnet sind. |
| Kill Chain<br>[sn_ti_stix2_kill_kette] | Stellt verschiedene Kill Chains dar. |
| Standort<br>[sn_ti_stix2_location] | Stellt einen geografischen Standort dar, der über STIX bereitgestellt wird. |
| Malware-Analyse<br>[sn_ti_stix2_malware_analysis] | Die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse, die für eine Malware-Instanz oder -Familie durchgeführt wurde. |
| Malware-Fähigkeit<br>[sn_ti_stix2_malware_capability] | Stellt allgemeine Fähigkeiten dar, die eine Malware-Familie oder -Instanz aufweist. |
| Malware-Betriebssystem<br>[sn_ti_stix2_m2m_malware_operating_system] | Erfasst alle Betriebssysteme (SCO-Softwaretypen), die Malware zugeordnet sind. |
| Malware<br>[sn_ti_stix2_malware] | Ein TTP-Typ, der schädlichen Code darstellt. |
| Markierungsdefinition<br>[sn_ti_stix2_marking_definition] | Stellt Anforderungen für die Verarbeitung oder Freigabe von STIX-Objekten dar. |
| Objektsichtung<br>[sn_ti_stix2_object_sighting] | Stellt Sichtungen von STIX-Objekten dar. |
| Objekt-Indikator-Beziehung<br>[sn_ti_stix2_m2m_object_indicator] | Erfasst alle Beziehungen zwischen STIX-Objekten und STIX-Indikatoren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
| --- | --- |
| Objekt-Objekt-Beziehung<br>[sn_ti_stix2_m2m_object] | Erfasst alle Beziehungen zwischen STIX-Objekten und anderen STIX-Objekten mit Ausnahme der Indikatoren. |
| Beziehung von Objekt und erkennbarem Element<br>[sn_ti_stix2_m2m_object_observable] | Erfasst alle Beziehungen zwischen erkennbaren STIX-Elementen und STIX-Objekten. |
| Beobachtete Datensichtung<br>[sn_ti_stix2_m2m_sighting_observed_data] | Sammelt alle Beobachtungsdatenobjekte, die einer Sichtung zugeordnet sind |
| Beobachtete Daten<br>[sn_ti_stix2_observed_data] | Übermittelt Informationen über Cybersicherheits-bezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-Observable Objects (SCOs). |
| Berichtstyp<br>[sn_ti_stix2_report_type] | Stellt den primären Zweck oder Betreff von Bedrohungsberichten dar. |
| Gemeldetes erkennbares Element<br>[sn_ti_stix2_m2m_malware_analysis_observable] | Sammelt alle erkennbaren Elemente, die der Malware-Analyse zugeordnet sind |
| STIX V2-Objekt<br>[sn_ti_stix2_object] | Gemeinsame übergeordnete Tabelle für STIX-Objekt. |
| STIX V2-Sichtung<br>[sn_ti_stix2_sighting] | Gemeinsame übergeordnete Tabelle für STIX-Sichtungstabellen. |
| Bedrohungsakteurrolle<br>[sn_ti_stix2_threat_actor_role] | Stellt Rollen dar, die von Bedrohungsakteuren übernommen werden können. |
| Bedrohungsakteur<br>[sn_ti_stix2_threat_actor] | Bedrohungsakteure sind tatsächliche Einzelpersonen, Gruppen oder Organisationen, von denen angenommen wird, dass sie mit böswilligen Absichten operieren. |
| Bedrohungsgruppierung<br>[sn_ti_stix2_threat_grouping] | Gruppiert alle STIX-Objekte, die einen gemeinsamen Kontext aufweisen. |
| Bedrohungshinweis<br>[sn_ti_stix2_threat_note] | Stellt Kontext und zusätzliche Analysen bereit, die nicht im entsprechenden STIX-Objekt enthalten sind. |
| Bedrohungsmeinung<br>[sn_ti_stix2_threat_opinion] | Bietet eine Bewertung der Genauigkeit von Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde. |
| Bedrohungsbericht<br>[sn_ti_stix2_threat_report] | Berichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren, z. B. eine Beschreibung eines Bedrohungsakteurs, |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Tabelle | Beschreibung |
|---|---|
| | einer Malware oder einer Angriffstechnik, einschließlich Kontext und zugehöriger Details. Sie werden verwendet, um zugehörige Threat Intelligence zu gruppieren und als umfassende Cyber-Bedrohungs-Story zu veröffentlichen. |
| Tooltyp<br><br>[sn_ti_stix2_tool_type] | Die Kategorien von Tools, die zum Ausführen von Angriffen verwendet werden können. |
| Tool<br><br>[sn_ti_stix2_tool] | Tools sind legitime Software, die von Bedrohungsakteuren für Angriffe verwendet wird. |
| Schwachstelle<br><br>[sn_ti_stix2_vulnerability] | Stellt eine Schwachstelle oder einen Fehler in den Anforderungen, Designs oder Implementierungen der Berechnungslogik (Beispielcode) dar, die in Software und einigen Hardwarekomponenten (Beispiel-Firmware) zu finden ist. Sie können direkt ausgenutzt werden, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems zu beeinträchtigen. |

## Legen Sie Threat Intelligence Eigenschaften fest

Threat Intelligence Mit -Eigenschaften können Sie steuern, wie verschiedene Aspekte der Systemfunktion funktionieren, einschließlich der Einstellung von API-Schlüsseln.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Eigenschaften**.
2. Legen Sie nach Bedarf die folgenden Eigenschaften fest.

#### Eigenschaften für Threat Intelligence

| Eigenschaft | Beschreibung |
|---|---|
| Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs<br><br>sn_ti.ip_lookup.web_site | Der Domänenname, der zum Abrufen zusätzlicher Informationen in Ihre IoC-Datenbank verwendet werden soll. Diese Eigenschaft wird von der Skripteinbindung ThreatAdditionalInfo verwendet, um zusätzliche Informationen in das Formular „Erkennbare Elemente“ einzufügen.<br><br>Standardwert: http://api.ipinfodb.com/v3/ip-country/ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Beschreibung |
| --- | --- |
| | **Hinweis:** Die Drittpartei-API von pinfodb.com ist kostenlos verfügbar und wird in vielen kommerziellen Softwareprogrammen verwendet. Wenn Sie ihn durch einen anderen Domänennamen ersetzen, müssen Sie auch den API-Schlüssel im nächsten Feld angeben. |
| Der für die Domäne zu verwendende API-Schlüssel, falls vorhanden<br><br>sn_ti.ip_lookup.api_key | Der API-Schlüssel zum Abrufen zusätzlicher Informationen in Ihre IoC-Datenbank. Diese Eigenschaft wird (zusammen mit der Eigenschaft sn_ti.ip_lookup.web_site) von der Skripteinbindung ThreatAdditionalInfo verwendet, um zusätzliche Informationen in das Formular „Erkennbare Elemente“ einzufügen. |
| Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn das erkennbare Element einem IoC zugeordnet oder als böswillig eingestuft wurde.<br><br>sn_ti.scan_ioc_before_sending<br><br>**Hinweis:** Sie müssen die Dauer in der nächsten Eigenschaft (sn_ti.scan_ioc_num_days) definieren. | Option, um die Ausführung der automatisierten Bedrohungssuche für ein erkennbares Element zu stoppen, wenn das erkennbare Element als böswillig oder mit einem IoC für die konfigurierte Dauer (in Tagen) erkannt wird. Wenn Sie die Bedrohungssuche für das erkennbare Element dennoch ausführen müssen, können Sie dies manuell tun.<br><br>Standardwert: Ja |
| Dauer (in Tagen)<br><br>sn_ti.scan_ioc_num_days | Option zum Definieren der Dauer, bis zu der die automatisierte Bedrohungssuche des erkennbaren Elements übersprungen wird.<br><br>Standardwert (in Tagen): 30 |
| Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn dies bereits ausgeführt wurde.<br><br>sn_ti.enable_threat_lookup_bypass<br><br>**Hinweis:** Sie müssen die Dauer in der nächsten Eigenschaft (sn_ti.threat_lookup_bypass_times) definieren. | Wenn bereits ein Ergebnis der Bedrohungssuche für ein erkennbares Element verfügbar ist, haben Sie die Möglichkeit, die erneute Ausführung der automatisierten Bedrohungssuche für dasselbe erkennbare Element zu überspringen, bis die konfigurierte Dauer abgelaufen ist.<br><br>Standardwert: Nein |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Beschreibung |
| --- | --- |
| | **Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen geeigneten Wert hinzufügen. |
| Dauer (in Minuten)<br><br>sn_ti.threat_lookup_bypass_time | Option zum Definieren der Dauer, nach der die automatisierte Bedrohungssuche des erkennbaren Elements erneut ausgeführt werden kann.<br><br>Standardwert (in Minuten): 0 |
| Legen Sie eine Gültigkeitsdauer für Benutzerüberschreibungen für die Suche nach erkennbaren Elementen fest.<br><br>sn_ti.enable_observable_finding_system_override<br><br>**Hinweis:** Sie müssen die Gültigkeit in der nächsten Eigenschaft (sn_ti.observable_finding_override_expiry) definieren. | Option zum Festlegen einer Gültigkeitsdauer für Benutzerüberschreibungen für die erkennbaren Ergebnisse. Das Ergebnis der Bedrohungssuche des erkennbaren Elements wird während dieser Gültigkeitsdauer nicht vom Basissystem geändert.<br><br>Standardwert: Nein.<br><br>**Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen geeigneten Wert hinzufügen. |
| Gültigkeit (in Minuten)<br><br>sn_ti.observable_finding_override_expiry | Option zum Definieren des Gültigkeitszeitraums der Suche nach erkennbaren Elementen.<br><br>Standardwert (in Minuten): keine |
| Wenn ein Angriffsmodus oder eine Angriffsmethode für die angegebene Anzahl von Tagen aus keiner Quelle empfangen wurde, markieren Sie sie als inaktiv<br><br>sn_ti.attack_mode_inactivate_days | Anzahl der Tage ab dem Zeitpunkt, zu dem ein Angriffsmodus/eine Methode zuletzt empfangen wurde, damit der Datensatz als inaktiv markiert wird.<br><br>Standardwert: 360<br><br>**Hinweis:** Das Kontrollkästchen **Aktiv** ist im Formular **„Angriffsmodus/ -methode“** standardmäßig nicht sichtbar. Sie können sie jedoch hinzufügen. Wenn Angriffsmodi/-methoden inaktiv sind, können sie nicht in anderen Formularen ausgewählt werden. |
| Wenn ein Indikator für die angegebene Anzahl von Tagen aus keiner Quelle empfangen wurde, markieren Sie ihn als inaktiv | Anzahl der Tage ab dem letzten Empfang eines Indikators für den |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaft | Beschreibung |
| --- | --- |
| sn_ti.indicator_inactivate_days | Datensatz, die als inaktiv markiert werden sollen.<br><br>Standardwert: 180<br><br>**Hinweis:** Das Kontrollkästchen **Aktiv** ist im **Indikatorformular** standardmäßig nicht sichtbar. Sie können sie jedoch hinzufügen. Wenn Indikatoren inaktiv sind, können sie nicht in anderen Formularen ausgewählt werden. |
| Die maximale Nutzlastgröße (in MB) für einen STIX-Anhang, der analysiert werden kann.<br><br>sn_ti.stix.max_payload_size | Gibt die maximale Nutzlastgröße für den STIX-Anhang an, den Sie analysieren können.<br><br>Standardwert: keiner<br><br>Maximal zulässiger Wert: Keine Begrenzung. |
| Maximale Zeit in Sekunden, die eine ausgehende HTTP-Verbindung wartet, um TAXII-Sammlungsdaten abzurufen<br><br>sn_ti.taxii.http.max_timeout | Gibt an, wie lange eine ausgehende HTTP-Verbindung maximal warten darf, bevor das nächste Paket mit TAXII-Erfassungsdaten abgerufen wird.<br><br>Standardwert: 300 |
| Maximale Anzahl von Objekten, die in einem REST-Aufruf von einem TAXII-Server abgerufen werden (gilt nur für TAXII-Versionen 2.0 und 2.1)<br><br>sn_ti.taxii.max_page_size | Gibt die maximale Anzahl von Objekten an, die in einem REST-Aufruf vom TAXII-Server für eine Seite abgerufen werden.<br><br>Standardwert: 5.000<br><br>Maximal zulässiger Wert: 50.000 |
| Maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII 2.X REST-Aufruf<br><br>sn_ti.taxii2.retry_count | Gibt die maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII-REST-Aufruf an.<br><br>Standardwert: 3 |

3. Klicken Sie auf **Speichern**.

## Definieren Sie eine Bedrohungsquelle

Sie können eine Liste von Threat Intelligence Bedrohungsquellen verwalten. Jede Quelle bietet die Möglichkeit, zu definieren, wie oft eine Quelle abgefragt wird. Sie können



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Bedrohungsquelle auch bei Bedarf ausführen, um die erforderlichen STIX-Daten (Structured Threat Information eXpression) zu importieren.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

### Warum und wann dieser Vorgang ausgeführt wird

Threat Intelligence verwendet zwei Technologien für den Import von bedrohungsbezogenen Informationen: STIX und Trusted Automated Exchange of Indicator Information (TAXII).

STIX bietet eine standardisierte, strukturierte Sprache für die Darstellung eines umfangreichen Satzes von Cyberbedrohungsinformationen, einschließlich Indikatoren für Gefährdungsaktivitäten (z. B. IP-Adressen und Datei-Hashes) sowie kontextbezogene Informationen zu Bedrohungen, z. B. Angriffsmodi/-methoden. die zusammen die Beweggründe, Fähigkeiten und Aktivitäten eines Cybergegners vollständiger charakterisieren. Daher liefern STIX-Daten wertvolle Informationen darüber, wie sich Ihr Unternehmen am besten gegen Cyberbedrohungen schützen kann.

Trusted Automated Exchange of Indicator Information (TAXII) wird verwendet, um den automatisierten Austausch von Informationen zu Cyberbedrohungen zu erleichtern. TAXII definiert eine Reihe von Services und Nachrichtenaustauschen, die die gemeinsame Nutzung von umsetzbaren Cyberbedrohungsinformationen über Organisations- und Produkt-/Servicegrenzen hinweg ermöglichen, um Cyberbedrohungen zu erkennen, zu verhindern und zu mindern. TAXII-Profile können als Repositorys für die gemeinsame Nutzung von STIX-formatierten Informationen eingerichtet werden. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **Bedrohungsquellen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Bedrohungsquelle. |
| Anwendung | Die Anwendung, die diesen Datensatz enthält. |
| Aktiv | Aktivieren Sie dieses Kontrollkästchen, um die Bedrohungsquelle zu aktivieren. |
| Erweitert | Aktivieren Sie diese Checkbox, um die Skripts in den Feldern **Integration Factory-Skript** und **Berichtsprozessor** anzuzeigen. |
| Beschreibung | Eine Beschreibung dieser Bedrohungsquelle. |

4. Füllen Sie die Felder im Abschnitt „ **Zeitplan** “ entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Run-Kosten | Die Häufigkeit, mit der die Integration ausgeführt werden soll: Täglich, Wöchentlich, Regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf der Einstellung dieses Felds angezeigt. |
| Tag | Der Tag, an dem die Integration ausgeführt werden soll. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Wenn Sie **Wöchentlich** im Feld **Ausführen** ausgewählt haben, werden in diesem Feld die Wochentage angezeigt.<br>○ Wenn Sie im Feld **Ausführen** die Option **Monatlich** ausgewählt haben, werden in diesem Feld die Tage des Monats angezeigt. |
| Zeit | Zeitpunkt, zu dem die Integration beginnen soll. |
| Wiederholungsintervall | Wenn Sie **Regelmäßig** im Feld **Ausführen** ausgewählt haben, wird in diesem Feld die Anzahl der Tage und Stunden angezeigt, bevor die Integration erneut ausgeführt wird. |
| Wird gestartet | Wenn Sie **Regelmäßig** im Feld **Ausführen** ausgewählt haben, werden in diesem Feld die Daten und die Uhrzeit angezeigt, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen. |
| Bedingt | Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten. |
| Bedingung | Wenn Sie das Kontrollkästchen Bedingt aktiviert haben, geben Sie hier die **Bedingungen** ein. |

**5.** Füllen Sie die Felder im Abschnitt „ **Bedrohungsdetails** “ entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Indikator | Der Indikator, der verwendet werden soll, wenn die Daten keinen explizit bereitstellen. Wenn die Sperrliste leer ist, wird für jedes erkennbare Element ein neuer Indikator erstellt. |
| Indikatortyp | Der Indikatortyp, der für Indikatoren verwendet werden soll, die erstellt werden und deren Daten nicht explizit einen Indikatortyp bereitstellen. |
| Angriffsmodus/-methode | Der zu verwendende Angriffsmodus/die zu verwendende Methode, wenn die Daten keinen explizit bereitstellen. |
| Erkennbarer Typ | Der erkennbare Typ, der für erkennbare Elemente verwendet werden soll, die erstellt werden und deren Daten nicht explizit einen erkennbaren Typ bereitstellen.[SI1] |
| Gewichtung | Geben Sie einen Gewichtungswert für diese Quelle ein, der in der Konfidenzberechnung verwendet werden soll. |

**Hinweis:**
Die Verwendung der Felder „ **Indikator“**, **„Indikatortyp“**, „ **Angriffsmodus/-methode**“ und **„Erkennbarer Typ** “ ist spezifisch für die Implementierung. Der Standardprozessor SimpleBlocklistProcessor verhält sich wie in den Tooltips beschrieben. Eine TAXII-Bedrohungsquelle ist jedoch vollständig datengesteuert. Jeder benutzerdefinierte Bedrohungsquellenprozessor kann eine eigene Strategie verwenden. Diese Felder sind im Grunde Elemente, die der Integration/dem Prozessor zur Verfügung stehen, und die Implementierung entscheidet, wie sie verwendet werden.

**6.** Füllen Sie die Felder im Abschnitt „ **Quellendetails** “ entsprechend aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Endpunkt | Geben Sie die URL des Webservice-Endpunkts ein, über den von Threat Intelligenceauf die Bedrohungsquelle zugegriffen wird. Klicken Sie auf das Schlosssymbol, um die URL zu sperren. |
| Verwenden Sie die REST-Nachricht | Wenn Sie eine REST-Nachricht benötigen, um auf die Bedrohungsquelle zuzugreifen, aktivieren Sie dieses Kontrollkästchen. Die Felder „ **REST-Nachricht** “ und **„REST-Methode“** werden zu Pflichtfeldern. |
| REST-Nachricht | Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Nachricht aus der Liste aus, oder klicken Sie auf **Neu**, um eine neue REST-Nachricht zu definieren. |
| REST-Methode | Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Methode aus der Liste aus, oder klicken Sie auf **Neu**, um eine neue REST-Methode zu definieren. |
| Integrationsskript | Das standardmäßige Integrationsskript ist **SimpleRESTSecurityDataIntegration**. Sie führt einen einfachen REST-Aufruf aus, speichert die Antwort als Anhang und gibt den Anhang an den Prozessor zurück. Dieses Skript erfüllt die Anforderungen der meisten Organisationen. Wenn Sie möchten, können Sie jedoch auf das Suchsymbol klicken und ein anderes Integrationsskript auswählen oder ein neues definieren. |
| Integrationswerksskript | Wenn die **Checkbox Erweitert** aktiviert ist, wird in diesem Feld das tatsächliche Skript für die Erstellung des Integrationsskripts angezeigt. Sie können das Skript nach Bedarf bearbeiten. Diese Fähigkeit ist für benutzerdefinierte Implementierungen nützlich. Integrationen im Basissystem erfordern normalerweise keine benutzerdefinierte Konstruktorlogik. |
| Berichtsprozessor-Skript | Das standardmäßige Integrationsskript ist **SimpleBlocklistProcessor**. Dieses Skript ist ein einfacher Prozessor, der eine einfache Sperrliste (einfach, d. h. ein einspaltiges Dokument mit erkennbaren Elementen wie URLs oder IP-Adressen) akzeptiert und erkennbare Elemente erstellt. Er verwendet die verschiedenen Felder für **Bedrohungsdetails**, um zu bestimmen, welche Felder festgelegt werden sollen, wenn erkennbare Elemente erstellt werden. |
| Prozessorwerksskript | Wenn die **Checkbox Erweitert** aktiviert ist, wird in diesem Feld das tatsächliche Skript für die Erstellung des Prozessors angezeigt. Sie können das Skript nach Bedarf bearbeiten. Dieses Skript ist im Allgemeinen für benutzerdefinierte Implementierungen nützlich. Die Integrationen im Basissystem erfordern normalerweise keine benutzerdefinierte Konstruktorlogik. |

7. Klicken Sie auf **Absenden**.

**Hinweis:**
Weitere Informationen zum Konfigurieren der Paginierung der Bedrohungsquelle finden Sie im Artikel KB1213825 .

## Erstellen Sie ein TAXII-Profil

Sie können TAXII-Profile für die gemeinsame Nutzung von STIX-formatierten Informationen verwalten. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder entsprechend aus.
4. Füllen Sie die Felder im Abschnitt „ **Discovery-Service-Konfiguration** “ entsprechend aus.
5. Füllen Sie die Felder im Abschnitt **„Sammlungsservice-Konfiguration** “ entsprechend aus.
6. Klicken Sie auf **Absenden**.

## IoC-Repository

Das IoC-Repository enthält STIX-Objekte. Jedes dieser Objekte enthält eine bestimmte Information.

Wenn Sie STIX-Objekte über Beziehungen kombinieren, ermöglichen Sie einfache oder komplexe Darstellungen von Cyber Threat Intelligence (CTI).

Threat Intelligence unterstützt die STIX-Versionen 1.1, 2.0 und 2.1.

### Angriffsmodi und -methoden

Angriffsmodi und -methoden, manchmal auch als Taktiken, Techniken und Verfahren (TTPs) bezeichnet, sind Darstellungen des Verhaltens von Cyberangreifern. Sie beschreiben in zunehmendem Detailgrad, was diese Angreifer tun und wie sie es tun. Angriffsmodi und -methoden gelten für STIX 1.1.

Beispielsweise kann ein Angriffsmodus/eine Angriffsmethode darin bestehen, mithilfe von Malware Anmeldeinformationen für Kreditkarten zu stehlen. Oder eine andere, verwandte Taktik (auf einer niedrigeren Detailebene) könnte darin bestehen, gezielte E-Mails mit Anhängen zu senden, die schädlichen Code enthalten, der beim Öffnen ausgeführt wird, Kreditkarteninformationen aus Tastenanschlägen erfasst und HTTP für die Kommunikation mit einem Befehls- und Steuerungsserver verwendet Informationen übertragen.

Angriffsmodi und -methoden gelten für STIX 1.1.

#### Definieren Sie einen Angriffsmodus/eine Methode

Angriffsmodi und -methoden werden mit STIX-Daten importiert, Sie können jedoch nach Bedarf neue Modi/Methoden hinzufügen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Klassifizierungs-Tag auswählen | Wenn Sie Klassifizierungs-Tags eingerichtet und aktiviert haben, um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Sensibilität des Angriffsmodus/der Angriffsmethode anzugeben.<br><br>Wenn Sie keine Klassifizierungs-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt. |
| Titel | Geben Sie einen beschreibenden Namen für diesen Angriffsmodus/diese Methode ein. |
| Malware-Typ | Wählen Sie den Malware-Typ für diesen Angriffsmodus/diese Methode aus. Die verfügbaren Malware-Typen werden als STIX-Daten vom Lieferantenserver abgerufen. |
| Quelle | Wählen Sie die Bedrohungsdatenquelle für diesen Angriffsmodus/diese Methode aus. Einige Datenquellen sind im Basissystem enthalten. Sie können nach Bedarf neue Datenquellen erstellen. |
| Angriffsmechanismus | Wählen Sie den Angriffsmechanismus für diesen Angriffsmodus/diese Methode aus. Angriffsmechanismen stellen die verschiedenen Techniken dar, die zum Angriff auf ein System verwendet werden. Die verfügbaren Angriffsmechanismen werden vom Lieferantenserver als STIX-Daten abgerufen. |
| Erstmals aufgetreten | Dieses Datum wird als STIX-Daten vom Lieferantenserver abgerufen. |
| Zuletzt aufgetreten | Dieses Datum wird als STIX-Daten vom Lieferantenserver abgerufen. |
| Typ Bedrohungsakteur | Wählen Sie den Bedrohungsakteurtyp für diesen Angriffsmodus/diese Methode aus. Bedrohungsakteurtypen charakterisieren böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich mutmaßlicher Absichten und bisher beobachtetem Verhalten. Die verfügbaren Bedrohungsakteurtypen werden als STIX-Daten vom Lieferantenserver abgerufen. |
| Beschreibung | Geben Sie eine Beschreibung des Angriffsmodus/der Angriffsmethode ein. |
| Handhabung | Geben Sie eine Anweisung für die Behandlung dieses Angriffsmodus/dieser Methode ein. |
| Beabsichtigte Wirkung | Geben Sie die beabsichtigte Auswirkung dieses Angriffstyps ein. |

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
Sie können eine der folgenden zugehörigen Listen anzeigen, um zusätzliche Informationen anzuzeigen.

| Zugehörige Liste | Beschreibung |
|---|---|
| Zugehörige Indikatoren | Listet zugehörige Kompromittierungsindikatoren (Indicators of Compromise, IoC) auf, die von der Bedrohungsquelle identifiziert wurden. |
| Modus/Methode des untergeordneten Angriffs | Listet Angriffsmodi/-methoden auf, die untergeordnete Elemente des übergeordneten Angriffsmodus/der übergeordneten Angriffsmethode sind. |
| Zugehörige Aufgaben | Listet Änderungen auf, die dem übergeordneten Angriffsmodus/der übergeordneten Angriffsmethode zugeordnet sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie einem Angriffsmodus/einer Angriffsmethode ein IoC hinzu

Zusätzlich zum Importieren von Indikatoren als STIX-Daten können Sie IoCs manuell zu einem Angriffsmodus/einer Angriffsmethode hinzufügen.

#### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie einen IoC hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugehörige Indikatoren**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den IoC zu suchen, den Sie hinzufügen möchten.
6. Fügen Sie den IoC mit dem Slushbucket der Liste „ **Zugehörige Indikatoren** “ hinzu.
7. Klicken Sie auf **Speichern**.

### Fügen Sie eine zugehörige Angriffsmodusmethode hinzu

Zusätzlich zum Importieren von Angriffsmodi/-methoden als STIX-Daten können Sie zugehörige Angriffsmodi/-methoden manuell hinzufügen.

#### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie einen zugehörigen Angriffsmodus bzw. eine zugehörige Methode hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **„Kind-Angriffsmodus/-methode“**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus bzw. die Methode zu finden, die Sie mit dem aktuellen Angriffsmodus in Beziehung setzen möchten.
6. Fügen Sie mit dem **Slushbucket** den Angriffsmodus/die Angriffsmethode der Liste „Modal/Methode des untergeordneten Angriffs“ hinzu.
7. Klicken Sie auf **Speichern**.

### Fügen Sie die zugeordnete Aufgabe einem Angriffsmodus/einer Angriffsmethode hinzu

Sie können zugehörige Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern sie auch manuell einem Angriffsmodus/einer Methode hinzufügen.

#### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**.
2. Klicken Sie auf den Angriffsmodus, dem Sie eine zugehörige Aufgabe hinzufügen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die zugehörige Liste Zugeordnete **Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu suchen, die Sie dem Angriffsmodus/der Angriffsmethode zuordnen möchten.
6. Fügen Sie die Aufgabe mit dem Slushbucket der Liste „Zugeordnete **Aufgaben“** hinzu.
7. Klicken Sie auf **Speichern**.

## Kompromittierungsindikatoren

Kompromittierungsindikatoren (Indicators of Compromise, IoC) sind Artefakte, die in einem Netzwerk oder Betriebssystem beobachtet werden und wahrscheinlich auf einen Angriff hinweisen. Typische IoCs sind Virensignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. IoC gilt für STIX 1.1 und 2.x.

Ein IoC kann ein einzelnes erkennbares Element oder eine Sammlung von erkennbaren Elementen sein (z. B. eine einzelne bekanntermaßen fehlerhafte URL oder das Vorhandensein einer bestimmten Datei und einiger bestimmter Registrierungsschlüsselwerte).

Nachdem IoCs in einem Prozess der Reaktion auf Incidents und Computerforensik identifiziert wurden, können sie zur Früherkennung zukünftiger Angriffsversuche mithilfe von Angriffserkennungssystemen und Antivirensoftware verwendet werden.

IoC gilt für STIX 1.1 und 2.x.

### Zeigen Sie ein IoC an

IoCs, manchmal auch als Indikatoren bezeichnet, werden in der Regel aus einer Bedrohungsdatenquelle als STIX-Daten abgerufen. Bei Bedarf können Sie auch IoCs erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.write

#### Prozedur

1. Nachdem die regelmäßige Aufgabe IoC-Daten aus der definierten Datenquelleabgerufen hat, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   Die abgerufenen IoCs werden aufgelistet.
2. Klicken Sie auf das IoC, das Sie anzeigen möchten.
3. Die folgenden Informationen werden angezeigt.

| Feld | Beschreibung |
|---|---|
| Klassifizierungs-Tag auswählen | Wenn Sie Sicherheits-Tags eingerichtet und aktiviert haben, um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des IoC anzugeben.<br><br>Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt. |
| Titel | Ein beschreibender Name für diesen Indikator. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Erstmals aufgetreten | Das erste Datum, an dem dieser Indikator im System beobachtet wurde. |
| Zuletzt aufgetreten | Das letzte Datum, an dem dieser Indikator im System beobachtet wurde. |
| Anzahl gefundener Fälle | Die Anzahl der Fälle, in denen der Indikator gefunden wurde. |
| Bezogene Anzahl | Die Anzahl, wie oft der Indikator aus definierten Bedrohungsquellen importiert wurde. |
| Notizen | Zusätzliche Hinweise zum Indikator. Dieses Feld kann auch JSON-Schlüssel/Wert-Paare enthalten. |

**4.** Sie können auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die mit dem aktuellen Indikator verknüpft sind. |
| Zugehöriger Angriffsmodus/-methode | Listet zugehörige Angriffsmodi/-methoden auf, die im Zusammenhang mit diesem Indikator identifiziert wurden. |
| Zugeordneter Typ | Listet andere Indikatortypen auf, die diesem IoC zugeordnet sind. |
| Indikatorquellen | Listet die Quellen dieses Indikators zusammen mit dem Konfidenzniveau der Quelle auf. |
| Zugehörige Aufgaben | Listet alle Aufgaben, Changes und Incidents auf, die dem IoC zugeordnet sind. |
| Indikator-Metadaten | Wenn das Feld **Notizen** gültige JSON-Schlüssel/Wert-Paare enthält, werden diese analysiert und angezeigt. Wenn keine JSON-Schlüssel/Wert-Paare vorhanden sind oder das JSON-Objekt ungültig ist, wird diese zugehörige Liste nicht angezeigt. |
| Sicherheitsanmerkungen | |
| Externe Referenzen des Indikators | |
| Zugehörige Kill Chain-Phasen | Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |

### Fügen Sie einem IoC ein zugehöriges erkennbares Element hinzu

Zusätzlich zum Importieren von erkennbaren Elementen als STIX-Daten können Sie einem IoC zugehörige erkennbare Elemente manuell hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.write

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugehörige erkennbare Elemente**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu suchen, das Sie mit dem IoC in Beziehung setzen möchten.
6. Fügen Sie das erkennbare Element mit dem **Slushbucket** der Liste „Zugehörige erkennbare Elemente“ hinzu.
7. Klicken Sie auf **Speichern**.

### Fügen Sie einem IoC einen zugehörigen Angriffsmodus/eine zugehörige Methode hinzu

Zusätzlich zum Importieren zugehöriger Angriffsmodi/-methoden als STIX-Daten können Sie einem IoC zugehörige Angriffsmodi/-methoden manuell hinzufügen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.write

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie einen zugehörigen Angriffsmodus/eine zugehörige Methode hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugehöriger Angriffsmodus/-methode**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus/die Methode zu finden, die Sie mit dem IoC in Beziehung setzen möchten.
6. Fügen Sie mit dem Slushbucket den Angriffsmodus/die Angriffsmethode der Liste **Zugehöriger Angriffsmodus/-methode** hinzu.
7. Klicken Sie auf **Speichern**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Identifizieren Sie zugeordnete Indikatortypen

Wenn für einen IoC keine zugeordneten Indikatortypen definiert sind, werden alle Arten von erkennbaren Elementen nachverfolgt. Wenn Sie jedoch einen oder mehrere Arten von Indikatoren einem IoC zuordnen, werden die Typen der erkennbaren Elemente eingeschränkt, die dem IoC zugeordnet werden können.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.write

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie einen Indikatortyp zuordnen möchten.
3. Klicken Sie auf die zugehörige Liste Zugeordneter **Typ**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikatortyp zu suchen, den Sie dem IoC zuordnen möchten.
6. Fügen Sie den Indikatortyp mit dem Slushbucket der Liste Zugeordneter **Typ** hinzu.
7. Klicken Sie auf **Speichern**.

### Identifizieren Sie Indikatorquellen

Indikatorquellen werden normalerweise automatisch als Teil des Bedrohungsimportprozesses verfolgt, es können jedoch weitere Quellen manuell hinzugefügt werden.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.write

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf den Indikator, dem Sie Indikatorquellen hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste „ **Indikatorquellen“**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Indikatorquelle zu finden, die Sie dem IoC zuordnen möchten.
6. Fügen Sie die Indikatorquelle mit dem Slushbucket der Liste „ **Indikatorquellen** “ hinzu.
7. Klicken Sie auf **Speichern**.

### Fügen Sie zugeordnete Aufgaben zu einem IoC hinzu

Sie können zugeordnete Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern auch manuell zu einem IoC hinzufügen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.write

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
2. Klicken Sie auf das IoC, dem Sie eine zugeordnete Aufgabe hinzufügen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die zugehörige Liste Zugeordnete **Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu finden, die Sie dem IoC zuordnen möchten.
6. Fügen Sie die Aufgabe mit dem Slushbucket der Liste „Zugeordnete **Aufgaben“** hinzu.
7. Klicken Sie auf **Speichern**.

## Erkennbare Elemente

Erkennbare Elemente stellen zustandsbehaftete Eigenschaften (z. B. der MD5-Hash einer Datei oder der Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind . Erkennbare Elemente gelten für STIX 1.1 und 2.x.

Sätze von erkennbaren Cyberelementen sind nützlich, um Gefährdungsindikatoren zu identifizieren, wenn sie mit kontextbezogenen Informationen kombiniert werden, die das Verhalten von Cyberbedrohungen darstellen.

Erkennbare Elemente gelten für STIX 1.1 und 2.x.

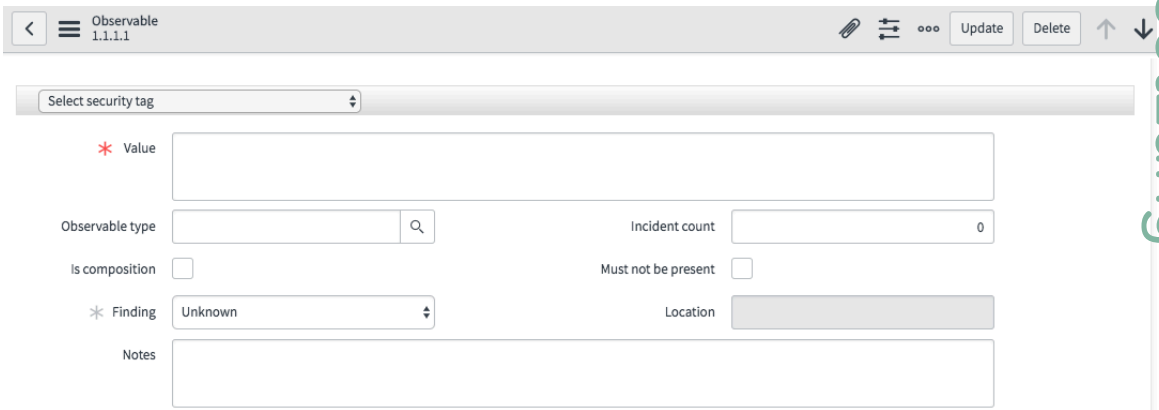
### Definieren Sie ein erkennbares Element

Erkennbare Elemente werden vom Lieferantenserver als STIX-Daten abgerufen. Sie können jedoch nach Bedarf erkennbare Elemente erstellen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf **Neu**.




3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Klassifizierungs-Tag auswählen | Wenn Sie Sicherheits-Tags eingerichtet und aktiviert haben, um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Vertraulichkeit des erkennbaren Elements anzugeben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt. |
| Wert | Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.<br>**Hinweis:**<br>Wenn ein Bedrohungsscan für eine IP-Adresse oder einen Hash, Malware oder einen anderen Fehler zurückgibt, wird die IP-Adresse oder der Hash-Wert automatisch der Tabelle „Erkennbares Element“ [sn_ti_observable] hinzugefügt. Daher kann im Formular „Erkennbare Elemente“ gesucht werden. |
| Erkennbarer Typ | Wählen Sie die Klassifizierung des erkennbaren Elements aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese erkennbaren Typen werden im Modul **„Erkennbare Typen** “ definiert. |
| Incident-Anzahl | Die Häufigkeit, in der der Wert des erkennbaren Elements gefunden wurde. |
| Ist Zusammensetzung | Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde.<br>Wenn der **erkennbare Typ** auf einen anderen **Wert als die Zusammensetzung**des erkennbaren Elements festgelegt ist und dieses neue erkennbare Element eine Zusammensetzung ist, aktivieren Sie dieses Kontrollkästchen.<br>Wenn der **erkennbare Typ** bereits auf **Zusammensetzung**des erkennbaren Elements festgelegt ist, ist das Kontrollkästchen aktiviert und schreibgeschützt.<br>Eine erkennbare Zusammensetzung ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält. |
| Ergebnis | Wählen Sie eine der folgenden Optionen aus:<br>○ **Böswillig**: Gibt an, dass das erkennbare Element für die Organisation schädlich ist.<br>○ **Verdächtig**: Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte.<br>○ **Bereinigen**: Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist.<br>○ **Unbekannt**: Gibt an, dass das Ergebnis des erkennbaren Elements noch nicht bestimmt wurde.<br>○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche.<br>**Hinweis:**<br>Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert. |
| Operator | Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Ist Zusammensetzung** aktiviert ist. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Elemente und ihre untergeordneten Elemente berücksichtigt, wenn entschieden wird, ob ein zugeordneter Indikator vorhanden ist.<br><br>Legen Sie dieses Feld auf **UND fest**, wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugeordneter Indikator als vorhanden betrachtet wird.<br><br>Legen Sie die Option auf **OR fest**, wenn eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugeordneter Indikator als vorhanden betrachtet wird. |
| Muss nicht vorhanden sein | Dieses Feld wird nur angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde.<br><br>Wenn diese Option ausgewählt ist, bedeutet dies, dass das Fehlen des erkennbaren Elements das potenzielle Problem ist (z. B. ein fehlender Registrierungsschlüssel). |
| Standort | Mit den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Laden Sie weitere IoC-Daten in dieses Feld laden. |
| Notizen | Geben Sie zusätzliche Notizen zum erkennbaren Element ein. |

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**. Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

| Zugehörige Liste | Beschreibung |
|---|---|
| Zugehörige Indikatoren | Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden. |
| Zugehörige Aufgaben | Listet Änderungen auf, die dem erkennbaren Element zugeordnet sind. |
| Untergeordnete erkennbare Elemente | Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden. |
| Übereinstimmende Ressourcen für IP | Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die über eine übereinstimmende IP-Adresse verfügen. |
| Quelle erkennbare Elemente | Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf. |
| Sicherheitsanmerkungen | Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden. |

### Fügen Sie einem erkennbaren Element ein zugehöriges IoC hinzu

Zusätzlich zum Importieren von erkennbaren Elementen als STIX-Daten können Sie einem IoC zugehörige erkennbare Elemente manuell hinzufügen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges IoC hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste **Zugehörige Indikatoren**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikator zu suchen, den Sie mit dem erkennbaren Element in Beziehung setzen möchten.
6. Fügen Sie den Indikator mit dem Slushbucket der Liste „ **Zugehörige Indikatoren** “ hinzu.
7. Klicken Sie auf **Speichern**.

## Fügen Sie zugeordnete Aufgaben zu einem erkennbaren Element hinzu

Sie können zugehörige Aufgaben (z. B. Changes und Incidents) nicht nur als STIX-Daten importieren, sondern sie auch manuell zu einem erkennbaren Element hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie eine zugeordnete Aufgabe hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste Zugeordnete **Aufgaben**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu suchen, die Sie dem erkennbaren Element zuordnen möchten.
6. Fügen Sie die Aufgabe mit dem Slushbucket der Liste „Zugeordnete **Aufgaben“** hinzu.
7. Klicken Sie auf **Speichern**.

## Fügen Sie ein zugehöriges erkennbares Element hinzu

Zusätzlich zum Importieren von erkennbaren Elementen als STIX-Daten können Sie zugehörige erkennbare Elemente manuell hinzufügen.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. **Klicken** Sie auf die zugehörige Liste Untergeordnete erkennbare Elemente.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu finden, das Sie mit dem aktuellen identifizieren möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Fügen Sie das erkennbare Element mit dem **Slushbucket** der Liste der untergeordneten erkennbaren Elemente hinzu.
7. Klicken Sie auf **Speichern**.

### Laden Sie weitere IoC-Daten

Abhängig von den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Informationen zum geografischen Standort für IP-Adressen und Websites im Formular „Erkennbare Elemente“ laden. Bei weiteren Anpassungen können Sie auch weitere Informationen hinzufügen, z. B. Ländervorwahlen, Ortsnamen.

#### Vorbereitungen

Die folgenden beiden Eigenschaften müssen festgelegt werden:

- **Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs** [sn_ti.ip_lookup.web_site]
- **Der API-Schlüssel, der für die obige Domäne verwendet werden soll, falls vorhanden** [sn_ti.ip_lookup.api_key]

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf die IP-Adresse oder URL des erkennbaren Elements, für das Sie weitere IoC-Daten anzeigen möchten.
   Das Feld **Standort** zeigt den geografischen Standort des IoC an.
3. Klicken Sie auf die Schaltfläche **Daten** anreichern, um die zusätzlichen IoC-Daten zu laden.
4. Sie können das Formular „Erkennbares Element“ auch konfigurieren, um weitere standortbezogene Felder hinzuzufügen, z. B. Ländercode und Ortscode.

**Hinweis:**
Um weitere standortbezogene Informationen zu laden, bearbeiten Sie die **Skripteinbindung ThreatAdditionalInfo** und geben den entsprechenden API-Schlüssel von der Website an, die die zusätzlichen Informationen bereitstellt.

### Identifizieren Sie Quellen für erkennbare Elemente

Wenn für ein erkennbares Element keine Quellen definiert sind, werden alle Arten von Quellen verwendet. Wenn Sie jedoch einem erkennbaren Element eine oder mehrere Bedrohungsquellen hinzufügen, werden die verwendeten Quellen eingeschränkt.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Klicken Sie auf das erkennbare Element, dem Sie Quellen für erkennbare Elemente hinzufügen möchten.
3. Klicken Sie auf die zugehörige Liste „ **Erkennbare Quellen“**.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Quelle zu suchen, die Sie dem erkennbaren Element zuordnen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Fügen Sie die Quelle des erkennbaren Elements mit dem Slushbucket der Liste „Erkennbare **Quellen** “ hinzu.
7. Klicken Sie auf **Speichern**.

### Suchvorgänge für erkennbare Elemente durchführen

Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Die ausgeführten Scan-Implementierungen hängen von den von Ihnen aktivierten ab.

#### Vorbereitungen

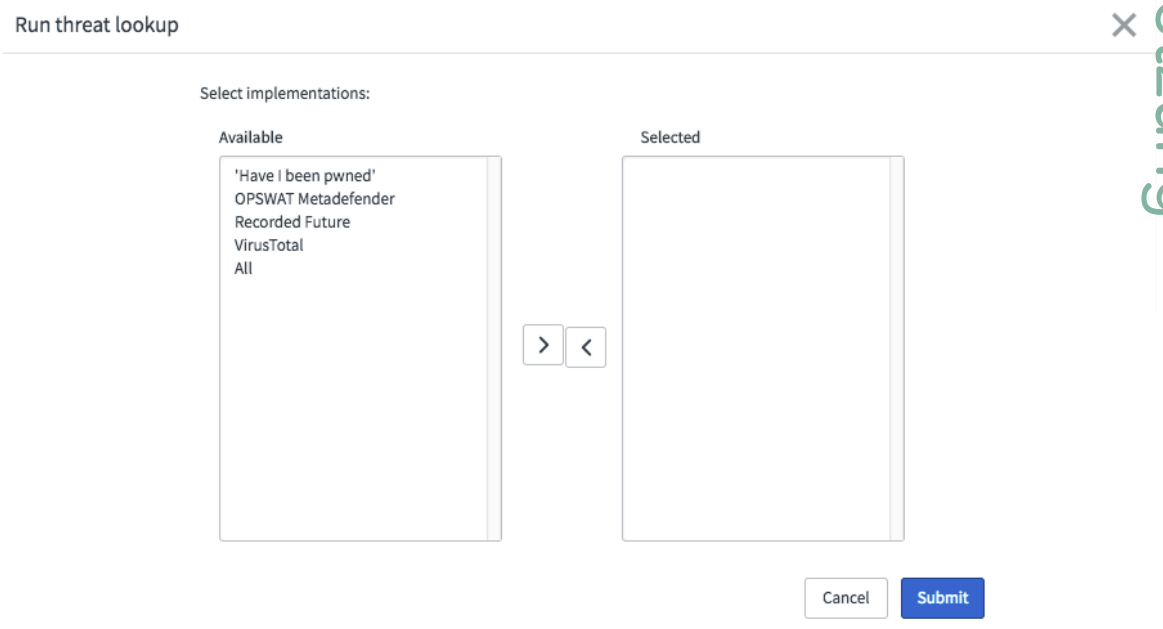
Bevor Sie Suchvorgänge durchführen können, müssen Sie das Threat Intelligence-Plugin aktivieren. Sie müssen auch das Plugin für mindestens eine der folgenden Scan-Implementierungen installieren:

- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations Wurde ich pwned?
- VirusTotal

Erforderliche Rolle: sn_ti.write

#### Prozedur

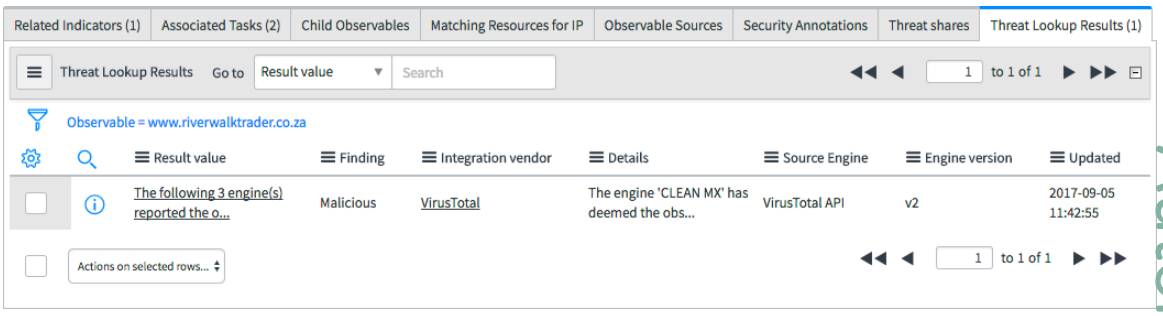
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche für mehr als ein erkennbares Element durchzuführen, wählen Sie die erkennbaren Elemente aus, klicken Sie **auf Aktionen für ausgewählte Zeilen**und wählen **Sie Bedrohungssuche ausführen**aus.
   - Um eine Suche für ein einzelnes erkennbares Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements und klicken Sie auf den zugehörigen Link **Bedrohungssuche** ausführen.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die Implementierungen der Bedrohungssuche aus, die Sie verwenden möchten, oder wählen Sie **Alle**, um Suchvorgänge mit allen aktiven Implementierungen durchzuführen, und klicken Sie dann auf **Absenden**.
   Eine Meldung zeigt an, dass die Bedrohungssuchen begonnen haben. Security Operations-Integration – Workflow „Bedrohungssuche“. wird ausgeführt und führt auch die Implementierungs-Workflows für die von Ihnen ausgewählten Implementierungen der Bedrohungssuche aus. Die Suchvorgänge werden ausgeführt, und die Ergebnisse werden generiert.
4. Wenn die Suchvorgänge abgeschlossen sind, können Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche** klicken, um die Ergebnisse anzuzeigen.




**Suchergebnis**der letzten Bedrohung: Sie können auch die neuesten Ergebnisse der Bedrohungssuche von jedem Integrationsanbieter anzeigen, wenn Sie auf die Registerkarte Suchergebnis der **letzten Bedrohung** klicken.

**Hinweis:**
Die Registerkarte „ **Suchergebnis der letzten Bedrohung“** ist nicht Teil des Basissystems.

Gehen Sie wie folgt vor, um diese Registerkarte zu aktivieren:

a. Klicken Sie mit der rechten Maustaste auf die Formularkopfzeile.

b. Navigieren zu **Konfigurieren** > **Zugehörige Listen**.

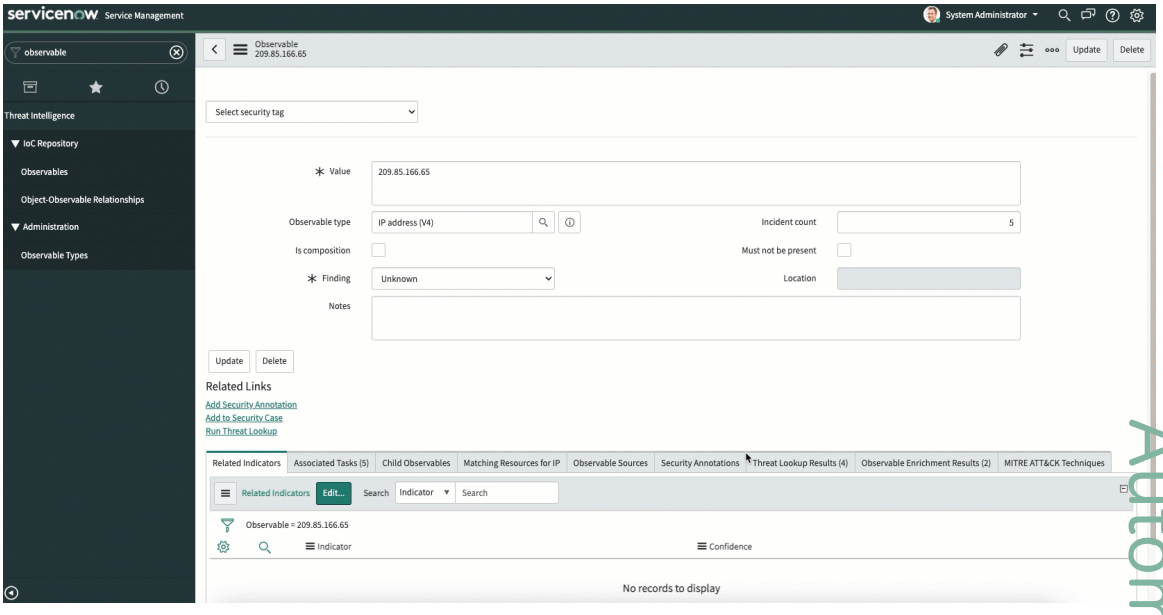
c. Suchen Sie in der Liste Verfügbar nach Suchergebnissen für **aktuelle Bedrohungen**, und verschieben Sie sie in die Liste Ausgewählt.

d. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

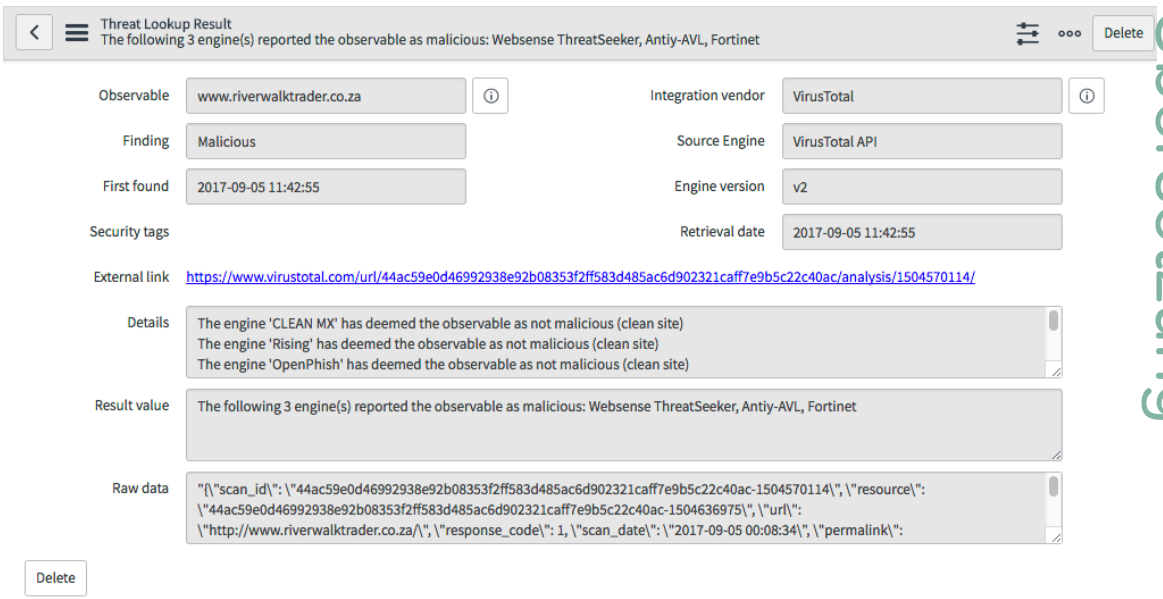
Sie können jetzt die aktuellen Ergebnisse der Bedrohungssuche von jedem Integrationsanbieter auf der Registerkarte **Recent Threat Search Result** (Suchergebnis der letzten Bedrohung) anzeigen.




5. Um zusätzliche Details anzuzeigen, einschließlich Rohergebnisse für eine bestimmte Suche, klicken Sie auf den **Wert Ergebnis**.

### Hinweis:

Wenn die Implementierungen von VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.




## Führen Sie eine Bedrohungsanreicherung für erkennbare Elemente durch

Sie können eine Threat Intelligence-Anreicherung für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Die ausgeführten Implementierungen hängen von den von Ihnen aktivierten ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

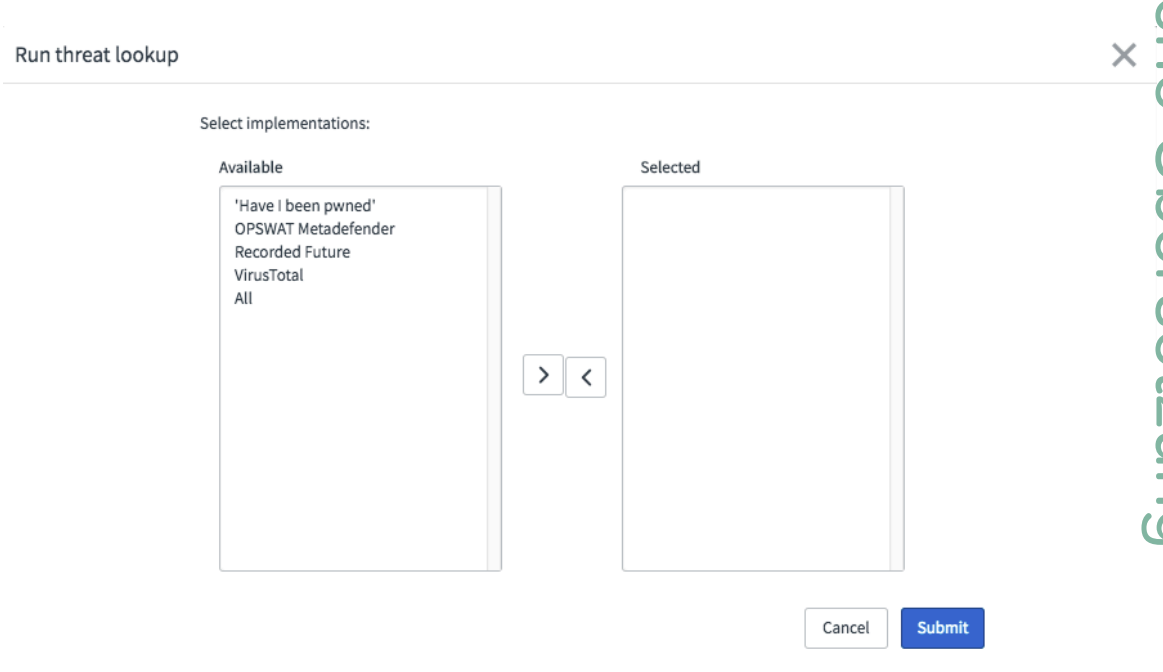
Bevor Sie die Ergänzung durchführen können, müssen Sie das Threat Intelligence-Plugin aktivieren. Sie müssen auch das Plugin für eine oder mehrere der Ergänzungsimplementierungen installieren:

- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations Wurde ich pwned?
- VirusTotal
- Wer ist?

Erforderliche Rolle: sn_ti.admin

## Prozedur

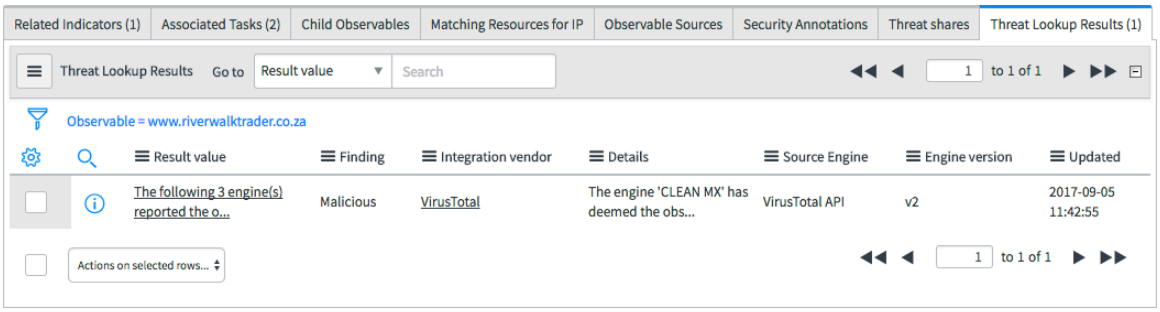
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche für mehr als ein erkennbares Element durchzuführen, wählen Sie die erkennbaren Elemente aus, klicken Sie **auf Aktionen für ausgewählte Zeilen**und wählen **Sie Bedrohungssuche ausführen**aus.
   - Um eine Suche für ein einzelnes erkennbares Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements und klicken Sie auf den zugehörigen Link **Bedrohungssuche** ausführen.




3. Wählen Sie die Implementierungen der Bedrohungssuche aus, die Sie verwenden möchten, oder wählen Sie **Alle**, um Suchvorgänge mit allen aktiven Implementierungen durchzuführen, und klicken Sie dann auf **Absenden**.
   Eine Meldung zeigt an, dass die Bedrohungssuchen begonnen haben. Security Operations-Integration – Workflow „Bedrohungssuche“. wird ausgeführt und führt auch die Implementierungs-Workflows für die von Ihnen ausgewählten Implementierungen der Bedrohungssuche aus. Die Suchvorgänge werden ausgeführt, und die Ergebnisse werden generiert.
4. Wenn die Suchvorgänge abgeschlossen sind, können Sie auf die Registerkarte **Ergebnisse der Bedrohungssuche** klicken, um die Ergebnisse anzuzeigen.

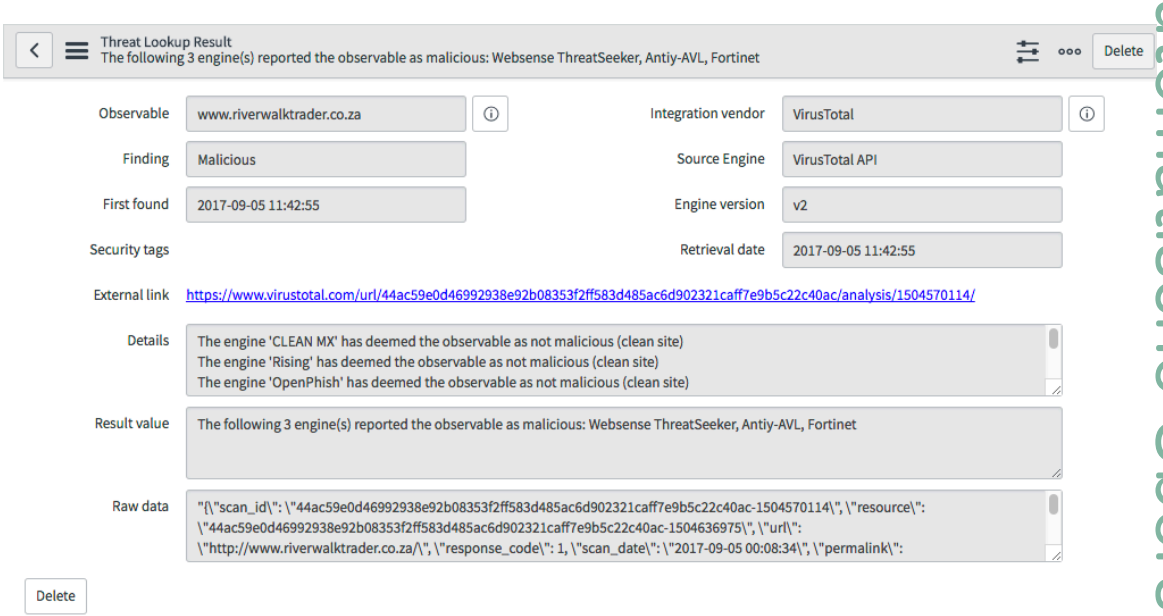
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Um zusätzliche Details anzuzeigen, einschließlich Rohergebnisse für eine bestimmte Suche, klicken Sie auf den **Wert Ergebnis**.

**Hinweis:**
Wenn die Implementierungen von VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.




## Angriffsmuster

Angriffsmuster sind eine Art von Taktiken, Techniken und Verfahren (TTPs), die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden. Angriffsmuster gelten für STIX 2.x.

Angriffsmuster werden zur Kategorisierung von Angriffen verwendet. Sie verallgemeinern bestimmte Angriffe auf die Muster, denen sie folgen, und liefern detaillierte Informationen darüber, wie Angriffe ausgeführt werden.

Zum Beispiel ist Spear-Phishing eine häufige Art von Angriff, bei der ein Angreifer eine sorgfältig gestaltete E-Mail-Nachricht an eine Partei sendet, mit der Absicht, sie dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen, um Malware zu übermitteln. Angriffsmuster sind spezifischer, z. B. kann Spear-Phishing durch einen bestimmten Bedrohungsakteur (z. B. dass das Ziel einen Wettbewerb gewonnen hat) ebenfalls ein Angriffsmuster sein.

### Definieren Sie ein Angriffsmuster

Definieren Sie ein Angriffsmuster, um die Kategorisierung von Angriffen zu unterstützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmuster**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffsmuster zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugehörige Kill Chain-Phasen | Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Vorgehensweisen | Listet die mit diesem Objekt verbundene Vorgehensweise auf, bei der es sich um technische oder automatisierte Antworten handelt (Anwenden von Patches, Neukonfiguration von Firewalls), um einen Angriff zu verhindern. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

## Kampagnen

Eine Kampagne ist eine Gruppierung gegnerischer Verhaltensweisen. Diese Verhalten beschreiben eine Reihe von schädlichen Aktivitäten oder Angriffen, die im Laufe der Zeit für eine bestimmte Gruppe von Zielen auftreten. Kampagnen gelten für STIX 2.x.

Kampagnen haben normalerweise gut definierte Ziele und können Teil eines Angriffssatzes sein.

Kampagnen werden häufig einem Angriffssatz und Bedrohungsakteuren zugeordnet. Die Bedrohungsakteure können die bekannte Infrastruktur aus dem Angriffssatz wiederverwenden oder eine neue Infrastruktur einrichten, die für die Durchführung dieser Kampagne spezifisch ist.

Kampagnen haben ein gemeinsames Ziel in Bezug auf die von ihnen verursachten Incidents für Personen oder Ressourcen, auf die sie abzielen, und die Ressourcen, die sie verwenden.

Zum Beispiel greift ein Vergehenssyndikat die Führungskräfte der ACME Bank an. Sie greifen an, indem sie eine bestimmte Variante von Malware und neue Server verwenden, um geheime Informationen über eine bevorstehende Fusion mit einer anderen Bank zu erhalten.

### Definieren Sie eine Kampagne

Definieren Sie eine Kampagne, um gegnerisches Verhalten zu gruppieren.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Kampagnen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die der Kampagne zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

## Vorgehensweise

Eine Vorgehensweise ist eine Aktion, die ausgeführt wird, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren. Vorgehensweisen gelten für STIX 2.x.

Vorgehensweisen beschreibt technische oder automatisierte Antworten (Anwenden von Patches, Neukonfiguration von Firewalls). Sie kann auch übergeordnete Aktionen wie Mitarbeiterschulungen oder Richtlinienänderungen beschreiben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Beispiel könnte eine Vorgehensweise zum Mindern einer Schwachstelle die Anwendung des Patches beschreiben, der die Schwachstelle behebt.

### Definieren Sie eine Vorgehensweise

Definieren Sie eine Vorgehensweise, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Vorgehensweisen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Vorgehensweise zugeordnet sind.

| Zugehörige Links | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Identitäten

Identitäten repräsentieren tatsächliche Personen, Organisationen oder Gruppen (ACME, Inc.) und Klassen von Personen, Systemen oder Gruppen (Finanzbranche). Identitäten gelten für STIX 2.x.

Das Identitäts-SDO kann grundlegende identifizierende Informationen, Kontaktinformationen und die Sektoren erfassen, zu denen die Identität gehört. Identität stellt Ziele von Angriffen, Informationsquellen, Objektersteller und Identitäten der Bedrohungsakteure dar.

### Definieren Sie Identitäten

Definieren Sie Identitäten, die tatsächliche Personen, Organisationen oder Gruppen darstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Identitäten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |

## Infrastruktur

Das Infrastruktur-SDO stellt eine Art von Taktiken, Techniken und Verfahren (TTPs) dar. Sie beschreiben alle Systeme, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen, die einen Zweck eines Angriffs unterstützen sollen. Infrastruktur gilt für STIX 2.x.

Die Elemente eines Angriffs werden durch andere SDOs oder SCOs dargestellt. Das Infrastruktur-SDO stellt jedoch eine benannte Gruppe von Daten dar, die die Infrastruktur bilden.

Beispiele für Infrastrukturen sind C2-Server, die bei einem Angriff verwendet werden, ein Gerät oder ein Server, der Teil einer Verteidigung ist, oder Datenbankserver, die Ziel eines Angriffs sind.

### Definieren der Infrastruktur

Definieren Sie eine Infrastruktur, die aus Systemen, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen besteht, die einen Zweck eines Angriffs unterstützen sollen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Infrastruktur**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen. Sie können der Infrastruktur auch andere Objekte zuordnen.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| | Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugeordnete Typen | Listet Indikatortypen auf, die diesem Objekt zugeordnet sind. |
| Zugehörige Kill Chain-Phasen | Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind. |
| Zugeordnete Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Beobachtete Daten | Listet die mit diesem Objekt verknüpften Beobachtungsdaten auf. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

## Angriffssatz

Ein Angriffssatz ist ein gruppierter Satz von Verhaltensweisen und Ressourcen von Angreifern mit gemeinsamen Eigenschaften. Ein Angriffssatz betrifft normalerweise eine einzelne Organisation. Angriffssatz gilt für STIX 2.x.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Angriffssatz kann mehrere Kampagnen oder andere Aktivitäten erfassen. Diese Aktivitäten weisen gemeinsame Attribute auf, die auf einen allgemein bekannten oder unbekannten Bedrohungsakteur hinweisen.

Eine neue Aktivität kann einem Angriffssatz zugeordnet werden, auch wenn die Bedrohungsakteure hinter dem Angriff nicht bekannt sind. Bedrohungsakteure können von der Unterstützung eines Angriffssatzes zur Unterstützung eines anderen wechseln oder mehrere Angriffssätze unterstützen.

Ein Angriffssatz ist das gesamte Angriffspaket und kann über einen längeren Zeitraum in mehreren Kampagnen verwendet werden, um potenziell mehrere Ziele zu erreichen.

### Definieren Sie einen Angriffssatz

Definieren Sie einen Angriffssatz, bei dem es sich um einen gruppierten Satz von Verhaltensweisen und Ressourcen von Angreifern mit gemeinsamen Eigenschaften handelt.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffssatz**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffssatz zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugehörige Angriffsmotivationen | Listet alle sekundären Beweggründe auf, warum dieser Angriffssatz etwas erreichen möchte. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

## Standorte

Ein Standort stellt einen geografischen Standort dar. Speicherorte werden hauptsächlich verwendet, um anderen SDOs Kontext zu geben. Standorte gelten für STIX 2.x.

Der Standort kann einige oder alle der folgenden Elemente enthalten: Region (Nordamerika), Bürgeradresse (New York, USA), Breitengrad und Längengrad.

Die Standort-SDO kann sich auf eine Identität oder einen Angriffssatz beziehen, um anzugeben, dass sich die Identität oder der Angriffssatz an diesem Standort befindet. Sie kann sich auch auf eine Malware oder ein Angriffsmuster beziehen, um anzugeben, dass sich das Zielopfer an einem bestimmten Standort befindet.

Beispielsweise kann ein Standort in einer Beziehung verwendet werden, um zu beschreiben, dass der Angriffssatz „Bourgeois Swallow“ aus Osteuropa stammt.

Mindestens eine der folgenden Eigenschaften oder Eigenschaften muss angegeben werden:

- region
- country
- Breitengrad und Längengrad

### Definieren Sie den Standort

Definieren Sie einen geografischen Standort, um anderen SDOs mehr Kontext bereitzustellen.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Standorte**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Standort zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |

## Malware

Malware ist eine Art von TTP, die schädlichen Code darstellt. Er bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Malware gilt für STIX 2.x.

Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems (OS) des Opfers zu gefährden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Malware-SDO charakterisiert, identifiziert und kategorisiert Malware-Instanzen und -Familien aus Daten, die aus der Analyse abgeleitet werden. Dieses SDO erfasst detaillierte Informationen darüber, wie die Malware funktioniert und was sie tut.

### Definieren Sie eine Malware

Definieren Sie eine Malware, die schädlichen Code darstellt.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugeordnete Typen | Listet Indikatortypen auf, die diesem Objekt zugeordnet sind. |
| Zugeordnete Fähigkeiten | Listet die Fähigkeiten auf, die identifiziert und diesem Objekt zugeordnet sind. |
| Zugehörige Kill Chain-Phasen | Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind. |
| Zugehörige Malware | Listet die mit diesem Objekt identifizierte zugeordnete Malware auf. |
| Zugehörige Betriebssysteme | Die Betriebssysteme, unter denen das Objekt ausgeführt werden kann. Dies gilt sowohl für virtualisierte Betriebssysteme als auch für solche, die auf Bare-Metal-Basis ausgeführt werden. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Vorgehensweisen | Listet die mit diesem Objekt verbundene Vorgehensweise auf, bei der es sich um technische oder automatisierte Antworten handelt (Anwenden von Patches, Neukonfiguration von Firewalls), um einen Angriff zu verhindern. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware-Analyse | Listet Malware-Analysedatensätze auf, die diesem Objekt zugeordnet sind. |
| Gemeldete erkennbare Elemente | Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet wurden. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |



## Malware-Analyse

Die Malware-Analyse erfasst die Metadaten und Ergebnisse einer Malware. Die Malware-Analyse gilt für STIX 2.x.

Die Malware-Analyse umfasst statische oder dynamische Analysen, die für eine Malware-Instanz oder -Familie durchgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definieren Sie die Malware-Analyse

Definieren Sie eine Malware-Analyse, die die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse erfasst, die für eine Malware-Instanz oder -Familie durchgeführt wird.

#### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware-Analyse**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu den Objekten anzuzeigen, die der Malware-Analyse zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugehörige Malware | Listet die mit diesem Objekt identifizierte zugeordnete Malware auf. |
| Gemeldete erkennbare Elemente | Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet wurden. |
| Installierte Software | Listet alle nicht standardmäßigen Software auf, die auf dem Betriebssystem installiert ist, das für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wird. |

## Beobachtete Daten

Beobachtete Daten übermitteln Informationen über Cybersicherheits-bezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe der STIX Cyber-observable Objects (SCOs). Beobachtete Daten gelten für STIX 2.x.

Mit „Beobachtete Daten“ wird sowohl eine einzelne Beobachtung einer einzelnen Entität (Datei, Netzwerkverbindung) als auch die Zusammenfassung mehrerer Beobachtungen einer Entität erfasst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Beobachtete Daten für sich allein (ohne Beziehungen) verwenden, um Rohdaten zu übermitteln, die aus einer beliebigen Quelle erfasst wurden. Zu den Quellen gehören Analystenberichte, Sandboxen sowie netzwerk- und hostbasierte Erkennungstools.

Beispielsweise können mit „Beobachtete Daten“ Informationen über eine IP-Adresse, eine Netzwerkverbindung, eine Datei oder einen Registrierungsschlüssel erfasst werden. Bei „Beobachtete Daten“ handelt es sich nicht um eine Intelligence-Assertion, sondern um Rohinformationen ohne Kontext für ihre Bedeutung.

### Beobachtete Daten definieren

Definieren Sie mithilfe der STIX Cyber-observable Objects (SCOs) beobachtete Daten, die Informationen über Entitäten im Zusammenhang mit Cybersicherheit wie Dateien, Systeme und Netzwerke übermitteln.

## Vorbereitungen

Erforderliche Rolle: sn_ti.admin

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Beobachtete Daten**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

## Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den beobachteten Daten zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Bedrohungsakteure

Bedrohungsakteure sind Einzelpersonen, Gruppen oder Organisationen, die mit böswilliger Absicht handeln. Threat Actors gilt für STIX 2.x.

Ein Bedrohungsakteur ist kein Angriffssatz, kann jedoch im Laufe der Zeit verschiedene Angriffssätze, Gruppen oder Organisationen unterstützen oder ihnen zugeordnet sein.

Bedrohungsakteure verwenden ihre Ressourcen und die Ressourcen eines Angriffssatzes, um Angriffe durchzuführen und Kampagnen gegen Ziele auszuführen.

Sie können Bedrohungsakteure anhand ihrer Beweggründe, Fähigkeiten, Ziele, ihres Entwicklungsstands, ihrer vergangenen Aktivitäten, ihrer Ressourcen, auf die sie Zugriff haben, und ihrer Rolle in der Organisation identifizieren.

### Definieren Sie Bedrohungsakteure

Definieren Sie Bedrohungsakteure, bei denen es sich um Einzelpersonen, Gruppen oder Organisationen handelt, die mit böswilliger Absicht handeln.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsakteure**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsakteur zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugeordnete Typen | Listet Indikatortypen auf, die diesem Objekt zugeordnet sind. |
| Zugeordnete Rollen | Listet die dem Bedrohungsakteur zugeordneten Rollen auf. |
| Zugehörige Angriffsmotivationen | Listet die zugehörigen Angriffsmotivationen mit dem Bedrohungsakteur auf. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |

## Bedrohungsgruppierungen

Ein Objekt vom Typ „Bedrohungsgruppierung“ bestätigt explizit, dass die referenzierten STIX-Objekte einen gemeinsamen Kontext haben. Bedrohungsgruppierungen gelten für STIX 2.x.

Ein Objekt vom Typ „Bedrohungsgruppierung“ stellt einen Datensatz dar, der bei ausreichender Analyse ausgereift ist, um einen Incident- oder Bedrohungsbericht als STIX-Berichtsobjekt zu übermitteln. Beispielsweise kann eine Gruppierung verwendet werden, um eine laufende Untersuchung eines Sicherheits-Ereignisse oder -Incident zu kennzeichnen.

Ein Objekt vom Typ „Bedrohungsgruppierung“ kann auch verwendet werden, um zu bestätigen, dass die referenzierten STIX-Objekte zu einem laufenden Analyseprozess gehören. Beispielsweise kann ein Bedrohungsanalyst mit anderen in seiner Trust-Community zusammenarbeiten, um eine Reihe von Kampagnen und Indikatoren zu untersuchen.

Das SDO der Bedrohungsgruppierung enthält eine Liste von Verweisen auf SDOs, SCOs und SROs sowie eine explizite Angabe des vom Inhalt gemeinsam genutzten Kontexts, eine Textbeschreibung und den Namen der Gruppierung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definieren Sie Bedrohungsgruppierungen

Definieren Sie Bedrohungsgruppierungen als Objekte mit einem gemeinsamen Kontext.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsgruppierungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

**Nächste Maßnahme**
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsgruppierung zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Gruppierte Objekte | Listet Objekte auf, die als Teil der Bedrohungsgruppierung gruppiert sind. |
| Gruppierte Indikatoren | Listet Indikatoren auf, die als Teil der Bedrohungsgruppierung gruppiert sind. |
| Gruppierte erkennbare Elemente | Listet erkennbare Elemente auf, die als Teil der Bedrohungsgruppierung gruppiert sind. |

## Markierungsdefinitionen

Das Markierungsdefinitionen-Objekt stellt eine bestimmte Markierung dar.

Datenmarkierungen stellen Einschränkungen, Berechtigungen und andere Anleitungen dar, wie Daten verwendet und freigegeben werden können.

Beispielsweise können Daten mit der Einschränkung freigegeben werden, dass sie nicht erneut freigegeben werden dürfen oder im Ruhezustand verschlüsselt werden müssen.

In STIX werden Datenmarkierungen mithilfe des Markierungsdefinitionsobjekts angegeben. Diese Definitionen werden mithilfe von Objektmarkierungen auf STIX-Objekte und über granulare Markierungen auf einzelne Eigenschaften von STIX-Objekten angewendet.

### Definieren Sie Markierungsdefinitionen

Definieren Sie Markierungsdefinitionen, die eine bestimmte Datenmarkierung darstellen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Markierungsdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Markierungsdefinition zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Markierte Objekte | Listen von Objekten, die mit der Markierungsdefinition markiert sind. |
| Markierte Indikatoren | Listen der Indikatoren, die mit der Markierungsdefinition markiert sind. |

## Bedrohungshinweise

Eine Bedrohungsnotiz übermittelt informativen Text, um zusätzliche Analysen bereitzustellen, die nicht in den STIX-Objekten, Markierungsdefinitionsobjekten oder Sprachinhaltsobjekten enthalten sind, auf die sich die Notiz bezieht. Bedrohungshinweise gilt für STIX 2.x.

Beispielsweise kann ein Analyst einem Kampagnenobjekt, das von einer anderen Organisation erstellt wurde, eine Notiz hinzufügen. Der Hinweis kann darauf hinweisen, dass sie Beiträge zu dieser Kampagne in einem Hacker-Forum gesehen hat.

Notizen werden in der Regel von menschlichen Analysten erstellt und bestehen aus an Menschen ausgerichtetem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Notiz erstellt hat.

### Definieren Sie Bedrohungshinweise

Definieren Sie Bedrohungshinweise, die Informationen übermitteln, um weiteren Kontext oder Analysen bereitzustellen, die in vorhandenen Objekten nicht verfügbar sind.

### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungshinweise**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsnotizen zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Zugeordnete Objekte | Listen von Objekten, für die die Bedrohungsnotizen gelten. |
| Zugeordnete Indikatoren | Listen der Indikatoren, für die die Bedrohungshinweise gelten. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind. |

## Bedrohungsmeinungen

Eine Meinung ist eine Bewertung der Richtigkeit der Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde. Bedrohungsmeinungen gelten für STIX 2.x.

Die Meinungseigenschaft erfasst den Grad der Zustimmung oder Nichtübereinstimmung anhand einer festen Skala. Die feste Skala unterstützt auch eine numerische Zuordnung, um konsistente statistische Operationen über Meinungen hinweg zu ermöglichen.

Beispielsweise kann ein Analyst aus einer verbrauchenden Organisation sagen, dass er einem Kampagnenobjekt „überhaupt nicht zustimmt“, und eine Erklärung dafür abgeben.

Meinungen sind subjektiv, und die Spezifikation regelt nicht, wie sie am besten interpretiert werden können.

Analysten erstellen Meinungen und bestehen aus an Menschen orientiertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Meinung erstellt hat.

### Definieren Sie Bedrohungsmeinungen

Definieren Sie Bedrohungsmeinungen als Bewertung der Richtigkeit der Informationen in einem STIX-Objekt.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsmeinungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsmeinung zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Zugeordnete Objekte | Liste der Objekte, für die die Bedrohungsmeinung gilt. |
| Zugeordnete Indikatoren | Liste der Indikatoren, für die die Bedrohungsmeinung gilt. |
| Zugehörige erkennbare Elemente | Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind. |

## Bedrohungsberichte

Bedrohungsberichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren. Bedrohungsberichte gelten für STIX 2.x.

Bedrohungsberichte enthalten eine Beschreibung eines Bedrohungsakteurs, einer Malware, einer Angriffstechnik, einschließlich Kontext und zugehöriger Details. Sie werden verwendet, um zugehörige Threat Intelligence zu gruppieren, sodass sie als umfassende Cyber-Bedrohungs-Story veröffentlicht werden kann.

Das SDO „Bedrohungsbericht“ enthält eine Liste von Verweisen auf STIX-Objekte zusammen mit einer Textbeschreibung und dem Namen des Berichts.

### Definieren Sie Bedrohungsberichte

Definieren Sie Bedrohungsberichte, die einen Bedrohungsakteur, Malware, Angriffstechnik, einschließlich Kontext und zugehörige Details, beschreiben.

### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsberichte**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsberichten zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Zugeordnete Typen | Listet Indikatortypen auf, die diesem Objekt zugeordnet sind. |
| Gemeldete Objekte | Liste der im Bedrohungsbericht gemeldeten Objekte. |
| Gemeldete Indikatoren | Listen der im Bedrohungsbericht gemeldeten Indikatoren |
| Gemeldete erkennbare Elemente | Listen der im Bedrohungsbericht gemeldeten erkennbaren Elemente |

## Sichtungen

Sichtungen geben an, dass ein Indikator oder Objekt gesehen wurde. Objekte können Malware, Tool, Bedrohungsakteur usw. sein.

Sichtungen verfolgen, wer und was das Ziel ist, wie Angriffe ausgeführt werden, und Trends im Angriffsverhalten nachzuverfolgen.

Das Sichtungsbeziehungsobjekt enthält zusätzliche Eigenschaften, die in den generischen Beziehungsobjekten nicht vorhanden sind. Diese zusätzlichen Eigenschaften stellen Daten dar, die für Sichtungsbeziehungen spezifisch sind.

Zum Beispiel eine Anzahl oder die Angabe, wie oft etwas gesehen wurde.

Die Sichtung wird als Beziehung erfasst, da Sie keine Sichtung haben können, es sei denn, Sie haben etwas, das gesichtet wurde.

- Was gesichtet wurde, z. B. Malware, Kampagne oder andere SDOs
- Wer es gesichtet hat und/oder wo es gesichtet wurde, dargestellt als Identität
- Was in Systemen und Netzwerken erkannt wurde, dargestellt als Beobachtungsdaten

### Definieren Sie Indikatorsichtungen

Definieren Sie Sichtungen, die angeben, dass ein Indikator gesehen wurde.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatorsichtungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Indikatorsichtung zugeordnet sind.

| Zugehörige Listen | Beschreibung |
|---|---|
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Beobachtete Daten | Listet die mit diesem Objekt verknüpften Beobachtungsdaten auf. |

## Definieren Sie Objektsichtungen

Definieren Sie die Objektsichtung, die beschreibt, dass ein Objekt (Malware, Tool, Bedrohungsakteur usw.) erkannt wurde.

### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

### Prozedur
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objektsichtungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Objektsichtung zugeordnet sind.

| Zugehörige Listen | Beschreibung |
|---|---|
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Beobachtete Daten | Listet die mit diesem Objekt verknüpften Beobachtungsdaten auf. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Tools

Tools sind legitime Software, die von Bedrohungsakteuren für Angriffe verwendet wird. Tools gelten für STIX 2.x.

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie zum Ausführen von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und dienen berechtigten Zwecken für Power-User, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

Zum Beispiel sind Remotezugriffstools (RDP) und Netzwerk-Scan-Tools (Nmap) Tools, die ein Bedrohungsakteur während eines Angriffs verwendet.

### Definieren Sie Tools

Definieren Sie Tools als legitime Software, die zum Ausführen von Angriffen verwendet wird.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Tools**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

#### Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Toolobjekt zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Zugehörige Kill Chain-Phasen | Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind. |
| Zugeordnete Typen | Listet Indikatortypen auf, die diesem Objekt zugeordnet sind. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Vorgehensweisen | Listet die mit diesem Objekt verbundene Vorgehensweise auf, bei der es sich um technische oder automatisierte Antworten handelt (Anwenden |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| | von Patches, Neukonfiguration von Firewalls), um einen Angriff zu verhindern. |
| Identitäten | Liste der Identitäten, die diesem Objekt zugeordnet sind. |
| Indikatoren | Listet zugehörige Kompromittierungsindikatoren (IoC) auf, die von der mit diesem Objekt verknüpften Bedrohungsquelle identifiziert wurden. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Standorte | Listet Standorte auf, die geografischen Kontext für dieses Objekt bereitstellen. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |
| Schwachstellen | Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die von Angreifern ausgenutzt wird und die diesem Objekt zugeordnet ist. |
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |

## Schwachstellen

Eine Schwachstelle ist eine Schwachstelle oder ein Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen. Schwachstellen gelten für STIX 2.x.

Die Schwachstelle oder der Fehler liegt in den Anforderungen, Designs oder Implementierungen des Codes, der in einer Software- oder Hardwarekomponente gefunden wurde. Diese Schwachstelle wird direkt ausgenutzt, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems zu beeinträchtigen.

CVE ist eine Liste von Informationssicherheitsschwachstellen und -risiken, die allgemeine Namen für öffentlich bekannte Probleme bereitstellt [CVE].

Beispiel: Wenn eine Malware CVE-2015-12345 ausnutzt, kann ein Malware-Objekt mit einem Schwachstellenobjekt verknüpft werden, das auf CVE-2015-12345 verweist.

### Definieren Sie Schwachstellen

Definieren Sie eine Schwachstelle als eine Schwachstelle oder einen Fehler in einer Software- oder Hardwarekomponente, die von Angreifern ausgenutzt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Schwachstellen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

### Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Schwachstellenobjekt zugeordnet sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Beziehungen anzeigen | Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.<br><br>Beziehungen anzeigen wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist. |
| Externe Referenzen | Listet externe Referenzen auf, die auf Nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen. |
| Angriffsmuster | Listet die Angriffsmuster auf, die bei der Kategorisierung von Angriffen helfen, die diesem Objekt zugeordnet sind. |
| Kampagnen | Listet Kampagnen auf, die diesem Objekt zugeordnet sind. |
| Vorgehensweisen | Listet die mit diesem Objekt verbundene Vorgehensweise auf, bei der es sich um technische oder automatisierte Antworten handelt (Anwenden von Patches, Neukonfiguration von Firewalls), um einen Angriff zu verhindern. |
| Infrastruktur | Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind. |
| Angriffssatz | Listet eine Reihe von Verhaltensweisen und Ressourcen von Angreifern mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind. |
| Malware | Listet schädlichen Code auf, der diesem Objekt zugeordnet ist. |
| Bedrohungsakteure | Listet Personen, Gruppen oder Organisationen auf, die mit der mit diesem Objekt verknüpften böswilligen Absicht handeln. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Zugehörige Links und Zugehörige Listen | Beschreibung |
|---|---|
| Tools | Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um mit diesem Objekt verbundene Angriffe auszuführen. |

## Beziehungen

Verwenden Sie die Beziehungsobjekte, um zwei SDOs oder STIX Cyber-observable Objects (SCOs) miteinander zu verknüpfen und zu beschreiben, wie sie sich zueinander verhalten.

STIX-Beziehungsobjekte (SROs) stellen Arten von Beziehungen zwischen verschiedenen STIX-Objekten dar. Die folgenden Beziehungsobjekte sind verfügbar:

- **Objekt-Objekt-Beziehung**: Dieses Objekt definiert Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts. Ein Beispiel für eine definierte Objekt-Objekt-Beziehung ist, dass ein Angriffsmuster eine Malware bereitstellt.
- **Objekt-Indikator-Beziehung**: Dieses Objekt definiert Beziehungen zwischen dem Indikatorobjekt und anderen SDOs. Ein Beispiel für eine definierte Objekt-Indikator-Beziehung ist, dass ein Indikator Nachweise für eine Kampagne erkennt.
- **Objekt-Erkennbare-Beziehung**: Dieses Objekt definiert Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO). Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus im Internet erkennbaren Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen.

### STIX-Objektbeziehungen

| Beziehungsobjekt | Beispielquelle | Beispiel Ziel | Beispielbeschreibung |
|---|---|---|---|
| Objekt-Objekt-Beziehungen | Angriffsmuster | Malware | Diese Beziehung beschreibt, dass dieses Angriffsmuster zur Bereitstellung dieser Malware-Instanz (oder -Familie) verwendet wird. |
| Objekt-Indikator-Beziehungen | Indikator | Angriffsmuster, Kampagne, Infrastruktur, Angriffssatz, Malware, Bedrohungsakteur, Tool | Diese Beziehung beschreibt, dass der Indikator Beweise für das zugehörige Angriffsmuster, die Kampagne, die Infrastruktur, den Angriffssatz, die Malware, den Bedrohungsakteur oder das Tool erkennen kann.<br><br>Der Nachweis ist möglicherweise nicht direkt. Beispielsweise kann der Indikator sekundäre Beweise für die Kampagne erkennen, z. B. Malware, die häufig von dieser |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**STIX-Objektbeziehungen (Fortsetzung)**

| Beziehungsobjekt | Beispielquelle | Beispiel Ziel | Beispielbeschreibung |
|---|---|---|---|
| | | | bestimmten Kampagne verwendet wird. |
| Objekt-Erkennbares Element-Beziehungen | Infrastruktur | Beobachtete Daten | Diese Beziehung beschreibt, dass der Indikator basierend auf Informationen aus einem beobachteten Datenobjekt erstellt wird.<br><br>Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus im Internet erkennbaren Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen. |

### Definieren Sie Objekt-Objekt-Beziehungen

Definieren Sie Beziehungen zwischen SDOs, mit Ausnahme des Indikatorobjekts.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

### Definieren Sie Objekt-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Indikator-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

### Definieren Sie Beziehungen zwischen Objekt und erkennbarem Element

Definieren Sie Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO).

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Erkennbares-Beziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

## STIX-Visualizer

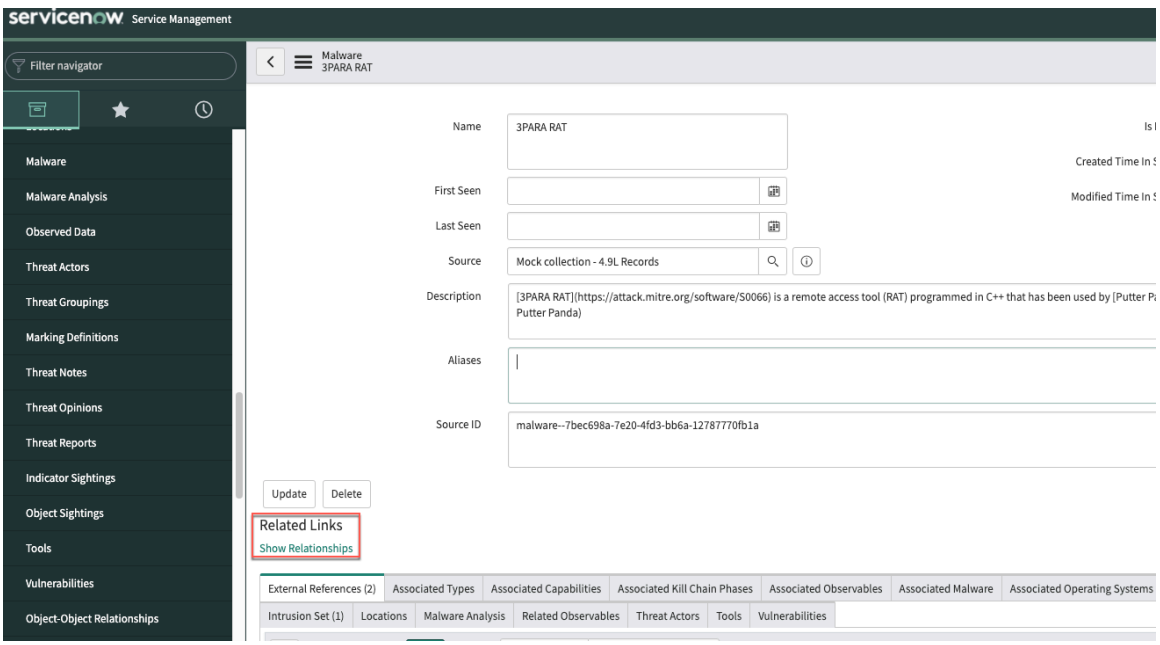
Die STIX-Visualisierung stellt die Struktur des STIX-Objekts und seine Beziehung visuell dar.

Weitere Informationen zum ausgewählten Objekt oder zur ausgewählten Beziehung finden Sie im Detailbereich.

Das Beziehungsdiagramm zeigt die Beziehungen für ein Objekt und bietet Kontext, den Sie untersuchen können. Sie können auf einen beliebigen Knoten im Diagramm klicken, um weitere Details anzuzeigen.

**Hinweis:**
Die STIX-Visualisierung ist für alle SDOs mit Ausnahme der Objekte „Bericht“ und „Beobachtete Daten“ verfügbar.

### Greifen Sie auf die STIX-Visualisierung zu

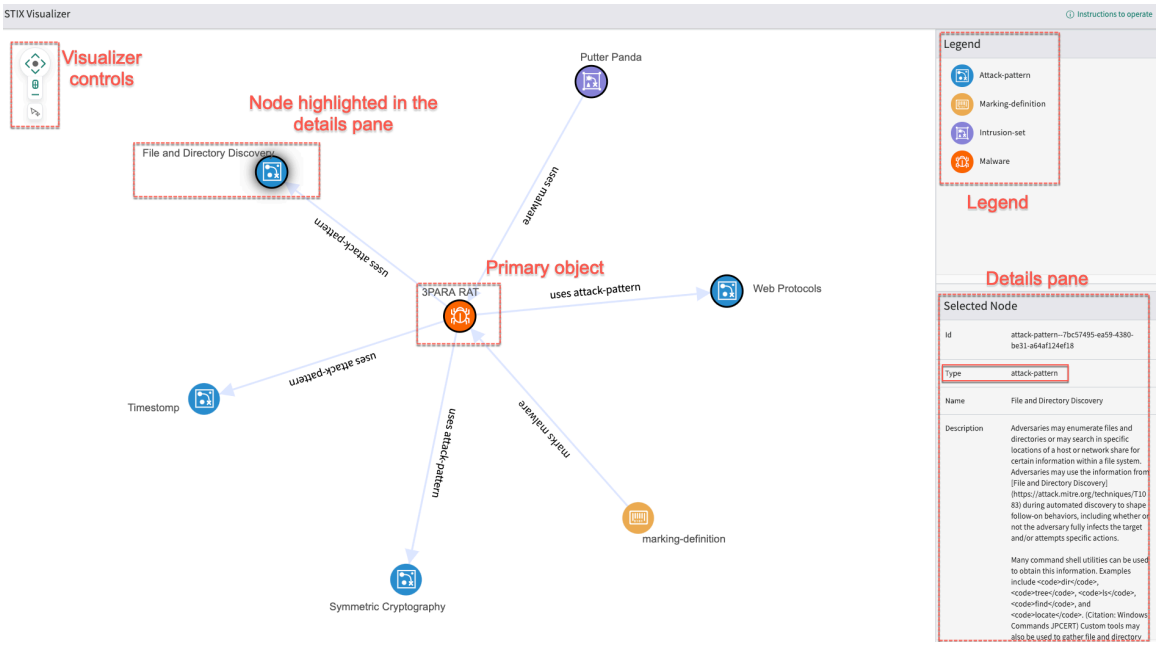



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Klicken Sie im Abschnitt „Zugehörige Links“ für eines der SDOs auf Beziehungen** anzeigen, um die STIX-Visualizer anzuzeigen.

### Zeigen Sie Details in STIX Visualizer an




In der Visualisierung können Sie das Objekt und seine Beziehung anzeigen, die Ihnen den Kontext für weitere Untersuchungen bietet. Visualizer verwendet Farben und Symbole, um verschiedene Informationen zu den Objekten darzustellen.

Sie können ein Objekt vergrößern, die Knoten ziehen oder anheften, um sich auf eine bestimmte Beziehung zu konzentrieren.

Klicken Sie auf ein beliebiges Objekt, um den Detailbereich zu öffnen. Im Detailbereich erhalten Sie weitere Informationen, die dem Objekt zugeordnet sind.

## MITRE-ATT&CK™ -Framework – Übersicht

Das Framework MITRE-ATT&CK ist eine Knowledge Base mit allgemeinen Taktiken, Techniken und Verfahren (TTP), auf die Ihre Organisation zugreifen kann, um spezifische Bedrohungsmodelle und Methoden gegen Cyberangriffe zu entwickeln.

### Übersicht

Das ATT&CK-Framework ( MITRE Adversarial Taktiken, Techniken und allgemeines Wissen) dokumentiert und verfolgt verschiedene Angreifertechniken, die in verschiedenen Phasen eines Cyberangriffs verwendet werden.

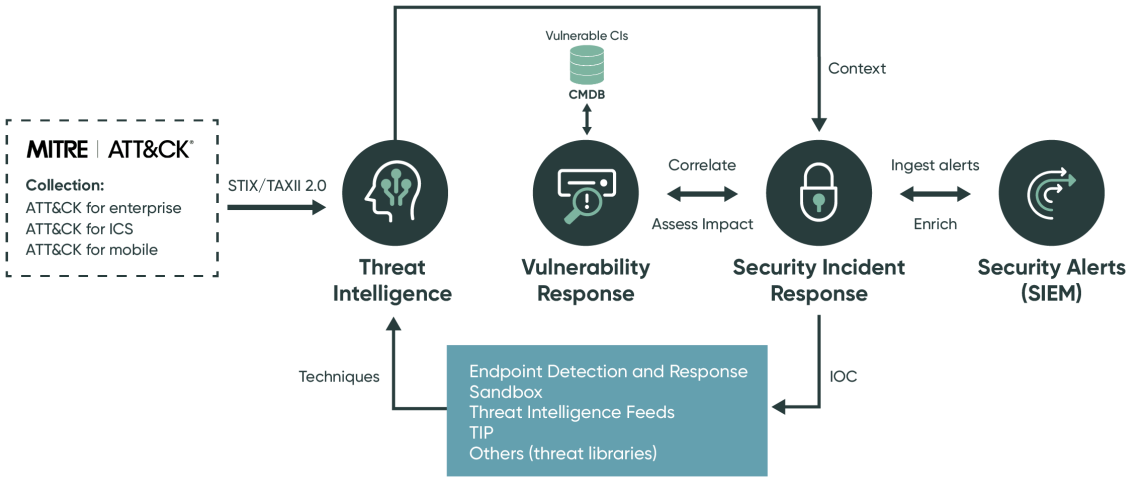
Mithilfe der Knowledge Base des Frameworks MITRE-ATT&CK kann die Cyberthreat Intelligence-Community Bedrohungen schnell identifizieren und Reaktionen auf Cyberangriffe koordinieren.

### MITRE-ATT&CK und Security Operations

Im folgenden Diagramm erfahren Sie, wie die Informationen von Security Operations mit Anwendungen von MITRE-ATT&CK fließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




- Die zugehörigen Listen namens vorinstalliert TAXII Client stellt eine Verbindung zum Server TAXII her, um die Datensammlungen für Threat Intelligencezu erfassen.
- Vorhandene SIEM-Integrationen (Security Information and Event Manager) erfassen ihre Bedrohungsdaten (Warnungen und Events) mit relevanten TTPs und sind Security Incidents zugeordnet.
- Wenn ein IoC einem Security Incident zugeordnetist, durchsucht Threat Intelligence Bedrohungsfeeds automatisch nach relevanten Informationen und sendet IoCs zur zusätzlichen Analyse an Drittanbieterquellen wie EDR, Sandbox oder TIP.
- Wenn eine Drittparteiquelle die Informationen MITRE-ATT&CK enthält, dann Threat Intelligence extrahiert die Technikinformationen und erweitert die Daten im Repository Threat Intelligence für Korrelation und Analyse.
- MITRE-ATT&CK gibt auch CVE-Kontextinformationen für jede Technik frei. Ihr Sicherheitsteam kann die verwendeten Techniken in Vulnerability Response überprüfen, um festzustellen, ob Ihre geschäftskritischen Assets gefährdet sind.

## MITRE-ATT&CK Matrizen, Taktiken und Techniken

Der Kern des MITRE-ATT&CK -Frameworks ist eine Matrix von Angreifertaktiken und -techniken. Die Reihenfolge der Taktiken stellt dar, was ein Angreifer in der Phase eines Incident erreichen möchte. Wenn Ihr Sicherheitsteam diese Sequenz versteht, haben Sie die Möglichkeit, den nächsten Schritt eines Angreifers zu antizipieren und die Kill Chain zu durchbrechen. ATT&CK besteht aus den folgenden Matrizen:

- Enterprise ATT&CK: Beschreibt die Verhaltensweisen und Aktionen eines Angreifers, um in einem Unternehmensnetzwerk und in der Cloud zu kompromittieren und dort zu operieren.

> **Hinweis:**
> Die Pre ATT&CK-Matrix wurde von MITRE veraltet und wird mit der Enterprise-Matrix zusammengeführt.

- ICS ATT&CK: Beschreibt die Aktionen, die ein Angreifer ausführt, während er in einem ICS-Netzwerk (Industrial Control Systems) agiert.
- Mobile ATT&CK: Beschreibt die Verhaltensweisen und Aktionen von Angreifern, die sich auf Mobilgeräte konzentrieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Taktiken stellen den Grund einer ATT&CK-Technik dar. Es ist das taktische Ziel des Angreifers für die Ausführung einer Aktion.

Techniken stellen dar, wie ein Angreifer ein taktisches Ziel erreicht, indem er eine Aktion ausführt.

Techniken können mehr als einer Taktik zugeordnet werden. Beispielsweise wird die Zugriffstoken-Manipulation von einem Angreifer verwendet, um entweder die Taktik der Berechtigungseskalation oder der Verteidigungsumgehung zu erreichen.

## Verwenden eines absichtsbasierten Ansatzes für die Reaktion auf Incidents

Eine absichtsbasierte Antwort verwendet ein dynamisches und kontextbezogenes Kill Chain-Framework, das Ihrem Unternehmen helfen kann, Security Incidents zu korrelieren und eine Vielzahl von Angriffen zu identifizieren. Ihr Sicherheitsteam kann eine absichtsbasierte Antwort verwenden, um zu verstehen, wie die Organisation angegriffen wird und was der Angreifer als Nächstes tun könnte. Mit dieser Art von Reaktion können Sie das Verhalten eines Angreifers vorhersagen, sodass Sie Ihre Ressourcen effektiv einsetzen können.

Mit Security Incident Responsekann Ihr Sicherheitsteam den Lebenszyklus jedes Security Incident von der Analyse bis zur Eindämmung verwalten, indem es sich auf Gefährdungsindikatoren (IoCs) wie IP-Adressen, Datei-Hashes und Domänen konzentriert.

Durch die Integration von Security Incident Response mit dem Framework MITRE-ATT&CK werden Security Incidents als Links in einem größeren unternehmensweiten Angriff behandelt.

## Wie Ihre Organisation von MITRE-ATT&CK in Security Operations profitieren kann

Die Verwendung des MITRE-ATT&CK -Frameworks kann Ihrer Organisation bei folgenden Aufgaben helfen:

- Statten Sie Sicherheitsanalysten mit MITRE-ATT&CK Taktiken, Techniken und Verfahren (TTPs) aus, um Security Incidents besser zu analysieren und darauf zu reagieren.
- Automatisieren Sie die Incident-Workflows mit dem Playbook zum Erkennen und Eindämmen von Bedrohungen im Kontext des MITRE-ATT&CK -Frameworks.
- Priorisieren Sie Indikatoren für Gefährdung und Bedrohungssuche mit Informationen von MITRE-ATT&CK.
- Machen Sie sich mit der allgemeinen Sicherheitslage Ihrer Organisation im Kontext des Frameworks MITRE-ATT&CK vertraut.

## MITRE-ATT&CK – Administration

Sie können Datenquellen einrichten, zuordnen, die allgemeine Technikerkennungsabdeckung zuordnen und das Repository MITRE-ATT&CK in Now Platformverwalten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erste Schritte mit dem Framework MITRE-ATT&CK

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres MITRE-ATT&CK -Frameworks beginnen.

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform, Threat Intelligenceund Security Incident Response zugewiesen haben. | Die folgenden Rollen werden in den -Funktionen von MITRE-ATT&CK verwendet:<br>• Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow Store und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu.<br>• sn_ti.admin<br>• sn_si.admin<br>• sn_si.analyst<br>• sn_ti.read<br>• sn_ti.write<br>• sn_ti.mitre_analyst – Die MITRE-Analystenrolle wurde eingeführt, um die übergreifende Navigation für die Funktionen MITRE zwischen Security Incident Response und Threat Intelligence Support Common zu ermöglichen. Mit dieser Rolle können Sie sowohl das Modul Threat Intelligence MITRE als auch das Modul Security Incident Response im schreibgeschützten Modus anzeigen.<br>• sn_si.read<br><br>Weitere Informationen finden Sie unter Threat Intelligence einrichten. |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung des Moduls MITRE-ATT&CK erforderlich sind, installiert und aktiviert sind. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br>• Threat Intelligence Support Common UI Components (sn_ti_seismic) – Version 1.0 oder höher<br>• Threat Intelligence Support Common – Version 12.0 oder höher |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| | • Threat Intelligence Version 12.0 oder höher<br>• Security Incident Response Version 12.0 oder höher<br><br>Weitere Informationen zum Einrichten Ihrer Now Platform -Instanz für die Integration finden Sie unter Berechtigungen für Security Operations-Produkte oder -Anwendungen anfordern und ServiceNow Store-Anwendungen aktivieren. |
| Domänentrennung | Überprüfen Sie den Abschnitt zur Domänentrennung, wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten. |

### Machen Sie sich mit dem Datenmodell MITRE zu STIX vertraut

Überprüfen Sie die von MITRE und STIX verwendete Terminologie, um das MITRE-ATT&CK™ -Framework in der Now Platformeffizient zu nutzen und zu verstehen.

## Zuordnung vonMITRE Objekten zu STIX .

STIX ist eine Sprache zur Beschreibung von Cyberbedrohungsinformationen auf standardisierte und strukturierte Weise. Das übergeordnete Datenmodell im Modul Threat Intelligence sind die Objekte STIX. Während die MITRE -Objekte eine Teilmenge des übergeordneten STIX -Datenmodells sind. Im MITRE-ATT&CK -Framework stellt MITRE ähnliche STIX -Informationen mit bestimmten Bezeichnungen und Objekten bereit.

**MITRE zu STIX Objektzuordnung**

| MITRE-Terminologie | STIX-Terminologie |
|---|---|
| Technik | Angriffsmuster |
| Mitigation | Vorgehensweise |
| Gruppen | Angriffssätze |
| Malware | Malware |
| Tool | Tool |

## Daten im Modul Threat Intelligence erweitern

Sie können eine Liste von Threat Intelligence Bedrohungsquellen verwalten und die erforderlichen STIX Daten importieren, die einen umfangreichen Satz von Informationen zu Cyberbedrohungen enthalten. Sie können auch die Profile TAXII verwenden, um den automatisierten Austausch von Informationen zu Cyberbedrohungen zu erleichtern.

**Hinweis:**
Weitere Informationen finden Sie unter Bedrohungsquellen definieren und TAXII-Profile erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Daten im Modul MITRE-ATT&CK erweitern

Sie können die Objekte „Malware“, „Gruppe“, „Mitigation“ und „Tool“ auf eine Technik im Repository MITRE-ATT&CK erweitern.

Sie können ein Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im Modul MITRE ATT&CK-Repository herstellen, aber Sie können den Beziehungstyp in diesem Modul nicht definieren. Um einen Beziehungstyp zu definieren, navigieren Sie zum **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** -Modul.

Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zum **IoC-Repository** > **Objekt-Objekt-Beziehungen** -Modul.

Sie können eine Gruppe erstellen und einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Objekt-zu-Objekt-Beziehungstyp zu definieren, müssen Sie dies im IoC-Repository tun.

**Hinweis:**
Weitere Informationen finden Sie unter erweitern MITRE-ATT&CK Daten und IoC-Repository.

### Domain Separation und MITRE-ATT&CK

Diese Übersicht über die Domänentrennung bezieht sich auf MITRE-ATT&CK. Mit Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

## Support-Stufe

Support: Standard.

## Funktionsweise der Domänentrennung mit MITRE-ATT&CK

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit den erforderlichen Rollen sn_ti.admin in der jeweiligen Domäne.
- Replizieren Sie Folgendes für jede Domäne:
  - TAXII Sammlungen

    **Hinweis:**
    - Aktivieren Sie die Sammlungen nicht in der globalen Domäne. Aktivieren Sie nur die Sammlungen, die repliziert und in Ihrer Domäne verfügbar sind.
    - Ändern Sie das Feld **Ausführen als** in den Sammlungen in den Benutzer mit der Rolle sn_ti.admin in der entsprechenden Domäne.

  - Definition der Technikabdeckung
  - Extraktionsregel für Technik
  - Erkennungsregeln – MITRE ATT&CK-Zuordnungen
  - Verringerungsabdeckung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

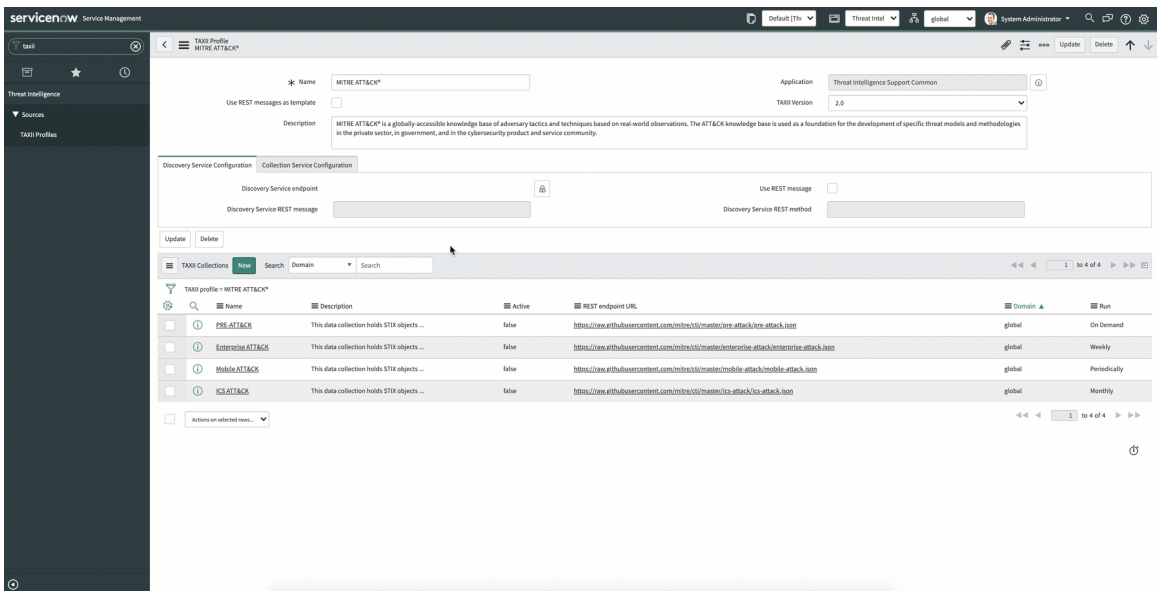
- Kopieren Sie alle Definitionsdatensätze der Abdeckung der Risikominderung.
- Kopieren Sie den Rechner für die Abdeckungsminderung, oder erstellen Sie einen neuen Rechner für die entsprechende Domäne.

○ Bedrohungsgruppe – Technik-Heatmap-Definitionen

### Replizieren Sie die TAXII-Sammlung

1. Navigieren zu **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
2. Verwenden Sie in der Kopfzeile die Domänenauswahl, um Ihre Domäne auszuwählen.
3. Wählen Sie die TAXII-Sammlung aus, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK).
4. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Einfügen und beibehalten**aus. Die doppelte TAXII-Sammlung wird unter der ausgewählten Domäne erstellt
5. Navigieren Sie zurück zum MITRE ATT&CK TAXII-Profil, um die doppelte TAXII-Sammlung anzuzeigen.

Die folgende Abbildung zeigt, wie Sie die Domäne TOP/Initech auswählen, die TAXII-Sammlung in der Domäne replizieren und die replizierte TAXII-Sammlung überprüfen.




### Richten Sie das Framework MITRE-ATT&CK™ ein

Aktivieren Sie das Profil MITRE-ATT&CK, und richten Sie eine regelmäßige Aufgabe ein, damit Sie MITRE-ATT&CK -Sammlungen für die Bedrohungserkennung in Ihrer Organisation einrichten können.

#### Vorbereitungen

Erforderliche Rolle: sn_ti.admin

#### Warum und wann dieser Vorgang ausgeführt wird

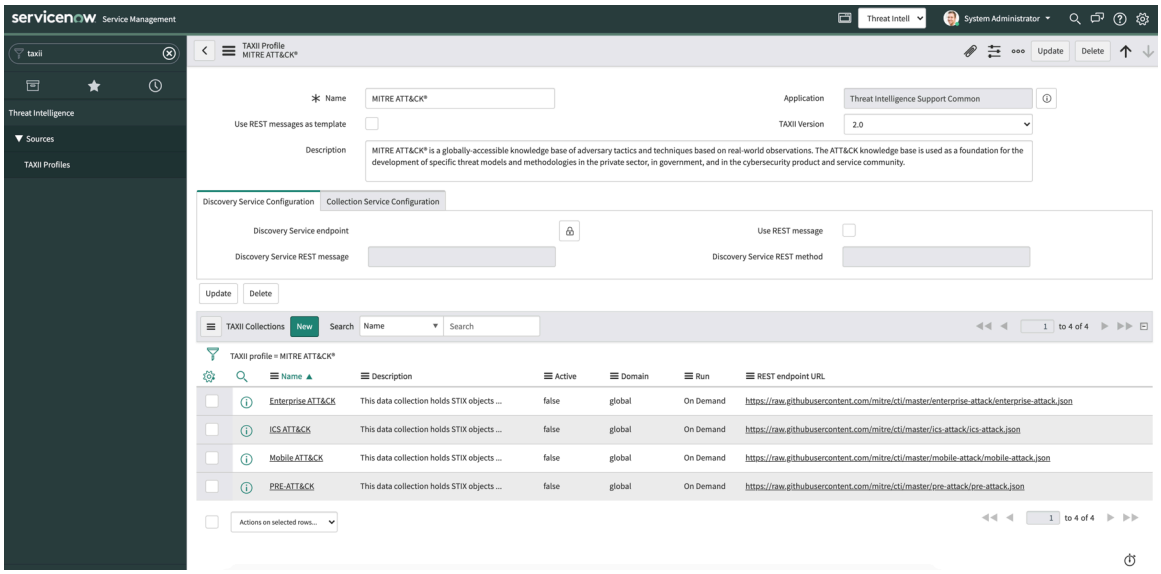
Der strukturierte Bedrohungsinformationsausdruck (STIX™) ist eine Sprache zur Beschreibung von Cyberbedrohungsinformationen auf standardisierte und strukturierte Weise. Mit STIX-Daten und Profilen für Trusted Automated Exchange of Indicator Information (TAXII™) können Sicherheitsteams freigegebene Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und aus anderen Quellen identifiziert wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**.
   Sie sehen die verfügbaren TAXII Profile.
2. Klicken Sie auf das **MITRE ATT&CK** -Profil, das mit dem Basissystem bereitgestellt wird.




3. Um die Sammlung TAXII zu aktivieren, setzen Sie die Option **Aktiv** für die Sammlung TAXII, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK), auf „true“.

| TAXII-Sammlung | Beschreibung |
|---|---|
| Unternehmens-ATT&CK | Beschreibt die Verhaltensweisen und Aktionen eines Angreifers, um in ein Unternehmensnetzwerk und eine Cloud einzudringen und dort zu operieren.<br>**Hinweis:**<br>Die Pre ATT&CK-Matrix wurde von MITRE veraltet und wird mit der Enterprise-Matrix zusammengeführt. |
| Mobile ATT&CK | Beschreibt die Verhaltensweisen und Aktionen von Angreifern, die sich auf Mobilgeräte konzentrieren. |
| ICS ATT&CK | Beschreibt die Aktionen, die ein Angreifer ausführt, während er in einem ICS-Netzwerk (Industrial Control Systems) agiert. |

4. Um die Sammlung regelmäßig zu aktualisieren, legen Sie die Option **Ausführen** für Ihre Organisation entsprechend fest.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist diese Option auf On Demand festgelegt.

### Hinweis:

a. Sammlungen werden als Teil des Threat Intelligence Core-Plugins paketiert. Durch die Installation oder Aktualisierung von Threat Intelligence Support Common - Version 12.0 oder höher und Threat Intelligence - Version 12.0 oder höher wird sichergestellt, dass Ihre Sammlungsdaten automatisch ausgefüllt werden.

b. Aktivieren Sie die Sammlung TAXII nur für die Sammlung, die Sie in Ihrer Organisation verwenden möchten, und deaktivieren Sie die anderen Sammlungen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, aktivieren Sie Enterprise ATT&CK auf der Sammlungsebene TAXII und auf der Matrizenebene. Deaktivieren Sie die anderen Mobile ATT&CK- und ICS ATT&CK-Matrizen in der Sammlung TAXII und auf der Matrizenebene.

c. Wenn Sie in den zugehörigen Listen TAXII Sammlungen für die Option Ausführen die Option Täglich auswählen, tritt ein Fehler auf, und die Option wird standardmäßig auf Bei Bedarf festgelegt. Dieser Fehler tritt auf, da die Planung der täglichen Datenaktualisierung von MITRE-ATT&CK eingeschränkt ist, um die Last auf den Servern MITRE zu optimieren. Außerdem aktualisiert MITRE die ATT&CK-Daten nur zweimal im Jahr.

d. Die TAXII -Sammlungen werden nur aktualisiert, wenn Sie die TAXII -Sammlung aktivieren.

e. Aktualisierungen vorhandener Sammlungen können vom MITRE -Server abgerufen werden, indem die Ausführungshäufigkeit in jeder Sammlung geplant wird.

f. Die Anpassungen, die Sie an den MITRE-ATT&CK -Repository-Daten vornehmen (Malware-, Gruppen-, Mitigation- und Tool-Objekte zu einer Technik) werden während geplanter Updates gespeichert.

g. MITRE aktualisiert die Knowledge Base MITRE-ATT&CK, in der einige Objekte als widerrufen oder veraltet identifiziert, neue Objekte hinzugefügt oder vorhandene Objekte geändert werden. Wenn MITRE eine Taktik oder Technik widerruft, werden diese Objekte in Now Platformals widerrufen markiert. Die widerrufenen Objekte werden im Repository beibehalten, sind jedoch nicht zur Verwendung in Now Platformverfügbar.

## Nächste Maßnahme

Nach Abschluss der Einrichtung des TAXII-Profils werden die Repository-Daten MITRE-ATT&CK in regelmäßigen Abständen in den Now Platform®importiert. Sie können diese Daten anzeigen, indem Sie zu navigieren **MITRE ATT&CK-Repository** > **Matrizen** und **MITRE ATT&CK-Repository** > **Techniken**.

### Matrizen verwalten

Verwalten Sie die Matrizen, die aus den MITRE TAXII -Sammlungen importiert wurden. Matrizen sind eine Sammlung von Taktiken und Techniken. Sie können die Matrizen anzeigen, um zu überprüfen, ob Ihre Sammlungen im Repository MITRE-ATT&CK verfügbar sind.

## Vorbereitungen

### Hinweis:

Überprüfen und stellen Sie sicher, dass nur die Matrix, die Sie in Ihrer Organisation verwenden möchten, auf „Aktiv“ gesetzt ist, und deaktivieren Sie die anderen Matrizen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, wird die Enterprise ATT&CK-Matrix auf der TAXII-Sammlungsebene und auf der Matrizenebene aktiviert. Deaktivieren Sie die anderen Mobile ATT&CK- und ICS ATT&CK-Matrizen in der Sammlung TAXII und auf der Matrizenebene.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

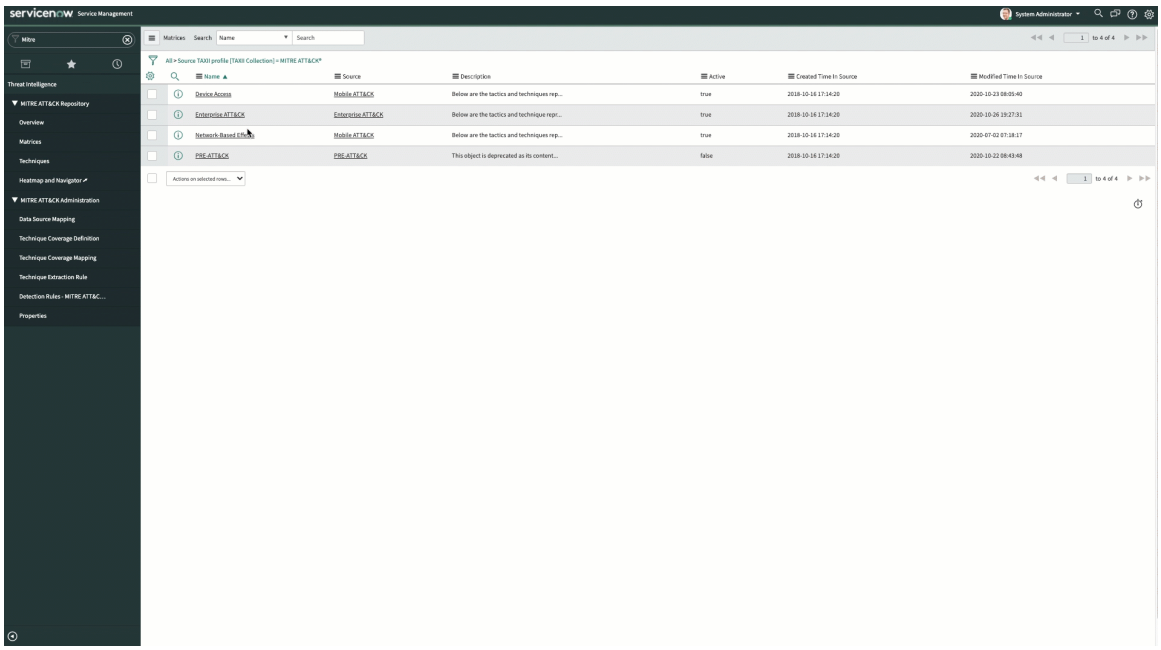
Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Matrizen**.
   Alle Matrizen sind standardmäßig deaktiviert.
2. Um eine Matrix zu aktivieren, zeigen Sie auf **Aktiv**, doppelklicken Sie, und wählen Sie **true**aus.
3. Um alle zugehörigen Informationen anzuzeigen, klicken Sie auf eine Matrix.
4. Um alle Taktiken anzuzeigen, die dieser Sammlung zugeordnet sind, klicken Sie auf die Registerkarte **MITRE-Taktiken**.
5. Um zusätzliche Details und die Techniken anzuzeigen, die einer ausgewählten Taktik zugeordnet sind, klicken Sie auf eine Taktik.
6. Wählen Sie auf der Registerkarte **MITRE ATT&CK-Techniken** eine Technik aus.
7. Zeigen Sie unter den zugehörigen Listen die Zuordnungen an, die für die von Ihnen ausgewählte Technik verfügbar sind.

   In der folgenden Abbildung sehen Sie den Navigationspfad von der Enterprise ATT&CK-Matrix zur Taktik „Erster Zugriff“ (TA0001) und dann zur Technik „Phishing“ (T1566). Auf der Seite „Angriffsmuster – Phishing-Technik“ können Sie die zugehörige Liste anzeigen – „Taktik“, „Untertechnik“, „Gruppe“, „Mitigation“, „Externe Referenzen“, „Malware“ und „Tools“.




## Nächste Maßnahme

Sie können die Informationen in einigen dieser zugehörigen Listenobjekte basierend auf der von Ihnen ausgewählten Technik erweitern. Sie können beispielsweise neue Informationen für „Gruppe“, „Mitigation“, „Externe Referenzen“, „Malware“ und „Tools“ hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Techniken verwalten

Verwalten Sie die Techniken, die aus den MITRE TAXII -Sammlungen importiert wurden. Die Techniken beinhalten verschiedene Möglichkeiten, die Angreifer entwickelt haben, um eine bestimmte Taktik anzuwenden. Sie können Techniken überprüfen und deaktivieren, die für Ihre Organisation nicht relevant sind. In STIXwerden Techniken als Angriffsmuster bezeichnet.

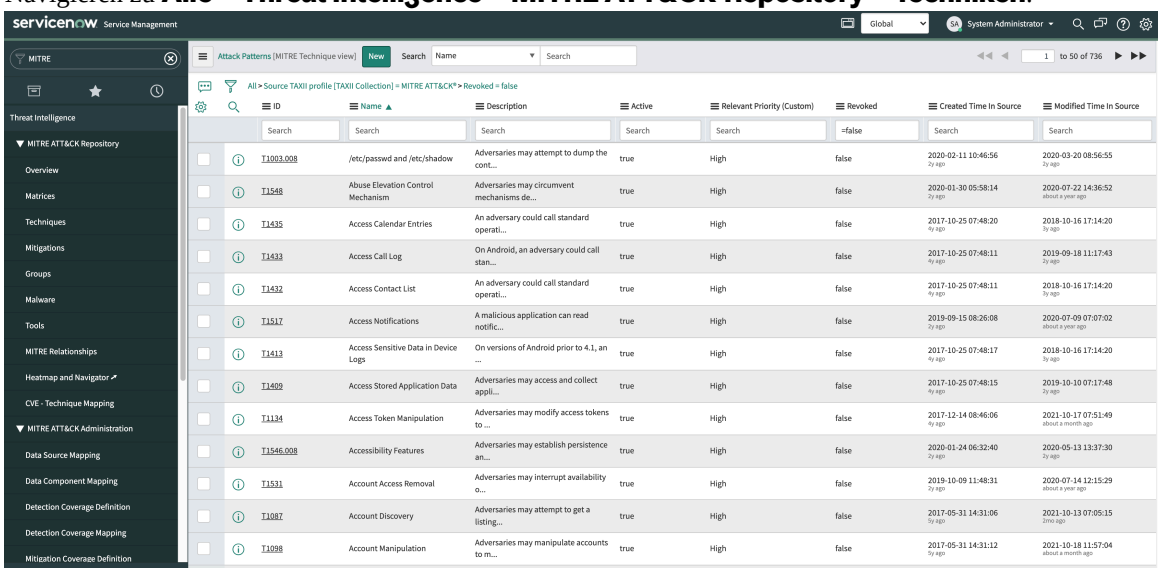
## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**.




   Die Liste der Techniken und Untertechniken wird jetzt aufgelistet.

2. Um Techniken zu überprüfen und zu deaktivieren, die für Ihre Organisation nicht relevant sind, wechseln Sie zur Listenansicht für die ausgewählte Technik, aktualisieren in der Spalte Aktiv die Einstellung auf **false**und speichern die Einstellung.
   Deaktivieren Sie die Techniken, die nicht von den anderen Objekten im MITRE-ATT&CK -Repository verwendet werden.

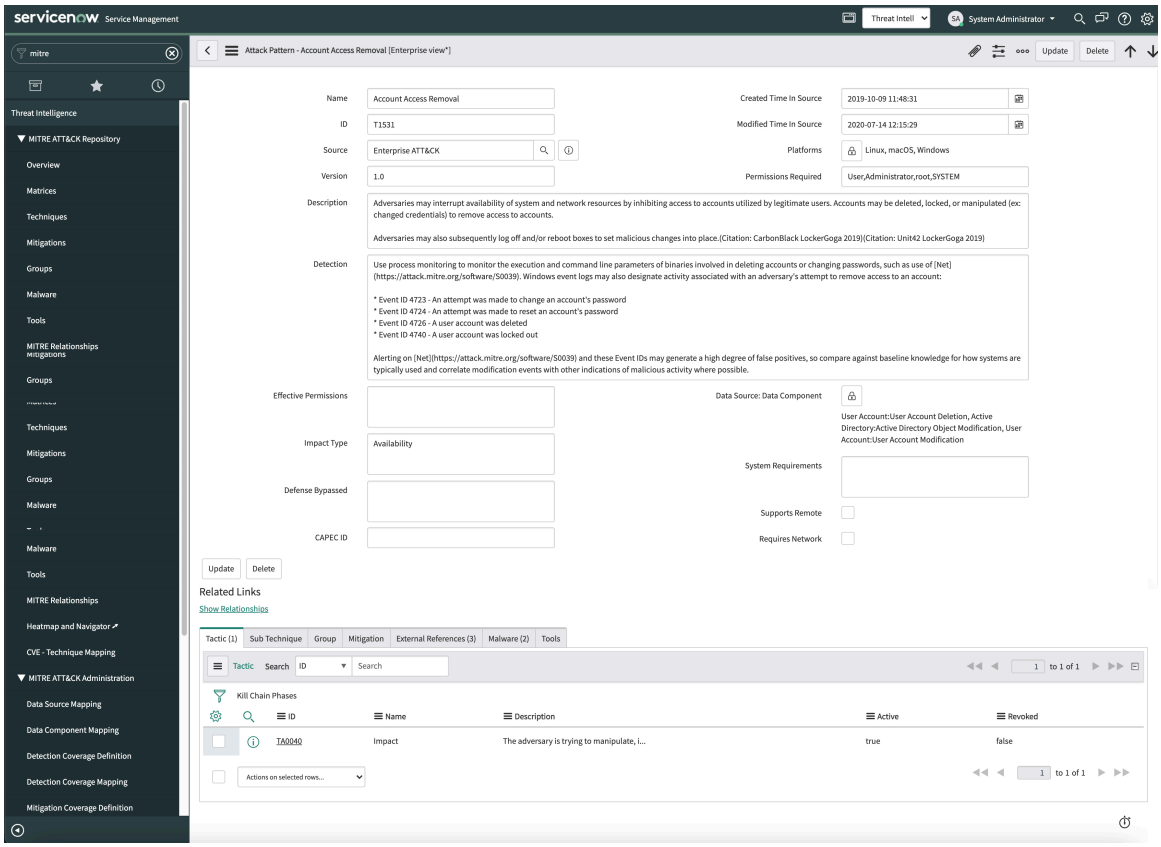
3. Um eine Technik zu priorisieren, weisen Sie im Feld **Relevante Priorität (Benutzerdefiniert)** eine Priorität zu.
   Die relevante Priorität des Basissystems ist auf Keine festgelegt. Das Feld „ **Relevante Priorität (Benutzerdefiniert)** “ wird nicht aus den MITRE-ATT&CK TAXII -Sammlungen importiert, sondern aus einem benutzerdefinierten Feld, das in Now Platformeingeführt wird. Sie können die relevanten Prioritätsinformationen verwenden, um Techniken in den Dashboards, während der Datenquellenzuordnung oder bei der Analyse der Heatmap zu filtern und zu priorisieren.

4. Klicken Sie auf eine Technik, um alle zugehörigen Informationen zu dieser Technik anzuzeigen.

   In der folgenden Abbildung können Sie die Details für jede Technik zum Entfernen des Kontozugriffs, ihre ID, Quelle und andere zugehörige Informationen anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Das von MITRE eingeführte Element „Datenquelle: Datenkomponente“ ersetzt das vorherige Feld „Datenquelle“. Die Datenkomponente stellt den Datenquellen eine zusätzliche Kontextebene bereit. Wenn Ihr MITRE-ATT&CK -Repository die alten TAXII -Sammlungen enthält, können Sie das Feld Datenquelle anzeigen. Andernfalls können Sie die Datenquellen mit dem zusätzlichen Kontext von Datenkomponenten im Feld Datenquelle: Datenkomponente anzeigen. Sie können das neue Datenkomponentenfeld nur anzeigen, wenn die Quelle Enterprise ATT&CK ist. Weitere Informationen finden Sie unter Datenkomponentenzuordnung.

5. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

### Nächste Maßnahme
Sie können die Informationen in einigen dieser zugehörigen Listenobjekte erweitern. Sie können beispielsweise neue Informationen für Gruppe, Verringerung und externe Referenzen hinzufügen.

## Verwalten Sie Risikominderungen

Verwalten Sie die Verringerungen, die aus den MITRE TAXII -Sammlungen importiert wurden. Mit Verringerungen können Sie verhindern, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. In STIXwerden Verringerungen als Vorgehensweisen bezeichnet.

### Vorbereitungen
Erforderliche Rolle:

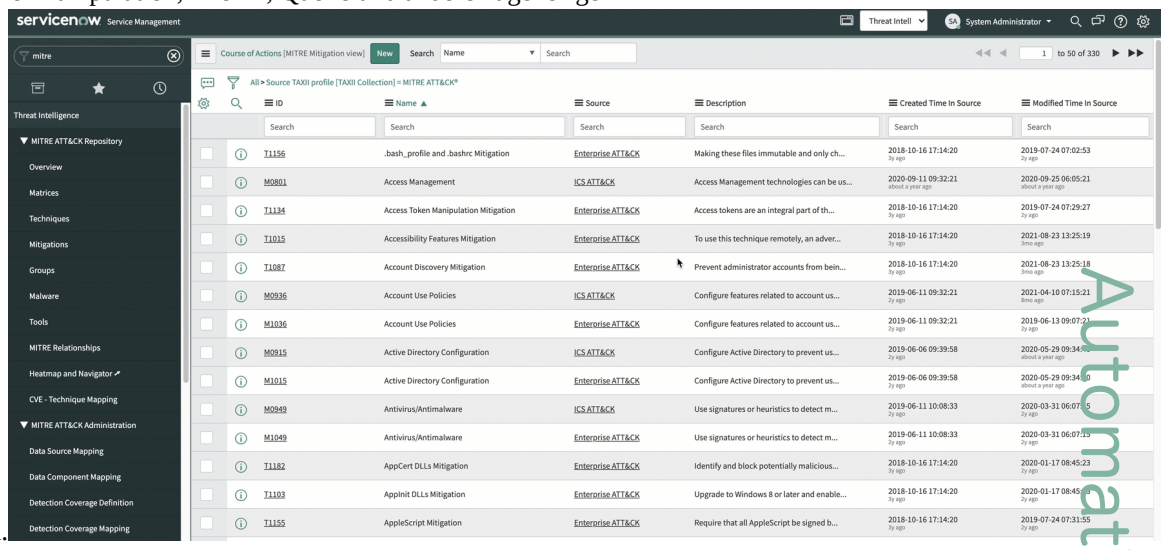
- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Mitigationen**.
   Die Verringerungen werden jetzt aufgelistet.
2. Klicken Sie auf eine Verringerung, um alle zugehörigen Informationen anzuzeigen.
   In der folgenden Abbildung sehen Sie die Details zur Verringerung der Zugriffstokenmanipulation, ihre ID, Quelle und andere zugehörige Informationen.




3. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

## Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Risikominderungsdaten hinzuzufügen oder zu ändern.

### Gruppen verwalten

Verwalten Sie die Gruppen, die aus den MITRE TAXII -Sammlungen importiert wurden. Gruppen sind Sätze zugehöriger Angriffsaktivitäten, die in der Sicherheits-Community unter einem gemeinsamen Namen verfolgt werden. Analysten verfolgen Aktivitätscluster unter Verwendung verschiedener Begriffe wie Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. In STIXwerden Gruppen als Angriffssätze bezeichnet.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

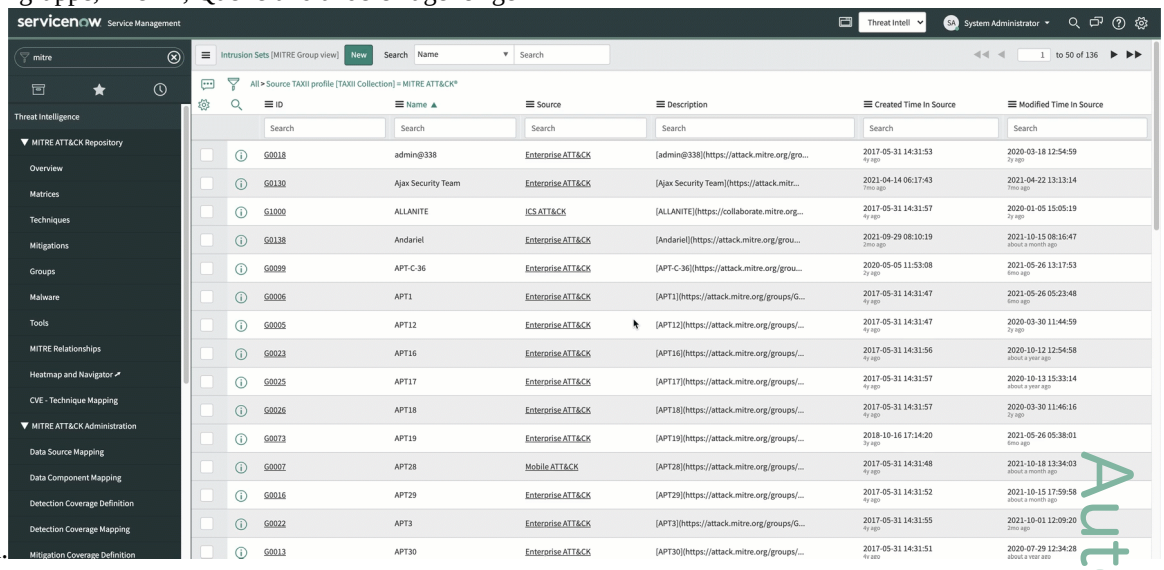
## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Gruppen**.
   Sie können die aufgelisteten Gruppen anzeigen.
2. Klicken Sie auf eine Gruppe, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die Ajax-Sicherheitsteamgruppe, ihre ID, Quelle und andere zugehörige Informationen.




3. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

> **Hinweis:**
> Um die Bedrohungsgruppen einem Sicherheitsfall für eine eingehendere Untersuchung zuzuordnen, klicken **Sie auf Zu Sicherheitsfall hinzufügen**.

## Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Gruppendaten hinzuzufügen oder zu ändern.

### Verwalten von Malware

Verwalten Sie die Malware-Informationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben. Malware ist eine Art von TTP, die schädlichen Code darstellt. Er bezieht sich auf ein Programm, das heimlich in ein System eingefügt wird. Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems (OS) des Opfers zu gefährden.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

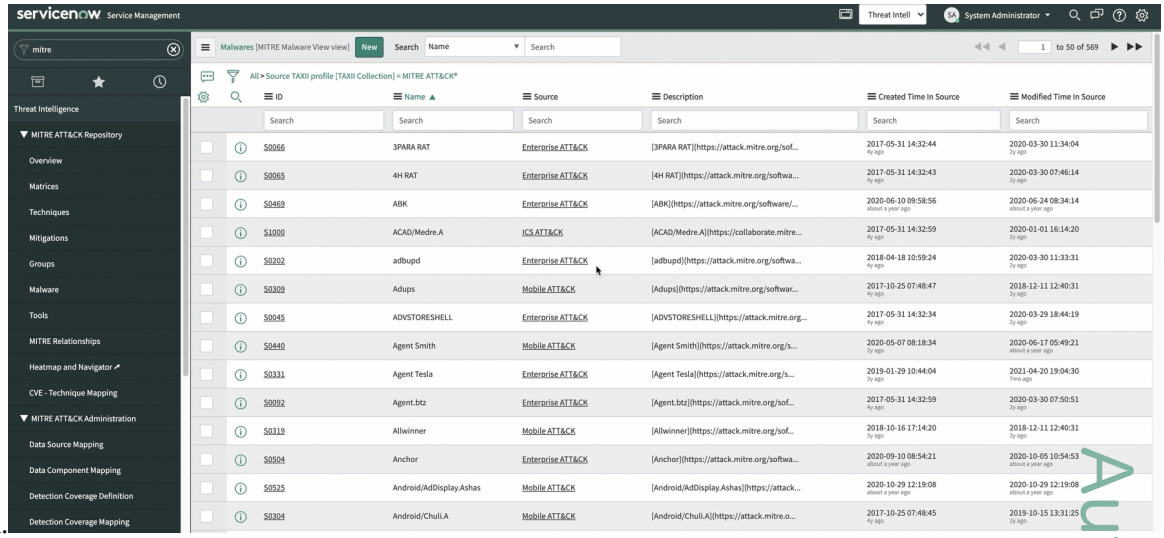
## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Malware**.
   Sie können die aufgelistete Malware anzeigen.
2. Klicken Sie auf eine Malware, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die 3PARA RAT-Malware, ihre ID, Quelle und andere zugehörige Informationen.




3. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

## Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Malware-Daten hinzuzufügen oder zu ändern.

### Tools verwalten

Verwalten Sie die Toolinformationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben. Tools sind legitime Software, die von Bedrohungsakteuren für Angriffe verwendet wird.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

## Warum und wann dieser Vorgang ausgeführt wird

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie zum Ausführen von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und dienen berechtigten Zwecken für Power-User, Administratoren, Netzwerkadministratoren oder sogar normale Benutzer.

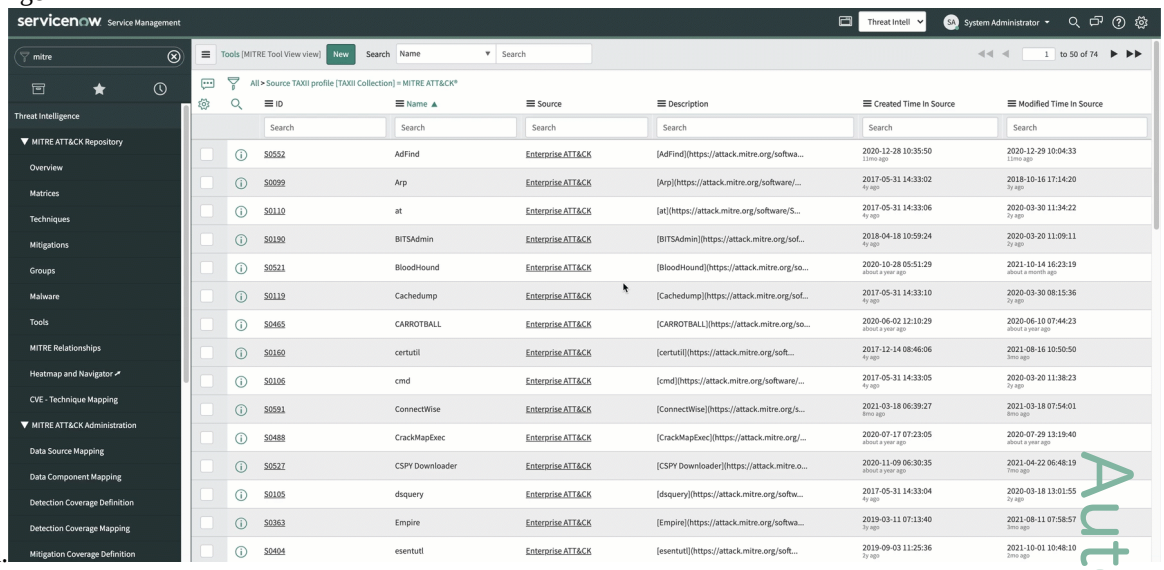
## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Tools**.
   Sie können die aufgelisteten Tools anzeigen.
2. Klicken Sie auf ein Tool, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für das Tool „Carrotbalg“, seine ID, seine Quelle und andere zugehörige Informationen.




3. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

## Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um die Tooldaten hinzuzufügen oder zu ändern.

### Verwalten MITRE Beziehungen

Verwalten Sie die MITRE -Beziehungsinformationen, die Sie aus den MITRE TAXII -Sammlungen importiert haben.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

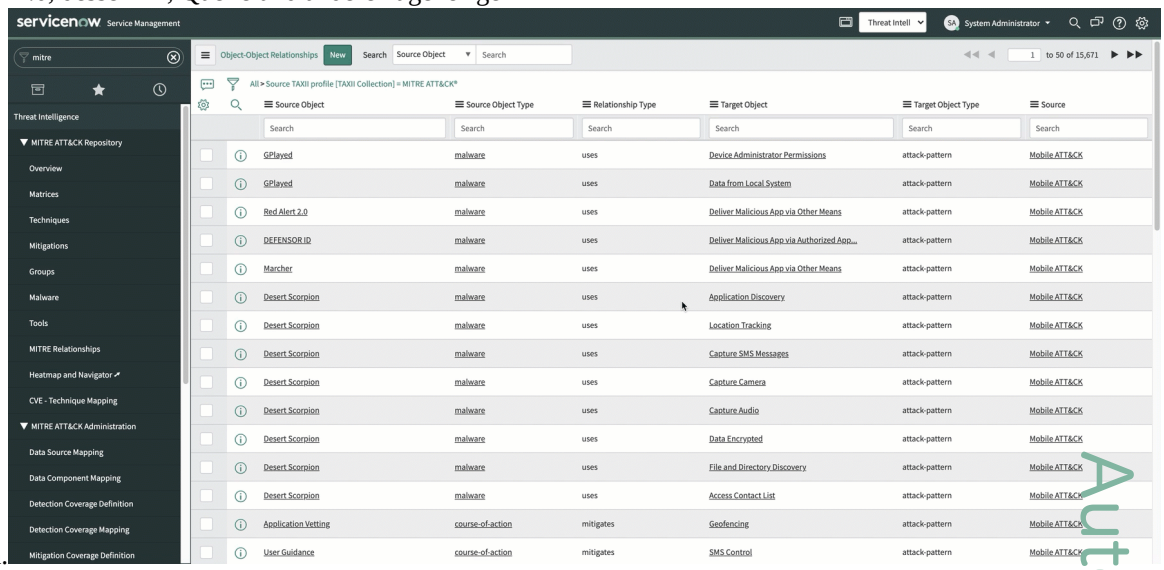
## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **MITRE-Beziehungen**. Sie können die aufgelisteten Tools anzeigen.
2. Klicken Sie auf ein Quellobjekt, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für das Objekt „Warnung rot“ 2.0, dessen ID, Quelle und andere zugehörige Informationen.




3. Um anzuzeigen, wie diese Objekte verknüpft sind, klicken Sie auf **Beziehungen**anzeigen.

## Nächste Maßnahme

Verwenden Sie das Modul „Techniken“, um MITRE-Beziehungsdaten hinzuzufügen oder zu ändern.

### CVE- und Technikzuordnung verwalten

Verwalten Sie die CVE- und Technikinformationen, die nach dem Import der MITRE TAXII -Sammlungen zugeordnet werden.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

**Hinweis:**
Das Modul **„CVE-Technikzuordnung“** ist nur verfügbar, wenn das Produkt Vulnerability Response in Ihrer Umgebung installiert ist.

## Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie die MITRE TAXII -Sammlungen importiert haben, können Sie die CVEs in Ihrer Umgebung und ihre Beziehung zu den zugehörigen MITRE-ATT&CK -Techniken anzeigen. Sie können auch Zuordnungen zu CVEs und den Angriffsmustern erstellen.

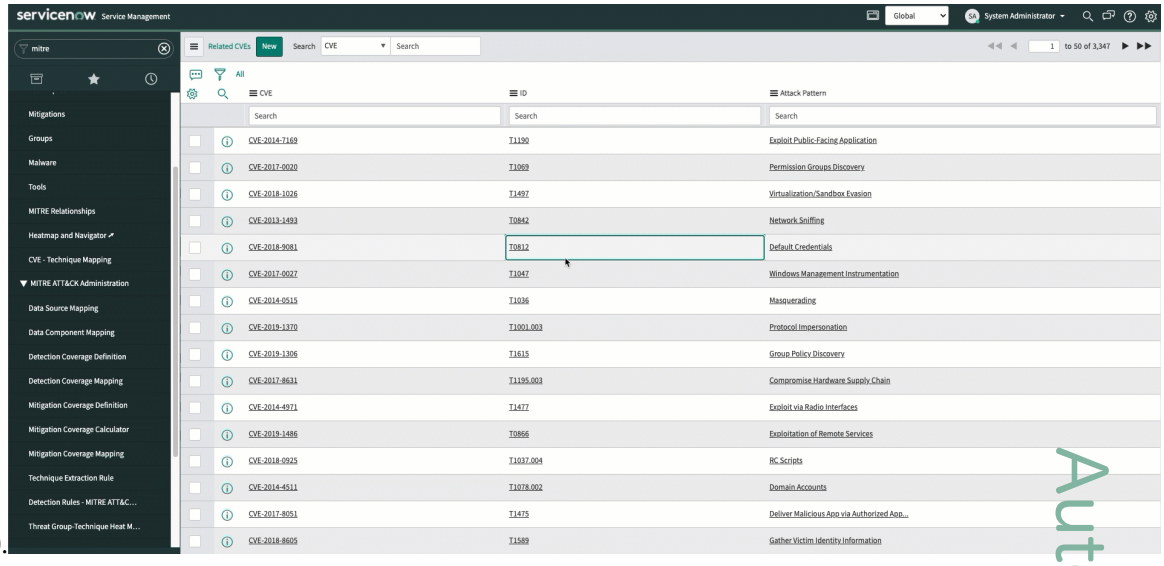
## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **CVE – Technikzuordnung**.
   Sie können die aufgelisteten CVEs und Techniken anzeigen.
2. Klicken Sie auf ein CVE, um den Eintrag in der Schwachstellendatenbank anzuzeigen.

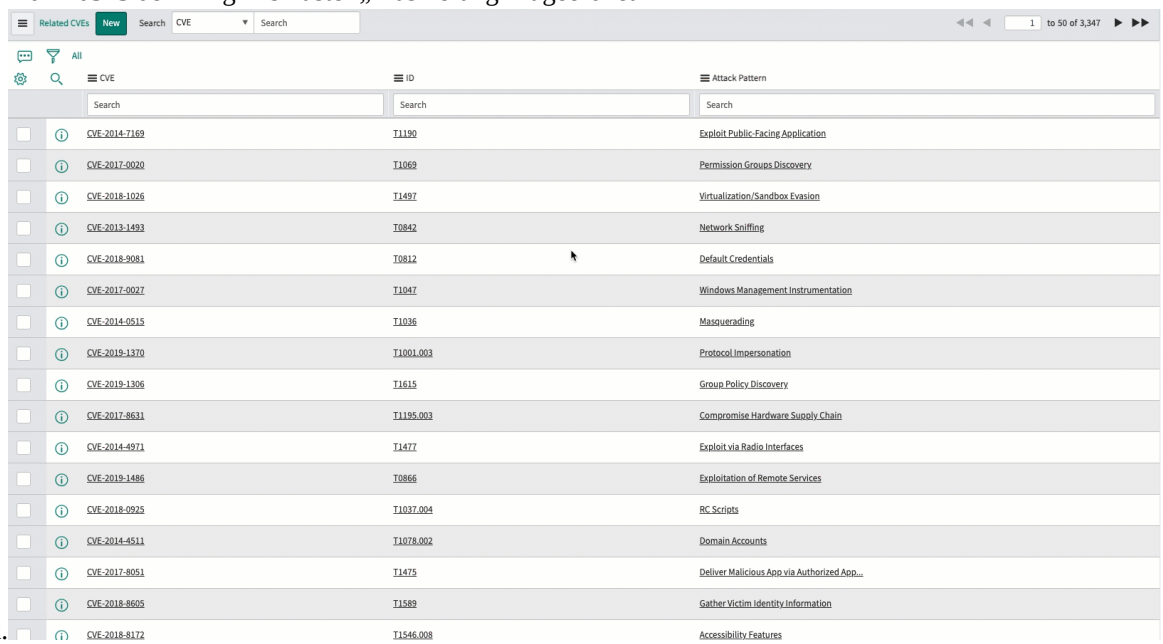
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung sehen Sie die Details für die CVE-Liste und den Eintrag in der Schwachstellendatenbank für CVE-2014-7169.




3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, ordnen Sie das CVE einem Angriffsmuster zu, und klicken Sie auf **Absenden**.
   In der folgenden Abbildung wird ein neuer Eintrag erstellt, indem CVE-2014-0515 dem Angriffsmuster „Maskierung“ zugeordnet wird.




Automatische Übersetzung

## Erweitern Sie die Daten MITRE-ATT&CK .

Erweitern Sie die Repository-Daten [ MITRE-ATT&CK in Now Platform, indem Sie sie anreichern.

### Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Erstellen, Schreibzugriff

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Objekte „Malware“, „Gruppe“, „Mitigation“ und „Tool“ auf eine Technik im Repository MITRE-ATT&CK erweitern.

Sie können ein neues Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im Modul MITRE ATT&CK-Repository herstellen, aber Sie können den Beziehungstyp in diesem Modul nicht definieren. Weitere Informationen zum Definieren von Beziehungstypen finden Sie unter Objekt-zu-Objekt-Beziehungen. Um einen Beziehungstyp zu definieren, navigieren Sie zum **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** -Modul.

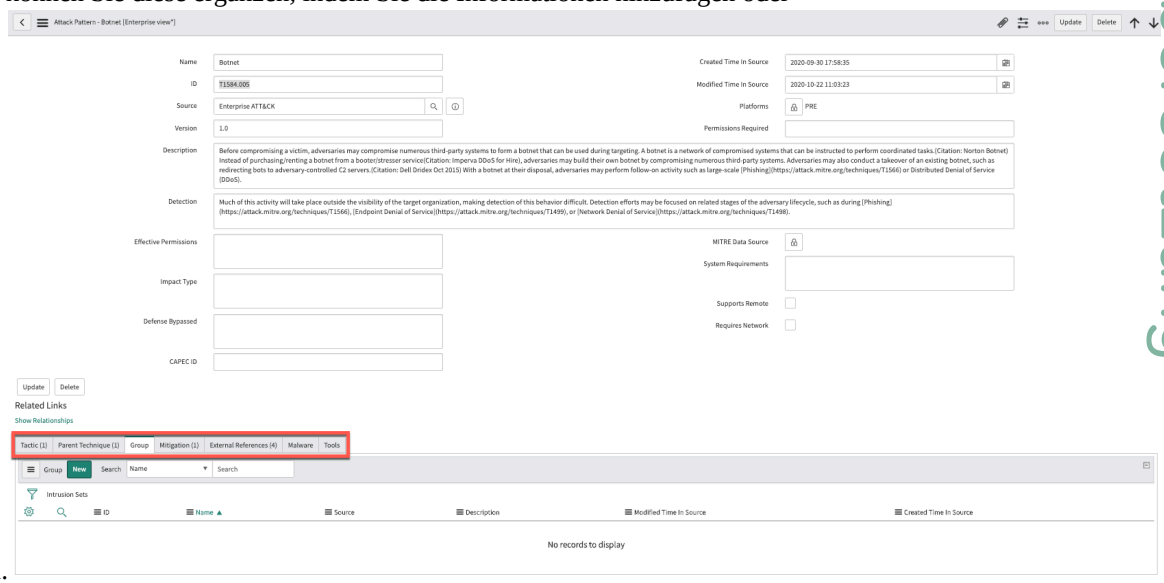
Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zum **IoC-Repository** > **Objekt-Objekt-Beziehungen** -Modul.

Sie können eine Gruppe erstellen und einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Objekt-zu-Objekt-Beziehungstyp zu definieren, müssen Sie dies im IoC-Repository tun.

**Hinweis:**
Alle Anpassungen, die Sie an den Objekten vornehmen, werden bei geplanten Updates gespeichert.

### Prozedur

1. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**.
2. Klicken Sie auf eine Technik oder Untertechnik, um alle zugehörigen Informationen zu dieser Technik anzuzeigen.
   In der folgenden Abbildung sehen Sie, dass die Botnet-Technik (T1584.005) keiner Gruppe zugeordnet ist. Wenn Sie zusätzliche Informationen zu einer Technik oder Untertechnik haben, können Sie diese ergänzen, indem Sie die Informationen hinzufügen oder ändern.

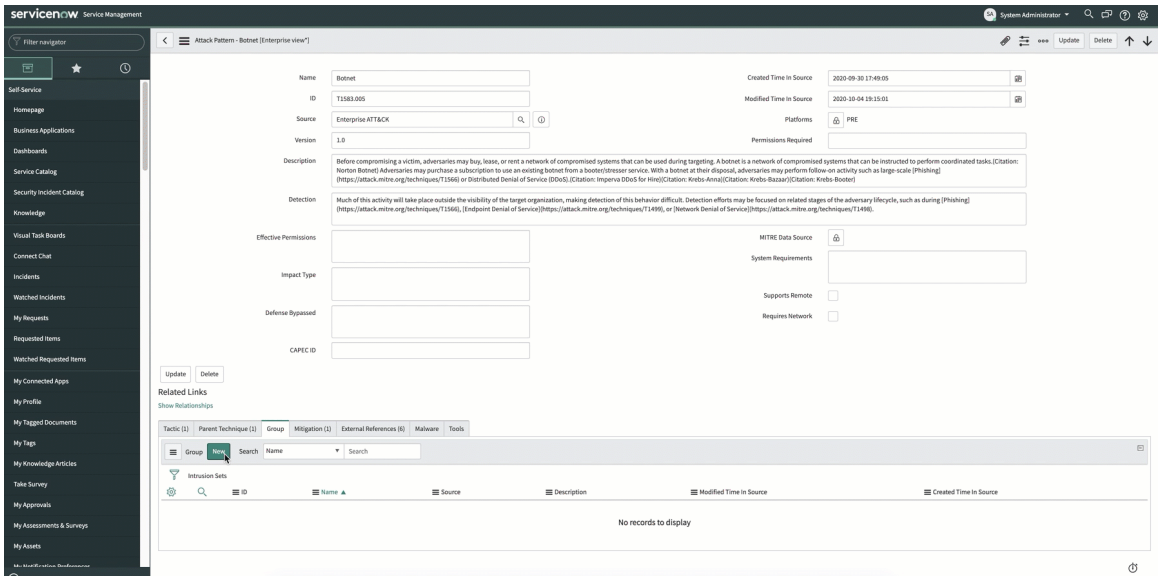



3. Klicken Sie auf eine zugehörige Liste, um ihre Daten anzureichern und sie einer neuen Gruppe zuzuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung wurde die Gruppe Custom1 der Botnet-Subtechnik zugeordnet.




## Definieren Sie die Datenquelle und die Zuordnung des Erkennungstools

Definieren Sie die Datenquellen- und Erkennungstool-Zuordnung für MITRE-ATT&CK -Taktiken und -Techniken. Die Datenquellenzuordnung bietet Einblicke in die Relevanz und Verfügbarkeit der Datenquellen und die Erkennungstools für die Überwachung der Datenquellen in Ihrer Umgebung.

### Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff

### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Datenquellen und Erkennungstools identifizieren, die Ihre Organisation benötigt, um die Techniken effektiv zu erkennen.

Wenn sich Ihre Organisation beispielsweise auf 5 Techniken konzentriert, benötigen Sie möglicherweise 10 Datenquellen und 10 Erkennungstools, um diese Quellen zu überwachen. Angenommen, Sie stellen fest, dass Ihre Organisation nicht über zwei Datenquellen und fünf Erkennungstools verfügt. Diese Übung gibt Ihnen Einblick in die Datenquellen und ihre Relevanz für Ihre Organisation. Außerdem können Sie Lücken in der Abdeckung identifizieren. Sie können sich auch auf die Verbesserung Ihrer Umgebung mit den richtigen Datenquellen und Erkennungstools konzentrieren.

Alle aktiven Taktiken, Techniken, IDs und Datenquellen werden basierend auf Ihrer automatisch ausgefüllt TAXII Profil

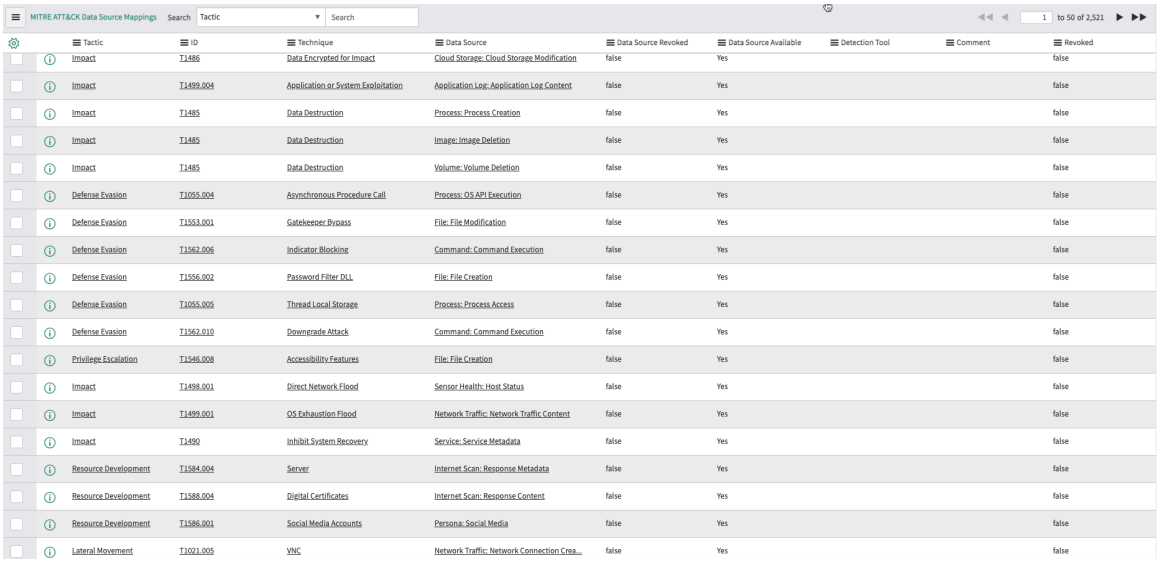
### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenquellenzuordnung**.

   Die folgende Abbildung zeigt die Liste der Taktiken, Techniken und deren IDs, die basierend auf Ihren Sammlungsaktualisierungen ausgefüllt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




| Tactic | ID | Technique | Data Source | Data Source Revoked | Data Source Available | Detection Tool | Comment | Revoked |
|---|---|---|---|---|---|---|---|---|
| Impact | T1486 | Data Encrypted for Impact | Cloud Storage: Cloud Storage Modification | false | Yes | | | false |
| Impact | T1499.004 | Application or System Exploitation | Application Log: Application Log Content | false | Yes | | | false |
| Impact | T1485 | Data Destruction | Process: Process Creation | false | Yes | | | false |
| Impact | T1485 | Data Destruction | Image: Image Deletion | false | Yes | | | false |
| Impact | T1485 | Data Destruction | Volume: Volume Deletion | false | Yes | | | false |
| Defense Evasion | T1055.004 | Asynchronous Procedure Call | Process: OS API Execution | false | Yes | | | false |
| Defense Evasion | T1553.001 | Gatekeeper Bypass | File: File Modification | false | Yes | | | false |
| Defense Evasion | T1562.006 | Indicator Blocking | Command: Command Execution | false | Yes | | | false |
| Defense Evasion | T1556.002 | Password Filter DLL | File: File Creation | false | Yes | | | false |
| Defense Evasion | T1055.005 | Thread Local Storage | Process: Process Access | false | Yes | | | false |
| Defense Evasion | T1562.010 | Downgrade Attack | Command: Command Execution | false | Yes | | | false |
| Privilege Escalation | T1546.008 | Accessibility Features | File: File Creation | false | Yes | | | false |
| Impact | T1498.001 | Direct Network Flood | Sensor Health: Host Status | false | Yes | | | false |
| Impact | T1499.001 | OS Exhaustion Flood | Network Traffic: Network Traffic Content | false | Yes | | | false |
| Impact | T1490 | Inhibit System Recovery | Service: Service Metadata | false | Yes | | | false |
| Resource Development | T1584.004 | Server | Internet Scan: Response Metadata | false | Yes | | | false |
| Resource Development | T1588.004 | Digital Certificates | Internet Scan: Response Content | false | Yes | | | false |
| Resource Development | T1586.001 | Social Media Accounts | Persona: Social Media | false | Yes | | | false |
| Lateral Movement | T1021.005 | VNC | Network Traffic: Network Connection Crea... | false | Yes | | | false |

| Feld | Beschreibung |
|---|---|
| Taktik | Ziel des Angreifers oder Grund für die Ausführung einer Aktion. |
| ID | Eindeutige Identität der Technik. |
| Technik | Wie ein Angreifer ein taktisches Ziel erreicht, indem er eine Aktion ausführt. |
| Datenquelle | Datenquelle, die der Technik zugeordnet ist. |
| Datenquelle widerrufen | Die Datenquelle wird widerrufen, wenn sie auf „wahr“ gesetzt ist, die Datenquellenzuordnung bleibt jedoch erhalten.<br><br>Wenn der Datenquellenwert nicht in MITREgefunden wird, wird der Wert Datenquelle widerrufen automatisch als „true“ markiert. Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Beziehungen zwischen Technik und Datenquelle in den aktualisierten MITRE Daten fehlen.<br><br>Standardwert: false |
| Datenquelle verfügbar | Verfügbarkeit der Datenquelle. |
| Erkennungstool | Tool, das die Datenquelle durch Erkennung der verwendeten Techniken ergänzt. Das Erkennungstool wird dem Warnungssensor in SIRzugeordnet. |
| Widerrufen | Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Beziehungen zwischen Technik und Datenquelle in den aktualisierten MITRE Daten fehlen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Standardwert: false |

2. Überprüfen Sie die aufgelisteten Datenquellen, und ändern Sie den Wert im Feld **Verfügbare Datenquelle** basierend auf Ihrer Umgebung.

3. **Hinweis:**
   Sie können diesen Eintrag nicht in der Listenansicht bearbeiten.

   Führen Sie im Feld **Erkennungstool** die folgenden Schritte aus:

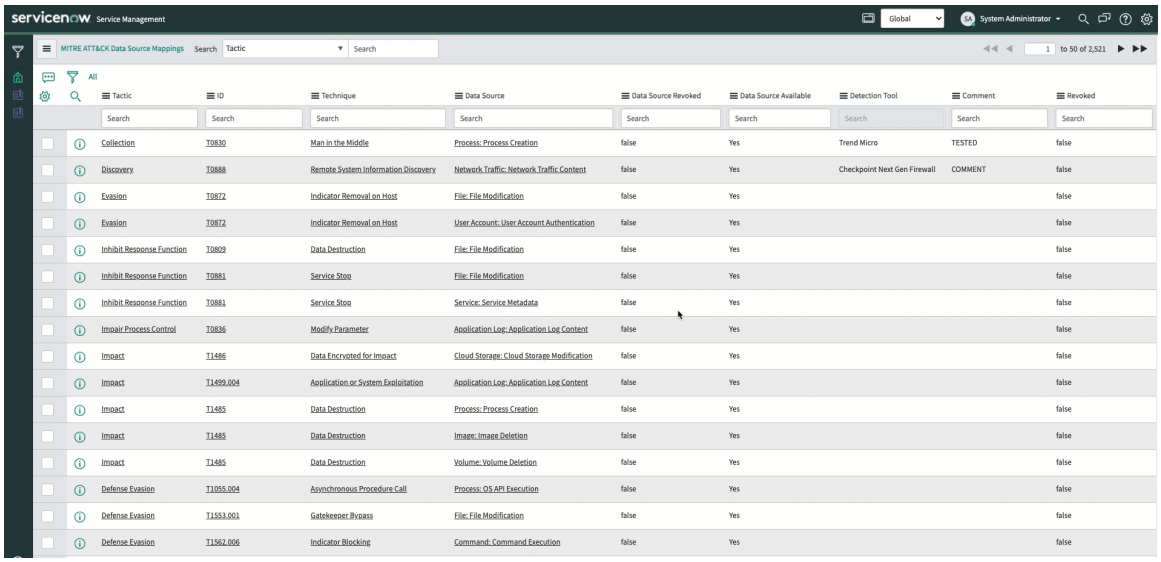
   a. Klicken Sie auf das Informationssymbol und dann auf **Datensatz öffnen**.

   b. Entsperren des **Erkennungstool-** Eintrags

   c. Verwenden Sie die Nachschlageliste, um ein Erkennungstool auszuwählen. Sie können mehrere Erkennungstools auswählen.

   d. Klicken Sie auf **Aktualisieren**.

   In der folgenden Abbildung werden mehrere Erkennungstools hinzugefügt, um die Datenquelle zu überwachen.




### Definieren Sie die Datenquellen- und Datenkomponentenzuordnung

Verwenden Sie die Datenkomponentenzuordnung, wenn Sie die neuesten TAXII Sammlungen verwenden und eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken aufrechterhalten möchten. Ordnen Sie die Datenquellen dem zusätzlichen Kontext von Datenkomponenten zu, der Datenquellen eine zusätzliche Kontextebene bietet, mit der Sie das Verhalten von Angreifern in MITRE-ATT&CK besser verstehen können.

### Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- sn_ti.read: Lesezugriff



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

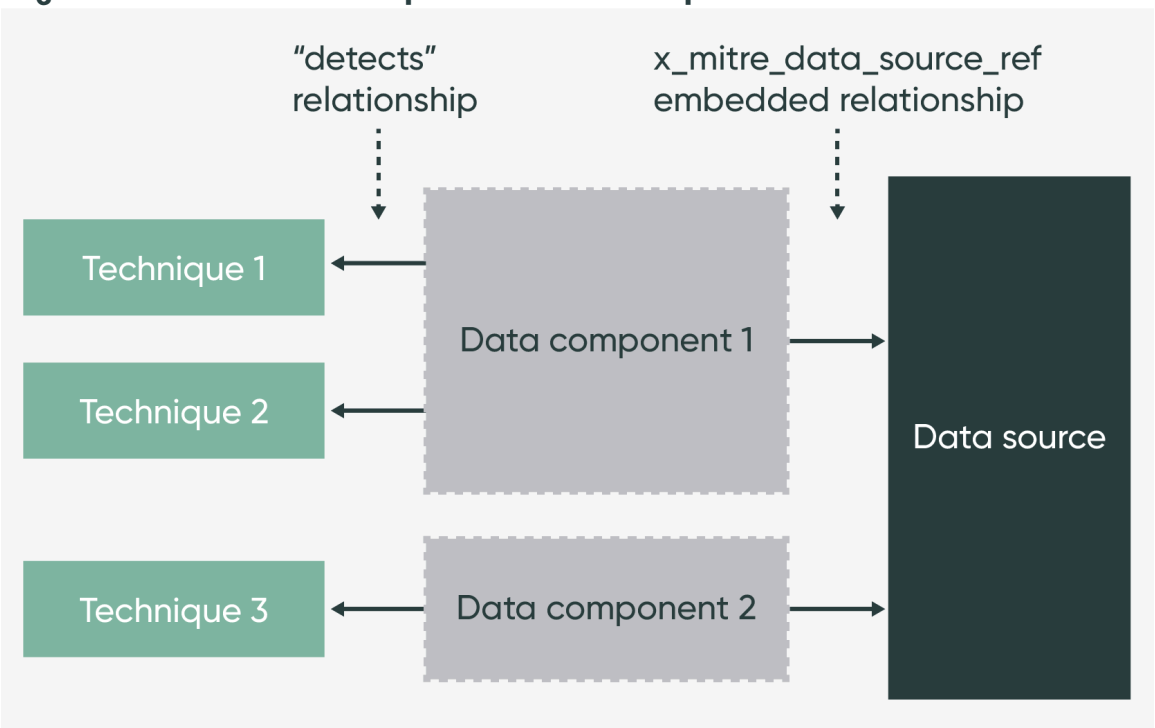
**Warum und wann dieser Vorgang ausgeführt wird**
Die Zuordnung der Datenquellen und Datenkomponenten bietet Einblick in die Datenquellen oder -komponenten und die Techniken, die für Ihre Organisation relevant sind.

Wenn sich Ihre Organisation beispielsweise auf 7 Techniken konzentriert, benötigen Sie möglicherweise 5 Datenquellen und 10 Datenkomponenten, um diese Quellen zu überwachen. Ihre Auswertung der internen Tools zeigt, dass Ihre Organisation nicht über zwei Datenquellen und vier Datenkomponenten verfügt. Diese Zuordnungsübung bietet Einblick in die Datenquellen, Komponenten und Techniken, ihre Relevanz für Ihr Unternehmen und die Identifizierung von Lücken in der Abdeckung. So können Sie Ihre Investitionen auf die richtigen Datenquellen und Warnungssensoren konzentrieren, um Bedrohungen durch Angreifer zu erkennen und zu mindern.

Das Framework MITRE-ATT&CK enthält eine aktualisierte Struktur für die Datenquellen – Datenquelle: Datenkomponente. Diese neue Form der Datenquelle bietet einen zusätzlichen Kontext für die Datenquellen. Das Datenquellenobjekt enthält den Namen der Datenquelle sowie wichtige Details zu den erfassten Daten (Datei, Prozess, Netzwerkdatenverkehr usw.) und bestimmte Werte oder Eigenschaften, die zum Erkennen des Verhaltens von Angreifern erforderlich sind.

Die folgende Abbildung zeigt die Strukturdarstellung MITRE-ATT&CK STIX™ für Datenquellen und Datenkomponenten. Sie können sowohl die Datenquellen als auch die Datenkomponenten anzeigen, die als benutzerdefinierte STIX™ Objekte erfasst wurden. Die Abbildung zeigt, dass jede Datenquelle eine oder mehrere Datenkomponenten enthält und jede Datenkomponente eine oder mehrere Techniken erkennt.

**Allgemeine Struktur von Datenquellen und Datenkomponenten**



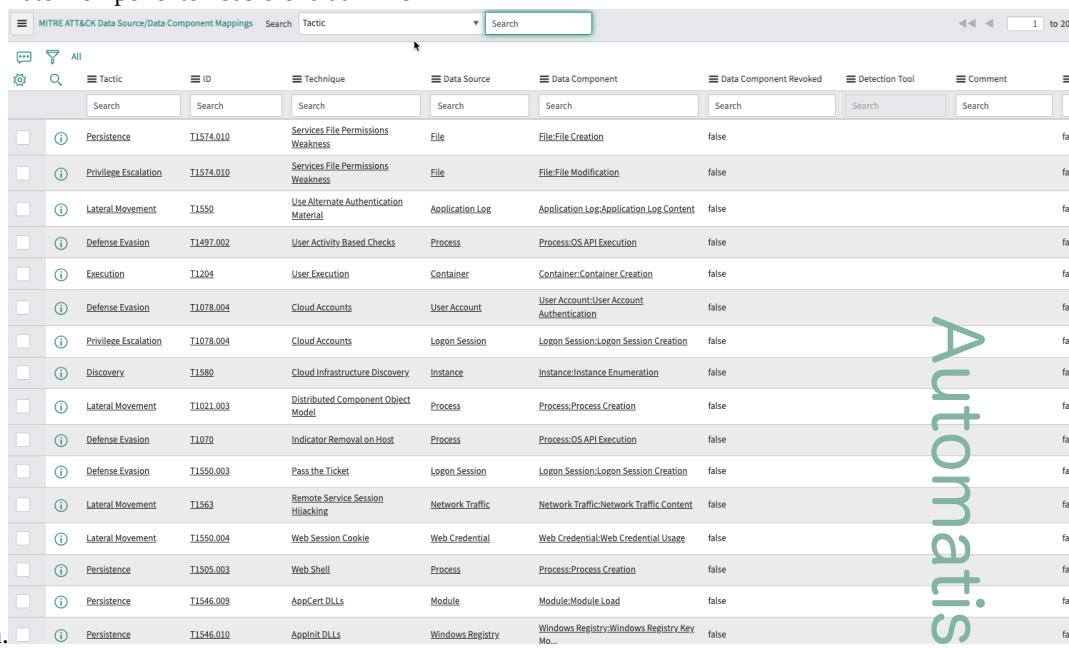

Sie können die Datenquellenzuordnung weiterhin verwenden, wenn Ihr MITRE-ATT&CK -Repository die alten TAXII -Sammlungen enthält und Sie Ihre Datenquellen verschiedenen Techniken zugeordnet haben. Verwenden Sie jedoch die Datenkomponentenzuordnung, wenn Sie die neuesten TAXII Sammlungen verwenden und eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken aufrechterhalten möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenkomponentenzuordnung**.
   Die folgende Abbildung zeigt die Liste der Taktiken, IDs, Techniken sowie die Datenquellen und Datenkomponenten basierend auf Ihren Sammlungsaktualisierungen.




| Feld | Beschreibung |
|---|---|
| Taktik | Ziel des Angreifers oder Grund für die Ausführung einer Aktion. |
| ID | Eindeutige Identität der Technik. |
| Technik | Wie ein Angreifer ein taktisches Ziel erreicht, indem er eine Aktion ausführt. |
| Datenquelle | Datenquelle, die der Technik zugeordnet ist. |
| Datenkomponente | Datenkomponente, die der Datenquelle zugeordnet ist. Eine Datenkomponente kann nur eine übergeordnete Datenquelle haben. |
| Datenkomponente widerrufen | Gibt an, ob die Datenkomponente in der Knowledge Base MITRE-ATT&CK widerrufen wurde. |
| Erkennungstool | Tool, das die Datenquelle durch Erkennung der verwendeten Techniken ergänzt. Das Erkennungstool wird dem Warnungssensor in SIRzugeordnet. |
| Anmerkung | Beschreibung der Datenquellen- und Datenkomponentenzuordnung. |
| Widerrufen | Gibt an, ob die Datenkomponente für die Technikzuordnung von MITRE-ATT&CKwiderrufen wird. |

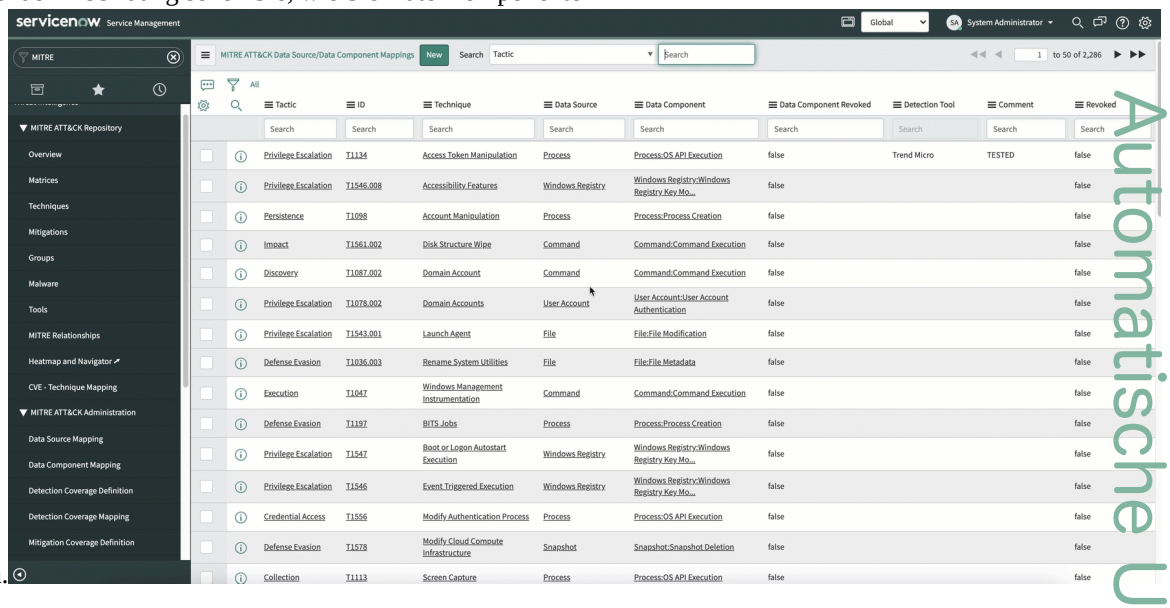
2. Überprüfen Sie die aufgelisteten Datenquellen und Datenkomponenten, und ändern Sie die Werte basierend auf Ihrer Umgebung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Befolgen Sie diese Schritte, um eine Datenkomponente hinzuzufügen.
   a. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Techniken**.
   b. Klicken Sie auf eine Technik, mit der Sie die Datenquelle ändern möchten: Datenkomponenteninformationen.
   c. Datenquelle entsperren: Datenkomponente.
   d. Verwenden Sie die Nachschlageliste, um MITRE-ATT&CK Datenkomponenten auszuwählen.
   e. Datenquelle sperren: Datenkomponente.
   f. Klicken Sie auf **Aktualisieren**.

In der folgenden Abbildung sehen Sie, wie Sie Datenkomponenten hinzufügen.




Automatische Übersetzung

## Definieren Sie die Abdeckung der Technikerkennung

Definieren Sie die Technik-Erkennungsabdeckung, die Ihre Organisation bestimmte Angreifertechniken messen und erkennen muss.

## Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

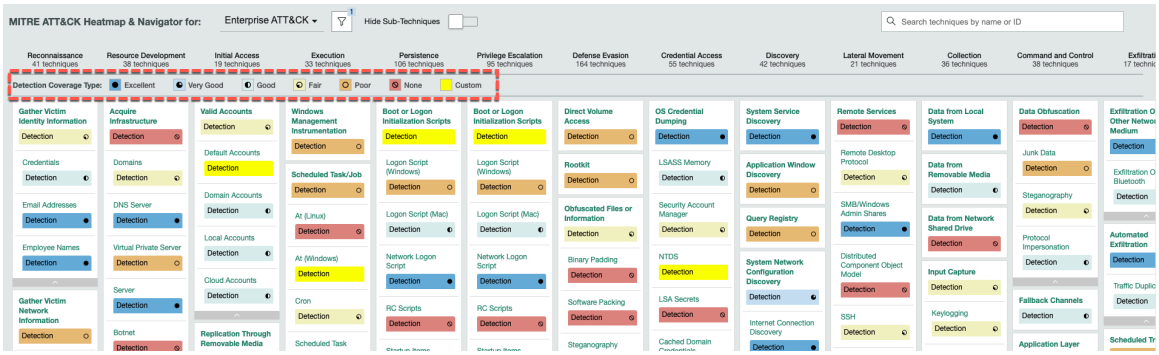
## Warum und wann dieser Vorgang ausgeführt wird

Die Definitionen der Technikabdeckung werden in der allgemeinen Technikerkennungszuordnung verwendet. Sie können die Technikabdeckung des Basissystems verwenden. Die Technikabdeckung des Basissystems besteht aus den Abdeckungstypen Keine, Schlecht, Mittel, Gut, Sehr gut und Ausgezeichnet. Die Technikabdeckung des Basissystems ist auch vordefinierten Farben zugeordnet. Sie können die Einträge und Farben des Abdeckungstyps anpassen oder eigene Einträge erstellen. Beispielsweise können Sie die Abdeckungstypen des Basissystems in Nicht zutreffend, Teilabdeckung und Vollständige Abdeckung ändern. Alternativ können Sie auch numerische Maßnahmen für die Abdeckungstypen erstellen, z. B. 0–25 Prozent, 25–50 Prozent und 50–100 Prozent. Die Art der Änderungen, die an der Basissystemabdeckung vorgenommen werden, ist nicht auf die freigegebenen Beispiele beschränkt.

Die Anpassungen, die Sie am Abdeckungstyp und an der Farbe vornehmen, werden in der gesamten Technikerkennungszuordnung und auch in der Heatmapverwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für den Abdeckungstyp nicht mit den Techniken in der Heatmap angezeigt. Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technikerkennungsabdeckung und die Abdeckungsfarben ändern. Wenn Sie jedoch vorhandene Felder aus der gesamten Technikerkennungsabdeckung löschen, werden in der Heatmap die Symbole für den Abdeckungstyp nicht angezeigt.




## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Erkennungsabdeckung**.
2. Überprüfen Sie die allgemeinen Technikerkennungseinträge, und passen Sie die Einträge für Ihre Umgebung an.

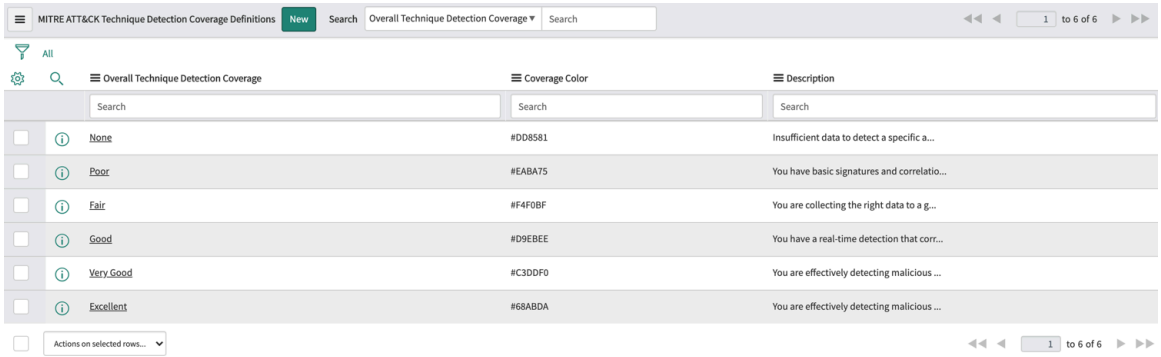
### Definition der Erkennungsabdeckung

| Feld | Beschreibung |
|---|---|
| Gesamtabdeckung der Technikerkennung | Name der gesamten Technik-Erkennungsabdeckung. Die Basissystem-Technikabdeckung besteht aus Keine, Schlecht, Mittel, Gut, Sehr gut oder Ausgezeichnet. |
| Abdeckungsfarbe | Farbe, die der Punktzahl der Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Technikerkennungsabdeckung in der Heatmap verwendet.<br><br>Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen. |
| Beschreibung | Gesamtabdeckung der Technikerkennung. Siehe Basissystemdefinition in der Bewertungsdefinition. |

Die folgende Abbildung zeigt die Definition der Erkennungsabdeckung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, schließen Sie die Einträge ab, und klicken Sie auf **Absenden**.

## MITRE-ATT&CK Bewertungsdefinition

Definieren Sie das Bewertungssystem MITRE-ATT&CK Ihrer Organisation, damit Sie messen können, wie effektiv Ihre Organisation bestimmte Angreifertechniken erkennen kann.

### Bewertungsdefinition

| Punktzahl | Punktzahlzuordnung | Beschreibung |
|---|---|---|
| Keine | 0 | Unzureichende Daten, um eine bestimmte Angreifertechnik zu erkennen. |
| Mangelhaft | 1 | Grundlegende Signaturen und Korrelationsregeln sind vorhanden, um bestimmte Angreifertechniken zu erkennen. Die Bedrohungserkennung erfolgt nicht in Echtzeit und deckt nur eine minimale Anzahl von Aspekten einer Technik ab. Beispielsweise erfolgt die Suche jeweils nur für einen Endpunkt. In Ihrer Organisation gibt es möglicherweise noch Tausende oder Hunderte von Events, die von der Suchmaschine überprüft und mit anderen Events korreliert werden müssen, um Ausreißer zu finden. Die Anzahl der Falschmeldungen ist hoch. |
| Befriedigend | 2 | Es werden in großem Umfang die richtigen Daten gesammelt, und die Datenqualität ist angemessen. Beispielsweise beginnt Ihre Organisation möglicherweise damit, Sysmon-Protokolle, ETW, PowerShell-Protokolle und ähnliches hinzuzufügen. Die Bedrohungserkennung erfolgt jedoch immer noch nicht in Echtzeit. Ihre Organisation verfügt möglicherweise nicht über die richtigen Tools, um die Daten effektiv zusammenzufassen und zu analysieren. Um die Daten genau zu analysieren, müssen sie Abfragen manuell ausführen und korrelieren. Die Anzahl der Falschmeldungen ist hoch. |
| Gut | 3 | Echtzeiterkennung, die mehrere Daten über Ihre Endpunkte hinweg korreliert und integriert. Die Bedrohungserkennung deckt viele Aspekte der Verfahren einer Technik ab.<br>Ihre Angreifer könnten möglicherweise die Erkennung umgehen, indem sie sie umgehen und verschleiern. Ihr Unternehmen kann Falschmeldungen leicht identifizieren und herausfiltern. Ihre Organisation verwendet grundlegende |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Bewertungsdefinition (Fortsetzung)**

| Punktzahl | Punktzahlzuordnung | Beschreibung |
|---|---|---|
| | | datenwissenschaftliche Techniken, um die Daten im zentralen Repository zu analysieren. |
| Sehr gut | 4 | Erkennen Sie schädliche Techniken effektiv in Echtzeit und decken Sie die meisten Aspekte der Verfahren einer Technik ab. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Umgehungs- und Verschleierungsmethoden umgehen, ist auf der Ebene „Gut“ schwieriger als. Ihr Unternehmen kann Falschmeldungen leicht identifizieren und herausfiltern. Ihre Organisation verwendet erweiterte datenwissenschaftliche Techniken, um die Angreifertechniken zu erkennen. |
| Ausgezeichnet | 5 | Erkennen Sie schädliche Techniken effektiv in Echtzeit und decken Sie alle Aspekte der Verfahren einer Technik ab. Ihre Organisation hat ein gutes Verständnis Ihrer Umgebung mit der richtigen Automatisierung und Qualität der Daten. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Umgehungs- und Verschleierungsmethoden umgehen, ist auf dieser Ebene nicht möglich. Die Anzahl der falsch-negativen Ergebnisse ist niedrig. |

## Ordnen Sie die Technikerkennungsabdeckung einer Technik zu

Ordnen Sie Ihre allgemeine Technikerkennungsabdeckung der Technik zu, mit der Ihr Unternehmen bestimmte Angreifertechniken erkennen kann.

### Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Technikerkennungsabdeckung verwenden, um einen Überblick über die allgemeine Technikerkennungsabdeckung Ihrer Organisation zu erhalten. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, sehen Sie die Art der Abdeckung, die Sie benötigen, um die Techniken des Angreifers zu erkennen.

Die Technik und die ID werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt. Der Abdeckungstyp und die Bewertungsdefinition, die Sie definiert haben, sind für als Option verfügbar, die Sie in der gesamten Technikerkennungsabdeckung auswählen können.

Sie können die gesamte Technikerkennungsabdeckung mit der Technik zuordnen, um die Zuordnung abzuschließen. Sie können eine Technik nur einer allgemeinen Technikerkennungsabdeckung zuordnen.

Die von Ihnen definierte Zuordnung der Technikerkennungsabdeckung wird in der Abdeckungsvisualisierung in der Heatmapverwendet.



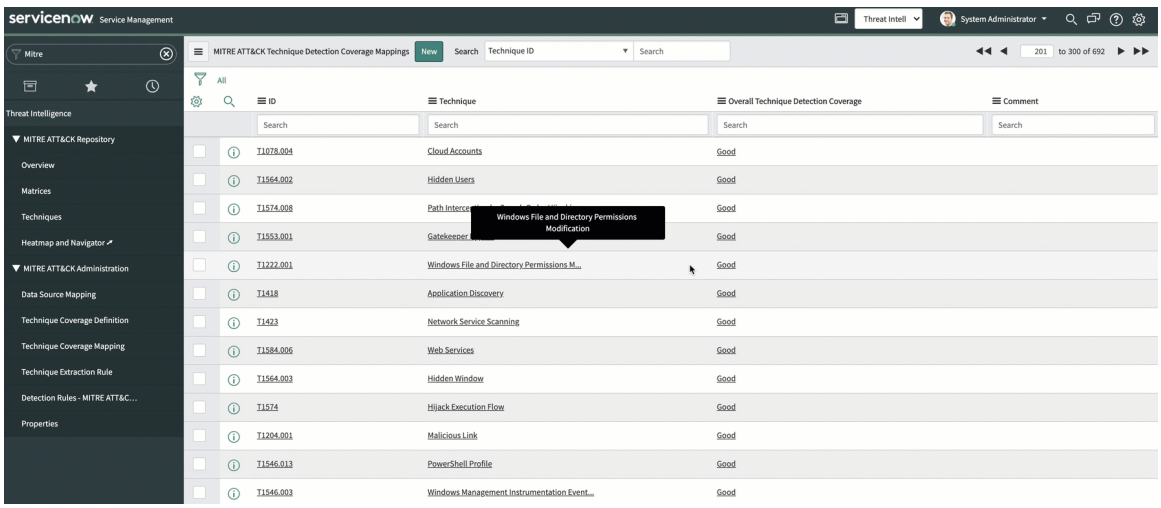
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Sie können die Gesamtabdeckung der Technikerkennung mithilfe Ihrer organisationsspezifischen Berechnungen ermitteln. Sie können ein beliebiges BAS-Produkt (Breach & Attack Simulation), das Cyber Analytics Repository (CAR) oder andere Methoden nach Bedarf verwenden, um die Bewertungsdefinition zu definieren, und sie in diesem Verfahren für die allgemeine Zuordnung der Technikerkennungsabdeckung verwenden.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Erkennung**.

   In dieser Abbildung sehen Sie, dass die Untertechnik „Cloud-Konten“ (T1078.004) eine hervorragende Abdeckung in der Organisation aufweist und dass die Gesamtabdeckung der Technik-Erkennung „ **Ausgezeichnet**“ zugeordnet ist.




2. Überprüfen Sie jede Technik, und ordnen Sie Ihre allgemeine Technik-Erkennungsabdeckung basierend auf Ihrer Definition der Erkennungsabdeckung und der Verfügbarkeit der Abdeckung Ihrer Organisation zu.

## Definieren Sie die Risikominderungsabdeckung

Definieren Sie die Risikominderungsabdeckung für jede Risikominderung, die einer Technik zugeordnet ist, damit Sie nachvollziehen können, wie gut Ihre Organisation die Angriffe aufgrund einer bestimmten Technik verhindern kann.

### Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- Erforderliche Rolle: sn_ti.read: Lesezugriff

### Warum und wann dieser Vorgang ausgeführt wird

Die Definitionen der Abdeckung durch Risikominderung werden in der allgemeinen Zuordnung der Abdeckung durch Risikominderung und Technik verwendet. Sie können die Risikominderungsabdeckung des Basissystems verwenden. Die Basissystem-Abdeckung zur Risikominderung besteht aus den Abdeckungstypen Keine, Schlecht, Mittel, Gut, Sehr gut und Ausgezeichnet. Die Basissystem-Mitigationsabdeckung ist auch vordefinierten Farben und Abdeckungsprozentsätzen zugeordnet. Sie können die Abdeckungstypen (Abdeckungstypen hinzufügen oder entfernen), die Abdeckungsprozentsätze für Unter- und Obergrenzen und Farben anpassen oder eine benutzerdefinierte Risikominderungsabdeckung erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Risikominderungsabdeckung und auch in der Heatmapverwendet.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Abdeckung durch Risikominderung**.
2. Überprüfen Sie die Einträge der Risikominderungserkennung, und passen Sie die Einträge für Ihre Umgebung an.

**Technik – Definition der Abdeckung durch Risikominderung**

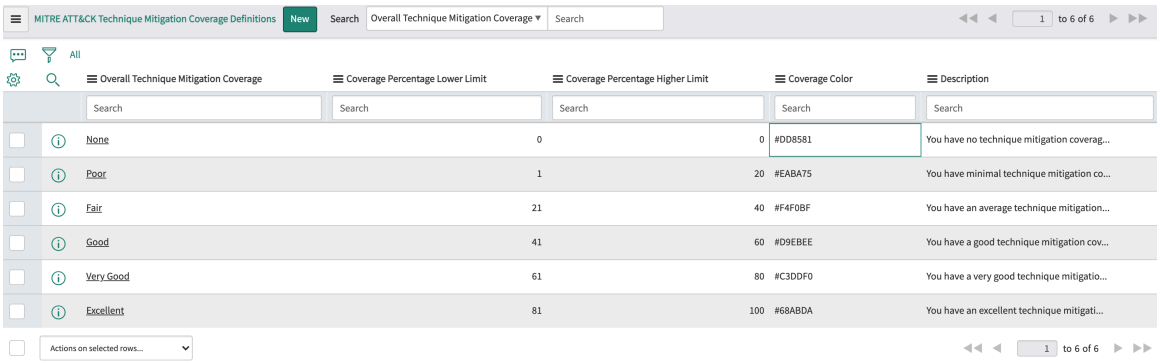
| Feld | Beschreibung |
|---|---|
| Gesamtabdeckung der Technikverringerung | Name der Technikminderungsabdeckung. Die Basissystem-Abdeckung zur Risikominderung besteht aus Keine, Schlechte, Mittel, Gut, Sehr Gut oder Ausgezeichnet. |
| Untergrenze des Abdeckungsprozentsatzes | Die untere prozentuale Grenze der Risikominderungsabdeckung. Definieren Sie die numerischen Werte zwischen 0 und 100. |
| Obergrenze des Abdeckungsprozentsatzes | Die höhere prozentuale Grenze der Risikominderungsabdeckung. Definieren Sie die numerischen Werte zwischen 0 und 100. |
| Abdeckungsfarbe | Farbe, die der Punktzahl der Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Technikminderungsabdeckung in der Heatmap verwendet.<br><br>Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen. |
| Beschreibung | Gesamtabdeckung der Erkennung von Risikominderungen. Weitere Informationen finden Sie in der Definition des Basissystems in der Definition der Technikminderungsabdeckung. |

**Hinweis:**
Stellen Sie sicher, dass Sie die Prozentbereiche der Abdeckung nicht überlappen, wenn Sie die Prozentgrenzen anpassen (niedriger oder höher). Beispiel: Wenn ein Abdeckungsdatensatz die Bereiche 0 bis 20 aufweist, muss der nächste aufeinander folgende Datensatz einen unteren Grenzwertbereich von 21 oder höher haben, um eine Überschneidung des Abdeckungsprozentsatzbereichs zu vermeiden.

Die folgende Abbildung zeigt die Definitionsliste der Abdeckung durch Risikominderung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, schließen Sie die Einträge ab, und klicken Sie auf **Absenden**.

## Definitionen der Technikverringerungsabdeckung

Definieren Sie die Risikominderungsabdeckung Ihrer Organisation, damit Sie bestimmte Angreifertechniken effektiv messen und erkennen können.

### Definitionen der MITRE ATT&CK-Technikverringerungsabdeckung

| Gesamtabdeckung der Technikverringerun | Untergrenze des Abdeckungsprozent | Obergrenze des Abdeckungsprozent | Abdeckungsfarbe | Beschreibung |
|---|---|---|---|---|
| Keine | 0 | 0 | #DD8581 | Sie haben keine Abdeckung durch Technikverringerung, und Ihre Verteidigungskontrollen können einen Angriff in keinem Szenario verhindern. |
| Mangelhaft | 1 | 20 | #EABA75 | Sie haben eine minimale Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist sehr hoch, und Ihre Verteidigungskontrollen können einen Angriff in 0 bis 20 Prozent der Szenarien verhindern. |
| Befriedigend | 21 | 40 | #F4F0BF | Sie haben eine durchschnittliche Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definitionen der MITRE ATT&CK-Technikverringerungsabdeckung (Fortsetzung)

| Gesamtabdeckung der Technikverringerung | Untergrenze des Abdeckungsprozent | Obergrenze des Abdeckungsprozent | Abdeckungsfarbe | Beschreibung |
|---|---|---|---|---|
| | | | | hoch, und Ihre Verteidigungskontrollen können einen Angriff in 21 bis 40 Prozent der Szenarien verhindern. |
| Gut | 41 | 60 | #D9EBEE | Sie verfügen über eine gute Technikminderungsabdeckung. Die Chancen eines Angriffs sind jedoch relativ hoch, und Ihre Verteidigungskontrollen können einen Angriff in 41 bis 60 Prozent der Szenarien verhindern. |
| Sehr gut | 61 | 80 | #C3DDF0 | Sie haben eine sehr gute Abdeckung durch Technikminderung. Die Wahrscheinlichkeit eines Angriffs ist gering, und Ihre Verteidigungskontrollen können einen Angriff in 61 bis 80 Prozent der Szenarien verhindern. |
| Ausgezeichnet | 81 | 100 | #68ABDA | Sie verfügen über eine hervorragende Abdeckung durch Technikminderung, und die Wahrscheinlichkeit eines Angriffs mit dieser Technik ist sehr gering, und Ihre Abwehrmaßnahmen können einen Angriff in 81 bis 100 Prozent |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Definitionen der MITRE ATT&CK-Technikverringerungsabdeckung (Fortsetzung)**

| Gesamtabdeckung der Technikverringerun | Untergrenze des Abdeckungsprozent | Obergrenze des Abdeckungsprozent | Abdeckungsfarbe | Beschreibung |
|---|---|---|---|---|
| | | | | der Szenarien verhindern. |

### Ordnen Sie Ihre Risikominderungsabdeckung einer Technik zu

Ordnen Sie Ihre Risikominderungsabdeckung der Technik zu, mit der Sie die allgemeine Risikominderungsstrategie Ihrer Organisation erkennen können.

### Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreib-, Löschzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

### Warum und wann dieser Vorgang ausgeführt wird

Mit Verringerungen können Sie verhindern, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. Jede MITRE-ATT&CK -Technik enthält Gegenmaßnahmen, die Sie in Ihrer Organisation bereitstellen können, um die Wahrscheinlichkeit eines Angriffs zu verringern. Sie können die Risikominderungsabdeckung verwenden, um sich einen Überblick über die allgemeine Risikominderungsstrategie Ihrer Organisation zu verschaffen. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, sehen Sie die Art der Abdeckung, die Sie haben, um die Techniken des Angreifers abzuschwächen.

Die Technik und die Risikominderungsinformationen werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt. Die von Ihnen definierte Definition der Risikominderungsabdeckung steht Ihnen in der Technik der Risikominderungsabdeckung zur Verfügung.

Sie können Risikominderungen identifizieren, die für Ihre Organisation relevant sind. Wenn eine Risikominderung relevant ist, können Sie definieren, ob die Risikominderungsstrategien bereitgestellt wurden. Sie können angeben, ob die Strategien als Teil der SOC-Richtlinie Ihrer Organisation angewendet werden. Sie können auch feststellen, ob Ihre Organisation über vorbeugende Tools verfügt, um die Techniken eines Angreifers abzuschwächen, und Sie können alle Sicherheitskontrollen zuordnen, die Ihre Organisation bereitgestellt hat, um Sicherheitsrisiken zu minimieren. Füllen Sie die Verringerungsabdeckung (Prozentsatz) für jeden der Datensätze aus.

Nach der Zuordnung der Informationen für jede der Techniken füllt der Rechner für die Mitigationsabdeckung automatisch die berechnete Technik-Mitigationsabdeckung aus. Um die Gesamtabdeckung der Risikominderung für eine Technik zu berechnen, müssen die Zuordnungsdatensätze der Technikminderung aktiv und für die Organisation relevant sein. Die Datensätze, die inaktiv und nicht relevant sind, werden bei der Berechnung der Gesamtabdeckung der Technikminderung nicht berücksichtigt. Basierend auf den Werten im Feld Berechnete Technikminderungsabdeckung und der Definitionder Risikominderungsabdeckung wird Ihre Gesamttechnik-Mitigationsabdeckung (Berechnet) ausgefüllt.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Risikominderungsabdeckung und auch in der Heatmapverwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Risikominderung**.
2. Überprüfen Sie jede Technik für die Risikominderungszuordnung, und aktualisieren Sie die **Risikominderungsabdeckung (Prozentsatz)**, um die Verfügbarkeit der Abdeckung für Ihr Unternehmen zu berechnen.

### Zuordnungen der Technikverringerungsabdeckung

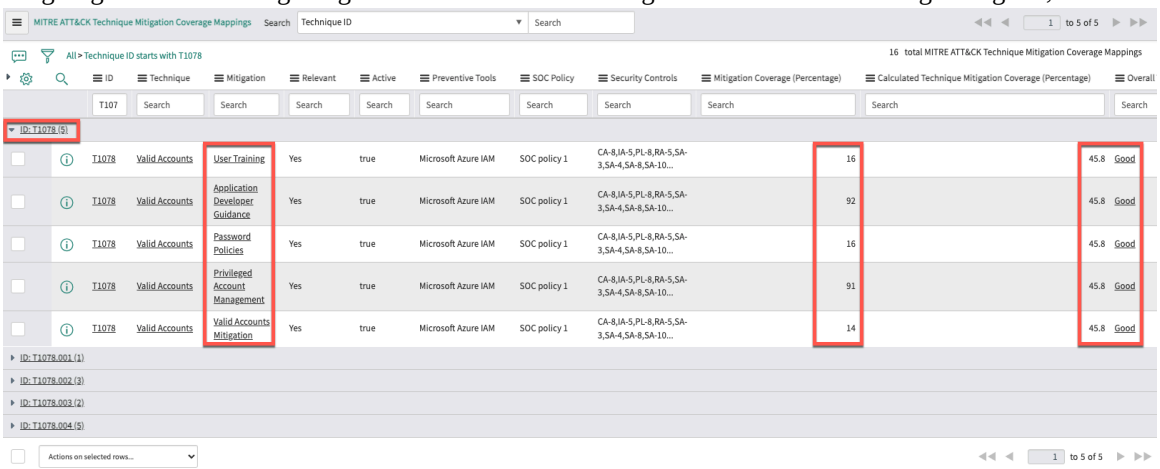
| Feld | Beschreibung |
|---|---|
| ID | Eindeutige Identität der Technik. Die IDs werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt. |
| Technik | Wie ein Angreifer ein taktisches Ziel erreicht, indem er eine Aktion ausführt. Die Technikinformationen werden automatisch für alle Sammlungen und Techniken ausgefüllt, die Sie aktiviert haben. |
| Mitigation | Mitigations, mit denen Sie verhindern können, dass ein Angreifer erfolgreich Techniken oder Untertechniken gegen Ihre Organisation ausführt. Die Risikominderungsinformationen werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt. |
| Relevant | Option, um anzugeben, ob die Verringerung für Ihre Organisation relevant ist. |
| Aktiv | Option, um anzugeben, ob die Risikominderungsstrategien in Ihrer Organisation bereitgestellt werden. Dies ist eine erforderliche Option, die zur Berechnung der Technikminderungsabdeckung erforderlich ist. |
| Präventive Tools | Option, um anzugeben, ob Ihre Organisation über präventive Tools verfügt, um die Techniken eines Angreifers abzuschwächen. |
| SOC-Richtlinie | Die SOC-Richtlinien, die die Risikominderungsstrategien in Ihrer Organisation definieren. |
| Sicherheitskontrollen | Die Sicherheitskontrollen Ihrer Organisation enthalten die Risikominderungsstrategien zur Minimierung von Sicherheitsrisiken. |
| Verringerungsabdeckung (Prozentsatz) | Ein Bewertungssystem zur Berechnung der Technikverringerungsabdeckung. Definieren Sie numerische Werte zwischen 0 und 100. Dies ist eine erforderliche Option, die zur Berechnung der Technikminderungsabdeckung erforderlich ist. |
| Berechnete Technik-Minderungsabdeckung (Prozentsatz) | Die berechnete Technikverringerungsabdeckung in Prozent. Dieser Wert wird basierend auf der im Mitigationsabdeckungsrechnerdefinierten Formel bestimmt. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Gesamtabdeckung der Technikminderung (Berechnet) | Die Gesamtabdeckung der Technikverringerung. Dieser Wert wird basierend auf der für Ihre Organisation definierten Risikominderungsabdeckung bestimmt. |
| Anmerkung | Beschreibung der Technik und der Zuordnung der Risikominderungsabdeckung. |
| Widerrufen | Die Technik zur Zuordnung der Abdeckung durch Risikominderung wird widerrufen. |

In dieser Abbildung sehen Sie, dass der Technik Valid Accounts fünf Minderungsmaßnahmen zugeordnet sind, jeweils mit einer Minderungsabdeckung von 16 für Benutzerschulungen, 92 für Anleitungen für Anwendungsentwickler und 16 für Passwortrichtlinien, 91 für die Verwaltung privilegierter Konten und 14 für gültige Konten Verringerung. Die berechnete Abdeckung durch Technikminderung beträgt 45,8 Prozent.




### Rechner für allgemeine Technikverringerungsabdeckung

Die Gesamtabdeckung der Technikverringerung wird basierend auf der Formel bestimmt, die im Rechner für die Verringerungsabdeckung definiert ist.

## Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- Erforderliche Rolle: sn_ti.read: Lesezugriff

## Warum und wann dieser Vorgang ausgeführt wird

- Sie können nur einen Rechner für die Risikominderungsabdeckung pro Domäne aktivieren.
- Der Basissystem-Rechner für die Abdeckung durch Risikominderung ist ein Durchschnittsrechner.
- Alle Anpassungen am Rechnerskript sollten sicherstellen, dass die endgültige Ausgabe ein numerischer Wert zwischen 0 und 100 ist.
- Die Definition der Abdeckung durch Risikominderung wird basierend auf dem Bereich der endgültigen Ausgabe angewendet.

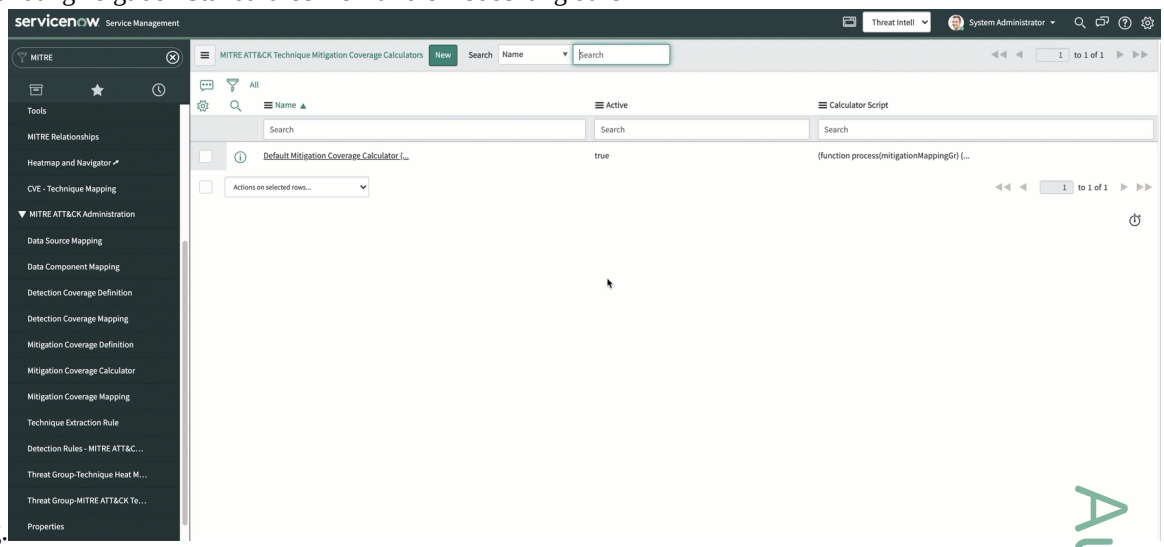
## Prozedur

Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Rechner für Abdeckung durch Risikominderung**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt den Standardrechner für die Abdeckung durch




Risikominderung.

### Erstellen und ordnen Sie Erkennungsregeln zu

Erstellen Sie Erkennungsregeln, und ordnen Sie sie den Taktiken und Techniken zu. Mit dieser Zuordnung können Sie die Abdeckung für die Erkennungsregeln in Ihrer Organisation anzeigen.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

## Warum und wann dieser Vorgang ausgeführt wird

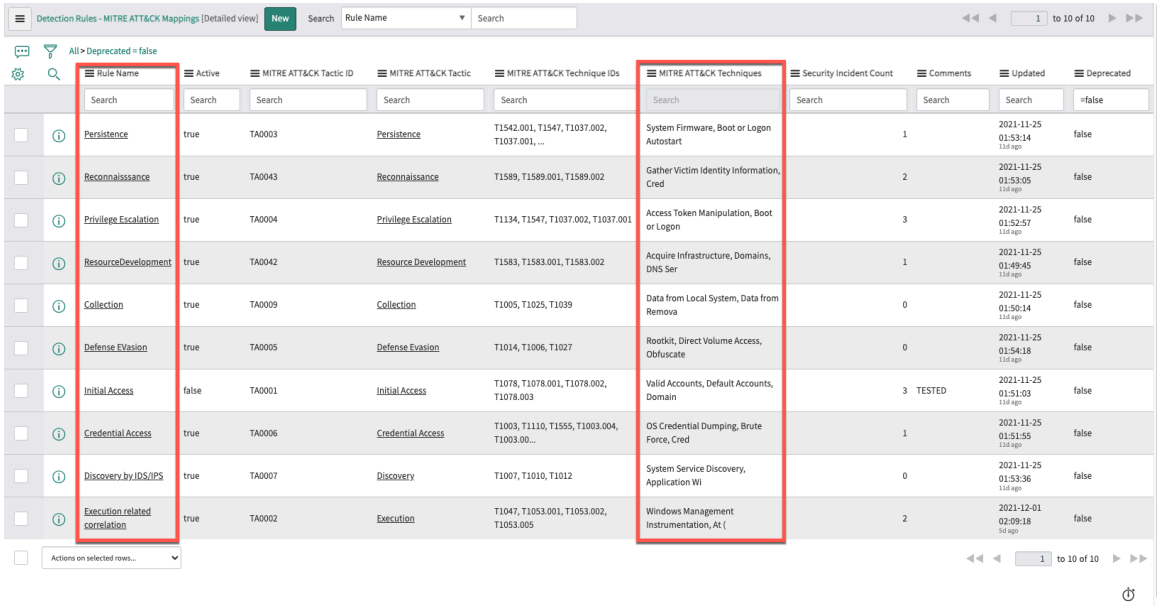
Mit der Erkennungsregelzuordnung kann Ihre Organisation sehen, welche Erkennungsregeln zur Identifizierung bestimmter Techniken verfügbar sind.

Der Hauptzweck der Zuordnung besteht darin, für Transparenz zu sorgen, ob Ihre Organisation über die erforderlichen Erkennungsregeln verfügt, um zu erkennen, wann eine Warnung oder ein Event als Ergebnis eines Angriffs eines Angreifers mit einer bestimmten Technik ausgelöst wird.

Sehen Sie sich beispielsweise die folgende Abbildung an, die eine Liste der Erkennungsregeln zeigt, die verschiedenen Techniken zugeordnet sind. Sie können diese Informationen auch in anzeigen der/die/das MITRE-ATT&CK -Navigator.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Wenn Sie nicht die Basissystem-SIEM-Regeln für die automatische Extraktion verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Event-Regel, die den Security Incident auslöst, im Namensfeld der Warnungsregel ausfüllen. Sie können das Feld „Warnungsregelname“ auch mithilfe der SIEM -Integration, E-Mail-Analyse, manueller Erstellung usw. ausfüllen. Weitere Informationen finden Sie unter Rollup MITRE-ATT&CK Informationen aus Erkennungsregeln.

### Hinweis:

Die Funktion „Erkennungsregeln“ wurde aktualisiert und umfasst nun die Zuordnung einer einzelnen Taktik zu mehreren Techniken. Zuvor konnten Sie eine einzelne Taktik einer einzelnen Technik zuordnen. Wenn Sie das Plugin Threat Intelligence von Version 12.0.4 auf eine höhere Version aktualisieren, überprüfen Sie die folgenden Punkte, bevor Sie die Erkennungsregeln im Modul MITRE-ATT&CK verwenden.

- Sie finden mehrere Datensätze in einem einzigen Datensatz zusammengeführt, wenn die Felder „Regelname“, „Warnungssensor“, „Quelle“, „Kategorie“, „Unterkategorie“ und MITRE-ATT&CK „[]“ gleich sind.
- Die alten Datensätze werden in der veralteten Spalte als „true“ und in der aktiven Spalte als „false“ markiert.
- Die neuen zusammengeführten Datensätze können verwendet werden und sind in der veralteten Spalte als „false“ und in der aktiven Spalte als „true“ markiert.
- Nachdem Sie das Upgrade überprüft haben und feststellen, dass alle Ihre Erkennungsregeln erfolgreich migriert wurden, können Sie die alten Datensätze löschen, die in der Spalte „Veraltet“ als „true“ markiert sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Erkennungsregeln – MITRE ATT&CK-Zuordnungen**.
2. Verwenden Sie eine der folgenden Methoden, um eine Erkennungsregel zu erstellen:
   Methode 1: Erkennungsregeln manuell erstellen

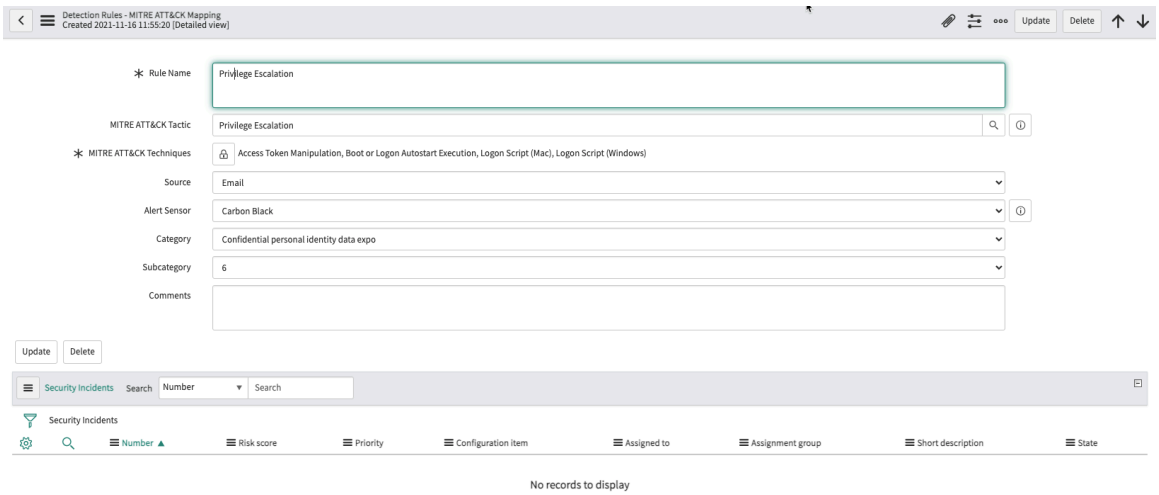


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie auf **Neu**, und füllen Sie im Formular die Felder aus.

**Erkennungsregeln – MITRE-ATT&CK Zuordnung**

| Feld | Beschreibung |
|---|---|
| Regelname | Name der Erkennungsregel |
| MITRE-ATT&CK Taktik | Relevante MITRE-ATT&CK Taktik. |
| MITRE-ATT&CK Techniken | Relevante MITRE-ATT&CK Technik. Sie können mehrere Techniken für eine einzelne Taktik auswählen. |
| Quelle | Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw. |
| Warnungssensor | Sicherheitsintegration, über die Sie die Warnungs- oder Event-Daten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen. |
| Unterkategorie | Unterkategorie, die das Problem weiter definiert. |
| Kategorie | Kategorie, die den Typ des Sicherheitsproblems angibt. |
| MITRE-ATT&CK Technik | Relevante MITRE-ATT&CK Technik. Sie können mehrere Techniken für eine einzelne Taktik auswählen. |
| Anzahl der Security Incidents | Die Anzahl der Security Incidents, an die die Techniken angehängt werden. Diese Anzahl wird angezeigt, wenn Sie das automatische Rollup von MITRE-ATT&CK Informationen aus Warnungsregeln zu Security Incidents aktiviert haben. |
| Überholt | Die Zuordnung der Erkennungsregel ist veraltet. |
| Aktiv | Option, um anzugeben, ob die Erkennungsregel aktiv ist und in Ihrer Umgebung bereitgestellt wird. |




**b.** Klicken Sie auf **Absenden**.

Methode 2: Erkennungsregeln importieren und erstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

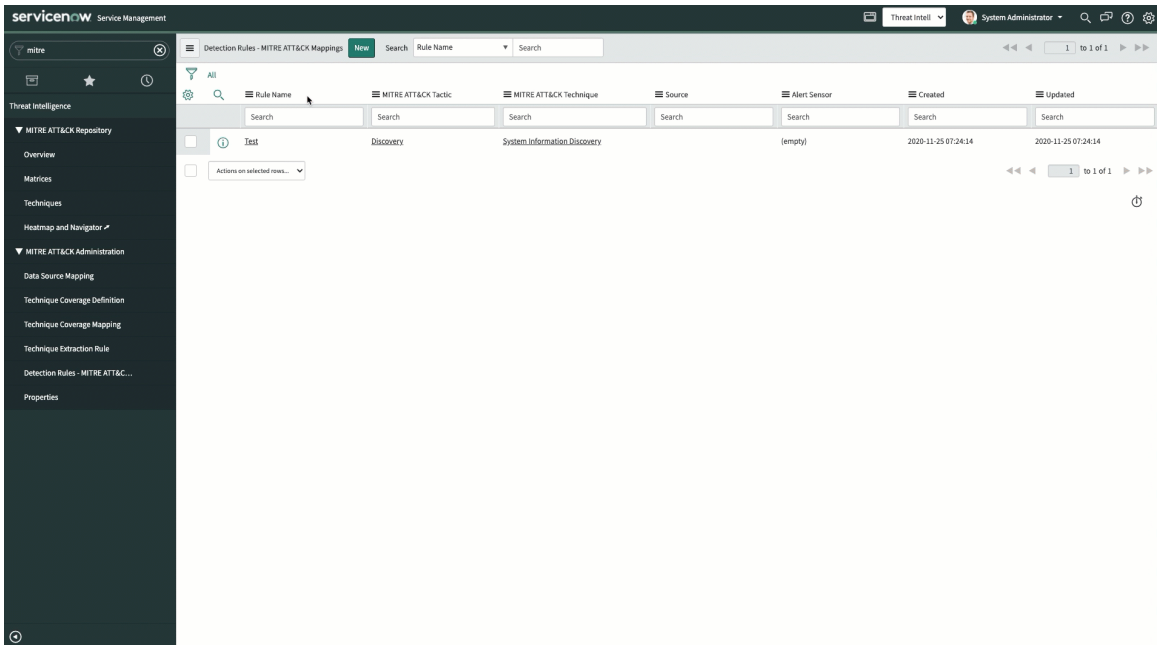
**a.** Klicken Sie mit der rechten Maustaste auf die Spaltenüberschrift Regelname.

**b.** Klicken Sie in der Liste auf **Importieren**.

**c.** Klicken **Sie auf Excel-Vorlage erstellen**.

**d.** Klicken Sie nach Abschluss des Exports auf **Herunterladen**. Eine Excel-Vorlage mit dem Dateinamen sn_ti_alert_rules_mitre_attack_technique_mapping wird auf Ihren Computer heruntergeladen.

In der folgenden Abbildung sehen Sie, wie Sie die Excel-Vorlage exportieren, die Details in die Tabelle eintragen, die Datei hochladen, eine Vorschau der Felder anzeigen und sie wieder in Now Platformimportieren.




**e.** Öffnen Sie die Tabelle, wählen Sie die zweite Blattregisterkarte aus, und überprüfen Sie Ihre Eingabe. Füllen Sie die Felder des Formulars aus, und speichern Sie die Datei.

### Importvorlage

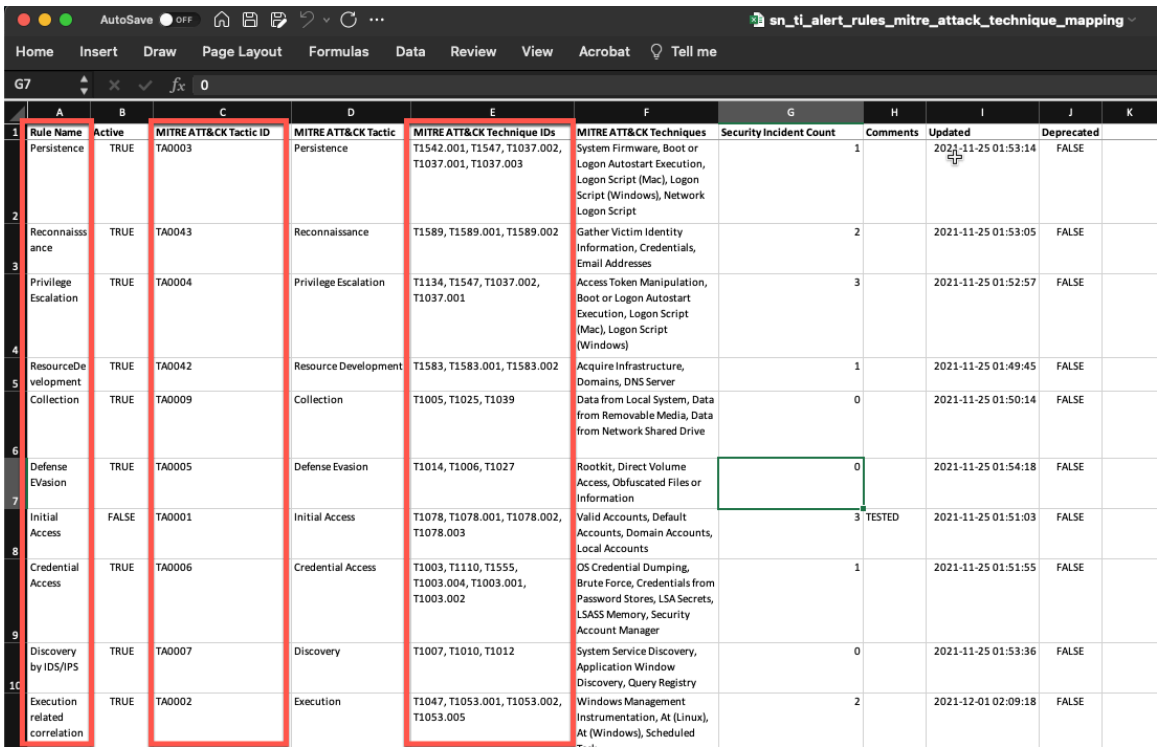
| Feld | Beschreibung |
|---|---|
| Regelname | Name der Erkennungsregel |
| Aktiv | Option, um anzugeben, ob die Erkennungsregel aktiv ist und in Ihrer Umgebung bereitgestellt wird. |
| Warnungssensor | Sicherheitsintegration, über die Sie die Warnungs- oder Event-Daten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen. |
| Kategorie | Kategorie, die den Typ des Sicherheitsproblems angibt. |
| Kommentare | Beschreibung der Erkennungsregel. |
| Überholt | Die Zuordnung der Erkennungsregel ist veraltet. |
| MITRE-ATT&CK Technik-IDs | MITRE-ATT&CK Technik-ID, z. B. T1546.008, für Eingabehilfefunktionen. |
| MITRE-ATT&CK Taktik-ID | MITRE-ATT&CK Taktik-ID, z. B. TA0003, für Persistenz. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Anzahl der Security Incidents | Die Anzahl der Security Incidents, an die die Techniken angehängt werden. Diese Anzahl wird angezeigt, wenn Sie das automatische Rollup von MITRE-ATT&CK Informationen aus Warnungsregeln zu Security Incidents aktiviert haben und die Erkennungsregel aktiv ist. |
| Quelle | Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw. |
| Unterkategorie | Unterkategorie, die das Problem weiter definiert. |
| MITRE-ATT&CK Taktik | Relevante MITRE-ATT&CK Taktik. |
| MITRE-ATT&CK Technik | Relevante MITRE-ATT&CK Technik. |

Die folgende Abbildung zeigt die Tabellenkalkulationsvorlage. Die erforderlichen Felder sind rot hervorgehoben: Regelname, MITRE-ATT&CK Taktik-ID und MITRE-ATT&CK Technik-ID.



| Rule Name | Active | MITRE ATT&CK Tactic ID | MITRE ATT&CK Tactic | MITRE ATT&CK Technique IDs | MITRE ATT&CK Techniques | Security Incident Count | Comments | Updated | Deprecated |
|---|---|---|---|---|---|---|---|---|---|
| Persistence | TRUE | TA0003 | Persistence | T1542.001, T1547, T1037.002, T1037.001, T1037.003 | System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script | 1 | | 2021-11-25 01:53:14 | FALSE |
| Reconnaissance | TRUE | TA0043 | Reconnaissance | T1589, T1589.001, T1589.002 | Gather Victim Identity Information, Credentials, Email Addresses | 2 | | 2021-11-25 01:53:05 | FALSE |
| Privilege Escalation | TRUE | TA0004 | Privilege Escalation | T1134, T1547, T1037.002, T1037.001 | Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows) | 3 | | 2021-11-25 01:52:57 | FALSE |
| ResourceDevelopment | TRUE | TA0042 | Resource Development | T1583, T1583.001, T1583.002 | Acquire Infrastructure, Domains, DNS Server | 1 | | 2021-11-25 01:49:45 | FALSE |
| Collection | TRUE | TA0009 | Collection | T1005, T1025, T1039 | Data from Local System, Data from Removable Media, Data from Network Shared Drive | 0 | | 2021-11-25 01:50:14 | FALSE |
| Defense EVasion | TRUE | TA0005 | Defense Evasion | T1014, T1006, T1027 | Rootkit, Direct Volume Access, Obfuscated Files or Information | 0 | | 2021-11-25 01:54:18 | FALSE |
| Initial Access | FALSE | TA0001 | Initial Access | T1078, T1078.001, T1078.002, T1078.003 | Valid Accounts, Default Accounts, Domain Accounts, Local Accounts | 3 | TESTED | 2021-11-25 01:51:03 | FALSE |
| Credential Access | TRUE | TA0006 | Credential Access | T1003, T1110, T1555, T1003.004, T1003.001, T1003.002 | OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager | 1 | | 2021-11-25 01:51:55 | FALSE |
| Discovery by IDS/IPS | TRUE | TA0007 | Discovery | T1007, T1010, T1012 | System Service Discovery, Application Window Discovery, Query Registry | 0 | | 2021-11-25 01:53:36 | FALSE |
| Execution related correlation | TRUE | TA0002 | Execution | T1047, T1053.001, T1053.002, T1053.005 | Windows Management Instrumentation, At (Linux), At (Windows), Scheduled | 2 | | 2021-12-01 02:09:18 | FALSE |

**f.** Klicken Sie auf **Datei** auswählen, und wählen Sie die Tabelle auf Ihrem Computer aus.

**g.** Klicken Sie auf **Hochladen**.

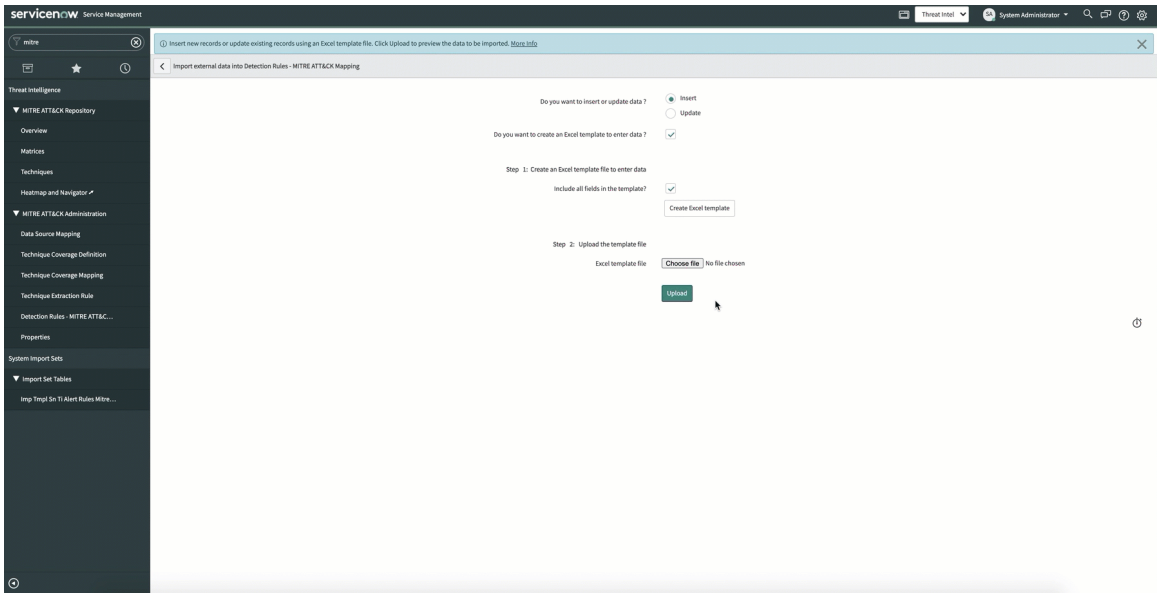
**h.** Klicken Sie **auf Vorschau für importierte Daten**.

**i.** Zeigen Sie eine Vorschau der Zuordnungen an, und klicken Sie auf **Import**abschließen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie die Tabelle hochladen, eine Vorschau der Daten anzeigen, Fehler überprüfen und den Importvorgang der Erkennungsregelzuordnung abschließen.




### Automatische Extrahierungsregeln für den Import von MITRE-ATT&CK Informationen

Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um die Informationen MITRE-ATT&CK aus vorhandenen Drittanbieterintegrationen zu importieren.

### Verwenden Sie automatische Extraktionsregeln für die Bedrohungssuche

Verwenden Sie die automatischen Extraktionsregeln für die Bedrohungssuche, um die MITRE-ATT&CK -Informationen aus vorhandenen Threat Intelligence Drittanbieterintegrationen zu importieren.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

## Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Threat Intelligence -Integration, z. B. Sandbox oder ein TIP, das MITRE-ATT&CK -Framework unterstützt und die MITRE-ATT&CK -Informationen auf jeder Integrationsebene analysiert werden, werden die Informationen in jedem Ergebnisdatensatz der Bedrohungssuche angezeigt. Allerdings analysieren nicht alle Threat Intelligence -Integrationen die MITRE-ATT&CK -Informationen. Die globale automatische Extraktionsregel für die Bedrohungssuche kann MITRE-ATT&CK Informationen aus allen Threat Intelligence Integrationen extrahieren.

Sie können festlegen, dass für die Informationen MITRE-ATT&CK automatisch ein Rollup aus den Ergebnissen der Bedrohungssuche zu einem Security Incident durchgeführt wird. Aktivieren Sie für ein automatisches Rollup der Ergebnisse der Bedrohungssuche in Security Incidents die Systemeigenschaft. Alternativ können Sie die Informationen für jede einzelne Bedrohungssuche manuell zusammenfassen.

Das Basissystem Threat Intelligence extrahiert automatisch die MITRE-ATT&CK -Informationen aus der Rohnutzlast der Drittparteiintegrationen in den Ergebnisdatensatz der



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungssuche, wenn die Threat Intelligence -Integration MITRE-ATT&CK -Informationen wie die Technik oder Taktik bereitstellt.

Wenn die Informationen MITRE-ATT&CK im Feld „Rohnutzlast“ des Bedrohungssuchdatensatzes nicht verfügbar sind, müssen Sie eine eigene Regel für die automatische Extraktion aus der Drittanbieterintegration definieren.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Technikextraktionsregel“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel für automatische Extraktion. |
| Regeltyp | Regeltyp der automatischen Extraktion. Wählen Sie **Bedrohungssuche aus**. |
| Automatische Extraktion ignorieren | Einstellung, dass standardmäßig deaktiviert ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK -Techniken. |
| Quell-Engine | Quell-Engine |
| Global | Quell-Engine-Einstellung. Wenn Sie die Quell-Engine auf **Global**festlegen, wird die Extraktion für alle Ergebnisse der Integration der Bedrohungssuche ausgeführt. |
| Beschreibung | Beschreibung der Regel für automatische Extraktion. |
| Prozessmethode | Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen. |
| Extraktion des regulären Ausdrucks | Option, die Sie für das **Zielfeld** angeben, wenn Sie die Extraktionsmethode für reguläre Ausdrücke verwenden. Regulärer Ausdruck ist die Standardeinstellung. |
| Skriptextraktion | Prozess, den Sie beim Ausführen eines Skripts auswählen. Das Skript überprüft Folgendes:<br>○ ThreatLookupResultSysId:sys_id des Ergebnisdatensatzes der Bedrohungssuche<br>○ sourceName: Name der Bedrohungssuchquelle. |
| Taktische Extraktion | Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte taktik- und technikbezogene Informationen enthält, können Sie |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | die Informationen extrahieren und an den Security Incident anhängen. |

4. Klicken Sie auf **Absenden**.

### Verwenden Sie SIEM-Regeln für automatische Extraktion

Verwenden Sie die SIEM-Regeln für die automatische Extraktion, um die MITRE-ATT&CK -Informationen aus vorhandenen Security Operations SIEM-Drittpartei-Integrationen zu importieren.

## Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

## Warum und wann dieser Vorgang ausgeführt wird

Die Technikextraktionsregel ist für alle Basissystem- Security Operations SIEM-Integrationen verfügbar, z. B. Splunk-, IBM QRadar- und ArcSight-Integrationen. Wenn Now Platform Warnungs- oder Event-Daten aus diesen SIEM-Integrationen erfasst und diese MITRE-ATT&CK Informationen enthalten, verarbeitet Now Platform die Rohnutzlast und extrahiert die Informationen MITRE-ATT&CK automatisch.

Wenn Ihr Now Platform Basissystem-SIEM-Integrationen enthält, bedeutet dies, dass die Technikextraktionsregeln bereits im Modul MITRE-ATT&CK erstellt wurden. Sie sollten die Regeln überprüfen und nach Bedarf ändern.

Aktivieren Sie entweder die SIEM-Regel für die automatische Extraktion oder die Warnungsregel.

## Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Technikextraktionsregel“.**

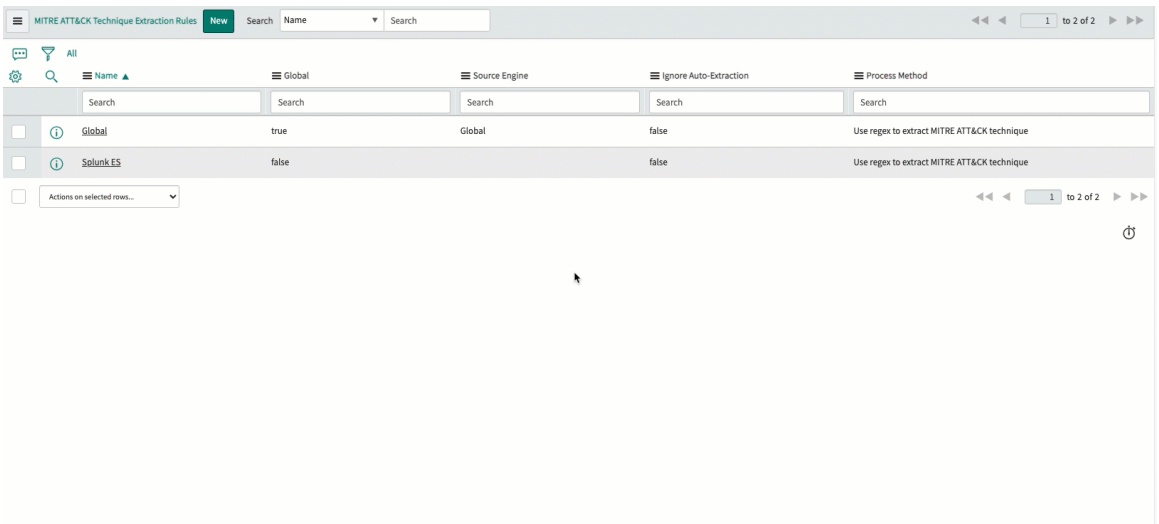
| Feld | Beschreibung |
|---|---|
| Name | Name der Regel für automatische Extraktion. |
| Regeltyp | Regeltyp der automatischen Extraktion. Wählen **Sie SIEM aus**. |
| Automatische Extraktion ignorieren | Einstellung, die standardmäßig deaktiviert ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK -Techniken. |
| Tabelle importieren | Importtabelle, die automatisch für SIEM-Basissystemintegrationen zugeordnet wird. Überprüfen Sie dieses Feld für andere SIEM-Integrationen auf die Informationen MITRE-ATT&CK, und ordnen Sie sie entsprechend zu. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Importfeld | Importfeld, das für Basissystem-SIEM-Integrationen automatisch zugeordnet wird. Überprüfen Sie dieses Feld für andere SIEM-Integrationen auf die Informationen MITRE-ATT&CK, und ordnen Sie sie entsprechend zu. |
| Beschreibung | Regel für automatische Extraktion. |
| Prozessmethode | Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen. |
| Extraktion des regulären Ausdrucks | Option, die Sie für das **Zielfeld** angeben, wenn Sie die Methode des regulären Ausdrucks verwenden. Die Extraktion regulärer Ausdrücke ist die Standardverarbeitungsmethode. |
| Skriptextraktion | Skriptverarbeitungsmethode, die Sie verwenden, wenn Sie anpassen möchten, wie die MITRE-ATT&CK -Informationen extrahiert werden. |
| Taktische Extraktion | Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte taktik- und technikbezogene Informationen enthält, können Sie die Informationen extrahieren und an den Security Incident anhängen. |

In der folgenden Abbildung sehen Sie ein Beispiel für die Extraktionsregel der SIEM-Technik Splunk Enterprise in der Formularansicht. Diese Regel ähnelt allen anderen Extraktionsregeln für SIEM-Techniken.




4. Klicken Sie auf **Absenden**.

### Überprüfen Sie die Zuordnung der Bedrohungsgruppe und der MITRE-ATT&CK -Techniken

Überprüfen Sie die Zuordnungsinformationen der Objekt-zu-Objekt-Beziehung für Bedrohungsgruppe und Techniken, die aus den MITRE TAXII -Sammlungen importiert werden. Mit dieser Zuordnung können Sie die Technikgruppe und die entsprechende Technikzuordnung anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

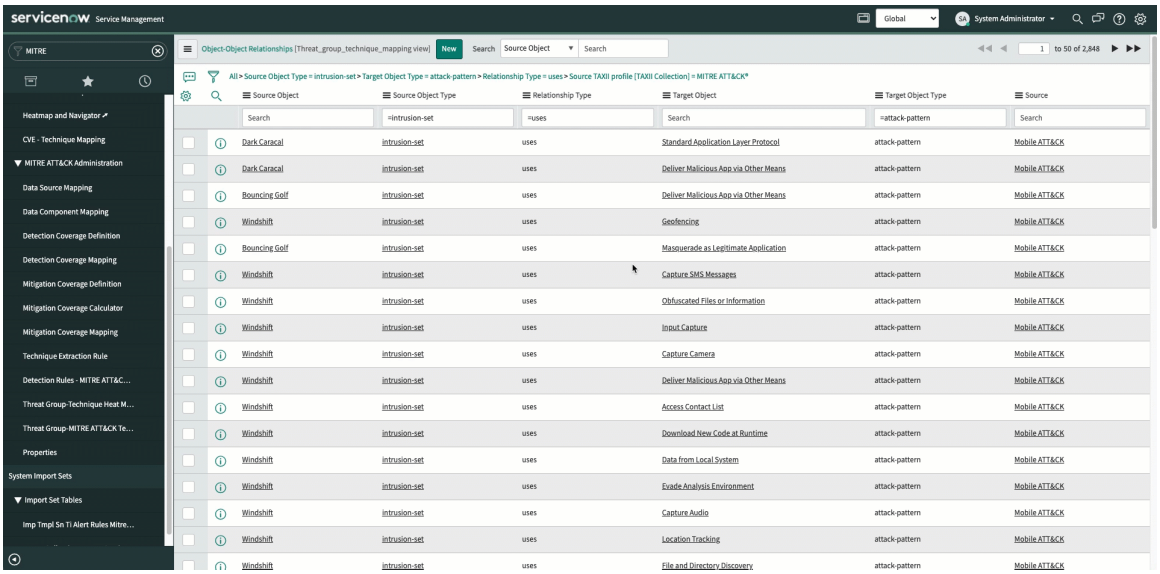
Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Bedrohungsgruppe – MITRE ATT&CK-Techniken**.
2. Klicken Sie mit der rechten Maustaste auf das **Quellobjekt**, und wählen Sie **Nach Quellobjekt** gruppieren aus, um alle einer Bedrohungsgruppe zugeordneten Angriffsmuster anzuzeigen.

   Die folgende Abbildung zeigt die Bedrohungsgruppe admin@338 und die verschiedenen Angriffsmuster, die von dieser Bedrohungsgruppe angenommen werden und Teil der Unternehmensangriffsquelle sind.




## Heatmap-Definition von Bedrohungsgruppe zu Technik

Definieren Sie die Heatmap-Definition der Bedrohungsgruppe für die Technik, damit Sie in der Heatmap die Angriffsmuster messen und erkennen können, mit denen Bedrohungsgruppen Ihre Organisation angreifen. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik steigt, wenn die Anzahl der Angreifer hoch ist.

### Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreibzugriff
- sn_ti.read: Lesezugriff

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Bedrohungsgruppentechnik-Heatmap**.
2. Überprüfen Sie die Heatmap-Definition von Bedrohungsgruppe zu Technik, und passen Sie die Einträge für Ihre Umgebung an.



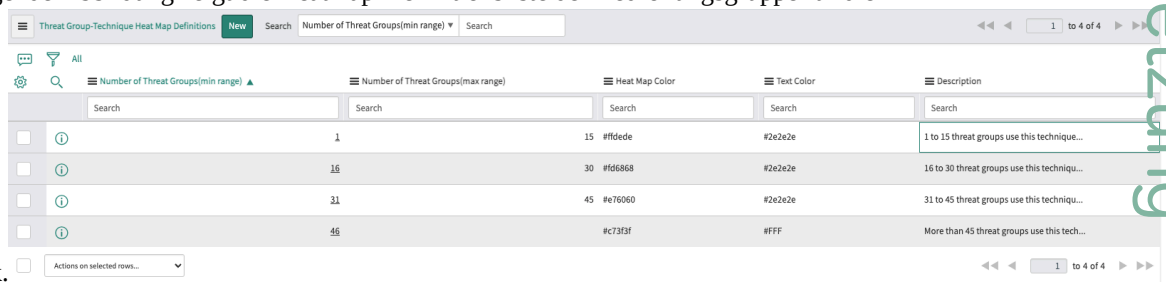
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Definitionen der Bedrohungsgruppentechnik-Heatmap

| Feld | Beschreibung |
|---|---|
| Anzahl der Bedrohungsgruppen (Mindestbereich) | Die Mindestanzahl von Bedrohungsgruppen, die eine bestimmte Technik verwenden. |
| Anzahl der Bedrohungsgruppen (Max.-Bereich) | Die maximale Anzahl von Bedrohungsgruppen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik steigt, wenn die Anzahl der Angreifer hoch ist. |
| Heatmap-Farbe | Farbe, die der Bedrohungsgruppenkategorie zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppenkategorie in der Heatmap hervorzuheben.<br><br>Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen. |
| Textfarbe | Farbe, die dem Bedrohungsgruppentext zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppen in der Heatmap hervorzuheben.<br><br>Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen. |
| Beschreibung | Beschreibung des Bedrohungsgruppenbereichs und der Definition. |

**Hinweis:**
Stellen Sie sicher, dass Sie die Anzahlbereiche der Bedrohungsgruppen nicht überlappen, wenn Sie den Bedrohungsgruppenbereich (Min. oder Max.) anpassen.

Die folgende Abbildung zeigt die Heatmap-Definitionsliste der Bedrohungsgruppe für die Technik.




3. Um einen Eintrag hinzuzufügen, klicken Sie auf **Neu**, schließen Sie die Einträge ab, und klicken Sie auf **Absenden**.

### Überprüfen Sie die Systemeigenschaften MITRE-ATT&CK .

Überprüfen Sie die Werte der Systemeigenschaft MITRE-ATT&CK.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin, sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Eigenschaften**.
2. Füllen Sie die Felder des Formulars aus.

**MITRE-ATT&CK Formular „Eigenschaften“**

| Feld | Beschreibung |
|---|---|
| Führen Sie einen automatischen Rollup der MITRE ATT&CK-Informationen von erkennbaren Elementen zu Security Incidents durch<br><br>[sn_ti.rollup_mitre_att&ck_technique_observable_si] | Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen zum Security Incident. Weitere Informationen finden Sie unter MITRE ATT&CK-Informationen erkennbaren Elementen zuordnen.<br><br>Standardwert: Ja |
| Fasst MITRE ATT&CK-Informationen automatisch aus den Ergebnissen der Bedrohungssuche in Security Incidents zusammen<br><br>[sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si] | Rollup von MITRE-ATT&CK Informationen aus den Ergebnissen der Bedrohungssuche zum Security Incident. Weitere Informationen finden Sie unter Automatische Extraktion der Bedrohungssuche.<br>Standardwert: Ja |
| Führen Sie einen automatischen Rollup von MITRE ATT&CK-Informationen aus Warnungsregeln zu Security Incidents durch<br><br>[sn_ti.rollup_mitre_att&ck_technique_alert_rule_si] | Rollup von MITRE-ATT&CK TTP-Informationen automatisch aus Warnungsregeln zu Security Incidents. Weitere Informationen finden Sie unter Zuordnungserkennungsregeln.<br>Standardwert: Nein |
| Fasst MITRE ATT&CK-Informationen automatisch von untergeordneten Security Incidents zum übergeordneten Security Incident zusammen<br><br>[sn_ti.rollup_mitre_att&ck_technique_child_si_to] | Fasst MITRE-ATT&CK Informationen automatisch von untergeordneten Security Incidents zum übergeordneten Security Incident zusammen.<br><br>Standardwert: Ja |
| Durch Aktivieren dieser Eigenschaft können Security Incident-Felder wie Kategorie und Unterkategorie mit Erkennungsregeln in der Tabelle „Erkennungsregeln – MITRE ATT&CK-Zuordnung“ zugeordnet werden<br><br>[sn_ti.enable_category_mapping_with_alert_rule] | Kategorie und Unterkategorie auf der Zuordnungsseite „Erkennungsregeln – MITRE ATT&CK “.<br><br>Standardwert: Nein |
| Zeit (in Stunden) zur Berechnung von „CVE – VUL-Anzahl“<br><br>[sn_ti.time_to_calculate_cve_vits_count] | Die geplante Zeit in Stunden zur Berechnung der CVE- und VUL-Informationen.<br><br>Standardwert: 24 |

3. Klicken Sie auf **Speichern**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Verwenden von MITRE-ATT&CK zum Erkennen und Analysieren von Bedrohungen

Verwenden Sie das MITRE-ATT&CK -Framework für Threat Intelligence und das SIR -Modul, um Bedrohungen für Ihre Organisation zu erkennen und zu analysieren.

## Verknüpfen MITRE-ATT&CK™ Sie Informationen mit Security Incidents

Ordnen Sie die MITRE-ATT&CK -Taktiken und -Techniken dem Security Incident zu, um die Analyse von Security Incidents und Bedrohungen zu verbessern.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie dem Security Incident die Informationen zu Taktiken und Techniken MITRE-ATT&CK hinzu, damit Sie Ihre Security Incident- und Bedrohungsinformationen für eine bessere Analyse korrelieren können. Beispielsweise kann Ihre Organisation Informationen im Zusammenhang mit Taktiken, Techniken und Verfahren (TTP) von Ihren Drittparteiquellen erhalten, z. B. Threat Intelligence -Berichte oder andere Quellen außerhalb der Security Incident Response. Fügen Sie diese Informationen dann wieder zu SIR hinzu, um die Korrelation und Bedrohungsanalyse zu verbessern.

Sie können die MITRE-ATT&CK -Informationen automatisch aus den Ergebnissen der automatischen Extraktion der Bedrohungssuche, aus erkennbaren Elementen oder aus einem untergeordneten Security Incident zu einem Security Incident zusammenfassen. Aktivieren Sie für ein automatisches Rollup zu Security Incidents die Systemeigenschaft. Alternativ können Sie die Informationen für jede einzelne Bedrohungssuche oder jedes erkennbare Element manuellzusammenfassen.

### Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie auf den zugehörigen Link **MITRE ATT&CK-Technik** zuordnen.
   Der Bereich MITRE ATT&CK-Technik zuordnen wird angezeigt.

   Diese Abbildung zeigt, wie Sie zur zugehörigen Liste navigieren und nach Technik zum Zuordnen MITRE-ATT&CK suchen, die Quelle Enterprise ATT&CK überprüfen, eine Taktik Auswirkung hinzufügen und eine Technik System Herunterfahren/Neustart hinzufügen.

   MITRE-Informationen mit Security Incident verknüpfen MITRE-Informationen mit Security Incident
4. Wählen Sie **Quelle**aus.

   **Hinweis:**
   Nur die Sammlungen und Matrizen, die aktiviert wurden, werden in der Quellliste angezeigt.

   Die Taktiken und Techniken, die der Quelle zugeordnet sind, stehen zur Auswahl. Sie können auch mehrere Quellen zuordnen.
5. Wählen Sie die **Taktik** und die **Techniken aus**.
6. **Wahlweise:** Überprüfen Sie die Informationen basierend auf der Relevanz für den Security Incident, und gehen Sie wie folgt vor:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Zuordnung vollständig zu entfernen, klicken Sie auf das Papierkorbsymbol. Durch Klicken auf dieses Symbol werden die Quelle und die zugehörigen Taktiken und Techniken gelöscht.
- Um eine Taktik zu entfernen, klicken Sie auf das Minuszeichen neben der Taktik.
- Um eine Technik zu entfernen, klicken Sie auf das x-Symbol neben der Technik.

**7.** Klicken Sie auf **Speichern**.

### Ergebnisse

Die Informationen MITRE-ATT&CK sind dem Security Incident zugeordnet. Sie können jetzt die zugehörigen Informationen in der **MITRE ATT&CK-Karte**anzeigen.

#### Ordnen MITRE-ATT&CK Sie Informationen geschlossenen Security Incidents zu

Sie können jetzt MITRE-ATT&CK Taktiken und Techniken den geschlossenen Security Incidents zuordnen, um die Analyse von Security Incidents und Bedrohungen zu verbessern.

MITRE-Informationen mit Security Incident verknüpfen MITRE-Informationen mit Security Incident

#### Karte MITRE-ATT&CK verwenden, um zugehörige Informationen in einem Security Incident anzuzeigen

Sie können die Karte MITRE-ATT&CK verwenden, um die MITRE-ATT&CK zugehörigen Informationen in einem Security Incident anzuzeigen.

Nachdem für die Informationen ein Rollup aus einer Bedrohungssuche, einem erkennbaren Element oder einer SIEM-Integration durchgeführt wurde, werden sie dem Security Incident hinzugefügt. Anschließend werden die zusammengefassten Informationen auf der Karte MITRE-ATT&CK angezeigt. Die **MITRE ATT&CK-Karte** bietet zwei Ansichten:

- Navigatoransicht: Diese Ansicht, die dem MITRE-ATT&CK -Navigator ähnelt, zeigt alle Techniken, die manuell hinzugefügt oder aus den Tabellen für erkennbare Elemente oder Bedrohungssuchen zusammengefasst wurden. **Ursprung der Techniken** anzeigen zeigt die Quelle der Technik an, wenn für sie manuell oder über eine Quelle ein Rollup durchgeführt wurde. **ID** anzeigen zeigt die Technik-ID an.

  Die folgende Abbildung zeigt, wie Sie zur Navigatoransicht der **MITRE ATT&CK-Karte** navigieren. Durch Klicken auf einen der verfügbaren Links werden die Informationen im Modul Threat Intelligence geöffnet.

  MITRE ATT&CK-Karte: Navigatoransicht und

- Listenansicht: In dieser Ansicht werden die Daten in einem Listen- oder Tabellenformat angezeigt. In dieser Ansicht können Sie alle Daten anzeigen, die auf verschiedene Tabellen und Gruppen verteilt sind.

  Die folgende Abbildung zeigt, wie Sie zur Listenansicht der MITRE ATT&CK-Karte navigieren. Durch Klicken auf einen der verfügbaren Links werden die Informationen im Modul Threat Intelligence geöffnet.

#### Ordnen Sie MITRE-ATT&CK Informationen erkennbaren Elementen zu

Ordnen Sie MITRE-ATT&CK Taktiken und Techniken einem erkennbaren Element zu, um die Analyse von Security Incidents und Bedrohungen auf granularer Ebene zu verbessern.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

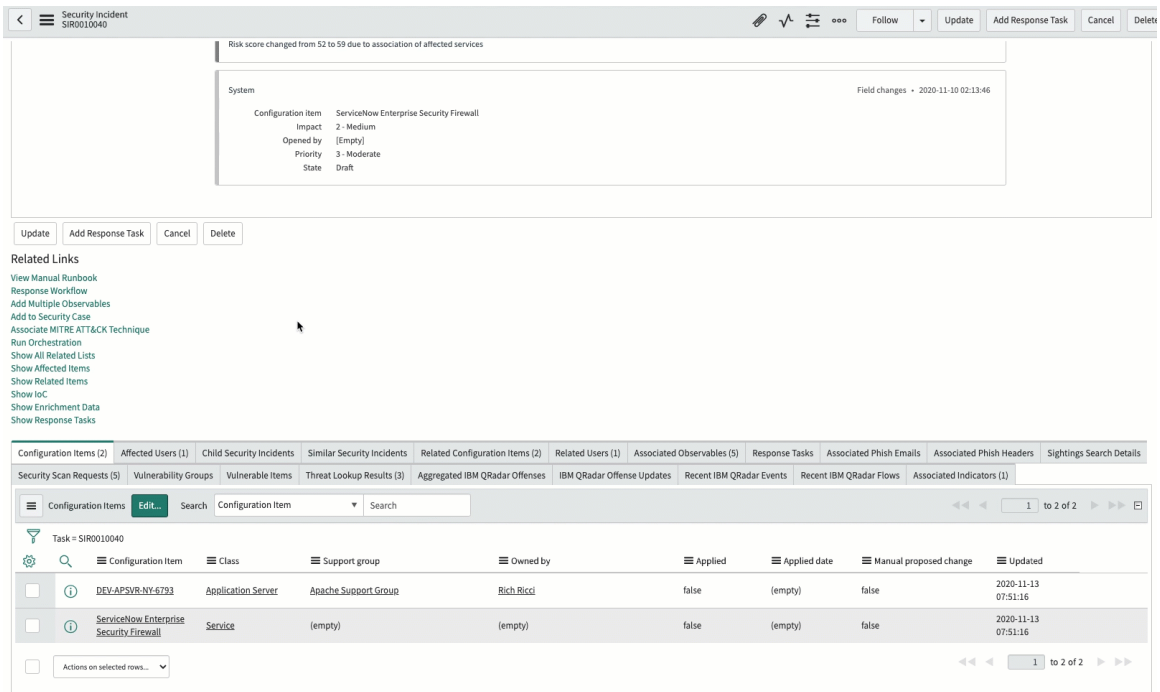
Einige SIEMs stellen möglicherweise MITRE-ATT&CK Informationen mit Events, Warnungen oder erkennbaren Elementen bereit. Um die MITRE-ATT&CK -Informationen auf einer granularen Ebene zuzuordnen, können Sie die Informationen mit einem erkennbaren Element hinzufügen.

Sie können für MITRE-ATT&CK Informationen automatisch von den erkennbaren Elementen zu einem Security Incident zusammenfassen. Aktivieren Sie für ein automatisches Rollup von erkennbaren Elementen zu Security Incidents die Systemeigenschaft. Alternativ können Sie die Informationen für jedes erkennbare Element manuell zusammenfassen.

### Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.
4. Zeigen Sie auf das erkennbare Element, das Sie zuordnen möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **MITRE ATT&CK-Technik zuordnen**aus.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik zuordnen**navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.




5. Überprüfen Sie in den Quelllisten die **Quelle**.

   **Hinweis:**
   Nur die Sammlungen und Matrizen, die aktiviert wurden, werden in der Quellliste angezeigt.

6. Überprüfen Sie die **Taktik** und die **Techniken**, und fügen Sie sie basierend auf der Relevanz für das erkennbare Element hinzu oder entfernen Sie sie.
7. Klicken Sie auf **Speichern**.

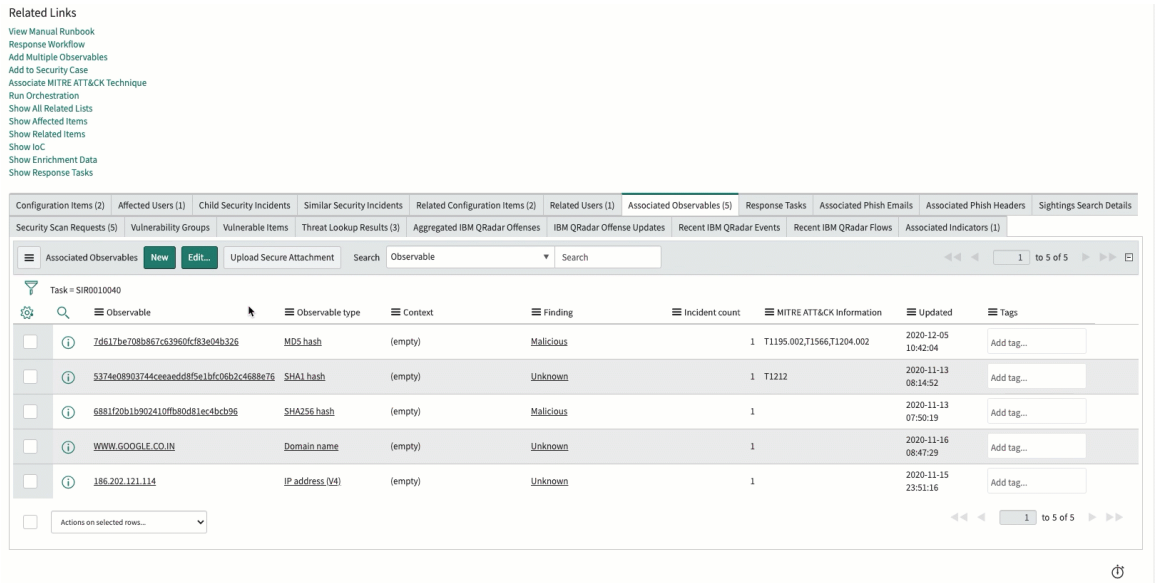


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die von Ihnen hinzugefügten Taktiken und Techniken werden in der Spalte MITRE-ATT&CK „ Informationen“ in der zugehörigen Liste der erkennbaren Elemente angezeigt.

8. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen“ **auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen bis hin zu Security Incidents, dann wird für die Informationen automatisch ein Rollup durchgeführt. Wenn Sie das automatische Rollup nicht aktiviert haben, müssen Sie dies manuell tun.

   Die folgende Abbildung zeigt, wie Sie ein erkennbares Element auswählen und für die Informationen MITRE-ATT&CK einen Rollup zu einem Security Incident durchführen.




9. Um eine zusammengefasste Ansicht der Techniken anzuzeigen, die den erkennbaren Elementen zugeordnet sind, wählen Sie zwei oder mehr erkennbare Elemente aus der Liste aus und klicken dann im Menü **Aktionen** in der Liste der ausgewählten Zeilen auf **MITRE ATT&CK-Informationen anzeigen**.

## Ergebnisse

Eine zusammengefasste Ansicht der MITRE ATT&CK-Informationen für die ausgewählten erkennbaren Elemente wird angezeigt.

### Ordnen MITRE-ATT&CK Sie Informationen dem Sicherheitsfall zu

Ordnen Sie MITRE-ATT&CK Taktiken und Techniken einem Sicherheitsfall zu, um die Verwaltung von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene zu verbessern.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Prozedur

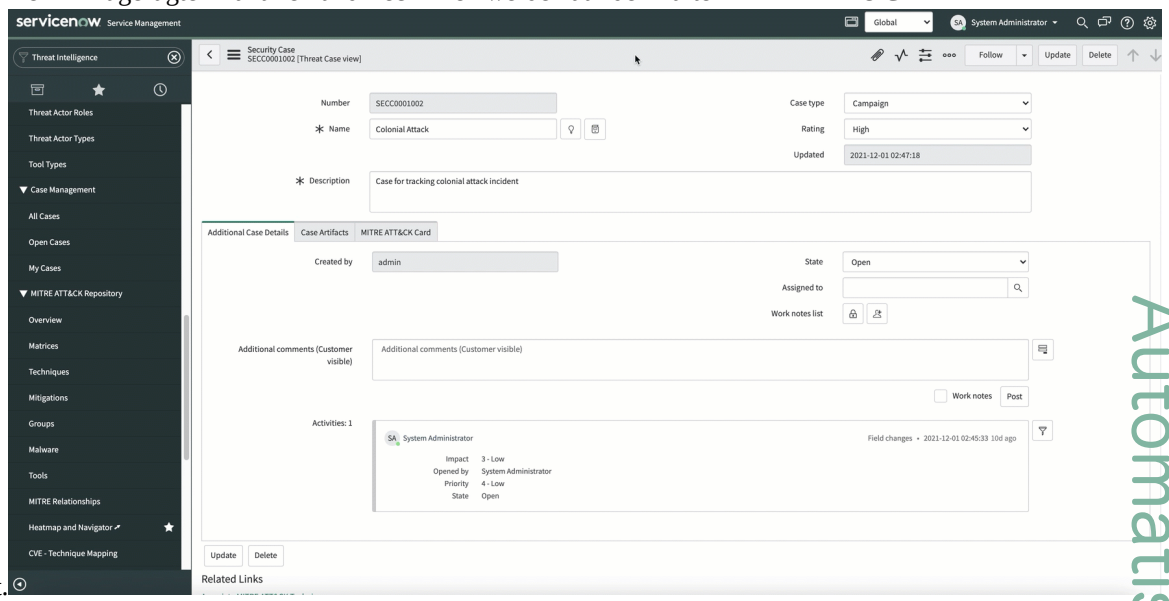
1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallverwaltung** > **Alle Fälle**.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.
3. Klicken Sie in der zugehörigen Liste auf **MITRE ATT&CK-Technik zuordnen**.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik zuordnen**navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Überprüfen Sie in den Quelllisten die **Quelle**.
5. Überprüfen Sie die **Taktik** und **Techniken**, und fügen Sie sie basierend auf der Relevanz für den Fall hinzu oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die von Ihnen hinzugefügten Taktiken und Techniken werden auf der Karte MITRE-ATT&CK angezeigt.




## Rollup von MITRE-ATT&CK Informationen anhand der Ergebnisse der Bedrohungssuche

Wenn Sie das automatische Rollup von MITRE-ATT&CK Informationen nicht aktiviert haben, können Sie dies manuell tun.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen aus den Ergebnissen der Bedrohungssuche zu Security Incident, dann wird für die Informationen automatisch ein Rollup durchgeführt. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.

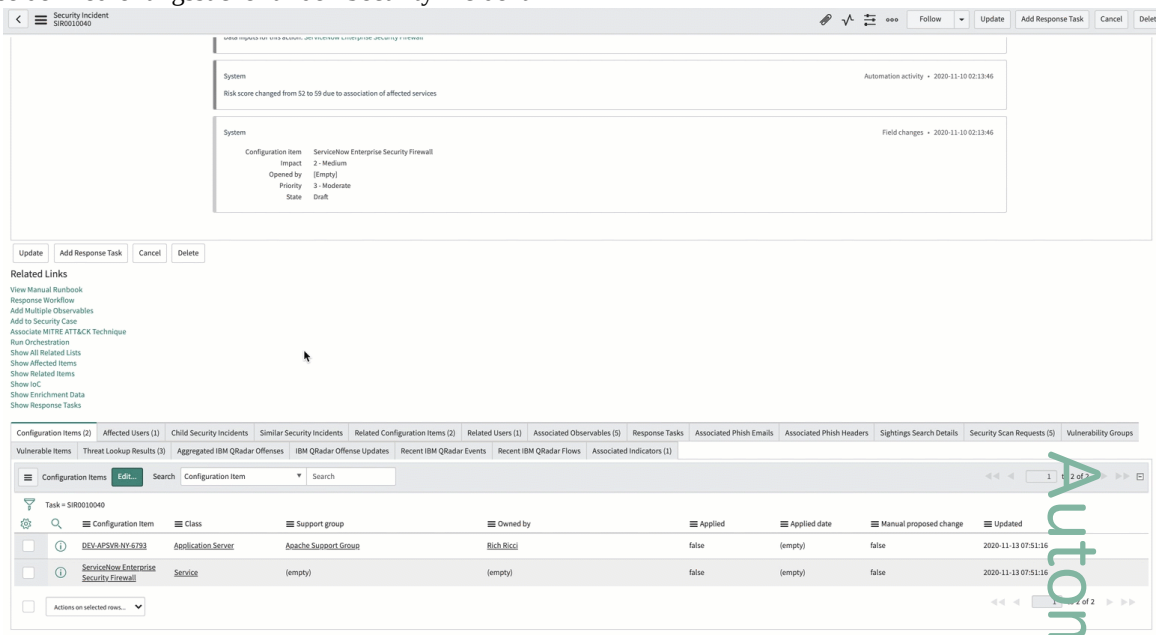
### Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Ergebnisse der Bedrohungssuche**.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü „Aktionen“ **auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können mehrere erkennbare Elemente auswählen und die Informationen zusammenfassen.
5. Klicken Sie auf **Neu laden**, um die Änderungen zu bestätigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie ein erkennbares Element auswählen und die Ergebnisse der Bedrohungssuche für den Security Incident




zusammenfassen.
Sie können die Karte MITRE-ATT&CK anzeigen, um zu bestätigen, dass für die Ergebnisse der Bedrohungssuche ein Rollup zum Security Incident durchgeführt wurde.

## Rollup MITRE-ATT&CK Informationen aus Erkennungsregeln

Aktivieren Sie das Rollup von MITRE-ATT&CK Informationen aus den Erkennungsregeln zu den Security Incidents, um die Analyse von Security Incidents und Bedrohungen zu verbessern.

### Vorbereitungen

Erforderliche Rolle: keine

Vergewissern Sie sich, dass Sie Folgendes durchgeführt haben:

- Aktivieren Sie im Modul „Eigenschaften“ die EigenschaftMITRE ATT&ACK-Informationen automatisch aus Warnungsregeln für Security Incidents zusammenfassen. Standardmäßig ist diese Option deaktiviert. Weitere Informationen finden Sie unter MITRE-ATT&CK-Systemeigenschaften überprüfen.
- Führen Sie eine Zuordnung von Erkennungsregeln zu MITRE-ATT&CK TTPs im Modul „ Erkennungsregeln – MITRE ATT&CK TTP -Zuordnung“ durch. Der Name der Erkennungsregel muss mit dem Namen der Warnungsregel übereinstimmen, die den Security Incident auslöst. Weitere Informationen finden Sie unter Erstellen und ordnen Sie Erkennungsregeln zu.

### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie nicht die Basissystem-SIEM-Regeln für die automatische Extraktion verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Event-Regel, die den Security Incident auslöst, im Namensfeld der Warnungsregel ausfüllen. Sie können das Feld „Name der Warnungsregel“ auch mithilfe von SIEM -Integration, E-Mail-Analyse, manueller Erstellung usw. ausfüllen.

Automatische Übersetzung

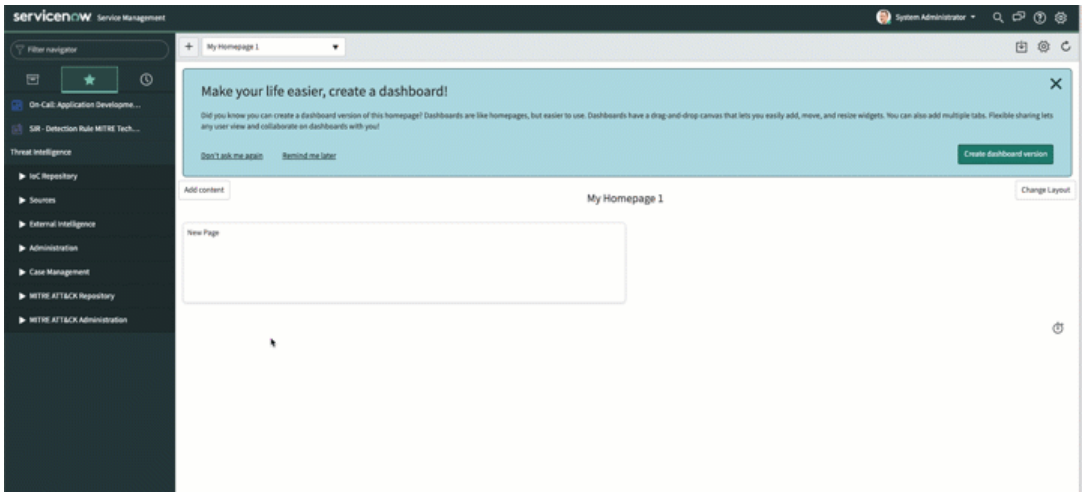
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **MITRE ATT&CK-Administration** > **Eigenschaften**.
2. Aktivieren Sie die Eigenschaft Rollup MITRE ATT&ACK-Informationen automatisch aus Warnungsregeln zu Security Incidents durchführen, und klicken Sie auf **Speichern**.
   Standardmäßig ist diese Option deaktiviert.
3. Sie müssen das Feld Name der **Warnungsregel** des Security Incident mit den erforderlichen Warnungsregeln ausfüllen.

   **Hinweis:**
   Stellen Sie sicher, dass Sie den genauen Namen der Warnungsregel hinzufügen. Um mehrere Regeln hinzuzufügen, müssen Sie die Regeln mit einem Komma-Trennzeichen hinzufügen.

4. Klicken Sie mit der rechten Maustaste auf das Formular, und klicken Sie auf **Speichern**.
   Wenn der Wert des Warnungsregelnamens im Security Incident mit einem Datensatz im Modul „Erkennungsregel – MITRE ATT&CK TTP Mapping“ übereinstimmt, werden die entsprechenden Techniken und Taktiken, die der Warnungsregel zugeordnet sind, automatisch mit dem Security Incident verknüpft.




5. Öffnen Sie den Security Incident, wählen Sie die **MITRE ATT&CK-Karte** aus, und überprüfen Sie, ob für die Techniken ein Rollup durchgeführt wird.
6. Aktivieren Sie die Option **Ursprung der Techniken** anzeigen, um den Ursprung der Techniken anzuzeigen.
   Der Ursprung der Techniken muss Erkennungsregelsein.

## Rollup MITRE-ATT&CK Informationen aus untergeordneten Security Incidents

Wenn Sie das automatische Rollup von MITRE-ATT&CK Informationen nicht aktiviert haben, können Sie dies manuell tun.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

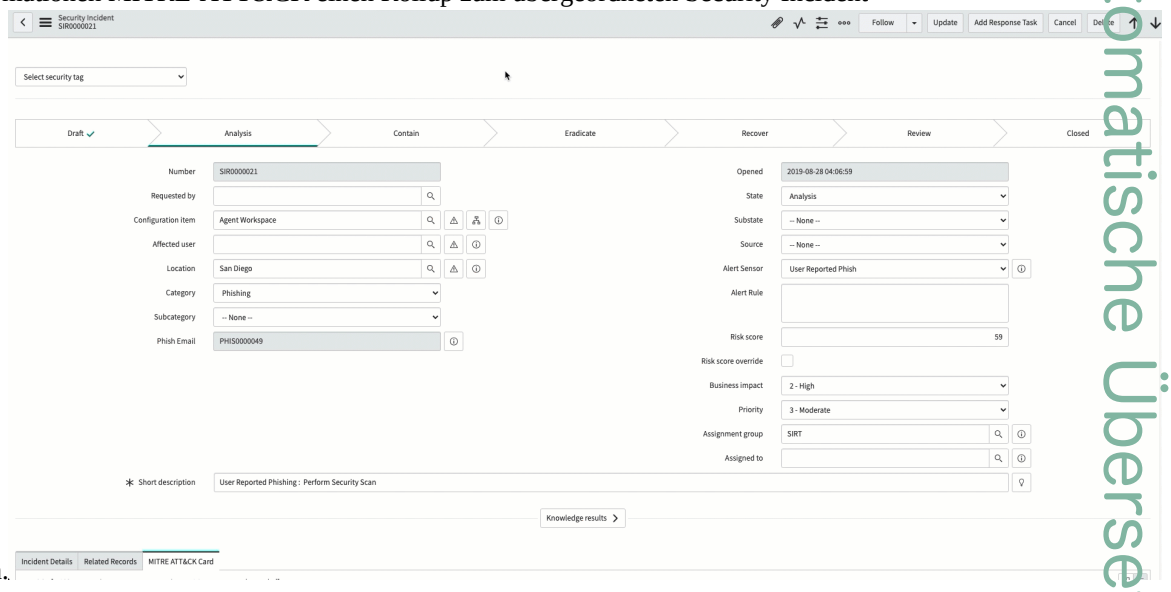
Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen aus untergeordneten Security Incidents, dann wird für die Informationen automatisch ein Rollup durchgeführt. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den übergeordneten Security Incident aus, den Sie mit den untergeordneten Informationen MITRE-ATT&CK anreichern möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Untergeordnete Security Incidents** aufrufen.
4. Wählen Sie den untergeordneten Security Incident aus, und klicken Sie dann im Menü „Aktionen“ **auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können auf **MITRE ATT&CK-Informationen** anzeigen klicken, um die MITRE-Informationen des untergeordneten Security Incident anzuzeigen, bevor Sie die MITRE ATT&CK-Informationen zusammenfassen.
5. Klicken Sie auf **Neu laden**, um die Änderungen zu bestätigen.
6. Klicken Sie auf die **MITRE ATT&CK-Karte**, um den Ursprung der Techniken anzuzeigen.
   Die folgende Abbildung zeigt, wie Sie einen untergeordneten Security Incident auswählen und für die Informationen MITRE-ATT&CK einen Rollup zum übergeordneten Security Incident durchführen.




Sie können die MITRE-ATT&CK-Karte anzeigen, um zu bestätigen, dass für die Informationen zum untergeordneten Security Incident MITRE-ATT&CK ein Rollup zum übergeordneten Security Incident durchgeführt wurde.

## Führen Sie Linkanalysen und Bedrohungssuche mit MITRE-ATT&CK -spezifischen Filtern durch

Korrelieren und führen Sie Linkanalysen von erkennbaren Elementen, Security Incidents und MITRE-ATT&CK zugehörigen Informationen durch, damit Ihr Unternehmen mit der Suche nach Bedrohungen beginnen kann.

### Vorbereitungen

Erforderliche Rolle: sn_ti.mitre_analyst, sn_si.read

### Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie die Security Incidents den Informationen von MITRE-ATT&CK zugeordnet haben, können Sie die spezifischen Filter von MITRE-ATT&CK für die Bedrohungssuche verwenden. Verwenden Sie die MITRE-ATT&CK -Filter mit den vorhandenen Security Incident Response -Filtern, um eine Linkanalyse zu korrelieren und durchzuführen.

Automatische Übersetzung

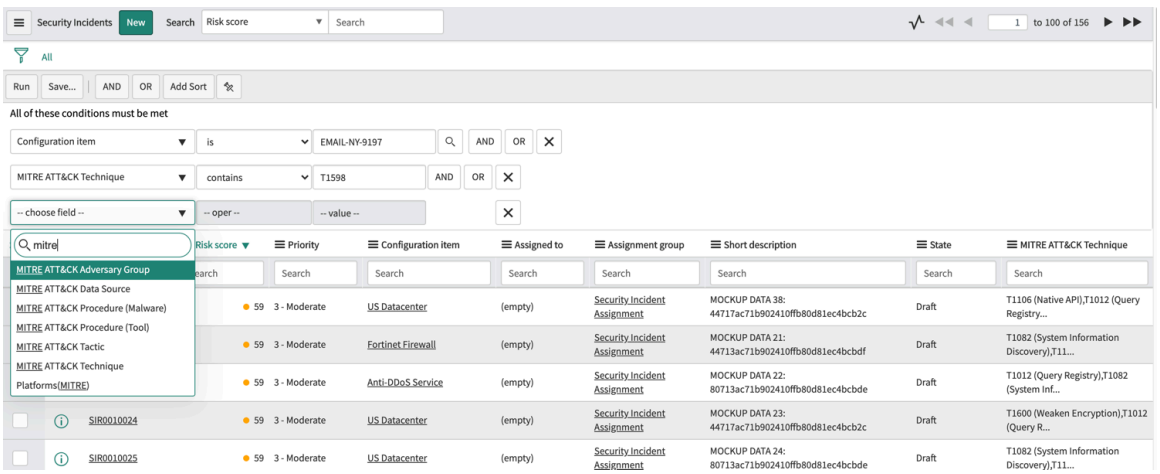
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Klicken Sie auf **Personalisierte Liste aktualisieren**, um die Spalten MITRE hinzuzufügen.
3. Wählen Sie eine Filterbedingung aus, damit Sie MITRE zugehörige Informationen und Zuordnungen zu Security Incidents oder erkennbaren Elementen anzeigen können:
   - MITRE-ATT&CK Angreifergruppe
   - MITRE-ATT&CK Datenquelle
   - MITRE-ATT&CK Verfahren (Malware)
   - MITRE-ATT&CK Vorgehensweise (Tools)
   - MITRE-ATT&CK Taktik
   - MITRE-ATT&CK Technik
4. Erstellen Sie eine Filterbedingung, die auf den oben genannten Kriterien basiert, und klicken Sie auf **Ausführen**, um eine Linkanalyse oder Korrelation zwischen Security Incidents, erkennbaren Elementen und MITRE-ATT&CK zugehörigen Informationen durchzuführen.

**Hinweis:**
Die Daten MITRE-ATT&CK werden als Zeichenfolge gespeichert, und Sie können für Filterbedingungen nur „ **contains** “ als Operator verwenden.

Wenn Sie beispielsweise überprüfen möchten, ob ein Konfigurationselement (CI) gefährdet ist, wählen Sie ein CI aus. Anschließend korrelieren Sie das CI mit vorhandenen Techniken, indem Sie eine MITRE-ATT&CK Technik-ID hinzufügen. Sie können dann Ihre Filterkriterien weiterentwickeln, um die Informationen zu korrelieren und die Bedrohungssuche durchzuführen.




## MITRE-ATT&CK Heatmap und Navigator

Sie können die Heatmap und den Navigator MITRE-ATT&CK für die grundlegende Navigation und zur Visualisierung Ihrer gesamten Technikerkennungsabdeckung verwenden.

## Übersicht über die Heatmap und den Navigator MITRE-ATT&CK .

Sie können den Navigator mit den primären Filtern für die grundlegende Navigation und Beobachtung von ATT&CK-Matrizen verwenden. Die Heatmap hebt das Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, in denen Ihre Organisation



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

keine Abdeckung hat. Dies ist verfügbar, nachdem Sie die Technikerkennungsabdeckung zugeordnet haben.

Mit der Heatmap und dem Navigator können Sie:

- Identifizieren Sie schnell und effizient die Erkennungsfähigkeiten Ihrer Organisation, und heben Sie Lücken in der Abdeckung der Technikerkennung hervor.
- Suchen Sie nach Bedrohungen und führen Sie eine Korrelation von Bedrohungen mithilfe der zugehörigen Funktionen durch.

### Greifen Sie auf die Heatmap und den Navigator MITRE-ATT&CK zu

Greifen Sie auf die Heatmap und den Navigator MITRE-ATT&CK zu, um die Matrix anzuzeigen, mit der Sie ATT&CK verwenden können.

#### Vorbereitungen
Erforderliche Rolle: sn_ti.read, sn_ti.mitre_analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können die Heatmap überprüfen, die Filter zur Korrelation verwenden und eine Linkanalyse der MITRE-ATT&CK Informationen, der erkennbaren Elemente und der Security Incidents in Ihrer Organisation durchführen.

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Heatmap und Navigator**.
   Die Heatmap und der Navigator werden in einer neuen Registerkarte geöffnet.
2. Wählen Sie die Quelle aus, um die Heatmap auszufüllen.

   **Hinweis:**
   Nur die Sammlungen und Matrizen, die aktiviert wurden, werden in der Quellliste angezeigt.

   In der folgenden Abbildung sehen Sie, wie Sie zur Heatmap und zum Navigator navigieren und die Quelle auswählen, in diesem Beispiel Enterprise ATT&CK.

   Navigieren Sie zu, und wählen Sie die Quelle aus, um die Heatmap auszufüllen
3. Verwenden Sie das Suchfeld, um anhand des Namens oder der ID schnell eine bestimmte Taktik oder Technik zu finden.

   Die folgende Abbildung zeigt, wie Sie nach einer Taktik, Technik oder darin enthaltenen Informationen suchen. Verwenden Sie die Suche, um schnell Detailinformationen zu einer bestimmten Taktik oder Technik anzuzeigen.
4. Klicken Sie auf **Filter**, und wählen Sie einen Filter aus den Filtern Primär oder Erweitert aus.
5. Klicken Sie auf **Anwenden**, und steuern Sie die Filter wie folgt:
   - Erstellen Sie eine benutzerdefinierte Ansicht, um Ihre Filter zu speichern. Sie können drei benutzerdefinierte Ansichtenerstellen und speichern.
   - Um die ausgewählten Filter zu entfernen, klicken Sie auf **Standardfilter wiederherstellen**, um Ihre gespeicherte Standardansicht zu laden.
   - Um alle Filter und Ihre vorhandene Ansicht zu löschen, klicken Sie auf **Alle Filter**löschen.

   **Hinweis:**
   Die Ansichten, die Sie speichern, sind spezifisch für einen Benutzer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf Untertechniken **ausblenden**, um alle Untertechniken aus der Heatmap-Ansicht zu entfernen.
   Wenn eine Technik über Untertechniken verfügt, können Sie auf das Erweiterungssymbol klicken, um die Untertechniken anzuzeigen.

### Verwenden der benutzerdefinierten Ansichten

Benutzerdefinierte Ansichten in der Heatmap und im Navigator MITRE-ATT&CK helfen Ihnen, Ihre bevorzugten Filter zu speichern und anzuzeigen, wenn Sie das nächste Mal auf der Heatmap landen.

**Hinweis:**
Sie können drei benutzerdefinierte Ansichten für jede MITRE-ATT&CK -Sammlung pro Benutzer erstellen und speichern.

## Erstellen Sie eine Ansicht

Nachdem Sie die erforderlichen Filter aus den Filtern Primär oder Erweitert ausgewählt haben, klicken Sie im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen **Sie Neue Ansicht erstellen aus**. Geben Sie den Namen der benutzerdefinierten Ansicht ein, und klicken Sie auf **Ansicht speichern**.

## Standardansichten

Klicken Sie auf **Save this as a default view (Als Standardansicht speichern)**, um die Ansicht direkt zu laden, wenn Sie das nächste Mal auf der Heatmap landen. Sie können für jede der Sammlungen eine Standardansicht festlegen.

**Hinweis:**
Wenn Sie das Plugin Threat Intelligence von einer älteren Version aktualisieren, wird Ihre vorhandene Standardansicht aus der alten Version als benutzerdefinierte Ansicht angezeigt.

Die Abbildung zeigt, wie eine benutzerdefinierte Ansicht in der Heatmap erstellt wird

## Aktualisieren Sie eine Ansicht

Sie können Aktualisierungen an einer vorhandenen benutzerdefinierten Ansicht vornehmen, indem Sie die erforderlichen Filter Primär oder Erweitert ändern. Wählen Sie eine benutzerdefinierte Ansicht aus, aktualisieren Sie die Filter nach Bedarf, klicken Sie dann im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen Sie **Ansicht** aktualisieren aus, um die Filter zu speichern.

Diese Abbildung zeigt, wie eine benutzerdefinierte Ansicht aktualisiert wird.

## Benutzerdefinierte Ansichten verwalten

Verwenden Sie die Kontrollkästchen neben jeder benutzerdefinierten Ansicht, um den ausgewählten benutzerdefinierten Ansichtsfilter anzuwenden.

Klicken Sie auf die Schaltfläche mit den Auslassungspunkten (⋯) neben jedem benutzerdefinierten Ansichtsnamen, um die benutzerdefinierten Ansichten wie folgt zu steuern:

- Legen Sie eine Standardansicht fest.
- Entfernen Sie eine benutzerdefinierte Ansicht als Standardansicht. Dadurch wird die benutzerdefinierte Ansicht nicht gelöscht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benennen Sie die benutzerdefinierte Ansicht um.
- Löschen Sie die benutzerdefinierte Ansicht.

Diese Abbildung zeigt, wie benutzerdefinierte Ansichten verwaltet werden.

### Exportieren Sie eine gespeicherte Ansicht

Um die gespeicherten benutzerdefinierten Ansichten in JSON-Dateien zu exportieren, klicken Sie im Header Filter auf Auslassungspunkte (⋯), und wählen Sie **Gespeicherte**Ansichten exportieren aus. Klicken Sie auf das Download-Symbol für die benutzerdefinierte Ansicht, die Sie auf Ihren lokalen Computer herunterladen möchten.

Diese Abbildung zeigt, wie benutzerdefinierte Ansichten exportiert werden.

### Importieren Sie eine Ansicht

Sie können nur JSON-Dateien importieren. Um die benutzerdefinierten Ansichten zu importieren, klicken Sie im Header Filter auf die Schaltfläche mit den Auslassungspunkten (⋯), und wählen Sie **Import view(json) aus**.

Überprüfen Sie beim Importieren von Ansichten die folgenden Bedingungen:

- Sie können nur das JSON-Dateiformat importieren.
- Sie können jeweils nur eine Ansicht oder Datei importieren.
- Sie können nicht importieren, wenn Ihre Filter bereits drei benutzerdefinierte Ansichten enthalten. Löschen Sie eine benutzerdefinierte Ansicht, und importieren Sie eine Ansicht.
- Sie können keine Ansicht mit einem vorhandenen benutzerdefinierten Ansichtsnamen importieren. Benennen Sie eine Ansicht vor dem Import um.

Diese Abbildung zeigt, wie eine Ansicht importiert wird.

#### Navigator mit primären Filtern

Verwenden Sie die primären Filter, um Techniken im MITRE-ATT&CK -Navigator zu filtern. Die Informationen im Repository MITRE-ATT&CK stehen zur Auswahl.

| Filter | Beschreibung |
|---|---|
| Angreifergruppe (Bedrohungsgruppe) | Sätze zugehöriger Angriffsaktivitäten, die in der Sicherheits-Community unter einem gemeinsamen Namen nachverfolgt werden. Gruppen können verschiedene Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen bedeuten. Sie können dem Filter **„Angreifergruppe (Bedrohungsgruppe)“** mehrere Gruppen hinzufügen.<br><br>Fügen Sie beispielsweise APT1 und AT12 hinzu, da beide Bedrohungsgruppen sind, die China zugeordnet sind. Beide Gruppen zielen zwar auf unterschiedliche Quellen ab, könnten jedoch ähnliche Techniken verwenden. |



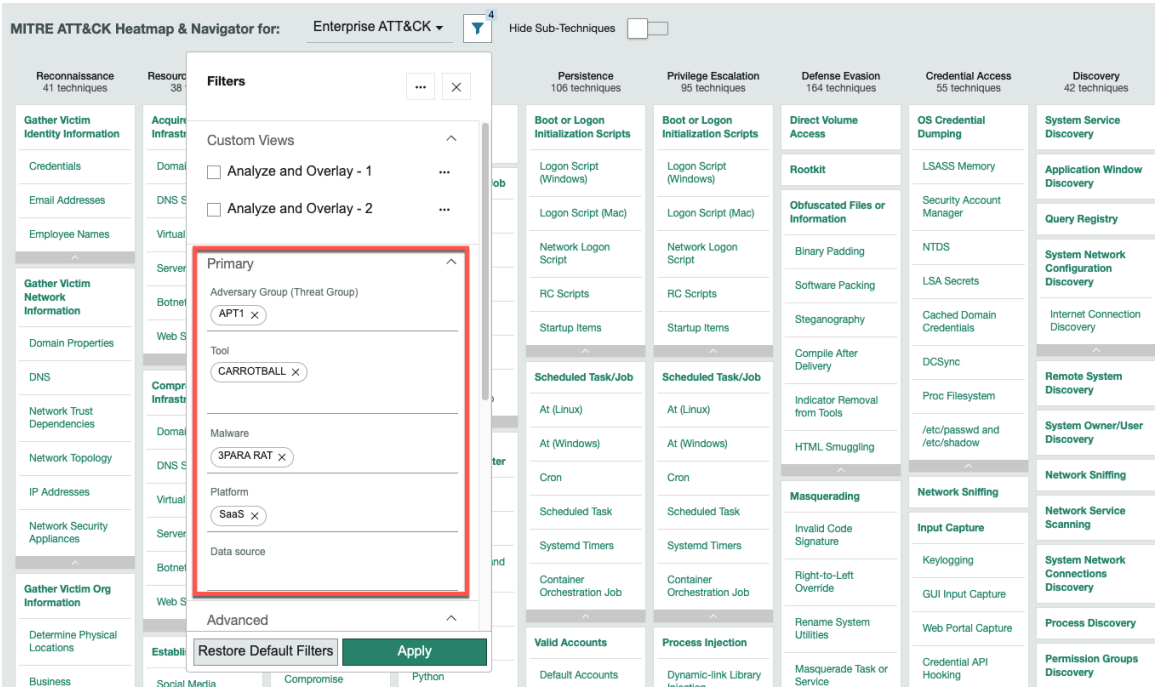
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Filter | Beschreibung |
| --- | --- |
| Tool | Legitime Software, die von Bedrohungsakteuren für Angriffe verwendet wird. Sie können verstehen, wie Bedrohungsakteure Kampagnen ausführen, wenn Sie wissen, wie und welche Tools von Bedrohungsakteuren verwendet werden. Tools umfassen sowohl Software, die nicht auf einem Unternehmenssystem gefunden wird, als auch Software, die als Teil eines Betriebssystems verfügbar ist, das bereits in einer Umgebung wie Microsoft Windows-Dienstprogramme vorhanden ist.<br><br>Zum Beispiel ist gsecdump ein öffentlich verfügbarer Dumper für Anmeldeinformationen, den die APT11-Angreifergruppe verwendet, um Passwort-Hashes und LSA-Geheimnisse (Local Security Authority) von Microsoft Windows-Betriebssystemen zu erhalten. |
| Malware | Kommerzielle, benutzerdefinierte Closed Source- oder Open Source-Software, die von Angreifern für böswillige Zwecke verwendet werden soll.<br><br>Beispiele sind PlugX, CHOPSTICK usw |
| Plattform | Taktiken und Techniken, die MITRE-ATT&CK in einer bestimmten Plattform darstellen.<br><br>Beispielsweise unterstützt MITRE-ATT&CK die folgenden Plattformen in der Enterprise ATT&CK-Matrix: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network. |
| Datenquelle | Datenquellen, die Sie in Ihrer Umgebung sammeln und zur Erkennung von MITRE-ATT&CK -Techniken verwenden.<br><br>Beispiele sind DLL-Überwachung und Browsererweiterungen. |

Die folgende Abbildung zeigt alle primären Filter, die im MITRE-ATT&CK -Navigator verfügbar sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Verwenden einer Heatmap mit primären und erweiterten Funktionen

Sie können eine Heatmap mit erweiterten Filtern verwenden, um eine Analyse durchzuführen, indem Sie Security Incidents mit MITRE-ATT&CK Informationen korrelieren.

## Zeigen Sie Technik-IDs an

Sie können die MITRE-ATT&CK Technik-IDs mit den Techniknamen anzeigen, wenn Sie den Filter **Technik-IDs anzeigen** auswählen.

Zeigen Sie Technik-IDs auf einer Heatmap an

## Zeigen Sie relevante Techniken nach Priorität an

Um die Techniken basierend auf ihrer relevanten Priorität im Navigator zu filtern, wählen Sie **Filter nach relevanter Priorität für Technik** und dann im Menü die **relevante Priorität** aus. Sie können mehrere Filterprioritäten zuweisen. Sie können auch auf die Techniken in der Heatmap verweisen, um die Priorität der Technik zu erfahren.

Die relevanten Prioritätsinformationen basieren auf der Priorisierung, die Sie im Feld Technik relevante Priorität festgelegt haben.

Diese Abbildung zeigt die Filterung nach relevanter Priorität.

## Zeigen Sie die Abdeckung der Technikerkennung an

Um die gesamte Technikerkennungsabdeckung in der Heatmap anzuzeigen, wählen Sie den Filter **Technikerkennungsabdeckung anzeigen** aus. Die Heatmap hebt das visuelle Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, in denen Sie keine Abdeckung haben. Die Bewertungsdefinition des Basissystems und die Farben wurden in der Technikerkennungsabdeckungdefiniert. Die Informationen wurden automatisch aus der gesamten Technikerkennungsabdeckung extrahiert.

Beispielsweise weisen rot markierte Bereiche der Heatmap auf eine fehlende Erkennung hin. Bereiche, die blau markiert sind, zeigen an, dass vollständige Erkennungsfunktionen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorhanden sind. Bereiche, die in Orange, Gelb und Hellblau markiert sind, spiegeln teilweise Erkennungsfähigkeiten wider.

- Die Farbvisualisierung basiert auf der Technikdefinition und Farbcodierung, die Sie definieren.
- Die Abdeckungsvisualisierung basiert auf der von Ihnen definierten Zuordnung der Technikerkennungsabdeckung.
- Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für den Abdeckungstyp nicht mit den Techniken in der Heatmap angezeigt.

**Hinweis:**
Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technikerkennungsabdeckung und die Abdeckungsfarben ändern.

In dieser Abbildung sehen Sie die Technikerkennungsabdeckung für alle Techniken und Untertechniken und den Abdeckungstyp mit ihren Farben und Symbolen.

Erkennungsabdeckung der Heatmap-Technik

## Zeigen Sie die Abdeckung der Technikminderung an

Um die allgemeine Technikminderungsabdeckung in der Heatmap anzuzeigen, wählen Sie den Filter Technikminderungsabdeckung anzeigen aus. Die Heatmap hebt das visuelle Spektrum der Abdeckung durch Risikominderung hervor, einschließlich der Bereiche, die Sie nicht abdecken. Die Verringerungsabdeckung, die Farben und die Prozentbereiche wurden in der Definitionder Verringerungsabdeckung definiert. Die Informationen werden aus der Gesamtabdeckung der Technikminderungextrahiert.

Zum Beispiel zeigen rot hervorgehobene Techniken keine Verringerungsabdeckung an, Orange zeigt eine schlechte Verringerungsabdeckung an und Blau zeigt eine hervorragende Verringerungsabdeckung an.

- Die Farbvisualisierung basiert auf der Definition der Technik zur Risikoverringerung und der Farbcodierung, die Sie definieren.
- Die Abdeckungsvisualisierung basiert auf der von Ihnen definierten Technikverringerungsabdeckungszuordnung.
- Wenn Sie die Definition der Basissystem-Abdeckung für Risikominderung ändern, werden die Symbole für den Typ der Risikominderungsabdeckung nicht mit den Techniken in der Heatmap angezeigt.

**Hinweis:**
Die Heatmap funktioniert wie erwartet, wenn Sie dieselben Felder wie die im Basissystem definierte Technik-Minderungsabdeckung und die Abdeckungsfarben ändern.

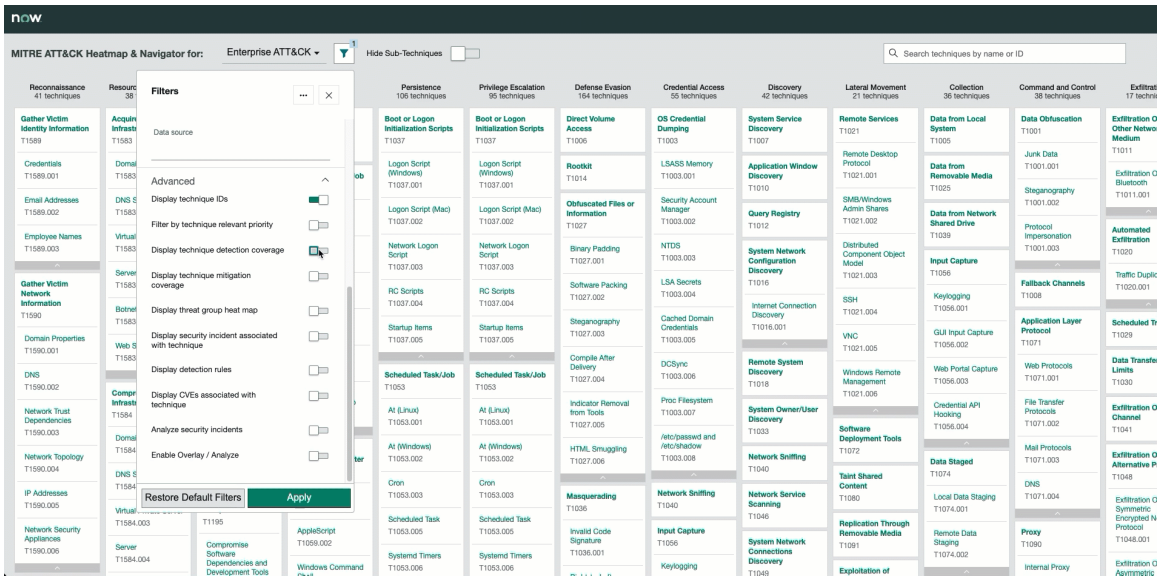
Diese Abbildung zeigt die Heatmap der Technikverringerungsabdeckung

## Zeigen Sie die Erkennungs- und Verringerungsabdeckung an

Sie können die Filter „Technikerkennung“ und „Technikminderungsabdeckung“ zusammen verwenden, um Einblicke in die Relevanz der Technikerkennung zu erhalten und die Abdeckung für Ihre Organisation zu verringern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Diese Abbildung zeigt, wie Erkennungs- und Verringerungsfilter zusammen verwendet werden.

## Zeigen Sie die Bedrohungsgruppe an

Um die Bedrohungsgruppe zu Technikinformationen in der Heatmap anzuzeigen, wählen Sie **Heatmap der Bedrohungsgruppe anzeigen aus**. Sie können die Anzahl der Bedrohungsgruppen messen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik steigt, wenn die Anzahl der Angreifer hoch ist. Die Bedrohungsgruppenbereiche und Heatmap-Farben wurden in der Heatmap -Definition der Bedrohungsgruppe – Technikdefiniert.

- Die Farbvisualisierung für die Heatmap und den Text basiert auf der Heatmap-Definition von Bedrohungsgruppe zu Technik.
- Die Visualisierung des Bedrohungsgruppenbereichs basiert auf der Zuordnung von Bedrohungsgruppe zu Technik.
- Sie können den **Heatmap-Filter „Bedrohungsgruppe anzeigen“** nicht verwenden, wenn die Technikerkennungsabdeckung oder die Technikminderungsabdeckung aktiviert ist. Diese Abbildung zeigt die Informationen zur Bedrohungsgruppe in der Heatmap.

## Zeigen Sie Security Incidents an, die der Technik zugeordnet sind

Um die Techniken anzuzeigen, die in Ihrer Organisation häufig genutzt werden und zu Security Incidents geführt haben, klicken Sie auf **Security Incident anzeigen, der der Technik zugeordnet**ist. Sie können weitere Informationen zu jedem der zugehörigen Security Incidents anzeigen, wenn Sie auf den Link klicken, der in einem neuen Fenster zur Analyse geöffnet wird. Security Incidents, die einer Technik zugeordnet sind.

- Priorität: Wählen Sie **Security Incident Priority** (Security Incident-Priorität) aus, um nach der Security Incident-Priorität zu filtern.
- Datumsbereich: Wählen Sie den Datumsbereich für **Security Incident** aus, um Sicherheitsprobleme nach dem Datumsbereich zu filtern.
- Falsch positive Meldungen: Wählen Sie **Security Incident** Falsch positive Meldungen filtern aus, um falsch positive Probleme zu entfernen. Wenn Sie diesen Filter auswählen, wird die Anzahl der Security Incidents reduziert, die in der Heatmap angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie diesen Filter mit dem Filter „ **Technikerkennungsabdeckung anzeigen** “ verwenden, erhalten Sie Einblicke in die Relevanz der Technikerkennungsabdeckung für Ihre Organisation bis zum ausgewählten Datum.

Wenn Sie beispielsweise beide Filter aktivieren, können Sie sehen, dass die Maskierungstechnik unter der Taktik „Defense Evasion“ keine Abdeckung hat. Wenn Sie genauer hinschauen, bezieht sich die Maskierungstechnik auf die Maskierungsaufgabe oder den Service, der auch ein Security Incident zugeordnet ist. Dies zeigt, dass in der Technikerkennungsabdeckung für die Maskierungstechnik eine Lücke besteht, und Sie sollten die allgemeine Technikerkennungsabdeckung überarbeiten.

### Zeigen Sie Erkennungsregeln an

Um anzuzeigen, ob Sie die Erkennungsregeln für eine bestimmte Technik definiert haben, klicken Sie auf **Erkennungsregeln anzeigen**. Sie können auch jede zugeordnete Erkennungsregel mit ihrer Definition anzeigen.

Diese Informationen basieren auf der Zuordnung der Erkennungsregeln, die Sie definiert haben. Zeigen Sie die zugehörigen Erkennungsregeln an.

### Zeigen Sie CVEs an, die der Technik zugeordnet sind

Um die Informationen zu allgemeinen Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVE) anzuzeigen, die jeder der Techniken zugeordnet sind, klicken Sie auf **CVEs anzeigen, die der Technik zugeordnet sind**. Die CVE-zu-Technik-Informationen basieren auf den Informationen, die im Modul „CVE – Technikzuordnung“verfügbar sind. Dies gibt Ihnen Einblick in bekannte Schwachstellen und informiert Sie darüber, ob Angreifer Ihre Organisation potenziell ausnutzen können.

**Wichtig:**
Die Heatmap wurde so erweitert, dass nur die relevanten CVEs angezeigt werden, die den VITs zugeordnet sind

Um VITs anzuzeigen, die mit CVEs und Techniken verknüpft sind, wählen **Sie VITs mit CVE und Techniken anzeigen aus**. Um Techniken ohne VITs weiter zu filtern, wählen Sie **Techniken ohne VITs ausblenden aus**. Die CVE- und VIT-Informationen, die Sie anzeigen, werden aus dem Produkt Vulnerability Response in Ihrer Umgebung abgerufen. Sie können die gefilterte Liste der CVEs und VITs in der Heatmap anzeigen und in der Heatmap zu jedem CVE oder VIT für jede Technik navigieren.

**Hinweis:**

- Die **Technik „Zugehörige CVEs anzeigen“** ist nur verfügbar, wenn das Produkt Vulnerability Response in Ihrer Umgebung installiert ist.
- Die VIT- und CVE-Informationen werden basierend auf der geplanten Aufgabe berechnet, die Sie im festgelegt haben MITRE-ATT&CK Eigenschaften. Die regelmäßige Aufgabe des Basissystems ist auf 24 Stunden festgelegt.

Wenn Sie diesen Filter mit dem Filter „ **Security Incident in Verbindung mit Technik anzeigen** “ verwenden, können Sie ermitteln, ob die bekannten Schwachstellen Security Incidents in Ihrer Organisation verursacht haben.

Sie können weitere Informationen zu jedem CVE anzeigen, um zu analysieren, ob das CVE für Ihre Organisation relevant ist. Zeigen Sie dazu die angreifbaren Elemente an. Wenn angreifbare Elemente erstellt werden, können Sie weitere Informationen zu zugehörigen CI-Informationen im Modul Vulnerability Response anzeigen. Sie können auch den Schweregrad



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Priorität überprüfen, um fundierte Entscheidungen zu treffen. Überprüfen Sie CVEs, um fundierte Entscheidungen zu treffen.

## Analysieren von Security Incidents

Um Security Incidents zu analysieren und die Techniken zu überprüfen, die von einem Angreifer für einen Angriff verwendet werden, klicken Sie auf **Security Incidents analysieren**. Sie können mehrere Security Incidents zur Analyse hinzufügen, indem Sie durch Kommas getrennte Zeichenfolgen verwenden.

Dieser Filter hilft Ihnen, einen Security Incident zu analysieren. Sie erfahren, warum der Incident aufgetreten ist, welche Techniken ausgenutzt wurden, ob bekannte Bedrohungsakteure beteiligt waren, ob die Bedrohungsakteure eine bestimmte Sequenz für einen Angriff verwendet haben usw. Da Sie mehrere Security Incidents gleichzeitig analysieren können, können Sie die Informationen korrelieren, um festzustellen, ob sie zusammenhängen oder ob es sich um einen isolierten Incident handelt. Wenn die Security Incidents zusammenhängen und Sie ein Muster beobachten, können Sie ihren Fortschritt in der Kill Chain überprüfen, um den Angriff zu stoppen oder eine Verteidigungsstrategie für Ihre Organisation zu entwickeln.

Wenn Sie den Filter **Security Incidents analysieren** mit primären Filtern verwenden, z. B. einer **Angreifergruppe**, können Sie korrelieren, ob bekannte Angreifer beteiligt sind. Wenn beispielsweise mehrere Security Incidents analysiert werden, sind die Techniken, die den Security Incidents zugeordnet sind, in Form einer Kill Chain vorhanden. Wenn Sie die Informationen mit dem Angreifer überschneiden, werden Sie eine Überschneidung zwischen den Techniken, die dem Security Incident zugeordnet sind, und den Techniken, die dem Angreifer zugeordnet sind, feststellen. Wenn beide Filter aktiviert sind, werden nur die überlappenden Technikinformationen angezeigt.

Analysieren von Security Incidents

## Überlagerung zur Analyse von Security Incidents und Angreifergruppen verwenden

Verwenden Sie den Filter **Überlagerung/Analysieren** aktivieren, um das Verhalten des Angreifers anzuzeigen und einen oder mehrere der Security Incidents zu analysieren und die Informationen zu korrelieren, um festzustellen, ob es sich bei einem Angriff um einen isolierten Incident oder einen koordinierten Angriff eines bekannten Angreifers handelt.

Beispielsweise können Sie jetzt die Security Incidents und das Verhalten des Angreifers in der Kill Chain in derselben Ansicht anzeigen. Diese Ansicht enthält Überschneidungsinformationen, die Sie über den Angriff und das bekannte Angreiferverhalten informieren. Auf diese Weise können Sie analysieren, ob es sich um einen isolierten Angriff oder einen koordinierten Angriff eines bekannten Angreifers handelt.

Durch Aktivieren des Overlay-Analysefilters werden alle primären Filter mit Ausnahme des **Angreifergruppenfilters** und der erweiterte Filter **Nach technikrelevanter Priorität** filtern beim Generieren einer Ansicht ignoriert.

Sobald Sie den Überlagerungsanalysefilter aktiviert haben, verwenden Sie die Farbpalette, um Farben für Folgendes zuzuweisen:

- Analysieren Sie den Security Incident
- Angreifergruppe
- Überlagerung



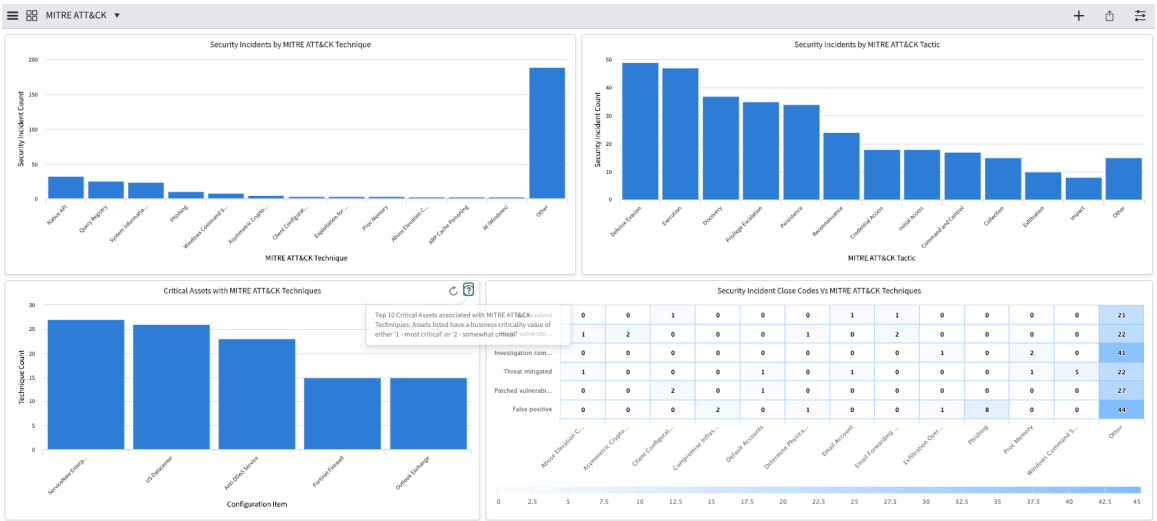
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, dass die Angreifergruppe APT18 über mehrere Techniken und Taktiken in der Kill Chain verteilt ist. Die Analyse zeigt auch, dass es drei Techniken gibt, die die Angreifergruppe und die Security Incidents, die Sie nachverfolgen, überlagern.
Diese Abbildung zeigt die Overlay-Informationen zu Angreifern und Security Incidents.

### Verwenden des Dashboards MITRE-ATT&CK .

Das Dashboard MITRE-ATT&CK bietet einen Überblick über die Datenquellenabdeckung, Taktiken und Techniken, die in Ihrer Organisation verwendet werden.

Das MITRE-ATT&CK -Übersichtsmodul zeigt MITRE-ATT&CK Informationen zu Security Incidents an, einschließlich Trends und Berichte. Sie können auf einen beliebigen Teil eines Widgets klicken (Balken, Datenpunkt, Tabelle usw.), um Daten anzuzeigen, die für diesen Teil spezifisch sind.




### Verwenden Sie das Dashboard MITRE-ATT&CK, um Ihre sicherheitsbezogenen Daten anzuzeigen

Verwenden Sie das Dashboard MITRE-ATT&CK, um einen Überblick über die Datenquellenabdeckung, Taktiken und Techniken zu erhalten, die in Ihrer Organisation verwendet werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

#### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Übersicht**.
2. Klicken Sie auf eines der folgenden Widgets, um zusätzliche Details anzuzeigen:
   - Security Incidents nach MITRE-ATT&CK Technik
   - Security Incidents nach MITRE-ATT&CK Taktik
   - Kritische Assets mit MITRE-ATT&CK Techniken
   - Abschlusscodes für Security Incident im Vgl. zu MITRE-ATT&CK -Techniken
   - MITRE-ATT&CK-Techniken nach Erkennungsabdeckung
   - MITRE-ATT&CK-Techniken nach Verringerungsabdeckung
   - Bedrohungsgruppen nach MITRE-ATT&CK-Technik
   - CVEs nach MITRE-ATT&CK-Technik

Automatische Übersetzung

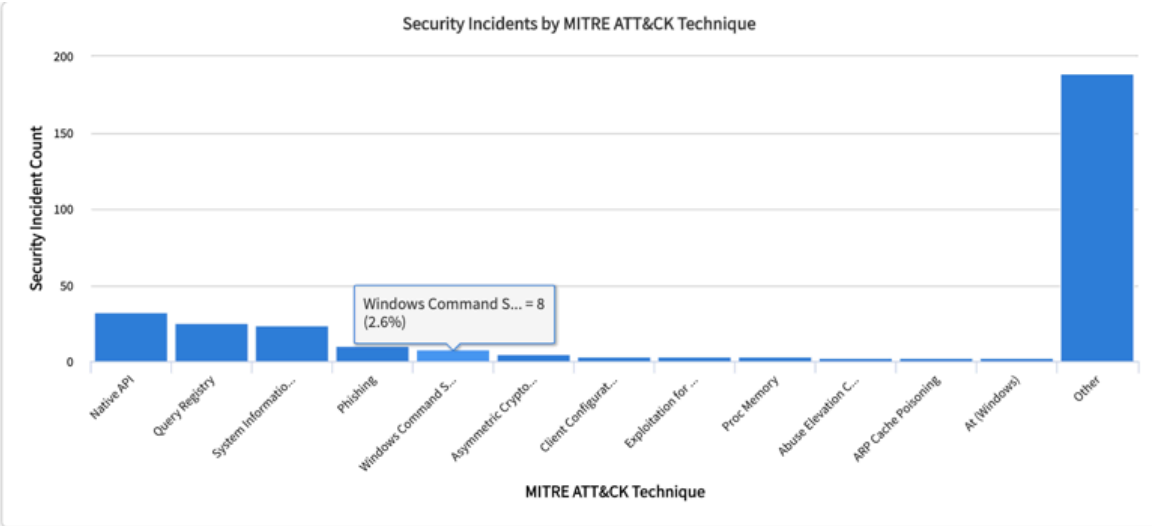
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MITRE-ATT&CK Widgets

Das MITRE-ATT&CK -Übersichtsmodul besteht aus Widgets, mit denen Sie die MITRE-ATT&CK -Informationen mit den Security Incident-Informationen in Ihrer Umgebung korrelieren können.

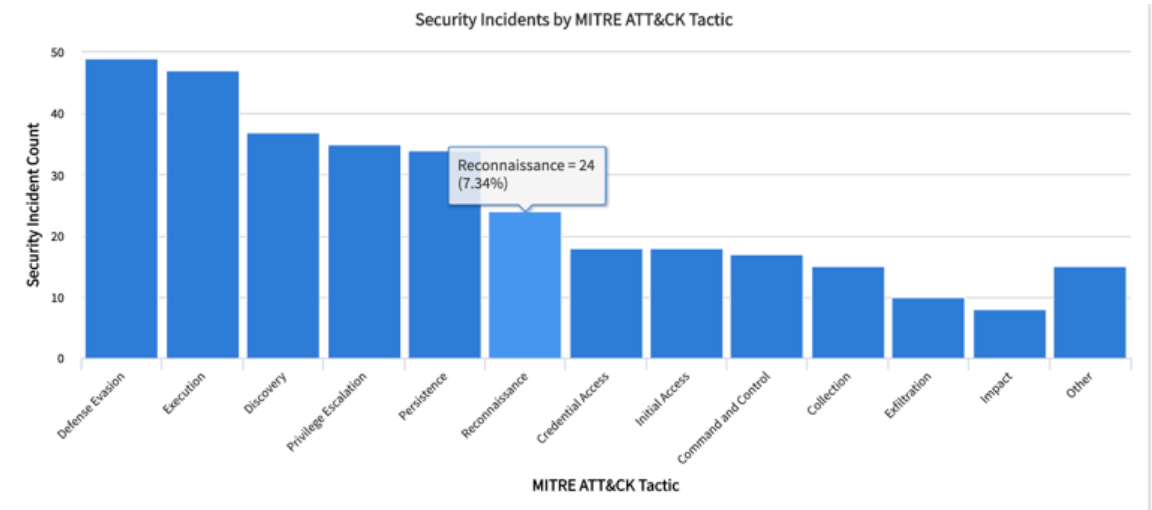
## Beispiel für Security Incidents nach MITRE-ATT&CK -Technik

In diesem Beispiel zeigt das Widget „ **Security Incidents nach MITRE ATT&CK-Technik** “ die Techniken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.




## Beispiel für Security Incidents nach MITRE-ATT&CK Taktik

In diesem Beispiel zeigt das Widget „ **Security Incidents nach MITRE ATT&CK** -Taktik“ die wichtigsten Taktiken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.



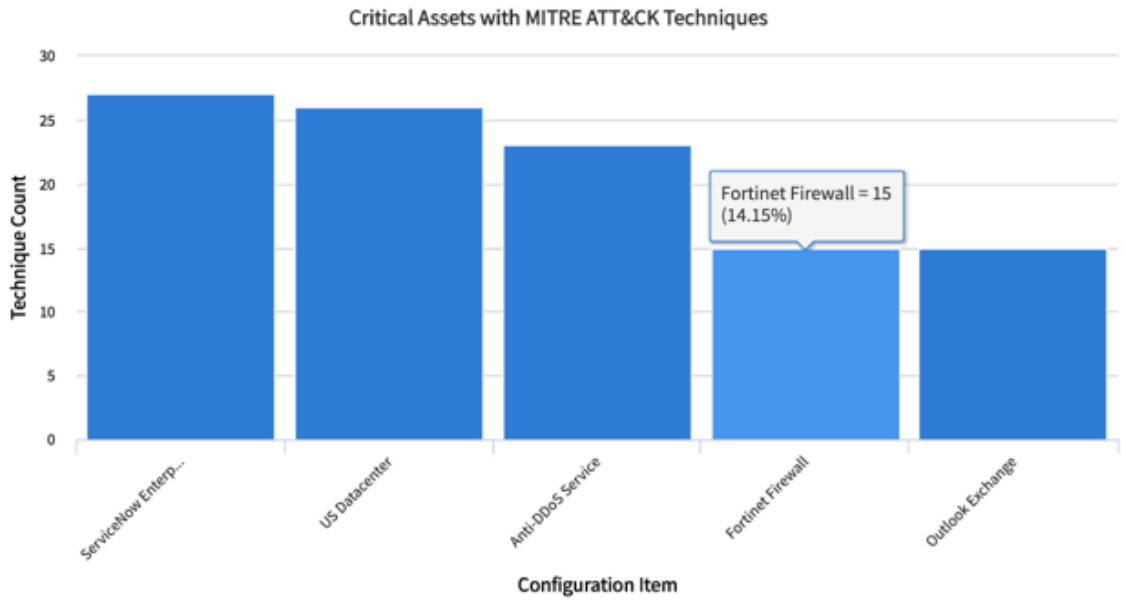

## Beispiel für kritische Assets mit MITRE-ATT&CK Techniken

In diesem Beispiel zeigt das Widget „ **Kritische Assets mit MITRE ATT&CK-Techniken** “ die 10 wichtigsten kritischen Assets an, die den Techniken MITRE-ATT&CK zugeordnet sind. Die Assets haben eine Geschäftskritikalität von 1 (äußerst kritisch) oder 2 (kritisch).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

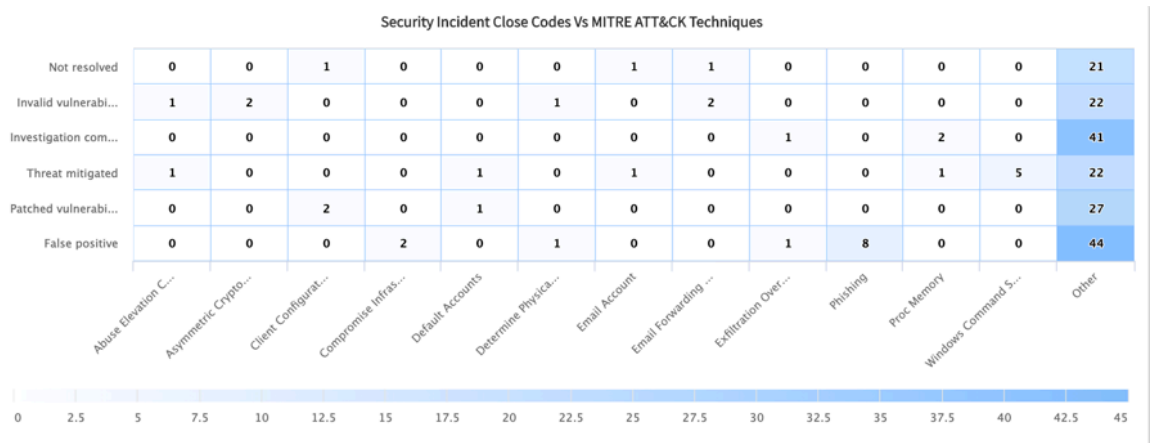
Mit diesem Bericht kann eine Organisation die Typen und die Anzahl der Techniken anzeigen, die bei Angriffen auf kritische Assets verwendet werden.




## Beispiel für Abschlusscodes für Security Incidents vs. MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget Abschlusscodes **für Security Incidents vs.** *MITRE-ATT&CK* -Techniken die Abschlusscodes für Security Incidents an, die den identifizierten häufigsten Techniken in der Umgebung einer Organisation zugeordnet wurden.

Die x-Achse zeigt die häufigsten Techniken an, die für Angriffe auf das Unternehmen verwendet wurden, und die y-Achse zeigt die geschlossenen Codes.



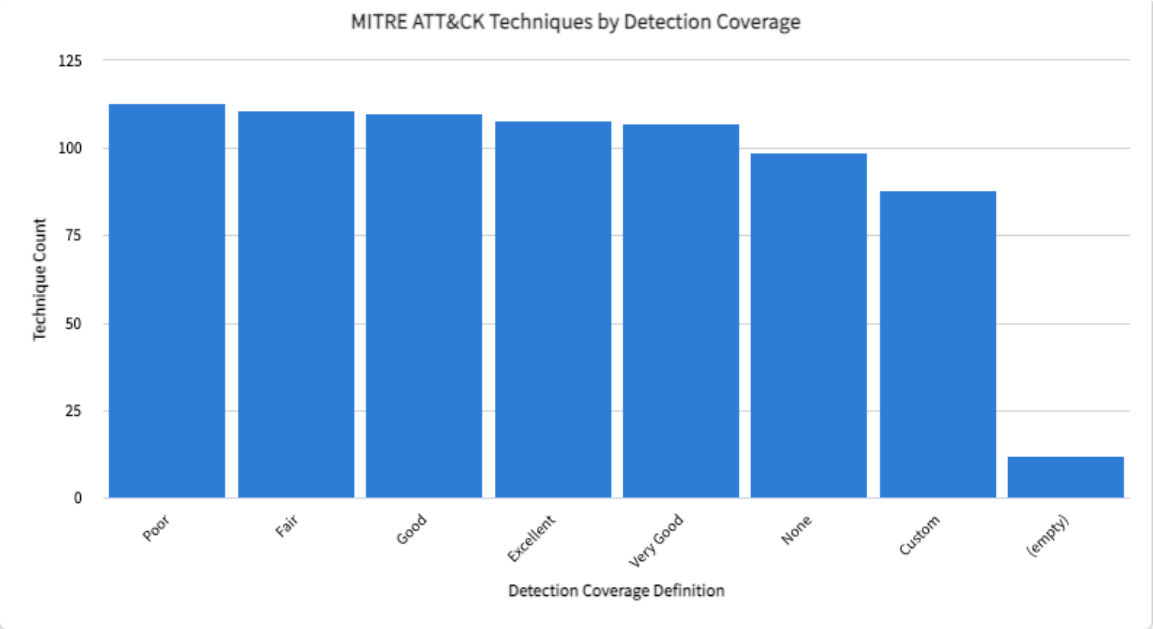

## Beispiel für die Erkennungsabdeckung nach MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **„MITRE-ATT&CK-Techniken nach Erkennungsabdeckung“** die Technikanzahl nach Erkennungsabdeckung in Ihrer Umgebung an.

Die x-Achse zeigt die Technikanzahl und die y-Achse die Erkennungsabdeckungstypen an.



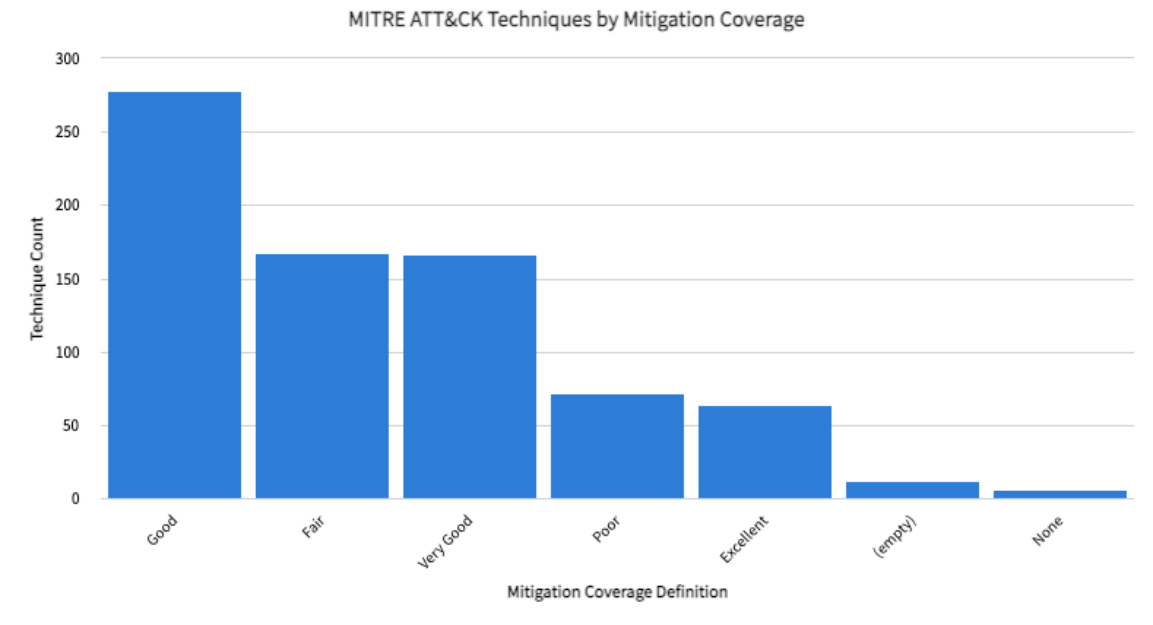
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




## Beispiel für eine Verringerungsabdeckung durch MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **„MITRE-ATT&CK-Techniken nach Mitigationsabdeckung“** die Technikanzahl nach Mitigationsabdeckung in Ihrer Umgebung an.

Die x-Achse zeigt die Technikanzahl und die y-Achse die Risikominderungsabdeckungstypen an.



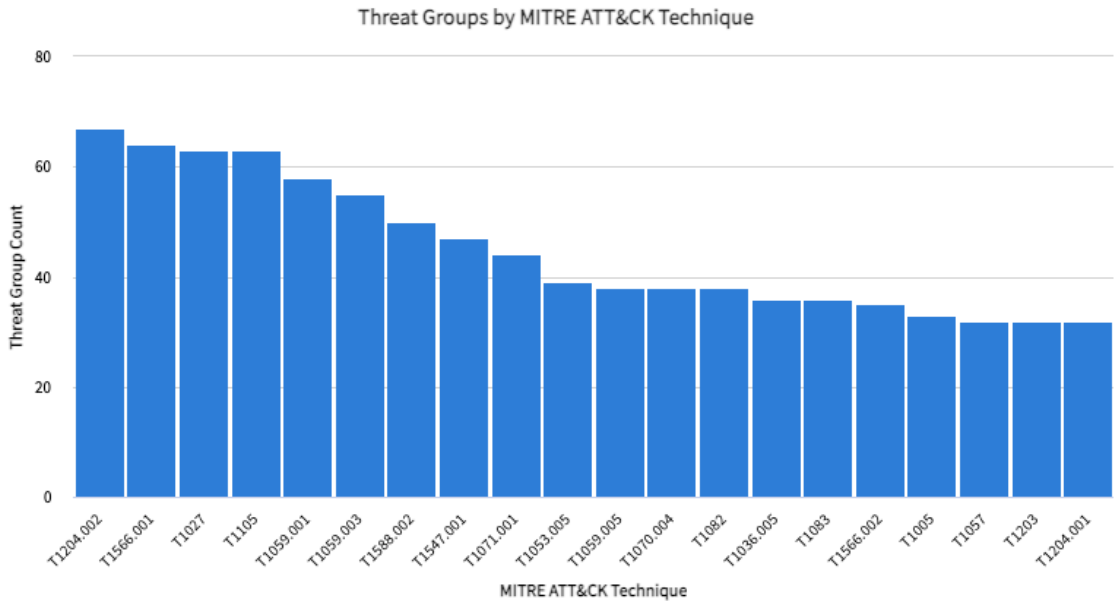

## Beispiel für Bedrohungsgruppen nach MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget „ **Bedrohungsgruppen nach MITRE-ATT&CK-Technik** “ die Techniken nach Anzahl der Bedrohungsgruppen an. Dieses Widget zeigt 20 Techniken mit der höchsten Bedrohungsgruppenanzahl an.

Die x-Achse zeigt die Anzahl der Bedrohungsgruppen und die y-Achse die MITRE-ATT&CK -Techniken an.

Automatische Übersetzung

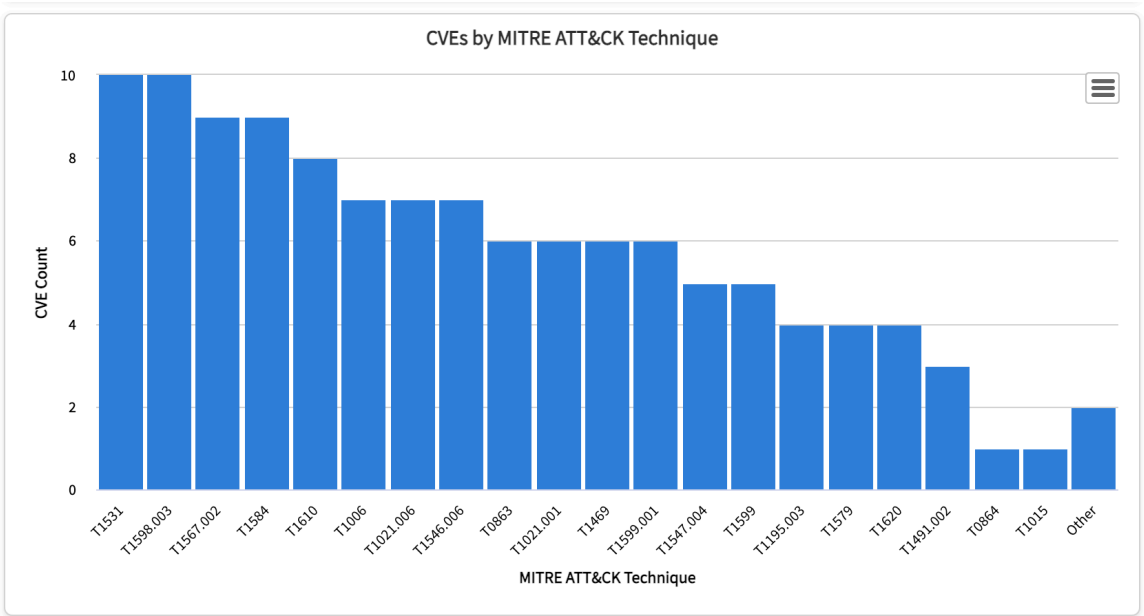
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




### Beispiel für CVEs nach MITRE-ATT&CK -Techniken

In diesem Beispiel zeigt das Widget **CVEs nach MITRE-ATT&CK-Technik** die Techniken mit der relevanten CVE-Anzahl in Ihrer Umgebung an.

Die x-Achse zeigt die relevante CVE-Anzahl und die y-Achse die MITRE-ATT&CK -Techniken an.




## Threat Intelligence – Administration

Das Threat Intelligence Basissystem ist bei der Aktivierung einsatzbereit. Sie können Datensätze zu bestimmten Modulen im Menü der Anwendung Administration hinzufügen, die meisten sind jedoch bereits mit branchenüblichen Informationen ausgefüllt.

Die folgenden Anwendungen sind im Modul „ **Administration** “ der Navigationsleiste Threat Intelligence verfügbar:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Threat Intelligence-Administrationsanwendungen

| Anwendung | Beschreibung |
|---|---|
| Eigenschaften | Threat Intelligence Mit -Eigenschaften können Sie steuern, wie verschiedene Aspekte der Systemfunktion funktionieren, einschließlich der Einstellung von API-Schlüsseln. |
| Angriffsmechanismen | Dieses Modul organisiert Angriffsmuster hierarchisch, basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle verwendet werden. |
| Angriffsmotivationen | Dieses Modul listet die möglichen Angriffsmotivationen auf, die die Stärke eines Angriffs durch einen Bedrohungsakteur oder Angriffssatz bestimmen. |
| Discovery-Methoden | In diesem Modul wird beschrieben, wie Security Incidents erkannt werden. |
| Feeds | Diese Funktion ist veraltet. |
| Indikatortypen | Dieses Modul wird verwendet, um Cyber-Bedrohungsindikatoren zu charakterisieren, die aus Mustern bestehen, die bestimmte erkennbare Bedingungen identifizieren, sowie kontextbezogene Informationen über die Bedeutung der Muster und wie und wann auf sie reagiert wird. |
| Infrastrukturtypen | Dieses Modul listet die möglichen Klassifizierungen der Infrastruktur auf. |
| Beabsichtigte Wirkungen | Diese Anwendung wird verwendet, um die beabsichtigte Wirkung eines Bedrohungsakteurs auszudrücken. |
| Malware-Fähigkeiten | Dieses Modul listet die möglichen Fähigkeiten von Malware auf. |
| Schadsoftwaretypen | Dieses Modul listet die möglichen Klassifizierungen von Malware auf. |
| Benachrichtigungen | Dieses Modul wird zum Erstellen von verwendet E-Mail-Benachrichtigungen . Dabei wird angegeben, wann sie gesendet werden, wer sie empfängt und was sie enthalten. |
| Erkennbare Typen | Dieses Modul listet die möglichen Klassifizierungen eines erkennbaren Elements auf, z. B. eine IP-Adresse oder einen Datei-Hash. |
| Berichtstypen | Dieses Modul listet die möglichen Klassifizierungen von Bedrohungsberichten auf. |
| Bedrohungsakteurrollen | In diesem Modul werden die Rollen der Bedrohungsakteure aufgelistet. |
| Bedrohungsakteurtypen | Dieses Modul charakterisiert böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich mutmaßlicher Absichten und bisher beobachtetem Verhalten. |
| Rechner für Funde der Bedrohungssuche | Dieses Modul berechnet die Ergebnisse basierend auf den erhaltenen Antworten. Bei Integrationen von Drittanbietern, die die berechneten Ergebnisse bereitstellen, ordnet der Rechner für Bedrohungssuchen die Ergebnisse den unterstützten Ergebnissen im System zu. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche. |
| Tooltypen | Dieses Modul listet die mögliche Klassifizierung von Tools auf. |

## Rechner für Funde der Bedrohungssuche

Der Rechner für die Suche nach Bedrohungen hilft Ihnen, die erkennbaren Ergebnisse basierend auf den erhaltenen Antworten zu berechnen.

Sie können einen Rechner für die Suche nach Bedrohungen für Ihre Integration erstellen und mithilfe eines Skripts bestimmen, wie Sie die verschiedenen erkennbaren Ergebnisse identifizieren möchten. Der Rechner für die Suche nach Bedrohungen enthält ein Beispielskript, das mit dem Basissystem geliefert wird. Sie können es verwenden, um die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkennbaren Ergebnisse zu identifizieren, oder Sie können dieses Skript entsprechend Ihren Anforderungen ändern.

Bei Integrationen von Drittanbietern, die die berechneten Ergebnisse bereitstellen, ordnet der Rechner für Ergebnisse der Bedrohungssuche die Ergebnisse unterstützten Ergebnissen im Basissystem zu.

### Ergebnisse der Rollup-Bedrohungssuche

Wenn Sie mehrere Ergebnisse der Bedrohungssuche für ein erkennbares Element von den verschiedenen Integrationsanbietern haben, werden die aktuellen Ergebnisse der Bedrohungssuche von allen Lieferanten berücksichtigt, und die gesamten Ergebnisse der erkennbaren Elemente werden wie folgt gekennzeichnet:

**Rollup der Ergebnisse der Bedrohungssuche**

| Letztes erkennbares Ergebnis | Gesamtergebnis des erkennbaren Elements |
|---|---|
| Böswillig | Wenn einer der Integrationsanbieter das erkennbare Element als „Böswillig“ meldet, wird die allgemeine Suche nach erkennbaren Elementen als „Böswillig“ gekennzeichnet. |
| Verdächtig | Wenn keiner der Integrationsanbieter das erkennbare Element als schädlich meldet, meldet einer von ihnen es als verdächtig, und dann wird das gesamte erkennbare Element als verdächtig markiert. |
| Clean | Wenn alle Integrationsanbieter das erkennbare Element als „sauber“ melden, wird das gesamte Ergebnis des erkennbaren Elements als „sauber“ markiert. |
| Unbekannt | Wenn keiner der Integrationsanbieter das erkennbare Element als „Böswillig“ oder „Verdächtig“ meldet und einer von ihnen es als „Unbekannt“ meldet, wird die allgemeine Suche nach erkennbaren Elementen als „Unbekannt“ markiert. |

#### Verwenden von Rechnern für Ergebnisse der Bedrohungssuche

Verwenden Sie den Rechner für die Suche nach Bedrohungen, um die erkennbaren Ergebnisse für Ihre Integration zu berechnen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.admin

**Prozedur**

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Rechner für Funde der Bedrohungssuche**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.
4. Klicken Sie auf **Aktualisieren**.

## Threat Intelligence-Integrationen

Das Basissystem von Threat Intelligence enthält Integrationen für Malware-Erkennungssoftwarepakete von Drittanbietern. Dieser Abschnitt enthält Anweisungen

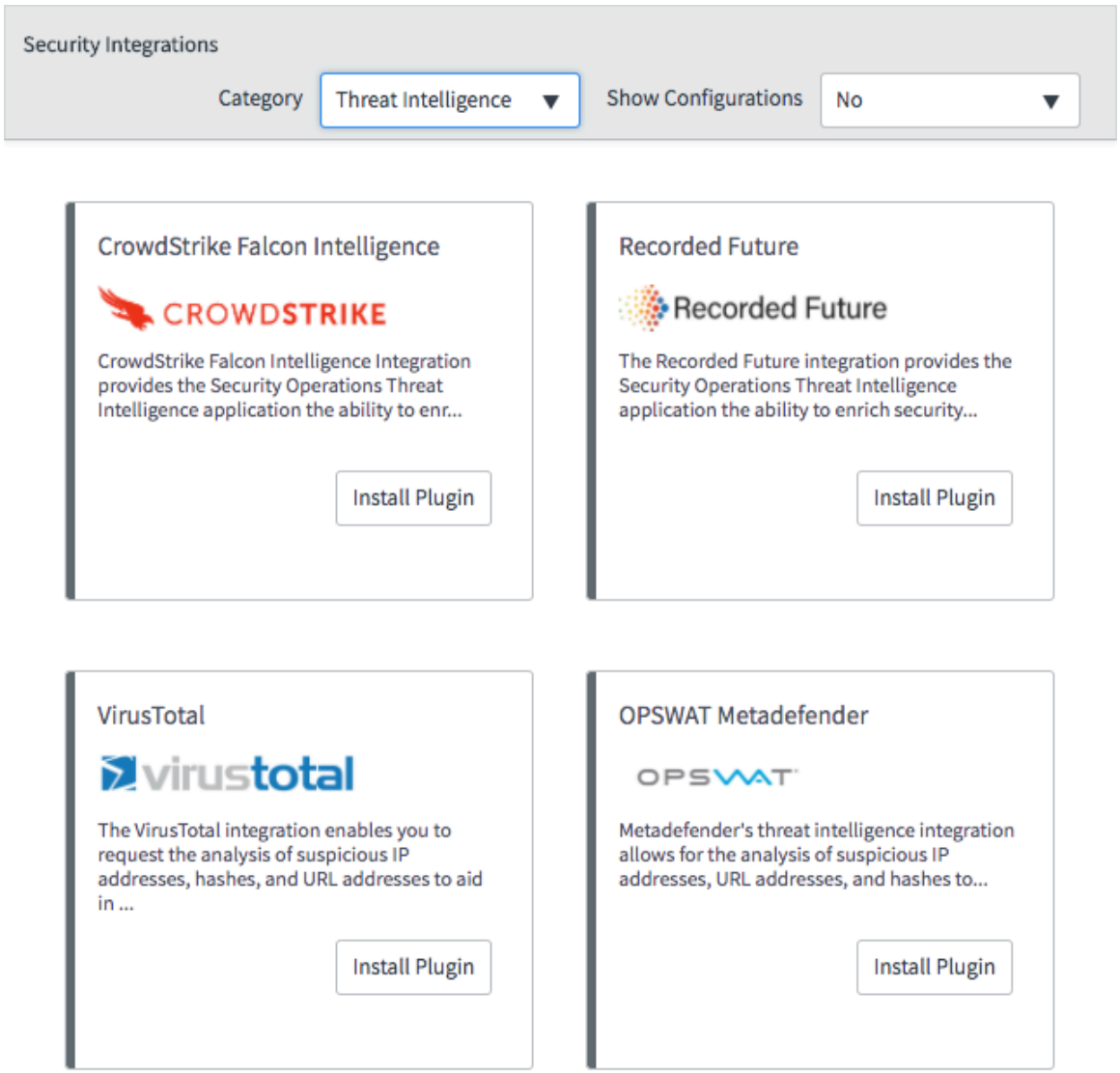
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zum Aktivieren der Plugins und zum Konfigurieren von ServiceNow und Integrationen von Drittanbietern. Außerdem sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen enthalten, die im Basissystem enthalten sind.

## Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Security Operations -Plugins aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.




Sie können die sichtbaren Integrationen mithilfe des Dropdown-Menüs „ **Kategorie** “ filtern. Im Dropdown-Menü „ **Konfigurationen** anzeigen“ können Sie mehrere Instanzen von Implementierungen anzeigen, die deren Erstellung zulassen.

## Schaltflächen auf Integrationskarten

Integrationskarten zeigen je nach aktuellem Status der Integration und Quelle der Karte unterschiedliche Schaltflächen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Schaltfläche | Beschreibung |
|---|---|
| Plugin installieren | Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren und die Integration zu aktivieren. Nach der Installation des Plugins ändert sich die Schaltfläche in **Konfigurieren**. |
| Konfigurieren | Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Für einige Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die Sie von der Website der Drittpartei-Integration erhalten haben. |
| Neu | Bei bestimmten Integrationen wie Carbon Black und IBM QRadar können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie für diese Integrationen auf **Neu**, nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die Implementierungen für die Verwendung konfigurieren. |
| Seite öffnen | Im Basissystem führt Ihre Instanz eine Abfrage an den ServiceNow Store für alle Anwendungen durch, die von Security Operations -Plugins abhängig sind. Wenn diese Anwendungen gefunden und die zugehörigen Anwendungs-Plugins aktiviert werden, werden Integrationskarten für sie mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie auf **Seite öffnen**, um auf die Website der Drittanbieteranwendung zuzugreifen und die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, ändert sich die Schaltfläche **Seite öffnen** in **Konfigurieren**. |

## CrowdStrike Falcon Intelligence-Integration

CrowdStrike Falcon Intelligence erweitert Threat Intelligence um Daten für Security Incidents und zugehörige erkennbare Elemente.

### Erkunden

- Integrationsüberblick CrowdStrike Falcon Intelligence
- Security Incident Response-Integrationen

### Einrichten

Aktivieren und konfigurieren Sie die CrowdStrike Falcon Intelligence -Integration

### Verwenden

- Suchvorgänge für erkennbare Elemente durchführen
- Workflow „Bedrohungssuche – CrowdStrike Falcon Intelligence “

### Entwickeln

- ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden

### Problembehandlung und Hilfe

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Integrationsüberblick CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence bietet Cybersicherheitsinformationen, die sich problemlos in Security Operationsintegrieren lassen.

**Hinweis:**
Das Threat Intelligence -Plugin ist erforderlich, um die CrowdStrike Falcon Intelligence -Integration zu implementieren.

### Aktivieren und konfigurieren Sie die CrowdStrike Falcon Intelligence -Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der CrowdStrike Falcon Intelligence -Integration, schnell aktivieren und einrichten. Bevor Sie CrowdStrike Falcon Intelligenceverwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen und den entsprechenden API-Schlüssel und die entsprechende ID hinzufügen.

#### Vorbereitungen
Erforderliche Rolle: admin

- Das Threat Intelligence -Plugin muss installiert und aktiviert sein, bevor Sie die CrowdStrike Falcon Intelligence -Integration verwenden können.
- Rufen Sie die API-Client-ID und den API-Clientschlüssel unter Ihrem CrowdStrike Falcon Intelligence -Profil ab.
- Wenn Sie die CrowdStrike Falcon Intelligence -Integration von einer früheren Version aktualisieren, müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die Integration unterstützt die OAuth2-Authentifizierung. Für dieses Update müssen Sie die **API-Client-ID** und den **API-Client-Secret** eingeben, um sich zu authentifizieren und die Konfiguration abzuschließen.
- Aktivieren Sie in den **API**-Bereichen des Portals CrowdStrike Falcon Intelligence die Einstellung **Lesen** für **Indikatoren (Falcon X)** oder **IoCs (Indicators of Compromise)**.

#### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie in der Karte CrowdStrike Falcon Intelligence auf **Konfigurieren**.
4. Füllen Sie die Felder im Formular aus, um die Konfiguration abzuschließen:

**CrowdStrike Falcon Intelligence Konfiguration**

| Feld | Beschreibung |
|---|---|
| **Name** | Name der Integration, z. B. `demo-1`. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| **API-Client-ID** | Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils im CrowdStrike Falcon Intelligence -Portal erhalten. |
| **API-Client-Geheimnis** | Geheimer Clientschlüssel, den Sie aus dem Einstellungsabschnitt Ihres Kontoprofils im CrowdStrike Falcon Intelligence -Portal erhalten. |

5. Klicken Sie auf **Absenden**.

## Ergebnisse

Nach der Konfiguration kann CrowdStrike Falcon Intelligence für die Suche nach erkennbaren Elementen in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

### Zugehörige Informationen

Suchvorgänge für erkennbare Elemente durchführen

### Workflow „Bedrohungssuche – CrowdStrike Falcon Intelligence “

Der Workflow „Bedrohungssuche – CrowdStrike Falcon Intelligence “ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen um einen von CrowdStrike Falcon Intelligenceerkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

## Vorbereitungen

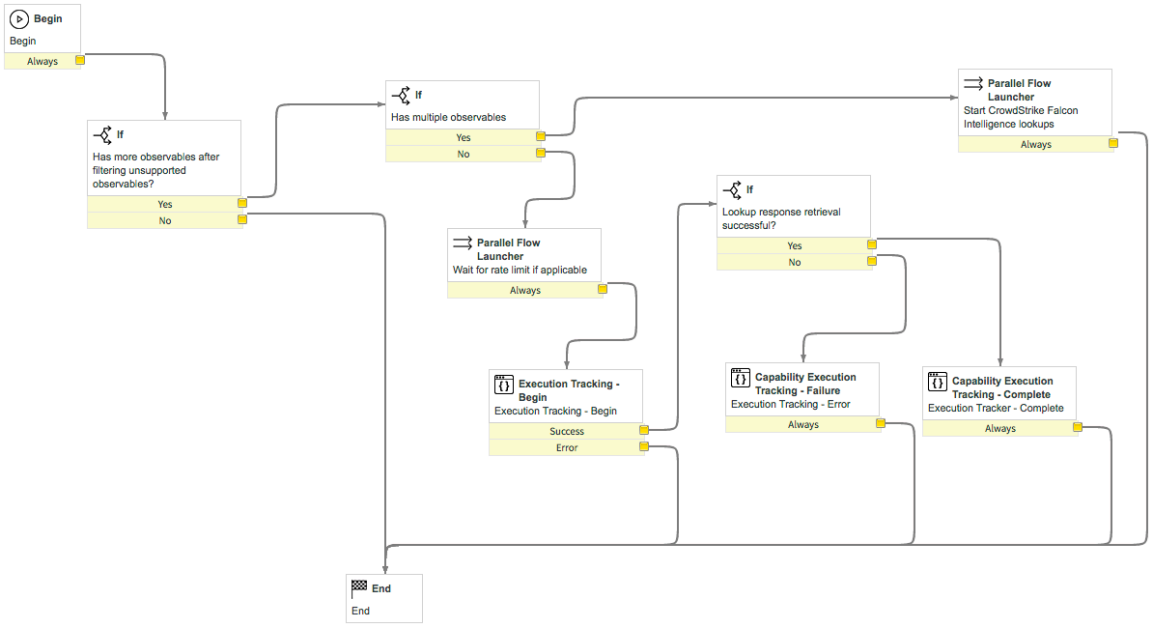
Erforderliche Rolle: admin

## Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird von Security Operations-Integration – Funktion „Bedrohungssuche“. ausgelöst, wenn Sie ein oder mehrere erkennbare Elemente in einer Beobachtungsliste veröffentlichen und die CrowdStrike Falcon Intelligence-Implementierung ausgewählt ist. Nach der Veröffentlichung können die Beobachtungslisten in der CrowdStrike Falcon Host-Software angezeigt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Weitere Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## Integration „Have I Been Pwned?“

Mit der Security Operations Have I Been Pwned? -Integration können Sie Suchvorgänge für Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob die personenbezogenen Daten von Benutzern durch Datenschutzverletzungen gefährdet wurden.

| | |
|---|---|
| **Erkunden**<br>Security Incident Response-Integrationen | **Einrichten**<br>• Setup der Integration mit Security Operations Have I Been Pwned? .<br>• Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? . |
| **Verwenden**<br>Suchvorgänge für erkennbare Elemente durchführen<br>Workflow „Bedrohungssuche – Have I Been Pwned? “ | **Entwickeln**<br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| **Problembehandlung und Hilfe** | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlerbehebung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### Setup der Integration mit Security Operations Have I Been Pwned? .

Have I Been Pwned? ist eine kostenlose Ressource, die verwendet wird, um zu bewerten, ob jemand gefährdet wurde, weil sein Online-Konto bei einer Datenschutzverletzung gefährdet oder „pwned“ war. Die Integration mit Security Operationsist problemlos möglich.

Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509 SSL-Zertifizierung aktualisieren.

Die Plugins Security Incident Response, Threat Intelligenceund Security Operations Have I Been Pwned? sind erforderlich, um die Integration von Security Operations Have I Been Pwned? zu implementieren.

### Aktivieren Sie die Integration mit Security Operations Have I Been Pwned? .

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der Security Operations Have I Been Pwned? -Integration, schnell aktivieren und einrichten. Bevor Sie die Have I Been Pwned? -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

#### Vorbereitungen

- Das Threat Intelligence -Plugin muss installiert und aktiviert sein, bevor Sie die Security Operations Have I Been Pwned? -Integration verwenden können.

Erforderliche Rolle: sn_si_admin

#### Prozedur

Laden Sie die Integration aus dem herunter ServiceNow Store.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? kann jetzt für Suchvorgänge für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

**Zugehörige Informationen**

Suchvorgänge für erkennbare Elemente durchführen

### Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie für die Integration eine SSL-Verbindung benötigen, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

#### Vorbereitungen

Erforderliche Rolle: admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie in der Adresszeile auf das Sperrsymbol.

   c. Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
   Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu**, und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

**Hinweis:**
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .



## Workflow „Bedrohungssuche – Have I Been Pwned? “

Der Workflow „Bedrohungssuche – Have I Been Pwned? “ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen um einen von Have I Been Pwned?erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

### Vorbereitungen

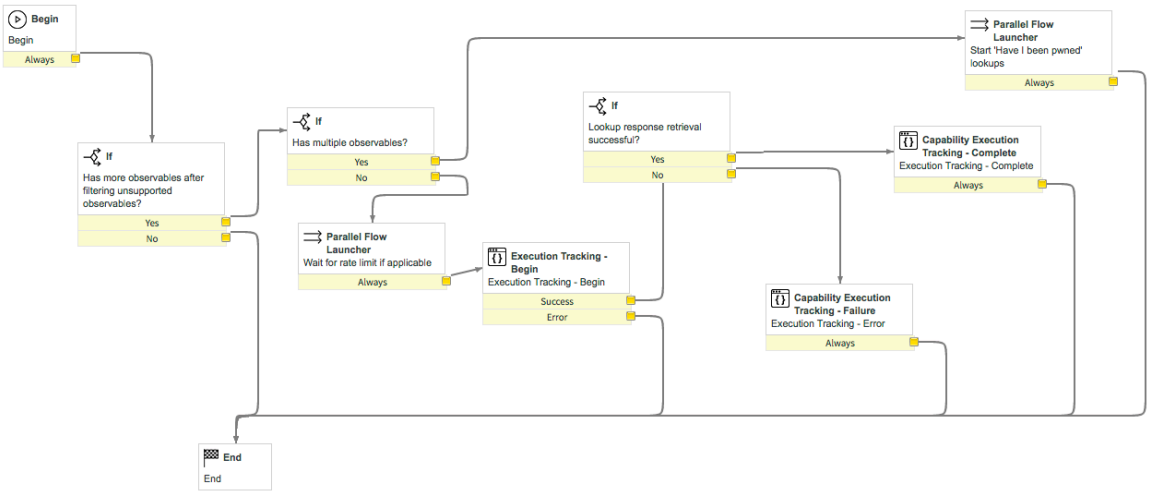
Erforderliche Rolle: sn_si_admin

### Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird von Security Operations-Integration – Funktion „Bedrohungssuche“. ausgelöst, wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Implementierung von Have I Been Pwned? ausgewählt ist. Weitere Informationen finden Sie unter Suchvorgänge für erkennbare Elemente durchführen.




Weitere Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## MISP integration for Security Operations

Mit MISP integration for Security Operationskönnen Sie Security Incidents mit Sichtungssuchen, Ergänzung erkennbarer Elemente untersuchen und Events in MISPerstellen oder aktualisieren. Mit MISPkönnen Sie gezielte Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der Falschmeldungen in Ihrer Umgebung reduzieren.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

## MISP-Übersicht

MISP, was für Malware Information Sharing Platformsteht, ermöglicht Ihnen den Austausch und die gemeinsame Nutzung von Bedrohungsdaten und Gefährdungsindikatoren (Indicators of Compromise, IoCs) über die anvisierte Malware und Angriffe innerhalb Ihrer Community vertrauenswürdiger Mitglieder. Sie können MISP Informationen auch für private oder offene Communities freigeben. Durch den Austausch von MISP Informationen können Sie gezielte Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der Falschmeldungen in Ihrer Umgebung reduzieren.

## MISP und Security Operations

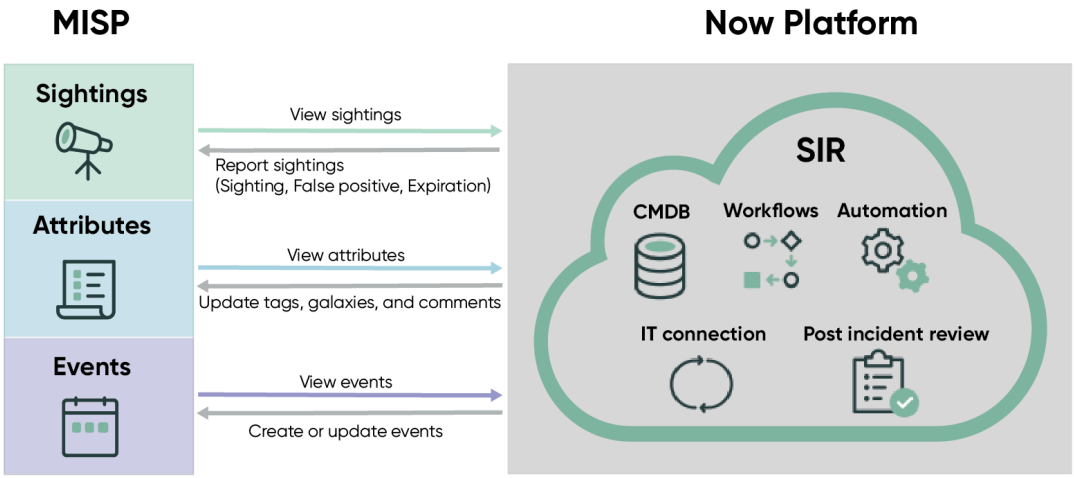
Im folgenden Beispiel erfahren Sie, wie die Informationen MISP mit Security Operations-Anwendungen fließen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Übersicht über MISP und Security Operations**

# Now Platform - MISP integration overview




## Schlüsselfunktionen

Diese Integration umfasst die MISP folgenden Funktionen:

- Stellen Sie eine Verbindung zu privat und öffentlich her MISP instances.
- Unterstützt die manuelle und automatische Sichtungssuche von erkennbaren Elementen.
- Führen Sie eine Sichtungssuche über die Fallverwaltung aus.
- Sichtungen für ein Attribut melden oder aktualisieren:
  - Erkennbares Element als Sichtung melden (global)
  - Erkennbares Element als falsch positiv melden (global)
  - Melden Sie ein erkennbares Element als abgelaufen
- Unterstützt die manuelle und automatische Ergänzung erkennbarer Elemente. Die Ergebnisse umfassen das Attribut MISP und Event-Informationen, die den erkennbaren Elementen zugeordnet sind.
- Attributanreicherung in MISP, einschließlich Hinzufügen oder Aktualisieren von Tags, Galaxienoder Kommentaren.
- Event-Erstellung in MISP von SIR: Unterstützt die manuelle und die automatische Erstellung von Events in MISP aus SIR.
- Aktualisieren Sie ein MISP -Ereignis aus SIR, einschließlich Hinzufügen oder Aktualisieren von Tags, Galaxienoder Attributen.
- Fügen Sie einem Security Incident zugeordnete erkennbare Elemente als Attribute hinzu MISP event.
- Automatisch extrahieren MITRE-ATT&CK™ Informationen aus MISP attributes und ordnen die Informationen SIR Security Incidents zu.
- Automatisch hinzufügen SIR MITRE-ATT&CK™ Informationen als Galaxien zu einem MISP event.

## Schlüsselkonzepte

Diese Integration umfasst die folgenden Schlüsselkonzepte, die Sie kennen müssen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MISP ist eine Threat Intelligence-Plattform (TIP). Sie verwenden TIPs, um Sicherheitsbedrohungsdaten in Echtzeit zu sammeln, zu korrelieren, zu kategorisieren, freizugeben und zu integrieren, um die Priorisierung von Aktionen und die Verhinderung, Erkennung und Reaktion von Angriffen zu unterstützen.
- MISP ist ein Threat Intelligence Management (TIM). Sie verwenden TIMs, um Bedrohungsdaten durch Kontext in Threat Intelligence umzuwandeln und Bedrohungen automatisch nach benutzerdefinierter Bewertung und Relevanz zu priorisieren.
- MISP Datenebene
  - Events sind Einkapselungen für kontextbezogene Informationen.
  - Attribute sind einzelne Datenpunkte, die Indikatoren oder Unterstützungsdaten sein können.
  - Objekte sind benutzerdefinierte Vorlagenattributkompositionen.
  - Objektreferenzen sind die Beziehungen zwischen den anderen Bausteinen.
  - Sichtungen sind zeitspezifische Vorkommen eines erkannten Datenpunkts.
- MISP Kontextebene
  - Tags sind Bezeichnungen, die an Events oder Attribute angehängt werden und aus Taxonomien stammen können.
  - Galaxiencluster sind Knowledge Base-Elemente, mit denen Sie Events oder Attribute kennzeichnen können, die aus Galaxien stammen.
  - Clusterbeziehungen bezeichnen vordefinierte Beziehungen zwischen Clustern.
- Indikatoren enthalten ein Muster, mit dem Sie verdächtige oder böswillige Cyberaktivitäten erkennen können.
- Attribute in MISP können Netzwerkindikatoren (IP-Adresse), Systemindikatoren (eine Zeichenfolge im Speicher) oder sogar Bankkontodetails sein. Die Attribute in MISP werden in anderen SIEMs oder Formaten wie STIXals erkennbare Elemente bezeichnet.
  - Ein Typ beschreibt das Attribut. Zum Beispiel MD5 oder eine URL.
  - Die Attributkategorie beschreibt ein Attribut. Zum Beispiel eine Nutzlastbereitstellung.
  - Ein IDS-Tag bestimmt, ob ein Attribut automatisch für die Erkennung verwendet werden kann.

**Hinweis:**
Weitere Informationen zu MISP -Konzepten finden Sie auf der MISP-Dokumentationswebsite

## Wie Ihre Organisation von profitieren kann MISP integration for Security Operations

Sicherheitsanalysten müssen ein Situationsbewusstsein für die Bedrohungslandschaft entwickeln und aufrechterhalten, was bedeutet, dass sie eine überwältigende Menge an Bedrohungsdaten manuell konsolidieren und integrieren müssen. Das Sammeln, Konsolidieren und Integrieren dieser Daten nimmt wertvolle Zeit in Anspruch, was die Erkennung und Analyse von Bedrohungen verlangsamt. MISP integration for Security Operations ermöglicht es Analysten, mehr Bedrohungen zu erkennen und schneller zu reagieren, indem MISP Security Intelligence in eine vorhandene Now Platform -Instanz integriert wird.

Mit MISP integration for Security Operationskann Ihre Organisation die folgenden Aktionen ausführen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ermöglichen Sie Ihren Sicherheitsanalysten, schnell und mit dem richtigen Kontext zu reagieren.
- Verbessern Sie die Effizienz Ihres Sicherheitsteams, indem Sie die Incident-Workflows zur Erkennung und Eindämmung von Bedrohungen automatisieren.
- Reduzieren Sie die Zeit für manuelle Untersuchungen, und ermöglichen Sie Sicherheitsanalysten, Indikatoren innerhalb von Now Platformzu operationalisieren und zu kuratieren.

## Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| MISP -Dokumentationswebsite | MISP-Dokumentationswebsite |
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |

### MISP – Administration

Sie können die MISP -Integration in Now Platform einrichten, um eine Sichtungssuche und Ergänzung erkennbarer Elemente durchzuführen und Events in MISPzu erstellen und zu aktualisieren.

### Erste Schritte mit MISP integration for Security Operations

Überprüfen Sie die folgenden Informationen, bevor Sie MISP integration for Security Operationseinrichten.

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform, Threat Intelligenceund Security Incident Response zugewiesen haben. | Die folgenden Rollen werden für alle MISP -Funktionen in Now Platformverwendet:<br>• Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow Store und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu.<br>• sn_si.admin und sn_ti.admin können die Integration konfigurieren und die automatischen MISP Event-Erstellungsprofile einrichten.<br>• sn_sec_misp.write – Die Analystrolle MISP verfügt über Lese- und Schreibberechtigungen für Daten von MISP, einschließlich Event- und Attributdaten.<br><br>Weitere Informationen finden Sie unter Threat Intelligence einrichten. |
| Weisen Sie die erforderlichen MISP Benutzerrollen zu. | Überprüfen Sie die MISP Benutzerrollen und Berechtigungen, die für die Verwendung der |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| | erforderlich sind MISP integration for Security Operations.<br><br>**Hinweis:**<br>Weitere Informationen zu den Benutzerrollen in MISPfinden Sie im Abschnitt „Rollen“ auf der MISP-Dokumentationswebsite . |
| Vergewissern Sie sich, dass Sie MISP Version 2.4.137 oder höher verwenden. | MISP integration for Security Operations wird mit einem Minimum getestet MISP Version 2.4.137 . |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung des Moduls MISP erforderlich sind, installiert und aktiviert sind. | Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten.<br>• Security Incident Response<br>• ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime)<br>• ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)<br><br>Weitere Informationen zum Einrichten Ihrer Now Platform -Instanz für die Integration finden Sie unter Berechtigungen für Security Operations-Produkte oder -Anwendungen anfordern und ServiceNow Store-Anwendungen aktivieren. |
| Domänentrennung | Überprüfen Sie den Abschnitt zur Domänentrennung, wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten. |

### MISP Benutzerrollen und Berechtigungen

Überprüfen Sie die Benutzerrollen, die in der MISP integration for Security Operations -Integration erforderlich sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergänzung erkennbarer Elemente und Sichtungssuchberechtigungen

**Hinweis:**

- *Alle* **ServiceNow** *MISP-Integrationsfunktionen benötigen die grundlegenden Berechtigungen zum* **Verwalten von Organisationsereignissen** *und* **Auth-Schlüsselzugriff**. *Stellen Sie sicher, dass Sie über diese grundlegenden Berechtigungen verfügen, bevor Sie fortfahren.*
- *Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert, zur Hostorganisation des entsprechenden MISP-Servers gehören.*

| MISP-Fähigkeit | Tagger | Tag-Editor |
|---|---|---|
| Ergänzung erkennbarer Elemente (schreibgeschützt) | # | # |
| Sichtungssuche (schreibgeschützt) | # | # |

### Sichtungsberechtigungen melden

| MISP-Fähigkeit | Sichtungsersteller |
|---|---|
| Sichtung melden | # |

### Attribut- und Ereignisberechtigungen

| MISP-Fähigkeit | Tagger | Tag-Editor |
|---|---|---|
| Bearbeiten Sie Event-/Attribut-Tags | # | # |
| Event-/Attribut-Galaxien bearbeiten | # | # |
| Bearbeiten Sie Attributkommentare | # | # |
| Fügen Sie dem Event ein neues Attribut hinzu | # | # |
| Erstellen Sie ein Event in MISP | # | # |



### Installieren und konfigurieren Sie MISP integration for Security Operations

Installieren und konfigurieren Sie MISP integration for Security Operations aus ServiceNow Store in Ihrer Instanz von Now Platform, damit Sie Security Incidents mit den Daten von MISP untersuchen können.

**Vorbereitungen**

Stellen Sie sicher, dass Sie die gültigen SSL-Zertifikate auf dem MISP-Server installiert haben.

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Laden Sie MISP integration for Security Operations aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel MISP- SIR/TI-Integration, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

**MISP Formular „SIR/TI-Integrationskonfiguration“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die MISP Instanzkonfiguration . |
| MISP Server-URL | URL für den Server MISP, der als REST-Endpunkt für den Server MISP ] dient |
| API-Schlüssel | API-Schlüssel, der für Ihren Benutzeraccount auf dem Server MISP konfiguriert ist Der API-Schlüssel entspricht dem **Authkey** auf dem MISP -Server. |
| Lokale Bereitstellung | Option, die Sie auswählen können, wenn Ihr MISP -Server in einer lokalen Instanz bereitgestellt wird. Wenn Sie die Option **Lokale Bereitstellung** auswählen, müssen Sie MID-Server verwenden, um eine Verbindung zum Server MISP herzustellen. |
| MID-Anwendung | Zeichenfolgenfeld, das den MID-Anwendungsnamen angibt, der für die Kommunikation mit MISPverwendet wird.<br><br>Dieses Feld ist erforderlich, wenn Sie die Option **Bereitstellung** vor Ort auswählen. Informationen zum Konfigurieren des MID Servers für Ihre Anwendung finden Sie unter MID Server für jede Anwendung konfigurieren |

5. Klicken Sie auf **Absenden**.

### Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird MISP - SIR/TI-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

## Überprüfen Sie die Integrationseinstellungen von MISP .

Überprüfen Sie die Einstellungen MISP integration for Security Operations, und ändern Sie die Standardsystemeigenschaften entsprechend Ihrer Umgebung.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Integrationseinstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MISP-Integrationseinstellungen

| Eigenschaftsname | | Beschreibung |
|---|---|---|
| Anreicherung erkennbarer Elemente | Zeit (in Stunden), bevor neue Daten abgerufen werden | Zeit in Stunden, bevor Sie neue Daten abrufen können.<br>Typ: Ganzzahl<br>Standardwert: 24 |
| Sichtungssuche | Führt automatisch eine Sichtungssuche aus, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden | Sichtungssuche, die immer dann ausgeführt wird, wenn ein neues erkennbares Element einem Security Incident zugeordnet wird.<br>Standardwert: Ja |
| | Suchintervall (in Tagen) für die Sichtungssuche in MISP | Anzahl der Tage, an denen die Sichtungssuchdaten in MISPdurchsucht werden. Verwenden Sie diese Option nur für die automatische Sichtungssuchfunktion.<br>Standardwert: 90 |
| Datensynchronisierung | Intervall (in Minuten) für Tags, die abgerufen und mit MISP synchronisiert werden sollen | MISP -Tags, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten in Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert.<br>Standardwert: 1440 (Minuten oder 24 Stunden) |
| | Intervall (in Minuten) zum Aktualisieren von MISP-Galaxien aus konfigurierten Quellen | MISP Galaxien, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten in Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert.<br>Standardwert: 1440 (Minuten oder 24 Stunden) |
| | Intervall (in Minuten) für Organisationen, die abgerufen und | MISP -Organisationen, die zum Zeitpunkt der Integrationskonfiguration |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Eigenschaftsname | | Beschreibung |
|---|---|---|
| | mit MISP synchronisiert werden sollen | abgerufen werden. Nachdem sich die Daten in Now Platformbefinden, definiert diese Eigenschaft die Häufigkeit, mit der die Daten mit dem Server MISP synchronisiert werden. Der Wert wird in Minuten definiert.<br><br>Standardwert: 1440 (Minuten oder 24 Stunden) |
| MITRE™ Technikextraktion | Führen Sie einen Rollup von MITRE-ATT&CK Techniken automatisch aus den Ergebnissen der Anreicherung erkennbarer MISP-Elemente (Tags) in Security Incidents durch | Rollup von MITRE-ATT&CK Informationen aus MISP Ergänzungsergebnissen erkennbarer Elemente (Tags) zum Security Incident<br><br>Standardwert: Ja |
| | Führen Sie einen Rollup von MITRE-ATT&CK Techniken automatisch aus den Ergebnissen der Ergänzung erkennbarer MISP-Elemente (Galaxien) in Security Incidents durch | Rollup von MITRE-ATT&CK Informationen aus den MISP Ergänzungsergebnissen erkennbarer Elemente (Galaxien) zum Security Incident<br><br>Standardwert: Ja |

**Hinweis:**

- Um die Extraktionsfunktionen der Technik [ MITRE™ in MISPzu verwenden, müssen Sie Aktivieren Sie die MITRE-ATT&CK -Funktion in Threat Intelligence -Modul.
- Mit MISP integration for Security Operations werden zwei Extraktionsregeln für die Basissystem-[ MITRE-ATT&CK -Technik für die Tags MISP - MISP Galaxien und MISP eingeführt. Weitere Informationen zu Regeln für die automatische Extraktion in MITRE-ATT&CKfinden Sie unter Technikregeln für automatische Extraktion zum Importieren von MITRE-ATT&CK-Informationen.

3. Klicken Sie auf **Speichern**.

### Ergebnisse

Ihre geänderten Integrationseinstellungen werden gespeichert und angewendet.

#### Konfigurieren Sie MISP Sichtungssuchen

Konfigurieren Sie Now Platform, um Sichtungssuchen nach erkennbaren Elementen in der Instanz MISP durchzuführen. Mit diesen Informationen können Sie bestimmen, wie oft Bedrohungen auftreten.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen , die für die Verwendung der bidirektionalen Funktionen von MISP erforderlich sind.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Der Workflow „Security Operations Integration - Sichtungssuche“ führt die Sichtungssuchen aus. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchvorgänge aus, die auf dem konfigurierten Workflow basieren.

MISP integration for Security Operations bietet ein Basissystem-Sichtungssuchprofil, mit dem Sie automatische Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen für erkennbare Elemente einer Organisation zugreifen und auch die externen Sichtungen anderer Organisationen anzeigen.

### Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Sichtungssuche: Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Sichtungssuchkonfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name für das Fähigkeitsprofil. |
| Ist gespeicherte Suche | Suchkonfiguration, die gespeichert wird, wenn Sie diese Option auswählen. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und nach Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen. |
| Sichtungssuchquelle | Quelle für die Sichtungssuche. Wählen Sie den Protokollspeicher MISP als Quelle aus. |
| Aktiv | Option, die die gespeicherte Suchkonfiguration aktiviert. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen. |
| Erkennbarer Typ | Typ des erkennbaren Elements, z. B. IP-Adresse, Hash-Wert, URL und Domänenname. |
| Maximales erkennbares Element pro Suche | Maximale Anzahl von erkennbaren Elementen, die Sie in einer Suchabfrage anzeigen können. |
| Suchen | Standardsuchzeichenfolge, die `$(observable)` ist. Sie definieren jedoch Ihre eigene Suchabfrage, indem Sie die unterstützten Parameter des Protokollspeichers MISP angeben. |

4. Klicken Sie auf **Absenden**.

### Ergebnisse

Sie haben ein MISP Sichtungssuchkonfigurationsprofil erstellt.

#### Konfigurieren Sie, wie ein automatisches Event erstellt wird

Konfigurieren Sie Now Platform, um automatisch Events in MISP] zu erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen , die für die Verwendung der bidirektionalen Funktionen von MISP erforderlich sind.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin

### Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Namensformular**

| Feld | Beschreibung |
|---|---|
| Name | Name des Profils für die automatische Event-Erstellung. |
| Beschreibung | Kurze Beschreibung des Profils. Eine detailliertere Beschreibung wird über die Attribute in der nächsten Phase der Event-Erstellung geteilt. |
| Bestellung | Reihenfolge des Profils, wenn die Auslöserbedingungen erfüllt sind. Der Standardwert ist 100. Belassen Sie diese Einstellung auf der Standardeinstellung.<br><br>Wenn Sie mehrere Profile erstellen, stellt dieser Wert eine Ausführungszeitpriorität bereit, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam nutzen. Das Profil mit der niedrigsten Nummer hat die höchste Priorität. |
| Quelle | MISP Quelle für die Event-Erstellung. |
| Aktiv | Option, die angibt, ob das Profil aktiv oder inaktiv ist. Die Option ist standardmäßig deaktiviert, um anzuzeigen, dass das Profil deaktiviert ist.<br><br>Dieses Profil ist erst aktiv, wenn Sie alle Profilkonfigurationsschritte abgeschlossen und auf Fertigstellen **geklickt**haben. |

4. Klicken Sie auf **Fortsetzen**.

#### Konfigurieren Sie Bedingungen für Event-Auslöser

Konfigurieren Sie die Event-Auslöserbedingungen in Now Platform, damit Sie automatisch ein Event in MISP auslösen können, wenn die Bedingungen erfüllt sind.

### Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Füllen Sie im Formular „Auslöserbedingungen“ die Details aus, die ein Event auslösen können. Sie können eine zusammengesetzte Logik erstellen, indem Sie die Auslösebedingungen angeben, die auf Security Incident-Feldern oder erkennbaren Feldern basieren. Sie können Events auch in MISP erstellen, wenn für erkennbare Elemente kein entsprechendes Event in MISPvorhanden ist. Sie können eine zusammengesetzte Logik erstellen, indem Sie eine Kombination der drei Auslösebedingungen verwenden: Auslöser basierend auf Security Incident-Feldern, Auslöser basierend auf erkennbaren Feldern und MISP-Ereignis erstellen, wenn ein erkennbares Element keine entsprechenden Ereignisse in MISP aufweist. Wenn Sie mehrere Auslöser auswählen, können Sie sie mithilfe der UND-Bedingung verbinden. Erwägen Sie die Erstellung eines Profils mit neuen Bedingungen, wenn Sie die ODER-Bedingung verwenden müssen.

### Formular „Event-Auslöserbedingungen“

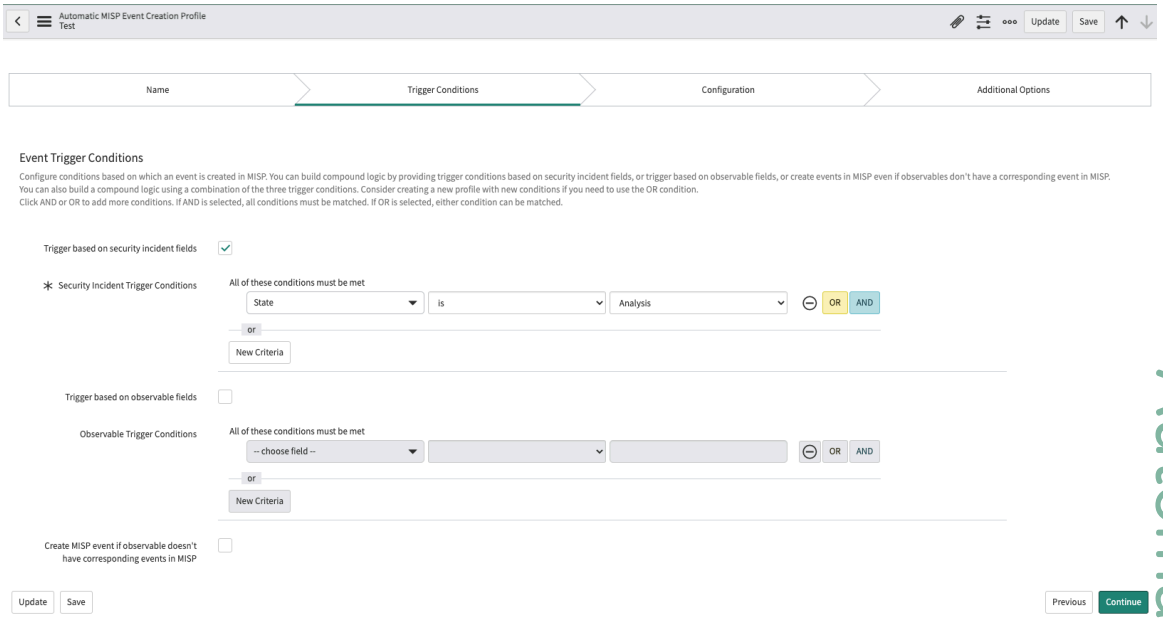
| Feld | Beschreibung |
|---|---|
| Auslöser basierend auf Security Incident-Feldern | MISP Event, das Sie erstellen können, wenn alle Auslösebedingungen für Security Incidents erfüllt sind. |
| Auslösebedingungen für Security Incident | Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder ODER. Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn OR ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. |
| Auslöser basierend auf erkennbaren Feldern | MISP Ereignis, das Sie erstellen können, wenn alle Auslöserbedingungen für erkennbare Elemente erfüllt sind. |
| Auslösebedingungen für erkennbare Elemente | Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder ODER. Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn OR ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. |
| Erstellen Sie ein MISP-Ereignis, wenn das erkennbare Element keine entsprechenden Ereignisse in MISP enthält. | MISP Event, das Sie erstellen können, wenn ein erkennbares Element keine entsprechenden Events in MISPhat. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Bedingungen für Event-Auslöser

Das folgende Beispiel zeigt die Bedingungen für Event-Auslöser beim Einrichten des Event-Erstellungsprofils MISP.




**2.** Klicken Sie auf **Fortsetzen**.

### Ordnen Sie die Event-Felder MISP zu

Ordnen Sie die MISP -Ereignisfelder in Now Platform zu, damit Security Incident-Informationen verfügbar sind, wenn MISP -Ereignisse erstellt werden.

## Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

## Prozedur

**1.** Füllen Sie die Felder des Formulars aus.

**Formular „Standardmäßige MISP-Event-Feldzuordnung“.**

| Feld | Beschreibung |
|---|---|
| Information zum Ereignis | Ereignisinformationen, die automatisch aus Now Platform Security Incident Responseerstellt werden.<br><br>Das Feld **Event** -Informationen unterstützt Substitutionsvariablen durch Verwendung von ${SIR FIELD LABEL}$. Während der Event-Erstellung werden diese Variablen durch die tatsächlichen Security Incident-Feldwerte ersetzt. Die Substitutionsvariable ${URL}$ wird durch die URL des Security Incident ersetzt. |
| Verteilung | Option, die steuert, wer dieses Event anzeigen kann, nachdem das Event veröffentlicht wurde. Diese |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Option steuert auch, ob das Event mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt, und die restriktivste Einstellung hat Vorrang. Die Verteilungsoptionen lauten wie folgt:<br>○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Event anzuzeigen. Das Event kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, wo nur Ihre Organisation Zugriff hat, um es anzuzeigen. Events mit dieser Einstellung werden nicht synchronisiert.<br>○ Nur diese Community: Ermöglicht Benutzern, die Teil Ihrer MISP Community sind, das Event anzuzeigen, einschließlich Ihrer eigenen Organisation, Organisationen auf diesem MISP Server und Organisationen, die MISP Server ausführen, die mit diesem Server synchronisieren. Alle anderen Organisationen, die eine Verbindung zu Ihren verknüpften Servern herstellen, können das Event nicht anzeigen.<br>○ Verbundene Communitys: Ermöglicht Benutzern, die Teil Ihrer MISP -Community sind, das Event anzuzeigen, einschließlich aller Organisationen auf diesem MISP -Server, aller Organisationen auf den MISP -Servern, die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen , der zwei Hops entfernt ist. Alle anderen Organisationen, die mit den verknüpften Servern verbunden sind, die zwei Hops entfernt sind, können das Event nicht anzeigen.<br>○ Alle Communitys: Gibt das Event für alle MISP Communities frei. |
| Bedrohungsstufe | Feld, das die Risikostufe des Ereignisse angibt. Sie können Incidents in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) kategorisieren. Dieses Feld kann auch als undefiniert belassen werden. Im Folgenden sind die Optionen aufgeführt: |

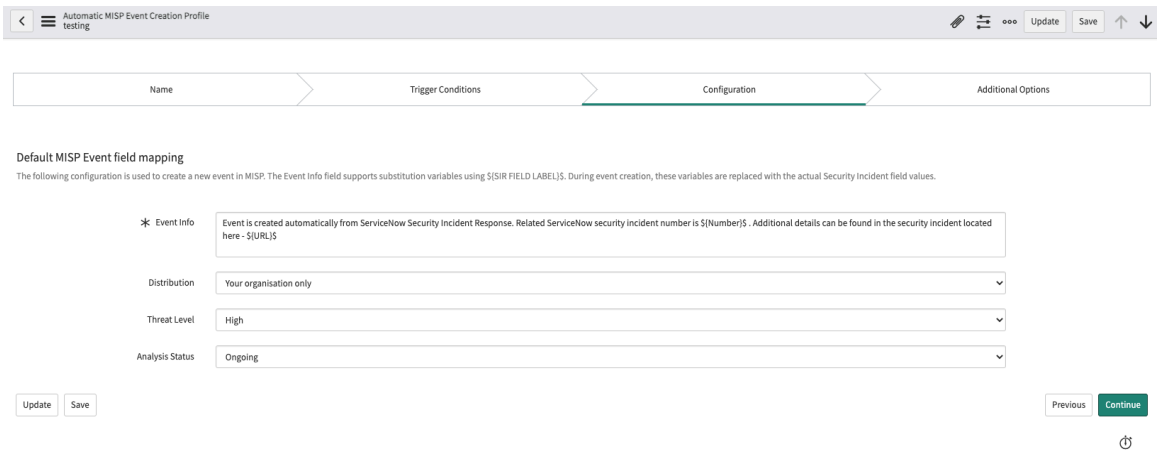


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ Niedrig: Allgemeine Massen-Malware<br>○ Mittel: Advanced Persistent Threats (APT)<br>○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe |
| Analysestatus | Aktuelle Phase der Analyse für das Event mit den folgenden möglichen Optionen:<br>○ Anfänglich: Die Analyse beginnt gerade<br>○ Laufend: Die Analyse wird ausgeführt<br>○ Abgeschlossen: Die Analyse ist abgeschlossen |

Das folgende Beispiel zeigt das Formular, das Sie zum Erstellen eines Events in MISP verwenden können.

**Standardmäßige MISP-Ereignisfeldzuordnung**




2. Klicken Sie auf **Fortsetzen**.

## Ordnen Sie SIR erkennbare Elemente als Attribute zu Ereignissen von MISP zu, oder ordnen Sie sie zu

Ordnen Sie die erkennbaren Typen Security Incident ResponseMISP den Attributtypen [] zu, da die Attributtypen MISP und die erkennbaren Elemente SIR unterschiedlich sein können.

### Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

### Warum und wann dieser Vorgang ausgeführt wird

MISP integration for Security Operations stellt eine Basissystemzuordnung bereit, die Sie verwenden, wenn Sie SIR erkennbare Elemente als Attribute zu einem MISP -Event hinzufügen.

Sie können die Basissystemzuordnung an Ihre Umgebung anpassen. Sie können beispielsweise mehrere SIR erkennbare Elemente nur einem Attributtyp MISP zuordnen. Wenn erkennbare Typen nicht zugeordnet sind, wird standardmäßig der **andere** MISP Attributtyp ausgewählt.

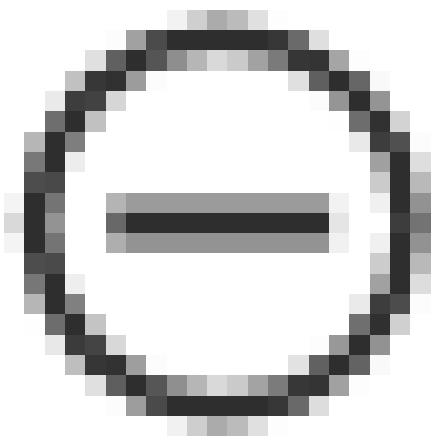


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Ordnen Sie im Formular „Zusätzliche Optionen“ das erkennbare Element SIR und die Attributtypen MISP zu.
2. Ordnen Sie die erkennbaren Typen Security Incident ResponseMISP den Attributtypen [] zu, wie in der folgenden Tabelle beschrieben.

### Zuordnung von erkennbarem SIR- und MISP-Attributtyp

| Feld | Beschreibung |
|---|---|
| Alle zugehörigen erkennbaren Elemente als Attribute hinzufügen | Option, die Sie aktivieren, um einem MISP -Event verfügbare erkennbare Elemente in einem Security Incident als Attribute hinzuzufügen.<br><br>Diese Option aktiviert die Zuordnung im Abschnitt „Zuordnung erkennbarer Typ zu Attributtyp“. |
| Zuordnung erkennbarer Typ zu Attributtyp | Option zum Zuordnen der erkennbaren Typen [ SIR zu den Attributtypen MISP. Sie können beispielsweise die CVE-Nummer in SIR dem Schwachstellenattribut in MISPzuordnen .<br><br>Sie können einen erkennbaren Typ [] nur einem Attributtyp MISPSIR hinzufügen.<br><br>Das Basissystem bietet eine Zuordnung der erkennbaren Typen [ SIR zu den Attributtypen MISP.<br><br>Wenn SIR erkennbare Typen keinem Attributtyp MISP zugeordnet sind, wird das erkennbare Element dem **anderen** Attributtyp in MISPzugeordnet.<br><br>Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Erkennbaren Typ**hinzufügen, suchen Sie nach dem erkennbaren Typ SIR ] und ordnen Sie ihn dann dem entsprechenden Attributtyp MISP zu.<br><br>Klicken Sie auf das Symbol<br><br>  , |

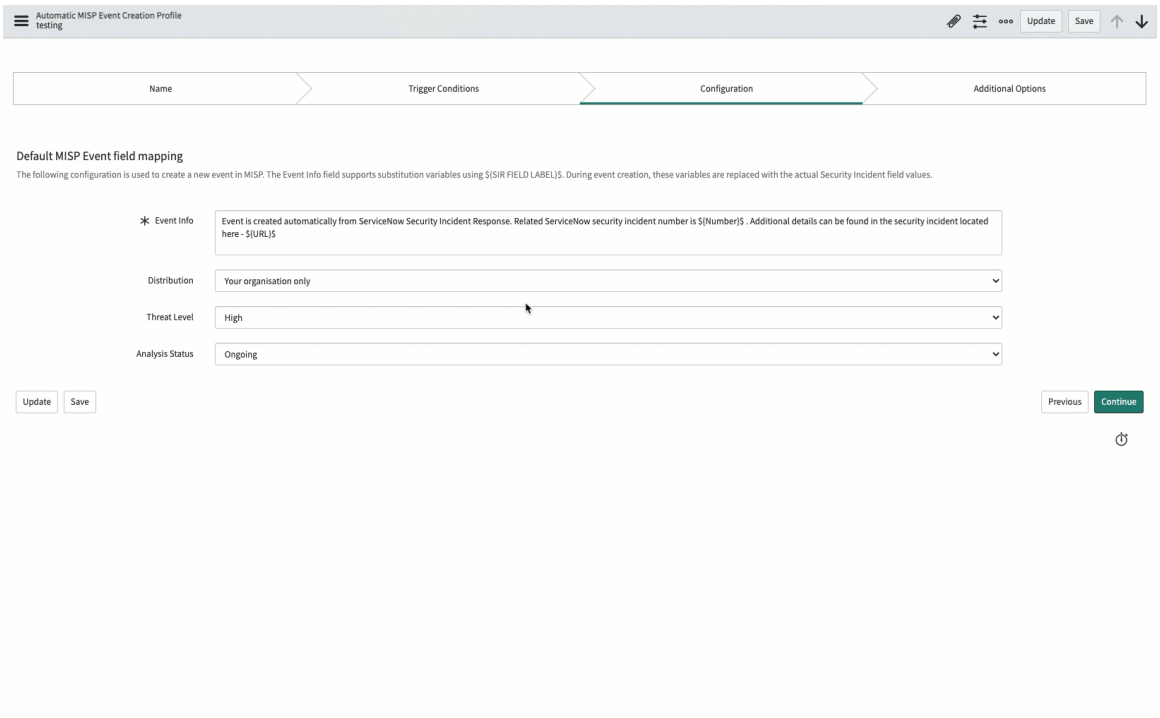


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | um die Attributzuordnungszuordnung SIR und MISP zu entfernen.<br><br>**Hinweis:**<br>Weitere Informationen zu MISP -Attributtypen finden Sie in der MISP-Dokumentation . |
| Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist. | Option, die Sie darüber informiert, dass, wenn ein erkennbares Element in SIRals schädlich markiert ist, für das entsprechende Attribut in MISP die IDS-Kennzeichnung aktiviert ist. Wenn die IDS-Kennzeichnung nicht festgelegt ist, wird das Attribut als kontextbezogene Information betrachtet und nicht für die automatische Angriffserkennung verwendet. |

Das folgende Beispiel zeigt, wie Sie zur Seite mit zusätzlichen Optionen navigieren. Auf dieser Seite können Sie die Zuordnung von erkennbaren SIR-Elementen und MISP-Attributtypen aktivieren, neue erkennbare Typen von SIR hinzufügen, z. B. das IPv6-Netzwerk und das IPv4-Netzwerk, und sie der Domänen-IP-Adresse des Attributtyps MISP zuordnen.

**Zuordnung von SIR erkennbaren Elementen und MISP Attributtypen**




## Synchronisieren Sie MITRE-ATT&CK Informationen mit MISP Events

Synchronisieren Sie die MITRE-ATT&CK -Informationen mit den MISP -Attributen, um die Analyse von Security Incidents und Bedrohungen zu verbessern.

### Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

Überprüfen Sie im Formular „Zusätzliche Optionen“ die Optionen zum Synchronisieren der MITRE-ATT&CK -Informationen mit den MISP -Attributen.

#### Formular „Erweiterte Optionen“

| Feld | Beschreibung |
|---|---|
| Synchronisieren Sie die Techniken des Security Incident MITRE-ATT&CK™ als lokale Galaxien mit dem Event MISP . | Option zum Synchronisieren der Security Incident-Techniken von Now Platform SIRMITRE-ATT&CK™ als lokale Galaxien im Event MISP.<br>**Hinweis:** Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden MISP -Servers gehören. |
| Synchronisieren Sie die Techniken des Security Incident MITRE-ATT&CK™ als globale Galaxien mit dem Ereignis MISP . | Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als globale Galaxien im Ereignis MISP. |

### Ergebnisse

Sie haben ein Profil erstellt, mit dem Sie Events in MISP automatisch aus Now Platformerstellen können. Sie können die Events jetzt in der zugehörigen Liste Zugeordnete MISP-Events anzeigen.

#### MISP Ereignisdaten

Sie können die Ereignisdaten von MISP überprüfen, um detaillierte Informationen zu den Ereignissen von MISP anzuzeigen.

## MISP Ereignisdaten in der Listenansicht

Greifen Sie über auf die Listenansicht zu **MISP** > **MISP-Ereignis-Daten**.

Verwenden Sie die Listenansicht, um einen schnellen Überblick über die MISP Event-Daten zu erhalten.

#### Listenansicht der MISP-Ereignisse

| Feld | Beschreibung |
|---|---|
| Event-ID | Event-ID, die von MISP zugewiesen wurde, als das Event zuerst erstellt oder auf den Server MISP importiert wurde. |
| Info | Kurzbeschreibung des Events. |
| Analyse | Aktuelle Phase der Analyse für das Event mit den folgenden möglichen Optionen: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Listenansicht der MISP-Ereignisse (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| | • Anfänglich: Die Analyse beginnt gerade<br>• Laufend: Die Analyse wird ausgeführt<br>• Abgeschlossen: Die Analyse ist abgeschlossen |
| Bedrohungsstufe | Risikostufe des Ereignisse. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als undefiniert belassen werden. Im Folgenden sind die Optionen aufgeführt:<br>• Niedrig: Allgemeine Massen-Malware<br>• Mittel: Advanced Persistent Threats (APT)<br>• Hoch: Ausgereifte APTs und 0-Tage-Angriffe |
| MISP-Tags | Tags, die dem Ereignis MISP zugeordnet sind. |
| MISP-Galaxien | Galaxien, die dem Ereignis MISP zugeordnet sind. |
| Besitzerorganisation | Organisation, die das Event in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar. |
| Erstellerorganisation | Organisation, die das Event in der Instanz MISP erstellt hat. |
| Verteilung | Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene als das Event haben. |
| MISP-Ereignis-Hyperlink | Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist. |
| MISP-Quelle | MISP Quelle, in der das Event erstellt wird. |

## MISP Ereignisdaten in der Formularansicht

Verwenden Sie die Formularansicht, um detaillierte Informationen zu den MISP -Events zu erhalten.

**MISP-Ereignisformularansicht**

| Feld | Beschreibung |
|---|---|
| Event-ID | Event-ID, die von MISP zugewiesen wurde, als das Event zuerst erstellt oder auf den Server MISP importiert wurde. |
| UUID | ID, die Events und Attribute eindeutig identifiziert |
| Erstellerorganisation | Organisation, die das Event in der Instanz MISP erstellt hat. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**MISP-Ereignisformularansicht (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| Besitzerorganisation | Organisation, die das Event in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar. |
| Erstelleranwender | Benutzer, der das Event in MISPerstellt hat. |
| Letzter Change | Datum, an dem das Event zuletzt geändert wurde. |
| MISP-Quelle | MISP Quelle, in der das Event erstellt wird. |
| Erstellungsdatum (in MISP) | Datum, an dem das Event erstellt oder erstmals auf dem Server MISP importiert wurde. |
| Bedrohungsstufe | Risikostufe des Ereignisse. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als undefiniert belassen werden. Im Folgenden sind die Optionen aufgeführt:<br>• Niedrig: Allgemeine Massen-Malware<br>• Mittel: Advanced Persistent Threats (APT)<br>• Hoch: Ausgereifte APTs und 0-Tage-Angriffe |
| Analyse | Aktuelle Phase der Analyse für das Event mit den folgenden möglichen Optionen:<br>• Anfänglich: Die Analyse beginnt gerade<br>• Laufend: Die Analyse wird ausgeführt<br>• Abgeschlossen: Die Analyse ist abgeschlossen |
| Verteilung | Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene als das Event haben. |
| Veröffentlicht | Status, ob das Event veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Events für alle berechtigten Exporte verwendet werden. Außerdem werden Benutzer benachrichtigt, die die Event-Warnungen abonniert haben. |
| MISP-Ereignis-Hyperlink | Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist. |
| Info | Kurzbeschreibung des Events. |
| Tags (lokal) | Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierung und Exportfilterung zu aktivieren. MISP Events werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden immer entfernt, bevor sie mit anderen MISP Instanzen und Communitys synchronisiert werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MISP-Ereignisformularansicht (Fortsetzung)

| Feld | Beschreibung |
|---|---|
| Tags (global) | Tags, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie MISP -Instanzen globale Tags hinzufügen, können Sie Events ändern. |
| Galaxien (lokal) | Galaxien, die in der Instanz MISP der Hostorganisation für Synchronisierung und Exportfilterung verfügbar sind. MISP Events werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen MISP -Instanzen und Community-Freigaben synchronisiert werden. |
| Galaxien (global) | Galaxien, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie globale Galaxien hinzufügen, MISP können Sie Events ändern. |

## Zugeordnete MISP Events

Sie können die zugeordnete Ereignislistenansicht MISP verwenden, um die Ereignisse anzuzeigen, die manuell oder automatisch im Kontext eines Security Incident erstellt wurden.

### Zugeordnete MISP-Ereignisse

| Feld | Beschreibung |
|---|---|
| Security Incident | SIR Security Incident.<br><br>Klicken Sie auf den Security Incident, um den Security Incident anzuzeigen. |
| MISP-Ereignis | MISP Event-ID<br><br>Klicken Sie auf das Event MISP, um das Event MISP in Now Platformanzuzeigen. |
| MISP-Quelle | MISP Quelle, in der das Event erstellt wird.<br><br>Klicken Sie auf die Quelle MISP, um die Quelle anzuzeigen. |
| Ereigniserstellungsmodus | Status, der angibt, ob das Event manuell oder automatisch mit dem Event-Erstellungsprofil erstellt wurde.<br><br>Klicken Sie auf das Event MISP, um das zugehörige Event MISP ] anzuzeigen. |
| Profil für die automatische Erstellung von Ereignissen | Event-Erstellungsprofil, das zum Erstellen des automatischen Events verwendet wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zugeordnete MISP-Ereignisse (Fortsetzung)

| Feld | Beschreibung |
|---|---|
| | Klicken Sie auf das Profil, um das Profil für die automatische MISP-Ereigniserstellung anzuzeigen. |

### MISP Benutzerinformationen

Sie können die Benutzerinformationsseite MISP verwenden, um alle zugeordneten Benutzer für Now Platform MISP integration for Security Operationsanzuzeigen.

### MISP-Anwenderinformationen

| Feld | Beschreibung |
|---|---|
| Quelle | Quelle MISP des Benutzeraccounts. |
| Anwender-ID | Benutzer-ID, die vom Server MISP zugewiesen wird, wenn ein Benutzeraccount erstellt wird. |
| Anwender-E-Mail | E-Mail-Adresse eines Benutzers. Nur Organisationsadministratoren können die E-Mail-Adressen der Benutzer ihrer eigenen Organisation sehen. |
| Organisation | Organisation, zu der ein Benutzer gehört. |
| Rollenname | Rollenname, der die Benutzerberechtigungen definiert, die einem Benutzer zugewiesen werden.<br>Weitere Informationen zu Rollen in MISPfinden Sie in der MISP-Dokumentation . |
| Rollen-ID | Benutzerrollen-ID in MISP. Zum Beispiel Perm-Administrator, Perm-Audit oder Perm-Tagger usw. |
| Berechtigung | Berechtigungen, über die ein Benutzer verfügt. Folgende Berechtigungen sind in MISP verfügbar:<br>• Schreibgeschützt<br>• Eigene Ereignisse verwalten<br>• Verwalten Sie Organisationsereignisse<br>• Verwalten Veröffentlichen von Organisationsereignissen |
| Sichtungsberechtigung | Berechtigung, mit der ein Benutzer Sichtungssuchen durchführen kann. |
| Tagger-Berechtigung | Berechtigung, mit der ein Benutzer Tagging durchführen kann. |

### Domain Separation und MISP

Die Domänentrennung wird in MISP unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

## Support-Stufe

Support: Standard.

## Funktionsweise der Domänentrennung mit MISP

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit den erforderlichen Rollen in Ihrer Domäne.
- Führen Sie die MISP integration for Security Operations -Verfahren in Ihrer Domäne aus.

### Problembehandlung bei der MISP-Integration

In diesem Abschnitt werden wichtige Tipps zur Problembehandlung behandelt, die Ihnen helfen können, häufige Probleme zu beheben, die beim Einrichten oder Ausführen der MISP-Integration auftreten können.

## SSL-Probleme

Wenn Sie eine Verbindung über die MISP-Integration herstellen, stellen Sie sicher, dass Sie ein gültiges CA-Zertifikat auf dem MISP-Server installiert haben, das nicht abgelaufen ist. Sie können RSA-Zertifikate oder eigene Zertifikate in Platform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MISP integration for Security Operations und MISP Benutzerrollen und Berechtigungen.

### Verwenden von MISP zum Untersuchen und Analysieren von Bedrohungen

Sie können die MISP -Daten im gesamten Now Platform Threat Intelligence -Modul und im Now Platform SIR -Modul verwenden, um Bedrohungen für Ihre Organisation zu untersuchen und zu analysieren.

### Sichtungssuchen in MISP

Sie können Sichtungssuchen für erkennbare Elemente in der Instanz MISP durchführen, um zu bestimmen, wie oft bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder Kommunikation mit einer schädlichen IP oder URL, in Ihrem Netzwerk auftreten. Jedes Vorkommen wird als Sichtung betrachtet.

## Sichtungen in MISP

Sichtungen geben an, dass ein Indikator, ein Objekt oder ein Attribut gesehen wurde und seine Gültigkeit bestätigt wird. Sichtungen in MISP sind ein System, mit dem Sie auf Attribute für ein Event reagieren können. Es wurde entwickelt, um Ihren Benutzern eine einfache Methode zu bieten, um zu bestätigen, dass sie ein bestimmtes Attribut gesehen haben, was ihm mehr Glaubwürdigkeit verleiht. Sie können ein Attribut mehrmals anzeigen.

**Hinweis:**
Erkennbare Elemente werden in MISP als Attribute bezeichnet.

Einige Attribute werden als falsch positive Werte betrachtet, was bedeutet, dass sie keine gültigen Sichtungen sind. Andere Attribute sind nur für eine bestimmte Dauer gültig, z. B. eine Phishing-Kampagne, die nur eine Woche lang ausgeführt wird. Sie können den Attributen, die für eine bestimmte Dauer gültig sind, ein Ablaufdatum zuweisen, aber jede Organisation kann einem Attribut nur ein gültiges Ablaufdatum zuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtungen, die in MISP von Benutzern von Organisationen erstellt werden, die auf dem entsprechenden MISP-Server als lokal gekennzeichnet sind, werden als interne Sichtungen bezeichnet. Sichtungen, die in MISP von Benutzern von Organisationen erstellt werden, die auf dem entsprechenden MISP -Server als remote markiert sind, werden als externe Sichtungen bezeichnet.

## Sichtungssuchen in SIR

Der Workflow „Security Operations Integration - Sichtungssuche“ führt die Sichtungssuche aus. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchvorgänge aus, die auf dem konfigurierten Workflow basieren.

Sichtungssuchen helfen Analysten, die Verbreitung einer Bedrohung im Laufe der Zeit zu bestimmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Die Ergebnisse sind in den zugehörigen Listen Security Incident Sichtungen, Sichtungssuchergebnisseund Sichtungssuchdetails enthalten.

Wenn Sie mit der Analyse eines Incident beginnen, können Sie Now Platform so einrichten, dass automatisch eine Sichtungssuche durchgeführt wird, oder manuell eine Suche nach erkennbaren Sichtungen durchführen, um andere Benutzer in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind.

### Aktivieren Sie automatische Sichtungssuchen in MISP

Aktivieren Sie die automatische Ausführung der Sichtungssuche in MISP, damit der Workflow „Security Operations Integration – Sichtungssuche“ immer dann ausgelöst wird, wenn neue erkennbare Elemente mit einem Security Incident verknüpft werden.

#### Vorbereitungen

Vergewissern Sie sich, dass die Sichtungssuchkonfigurationsprofil für MISP ist aktiv.

Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie aktivieren Die Sichtungssuchfunktion wird automatisch in ausgeführt MISP -Integrationskonfiguration, wird die Sichtungssuche in MISP ausgelöst, wenn neue erkennbare Elemente mit einem Security Incident verknüpft werden. Standardmäßig ist die Option **Sichtungssuche automatisch ausführen, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden** aktiviert.

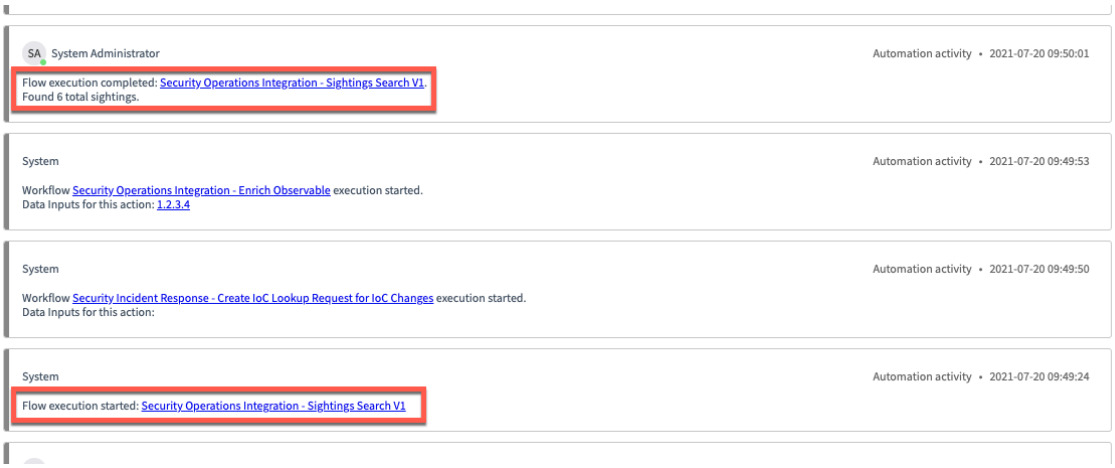
#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, die Sie in den MISP Sichtungssuchdaten anzeigen möchten.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.
   Eine Arbeitsnotiz wird veröffentlicht, wenn der Workflow Security Operations Integration - Sichtungssuche ausgelöst wurde.

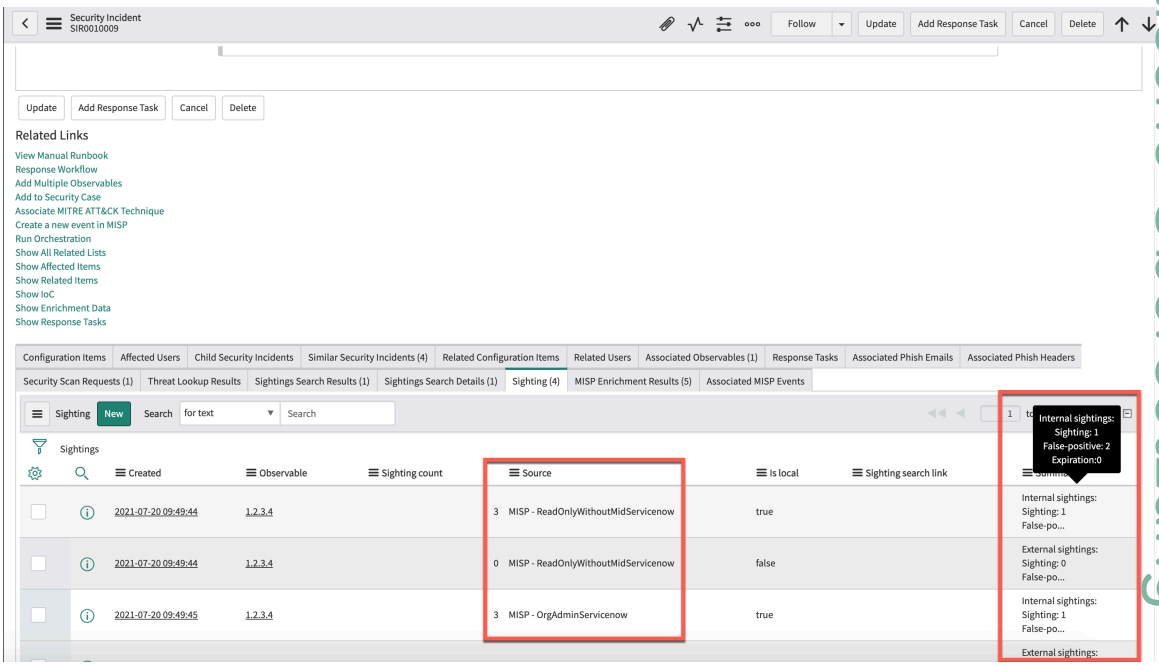


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt den Abschnitt „Arbeitsnotizen“.




4. Zeigen Sie die zusammengefassten Informationen von erkennbaren Elementen an, die für alle Events (global) angezeigt und nach internen oder externen Sichtungen kategorisiert werden, nachdem die Workflow-Ausführung abgeschlossen ist.
   Zeigen Sie die Informationen in den zugehörigen Listen „ Sichtungen“, „ Sichtungssuchergebnisse “ und „ Sichtungssuchdetails “ an. Das folgende Beispiel zeigt den Sichtungssuchdatensatz, der in der zugehörigen Liste „Sichtungen“ erstellt wurde.




### Sichtungssuchdatensatz

| Feld | Beschreibung |
|---|---|
| Erstellt | Datum und Uhrzeit der Erstellung des Sichtungssuchdatensatzes. |
| Erkennbares Element | Erkennbares Element, nach dem von der Abfrage gesucht wird. |
| Sichtungsanzahl | Anzahl der internen und externen Sichtungen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Quelle | Quelle des erkennbaren Elements. Wenn das erkennbare Element aus einer MISP -Organisation stammt, werden dem Datensatz die Wörter MISPvorangestellt. |
| Ist lokal | Status, ob die Sichtung von einem internen Benutzer gemeldet wurde. |
| Sichtungssuchlink | Sichtungssuchlink in der Instanz MISP. |
| Zusammenfassung | Typ der Sichtungen, die dem Datensatz zugeordnet sind. Die drei Arten von Sichtungen sind „Sichtung“, „Falsch positiv“ und „Ablauf“.<br><br>Die Spalte Zusammenfassung wird nur angezeigt, wenn MISP integration for Security Operations installiert ist. Wenn andere Quellen als MISP angezeigt werden, ist der Spalteneintrag Zusammenfassung für diesen Datensatz leer. |

### Führen Sie eine manuelle Sichtungssuche in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in der Anwendung Now Platform MISP integration for Security Operations durch, um die Verbreitung einer Bedrohung im Laufe der Zeit zu bestimmen.

#### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, nach denen Sie die Sichtungssuche MISP ausführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen auf **Sichtungssuche ausführen**.
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld „Sichtungssuche ausführen“ wird geöffnet.
5. Geben Sie den Datumsbereich an, in dem nach den Sichtungssuchdaten gesucht werden soll.

**Dialogfeld „Sichtungssuche ausführen“.**

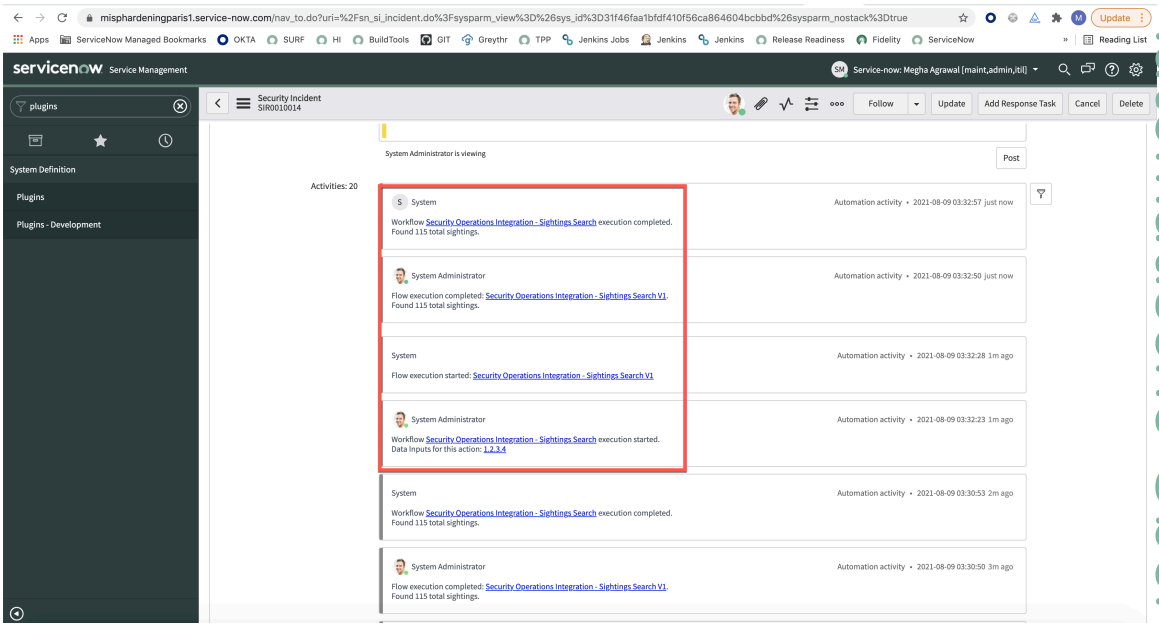
| Feld | Beschreibung |
|---|---|
| Letzte | Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage. |
| zwischen | Zu durchsuchender Datumsbereich. Standarddaten:<br>○ Datum und Uhrzeit der Erstellung des Incident.<br>○ Datum und Uhrzeit, d. h. sieben Tage vor der Eröffnung des Incident. |

6. Klicken Sie auf **Suche**.
   Das folgende Beispiel zeigt die Ergebnisse der manuellen Sichtungssuche in den Arbeitsnotizen.




## Ergebnisse

Ein Sichtungssuchdatensatz wird erstellt. Nach Abschluss der Workflow-Ausführung können Sie die zusammengefassten Informationen der erkennbaren Elemente anzeigen, die für alle Events (global) gelten und nach ihren internen oder externen Sichtungen kategorisiert sind. Zusammengefasste und zugehörige Sichtungsdaten werden im Security Incident unter den zugehörigen Listen „ Sichtungen“, „Sichtungssuchergebnisse“ und „Sichtungssuchdetails“ angezeigt.

### Melden Sie Sichtungen an MISP

Melden Sie Sichtungen von Bedrohungsdaten, damit Sie auf Falschmeldungen in Ihren Daten reagieren und Ihr Bewusstsein für das Auftreten einer echten positiven Bedrohung schärfen können. Sie können auch ein Ablaufdatum für ein bestimmtes erkennbares Element oder Attribut hinzufügen.

## Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Mit MISP integration for Security Operations können Sie Sichtungen global für alle Events an MISP melden. Um eine Sichtung für ein bestimmtes Ereignis zu melden, müssen Sie die Instanz MISP verwenden und die Sichtung lokal melden.

Um eine Sichtung an MISPzu melden, muss das erkennbare Element oder das Attribut in der Instanz MISP verfügbar sein.

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Sichtungen an MISP melden möchten.
3. Klicken Sie auf **Alle zugehörigen Listen anzeigen** und die zugehörige Liste „Sichtungen“ anzeigen.
4. Wählen Sie das erkennbare Element aus, und wählen Sie im Menü Aktionen eine der folgenden Optionen aus. Wenn Sie erkennbare Elemente auswählen, die nicht spezifisch für eine Quelle MISP sind, wird im Menü Aktionen die Anzahl der relevanten Quellen MISP angezeigt. Das folgende Beispiel zeigt vier von acht erkennbaren Elementen, die für MISPrelevant sind. Das folgende Beispiel zeigt das Aktionsmenü und die relevanten erkennbaren Elemente für die Übermittlung.

**Menü „Aktionen“, in dem die relevanten erkennbaren Elemente für die Übermittlung angezeigt werden**

5. **Wahlweise:** Wenn Sie die Option **MISP: Sichtungen erkennbarer Elemente melden** ausgewählt haben, müssen Sie die Felder des Dialogfelds Sichtungen erkennbarer Elemente an MISP melden ausfüllen.

**Dialogfeld „Erkennbare Sichtung melden an MISP “**

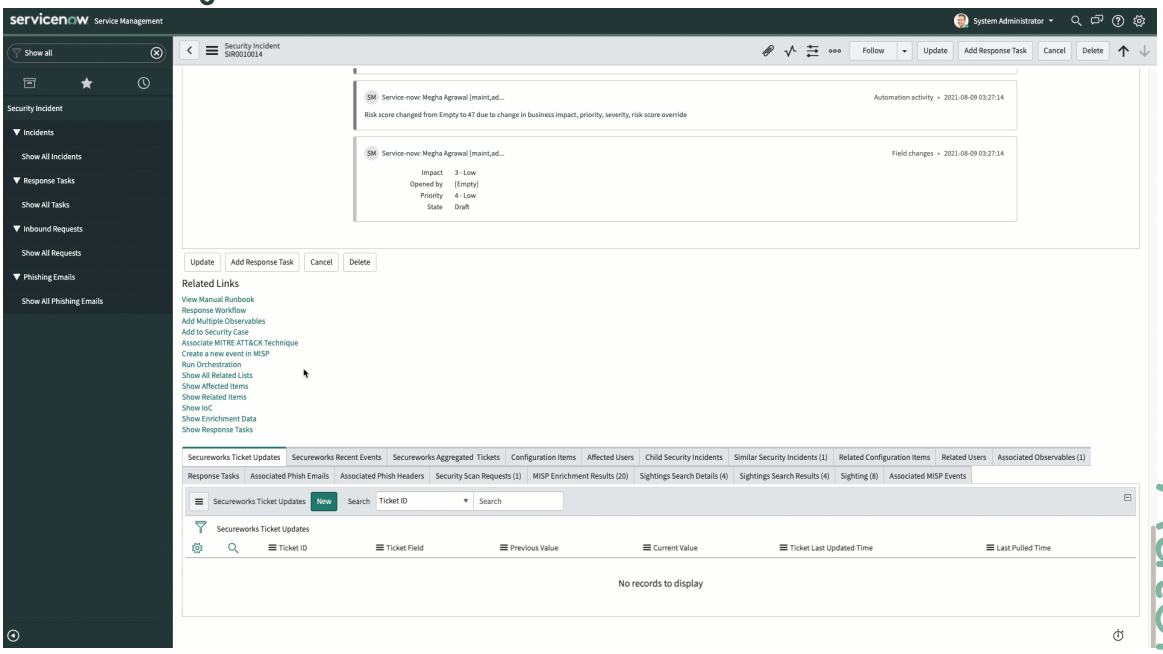
| Feld | Beschreibung |
|---|---|
| Quelle | Quellfeld, das der Quelle MISP der Sichtung entspricht. |
| Datum | Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element gesichtet wurde. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPeingetragen . |

Das folgende Beispiel zeigt, wie Sie im Security Incident zur zugehörigen Liste „Sichtungen“ navigieren. In dieser Liste können Sie ein erkennbares Element auswählen und die Sichtung des erkennbaren Elements an MISPmelden. Die Erfolgsmeldung zeigt, dass die Sichtung erfolgreich an MISPübermittelt wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Meldet Sichtungen erkennbarer Elemente an MISP




**a.** Klicken Sie **auf Sichtung melden**.

6. **Wahlweise:** Wenn Sie die Option **MISP: Erkennbares Element als falsch positiv** melden ausgewählt haben, sollten Sie die Felder des Dialogfelds „Erkennbares Element als falsch positiv melden an MISP “ ausfüllen.

### Dialogfeld „Erkennbares Element als falsch positiv melden“ an MISP

| Feld | Beschreibung |
|---|---|
| Quelle (optional) | Quellfeld, das der Quelle MISP entspricht. Verwenden Sie dieses Feld, um das erkennbare Element als falsch positiv zu deklarieren. |
| Datum | Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element als falsch positiv eingestuft wurde. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPeingetragen . |

**a.** Klicken Sie **auf Falsch positive Meldungen**.

7. **Wahlweise:** Wenn Sie die Option **MISP: Erkennbares Element als abgelaufen melden** ausgewählt haben, sollten Sie die Felder des Dialogfelds „Ablauf erkennbarer Elemente melden an MISP “ ausfüllen.

### Dialogfeld „Ablauf erkennbarer Elemente an MISP melden“.

| Feld | Beschreibung |
|---|---|
| Quelle | Quellfeld, das der Quelle MISP entspricht. Verwenden Sie dieses Feld, um ein erkennbares Element als abgelaufen festzulegen. |
| Datum | Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element abgelaufen ist. Wenn das Datum |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in MISPeingetragen . |

**a.** Klicken Sie **auf Berichtablauf**.

### Ergebnisse

Die Sichtungen werden erfolgreich auf den Server MISP aktualisiert.

## Ergänzung erkennbarer Elemente in MISP

Durch die Anreicherung von erkennbaren Elementen mit zusätzlichen Informationen aus verschiedenen MISP -Quellen während Untersuchungen zur Reaktion auf Incidents können Sie identifizierte Bedrohungen eindämmen.

## Aktivieren Sie die automatische Ergänzung erkennbarer Elemente in MISP

Aktivieren Sie die automatische Ergänzung erkennbarer Elemente in Now Platform MISP, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden.

### Vorbereitungen

- Aktivieren Sie die Systemeigenschaft Security Incident Response für die Option **Aktiviert oder deaktiviert die geplante Aufgabe, Erkennbare Security Incident** -Elemente suchen, um die Ergänzungsfunktion für erkennbare Elemente in SIRauszulösen.
- Erforderliche Rolle: sn_si.analyst

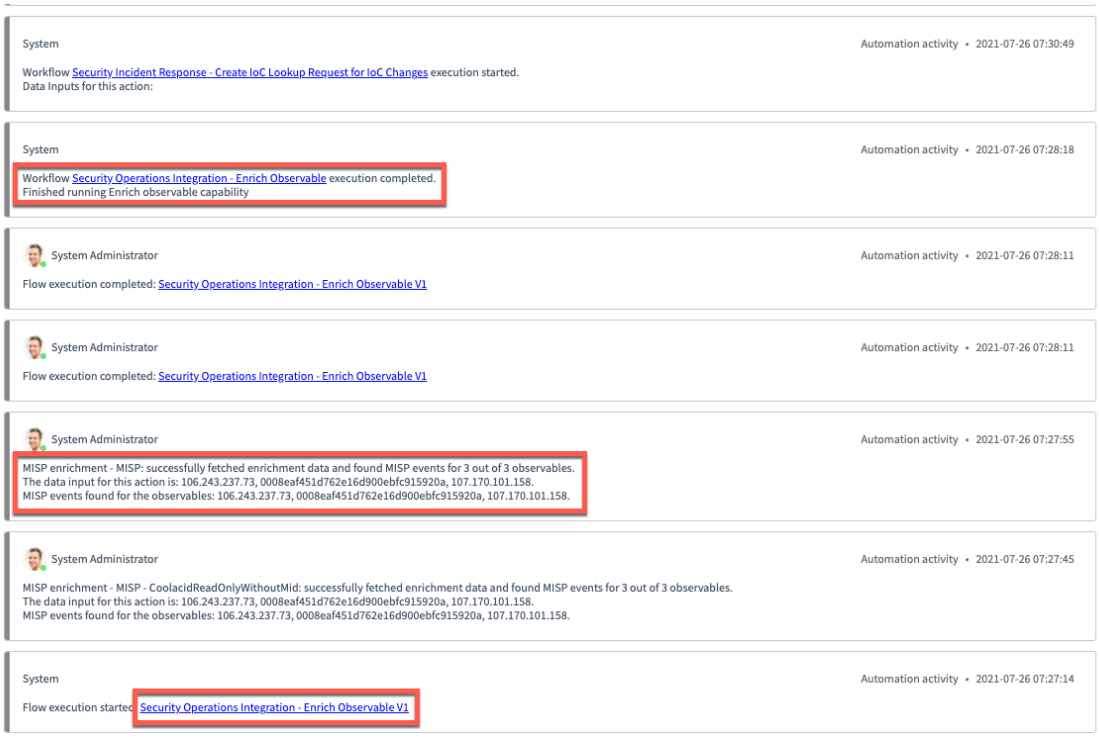
### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Daten zu erkennbaren Elementen in MISP anreichern möchten.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.

   Das folgende Beispiel zeigt, dass eine Arbeitsnotiz veröffentlicht wird, wenn der Workflow „Security Operations Integration – Erkennbares Element anreichern“ ausgelöst wird.



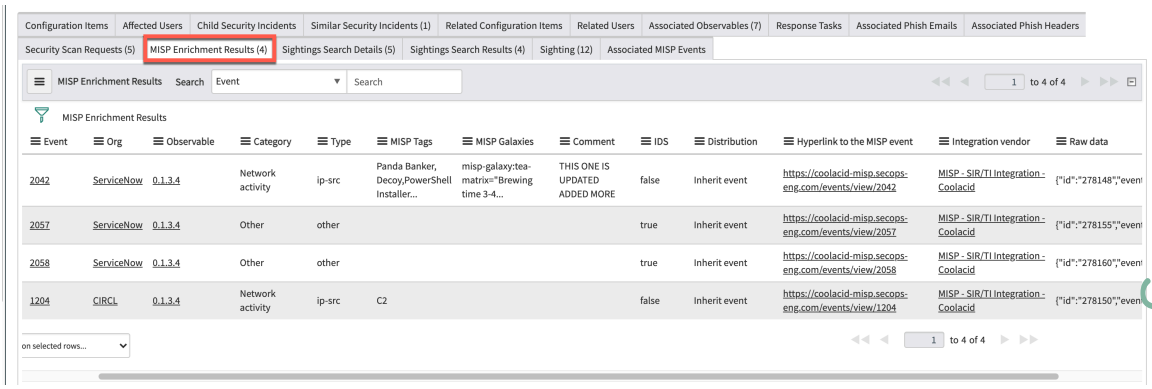
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Zeigen Sie in der zugehörigen Liste MISP Ergänzungsergebnisse des Security Incident die Ergänzungsergebnisse an, nachdem die Workflow-Ausführung abgeschlossen ist.

**Hinweis:**
Sie müssen so konfigurieren, dass die zugehörige Liste MISP Ergänzungsergebnisse in den zugehörigen Listen für Security Incidents angezeigt wird. Weitere Informationen finden Sie unter Konfiguration der zugehörigen Liste.

Das folgende Beispiel zeigt die Ergänzungsergebnisse in MISP.




Die folgende Tabelle zeigt die MISP-Ergänzungsergebnisse.

### MISP-Anreicherungsergebnisse

| Feld | Beschreibung |
|---|---|
| Ereignis | ID des Events. Klicken Sie auf „Öffnen“, um den Datensatz in der Instanz Now Platform anzuzeigen. |
| Org | Organisation, die das Event ursprünglich erstellt hat. |
| Erkennbares Element | Erkennbares Element, das dem Event zugeordnet ist. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Kategorie | Kategorie des Attributs.<br>Zeigen Sie die Liste der Kategorien in der MISP-Dokumentation an. |
| Typ | Typ des Attributs.<br>Zeigen Sie die Liste der Typen in der MISP-Dokumentation an. |
| MISP-Tags | Liste der Tags, die dem Attribut MISP zugeordnet sind. |
| MISP-Galaxien | Liste der Galaxien, die dem Attribut MISP zugeordnet sind. |
| Anmerkung | Kontextbezogener Kommentar zur weiteren Beschreibung des Attributs. Diese Kommentare werden nicht für die Korrelation verwendet und dienen nur der Information. |
| IDS | Kompromittierungsindikator, der es ermöglicht, ihn in alle berechtigten Exporte aufzunehmen. |
| Verteilung | Verteilung des Attributs nach der Veröffentlichung. Ein Attribut kann eine andere Verteilungsebene als das Event haben. In beiden Fällen wird die niedrigste Verteilungsebene verwendet. |
| Hyperlink zum MISP-Ereignis | Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist. |
| IntegrationsVendor | Integrationsanbieter, der die Daten für die Anreicherung bereitstellt. |
| Rohdaten | Rohdaten, die dem Attribut MISP zugeordnet sind. |

### Führen Sie eine manuelle Ergänzung erkennbarer Elemente in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Ergänzung erkennbarer Elemente durch, damit Sie erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen MISP Quellen anreichern können.

#### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Erforderliche Rolle: sn_si.analyst

#### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Ergänzung durchführen möchten.
3. Klicken Sie **auf Alle zugehörigen Listen anzeigen** und die Registerkarte **Zugeordnete** erkennbare Elemente anzeigen.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü Aktionen auf **Anreicherung erkennbarer Elemente ausführen**.
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld „Anreicherung erkennbarer Elemente ausführen“ wird angezeigt.
5. Wählen Sie eine Quelle MISP aus, und wählen Sie in der Spalte Ausgewählt eine Implementierung aus, um die ausgewählten erkennbaren Elemente anzureichern.

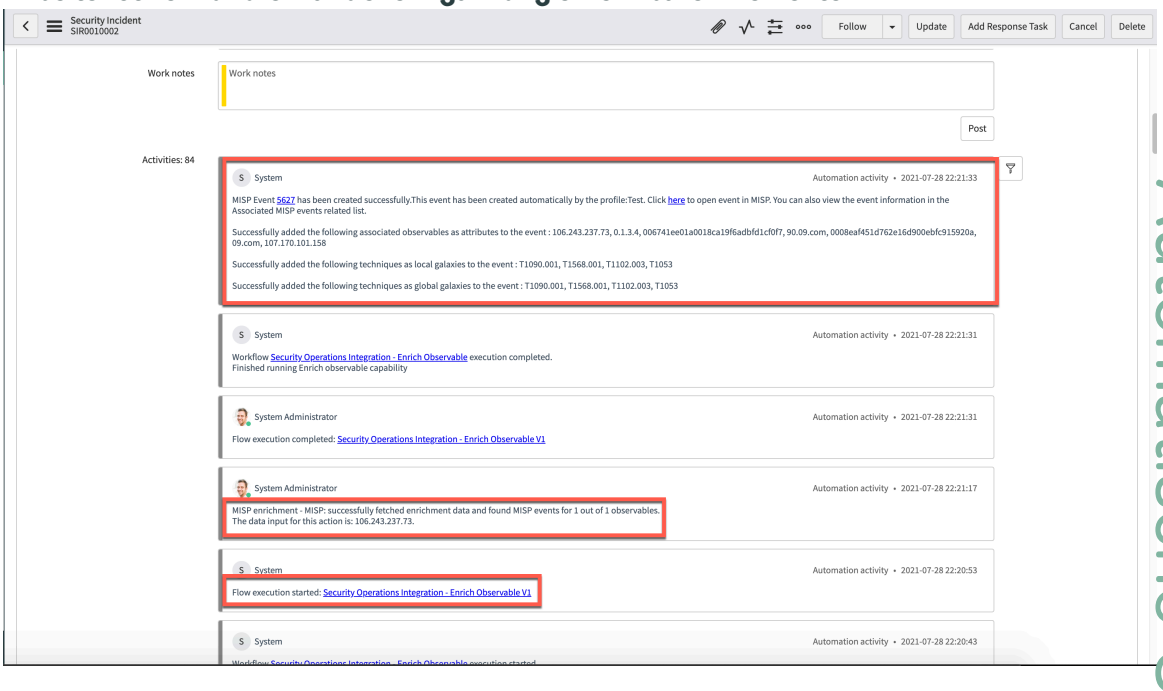


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Eine Arbeitsnotiz zeigt, dass der Workflow „Security Operations Integration – Erkennbares Element anreichern“ ausgelöst wurde. Die zugehörigen Implementierungs-Workflows werden ausgeführt, um die Ergänzung durchzuführen. Sie können die Arbeitsnotizen im Security Incident anzeigen, um den Status anzuzeigen.

   Das folgende Beispiel zeigt, wie die Arbeitsnotizen für eine manuelle Ergänzung erkennbarer Elemente angezeigt werden.

**Arbeitsnotizen für die manuelle Ergänzung erkennbarer Elemente**




In der Ergänzungsnachricht wird das erstellte Event aufgelistet. Sie können das Event in der Instanz Now Platform oder MISP anzeigen und die Details des Datensatzes auf der Registerkarte MISP-Ergänzungsergebnisse anzeigen.

## Fügen Sie Tags zu Attributen MISP hinzu, oder entfernen Sie sie

Fügen Sie Tags in MISP hinzu, oder entfernen Sie sie, um Events oder Attribute zu klassifizieren. Sie können Tagging global verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn MISP Events während der Klassifizierung nicht geändert werden sollen.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Vergewissern Sie sich, dass das Attribut, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente, Attribute oder Ereignisse enthält, für die Sie die Tags hinzufügen möchten.
3. Klicken Sie auf **Alle zugehörigen Listen** anzeigen und die zugehörige Liste MISP-Ergänzungsergebnisse anzeigen.
4. Klicken Sie auf das Vorschausymbol ⓘ neben einem Datensatz, und klicken Sie dann auf **Datensatz öffnen**.
   Das folgende Beispiel zeigt, wie Sie die **MISP** -Ergänzungsergebnisse überprüfen und einen MISP -Ergänzungsdatensatz öffnen.

   **MISP-Ergänzungsergebnisdatensatz**
   Der MISP-Ergänzungsergebnisdatensatz wird geöffnet
5. Überprüfen Sie den MISP-Ergänzungsergebnisdatensatz.

**MISP-Anreicherungsergebnis**

| Feld | Beschreibung |
|---|---|
| Erkennbares Element | |
| Ereignis | Event-ID, die vom Server MISP zugewiesen wurde, als das Event zuerst erstellt oder in MISPimportiert wurde.<br><br>Zeigen Sie eine Vorschau des Events an, oder klicken Sie auf den Datensatz, um die Event-Daten auf der Seite MISP „ Event-Daten“ anzuzeigen. |
| Org | Organisation, die das Attribut MISP erstellt hat. |
| Kategorie | Kategorie des Attributs, das Sie dem spezifischen Event in MISPhinzufügen. Sie können eine Option auswählen, z. B. eine interne Referenz, Netzwerkaktivität, Finanzbetrug usw. |
| Typ | Typ des Attributs MISP. |
| IntegrationsVendor | Integrationsanbieter, der die Daten für die Ergänzung erkennbarer Elemente bereitstellt. |
| Erstellungsdatum (in MISP) | Datum, an dem das Event erstmals erstellt oder in MISPimportiert wurde. |
| IDS | Status, ob ein erkennbares Element in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP wird ebenfalls als „true“ markiert. |
| Verteilung | Steuerelemente der Verteilungsoption, z. B. wer dieses Event anzeigen kann, nachdem es veröffentlicht wurde. Diese Option steuert auch, ob das Event mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt, und die restriktivste Einstellung hat Vorrang. Die Verteilungsoptionen lauten wie folgt: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Event anzuzeigen. Das Event kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, wo nur Ihre Organisation Zugriff hat, um es anzuzeigen. Events mit dieser Einstellung werden nicht synchronisiert.<br>○ Nur diese Community: Ermöglicht Benutzern, die Teil Ihrer MISP Community sind, das Event anzuzeigen, einschließlich Ihrer eigenen Organisation, Organisationen auf diesem MISP Server und Organisationen, die MISP Server ausführen, die mit diesem Server synchronisieren. Alle anderen Organisationen, die mit diesen verknüpften Servern verbunden sind, können das Event nicht anzeigen.<br>○ Verbundene Communities: Ermöglicht Benutzern, die Teil Ihrer Community MISP sind, das Event anzuzeigen, einschließlich aller Organisationen auf diesem Server MISP, aller Organisationen auf Servern MISP, die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen , also zwei Hops entfernt). Alle anderen Organisationen, die mit den verknüpften Servern verbunden sind, die zwei Hops entfernt sind, können das Event nicht anzeigen.<br>○ Alle Communitys: Gibt das Event für alle MISP Communities frei, wodurch das Event frei verfügbar ist. |
| Hyperlink zum MISP-Ereignis | Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist. |
| Rohdaten | Rohdetails für den Datensatz der Ergänzung erkennbarer Elemente. |
| Anmerkung | Kommentare, die Sie für die Attribute hinzufügen. Diese Kommentare dienen nur zu Informationszwecken und werden nicht für die Korrelation verwendet. |
| Tags (lokal) | Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierung und Exportfilterung zu aktivieren. MISP Events werden nicht geändert, wenn Sie lokale Tags verwenden. Diese Tags werden immer |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | entfernt, bevor sie mit anderen MISP -Instanzen und Freigabe-Communities synchronisiert werden. |
| Tags (global) | Tags, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie globale Tags zu MISP -Instanzen hinzufügen, ändern Sie Events. |
| Galaxien (lokal) | Galaxien, die in der Instanz MISP der Hostorganisation für Synchronisierung und Exportfilterung verfügbar sind. MISP Events werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese Galaxien werden immer entfernt, bevor sie mit anderen MISP Instanzen und Communitys synchronisiert werden. |
| Galaxien (global) | Galaxien, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie globale Galaxien hinzufügen, werden MISP Events geändert. |

6. Um ein lokales oder globales Tag zu bearbeiten, klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen:

   - **Tags (lokal)**
   - **Tags (global)**

7. Geben Sie im Dialogfeld „MISP-Attribut-Tags“ den Namen des zu suchenden und hinzuzufügenden Tags ein.
8. Klicken Sie **auf Tags für MISP-Attribut aktualisieren**.

   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen und hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsmeldung zeigt, dass alle Tags in MISPaktualisiert wurden.

   Hinzufügen lokaler Tags im MISP-Attribut.
   Die Tags werden auf dem Server MISP erfolgreich aktualisiert.

9. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu** laden.

### Fügen Sie einem MISP -Ereignis oder -Attribut Galaxien hinzu, oder entfernen Sie sie

Fügen Sie Galaxien in MISP hinzu, oder entfernen Sie sie, damit Sie diese Objekte als Cluster in MISP klassifizieren und an MISP Events oder Attribute anhängen können.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden MISP -Servers gehören.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write

### Prozedur

1. Klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen.

   - **Galaxien (lokal)**
   - **Galaxien (global)**

2. Füllen Sie im Dialogfeld „MISP-Event-Galaxien“ die Details aus.

   **Dialogfeld „MISP-Event-Galaxien“.**

| Feld | Beschreibung |
|---|---|
| Event-ID | Event-ID, die vom Server MISP zugewiesen wurde, als das Event zuerst erstellt oder in MISPimportiert wurde. |
| Namespace | Namespace, in dem die Galaxie gespeichert ist. Sie können Namespaces verwenden, um ähnliche Galaxien zu gruppieren. |
| Galaxien | Galaxie, in der Sie die Clusterinformationen speichern |
| Cluster | Informationen zu den Clustern in der Galaxie. |

3. Klicken Sie **auf Galaxien für MISP-Attribut aktualisieren**.
   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Galaxien den veralteten Namespace und die Galaxie Enterprise Attack - Attack Pattern auswählen und die Clusterinformationen hinzufügen können. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

   Hinzufügen von Galaxie-Informationen in MISP über die Now Platform

4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu** laden.

### Ergebnisse

Die Galaxie-Informationen wurden erfolgreich auf dem Server MISP aktualisiert.

## Fügen Sie dem Attribut MISP Kommentare hinzu

Fügen Sie Kommentare für die Attribute MISP hinzu. Die Kommentare, die Sie hinzufügen, dienen nur zu Informationszwecken und werden nicht für die Korrelation von MISP Daten verwendet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Vergewissern Sie sich, dass das Attribut, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Erforderliche Rolle: sn_sec_misp.write

### Prozedur

1. Klicken Sie auf das Bearbeitungssymbol im Feld Kommentar.
2. Geben Sie Ihren Kommentar in das Feld Attributkommentar ein.
3. Klicken Sie **auf Kommentar zu MISP-Attribut aktualisieren**.
   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol neben dem Kommentarfeld einen Kommentar hinzufügen und dann das Attribut MISP aktualisieren können. Nachdem der Kommentar aktualisiert wurde, können Sie die Erfolgsmeldung anzeigen.

   Hinzufügen von Galaxie-Informationen in MISP über die Now Platform.
4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie in der Erfolgsmeldung auf **Formular neu** laden.

### Ergebnisse

Der Kommentar wurde erfolgreich auf dem Server MISP aktualisiert.

#### Events in MISP verwalten

Sie können Events in MISP automatisch oder manuell über Now Platformerstellen. Sie können die Event-Daten auch in MISP über Now Platformbearbeiten.

#### Es werden automatisch erstellte Events in überprüft MISP

Sie können die automatisch erstellten Events überprüfen, nachdem Sie das Event-Erstellungsprofil in Ihrer Now Platform -Instanz konfiguriert haben.

## Profil für die automatische Event-Erstellung

Die Konfiguration des Profils für die automatische Event-Erstellung erfolgt über die Benutzerrollen sn_si.admin oder sn_ti.admin in **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen** -Modul.

## Anzeigen der Event-Daten MISP .

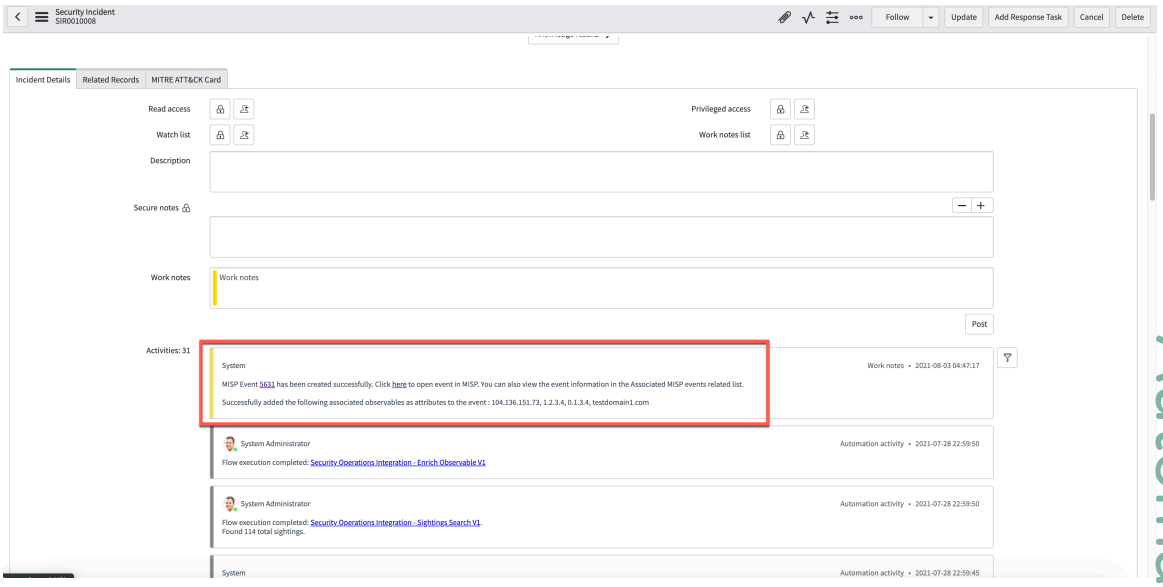
Sie können die erstellten Events wie folgt anzeigen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

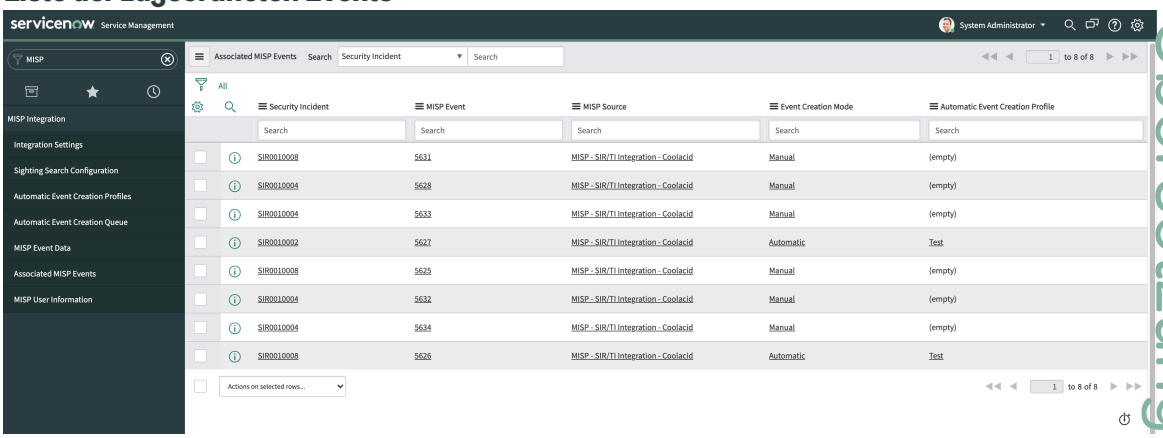
- Zeigen Sie die Arbeitsnotizen für die erstellten Events an. Sie können die Event-Details in der Instanz Now Platform und auch so anzeigen, wie sie auf dem Server MISP angezeigt werden, wie im folgenden Beispiel gezeigt.

**Arbeitsnotizen für erstellte Events**




- Klicken Sie auf die zugehörige Liste Zugeordnete MISP-Ereignisse. Hier können Sie das Event in Bezug auf den Security Incident und die Ressourcen MISP anzeigen, wie im folgenden Beispiel gezeigt.

**Liste der zugeordneten Events**

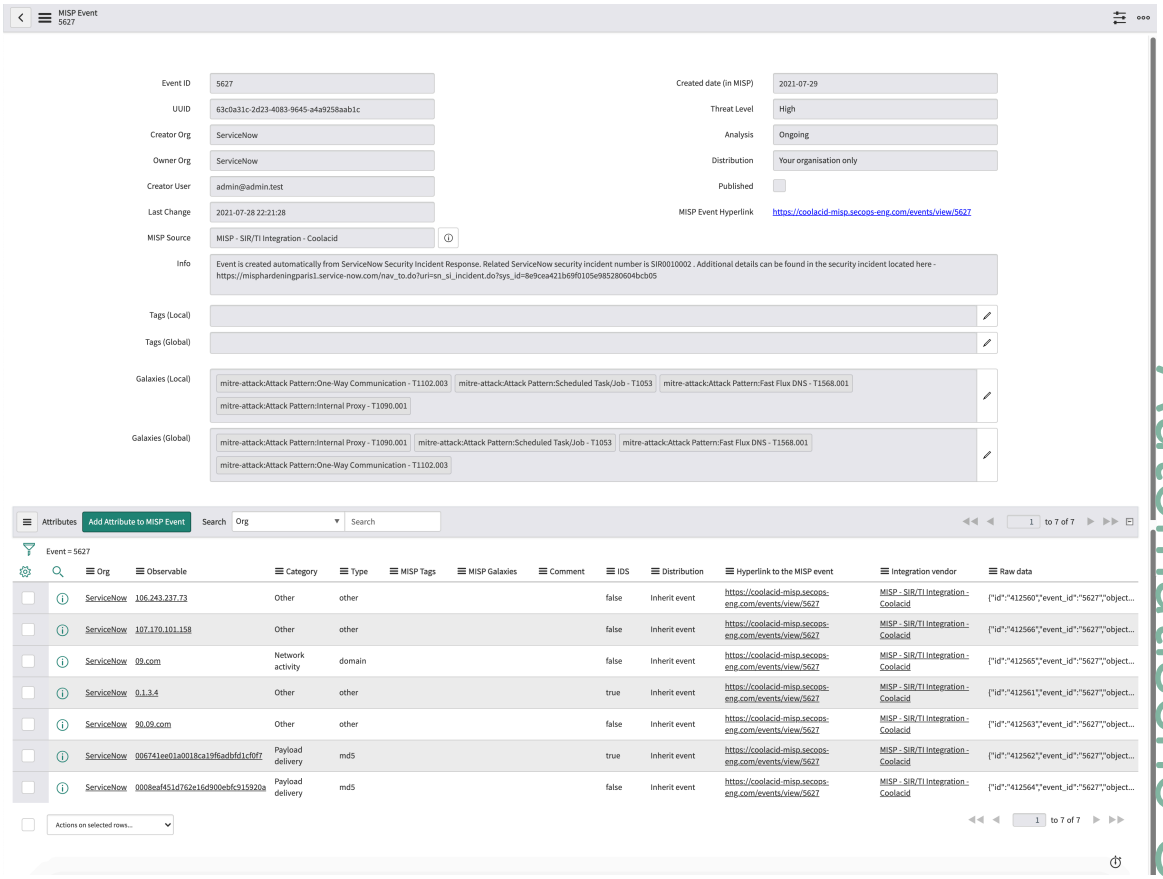





© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die Ereignisdaten MISP in der Formularansicht an, um die detaillierten Informationen zu den Ereignissen MISP zu überprüfen, wie im folgenden Beispiel gezeigt.

**Event-Daten in der Formularansicht**




### Erstellen Sie ein Event manuell in MISP

Erstellen Sie Events in MISP manuell aus Now Platform, um kontextbezogene Informationen zu erfassen, die als Attribute und Objekte dargestellt werden.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Erforderliche Rolle: sn_sec_misp.write

### Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie ein Event erstellen möchten.
3. Klicken **Sie auf Neues Event in MISP erstellen**.
4. Geben Sie im Dialogfeld „Neues Event in MISP erstellen“ die Details ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie ein Event im MISP-Dialogfeld

| Feld | Beschreibung |
|---|---|
| Datum | Erstellungsdatum des Ereignisses in MISP. |
| Information zum Ereignis | Ereignisinformationen, die automatisch aus Now Platform Security Incident Responseerstellt werden. |
| Bedrohungsstufe | Risikostufe des Ereignisse. Sie können die Incidents in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) kategorisieren. Dieses Feld kann auch als undefiniert belassen werden. Im Folgenden sind die Optionen aufgeführt:<br>○ Niedrig: Allgemeine Massen-Malware<br>○ Mittel: Advanced Persistent Threats (APT)<br>○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe |
| Quelle | MISP Quelle für die Event-Erstellung. |
| Verteilung | Option, die steuert, wer dieses Event anzeigen kann, nachdem das Event veröffentlicht wurde. Diese Option steuert auch, ob das Event mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen geerbt. Die restriktivste Einstellung hat Vorrang. Die Verteilungsoptionen lauten wie folgt:<br>○ Nur Ihre Organisation: Ermöglicht nur den Mitgliedern Ihrer Organisation, dieses Event anzuzeigen. Das Event kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, wo nur Ihre Organisation Zugriff hat, um es anzuzeigen. Events mit |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | dieser Einstellung werden nicht synchronisiert.<br>○ Nur diese Community: Ermöglicht Benutzern, die Teil Ihrer MISP Community sind, das Event anzuzeigen, einschließlich Ihrer eigenen Organisation, Organisationen auf diesem MISP Server und Organisationen, die MISP Server ausführen, die mit diesem Server synchronisieren. Alle anderen Organisationen, die mit verknüpften Servern verbunden sind, können das Event nicht anzeigen.<br>○ Verbundene Communities: Ermöglicht Benutzern, die Teil Ihrer Community MISP sind, das Event anzuzeigen, einschließlich aller Organisationen auf diesem Server MISP, aller Organisationen auf Servern MISP, die mit diesem Server synchronisiert werden, und der Hosting-Organisationen von Servern, die eine Verbindung zu einem beliebigen Server herstellen , der zwei Hops entfernt ist. Alle anderen Organisationen, die mit den verknüpften Servern verbunden sind, die zwei Hops von diesem Server entfernt sind, können das Event nicht anzeigen.<br>○ Alle Communitys: Gibt das Event für alle MISP Communities frei. |
| Analyse | Aktuelle Phase der Analyse für das Event mit den folgenden möglichen Optionen: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | | Beschreibung |
|---|---|---|
| | | ○ Anfänglich: Die Analyse beginnt gerade<br>○ Laufend: Die Analyse wird ausgeführt<br>○ Abgeschlossen: Die Analyse ist abgeschlossen |
| Erweiterte Optionen | Alle SIR-zugeordneten erkennbaren Elemente als Attribute zum MISP-Event hinzufügen | Option zum Hinzufügen verfügbarer erkennbarer Elemente in einem Security Incident zu einem MISP -Ereignis als Attribute.<br>Diese Option aktiviert die Option **Attribut-IDS festlegen, wenn erkennbares Element böswillig** ist. |
| | Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist. | Erkennbares Element, das in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP wird ebenfalls als „true“ markiert. |
| | MITRE ATT&CK-Techniken des Security Incident als lokale Galaxien im MISP-Ereignis synchronisieren | Option zum Synchronisieren der Security Incident-Techniken von Now Platform SIRMITRE-ATT&CK™ als lokale Galaxien im Event MISP. |
| | MITRE ATT&CK-Techniken des Security Incident als globale Galaxien im MISP-Ereignis synchronisieren | Option zum Synchronisieren der Now Platform SIR Security Incident-Techniken MITRE-ATT&CK™ als globale Galaxien im Ereignis MISP. |

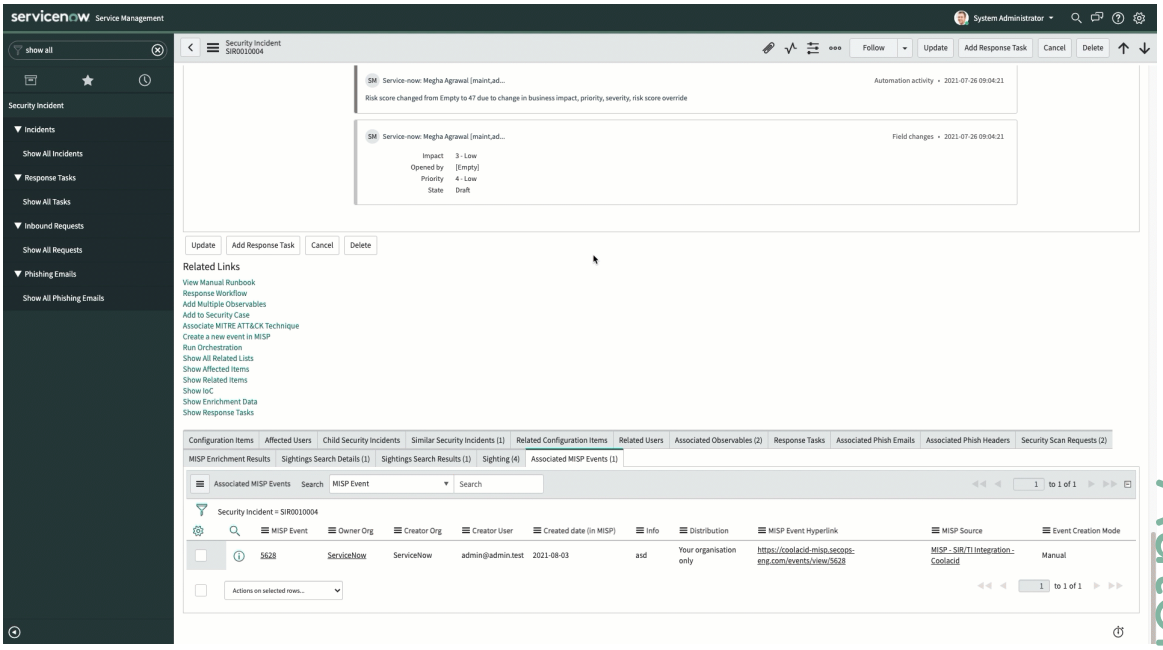
5. Klicken **Sie auf Neues MISP-Ereignis erstellen**.

Das folgende Beispiel zeigt, dass Sie durch Erstellen eines Events in MISPdie Ergebnisse im Security Incident anzeigen können. Sie können auch die Arbeitsnotizen, das Event in der Instanz Now Platform und das Event auf dem Server MISP anzeigen, wie im folgenden Beispiel gezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen Sie ein Event in MISP manuell über die Now Platform




Sie können die Ergebnisse auf folgende Arten anzeigen:

- Eine Erfolgsmeldung wird oben auf der Security Incident-Seite angezeigt. Sie können die Event-Details in der Instanz Now Platform und auf dem Server MISP anzeigen.
- In den Arbeitsnotizen können Sie die Erfolgsmeldung mit weiteren Details anzeigen. Sie können die Event-Details auch in der Instanz Now Platform und auf dem Server MISP anzeigen.
- In der zugehörigen Liste Zugeordnete MISP-Ereignisse können Sie das Event in Bezug auf den Security Incident und die MISP -Ressourcen anzeigen.

## Fügen Sie einem MISP -Event Attribute hinzu

Fügen Sie einem Event Attribute hinzu, z. B. Typ, Kategorie und andere kontextbezogene Informationen zum Event.

### Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Vergewissern Sie sich, dass das Event, zu dem Sie das Attribut hinzufügen oder aktualisieren, zu derselben Organisation gehört wie der Benutzer MISP.
- Erforderliche Rolle: sn_sec_misp.write

### Prozedur

1. Navigieren zu **Alle** > **MISP** > **Zugeordnete MISP-Ereignisse**.
   Sie können auch in jedem Security Incident zur zugehörigen Liste Zugeordnetes MISP-Ereignis navigieren.
2. Klicken Sie auf das MISP-Ereignis, für das Sie ein Attribut hinzufügen möchten.
3. Klicken **Sie auf Attribut zu MISP-Ereignis hinzufügen**.
4. Füllen Sie im Dialogfeld Attribut zu Event hinzufügen die Details aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Dialogfeld „Attribut zu Event hinzufügen“**

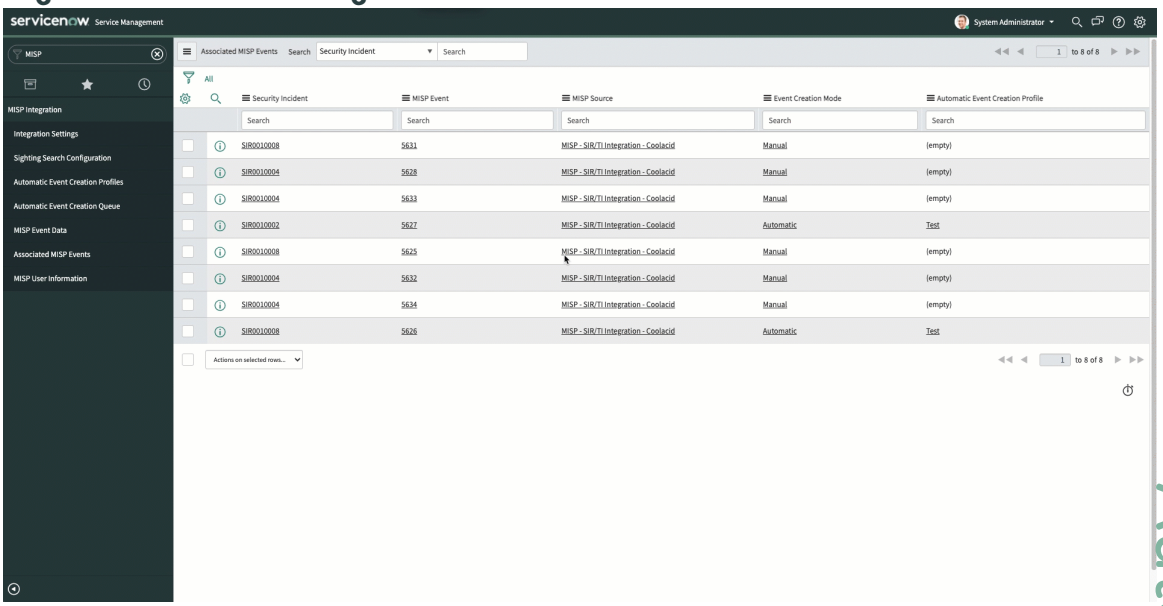
| Feld | Beschreibung |
|---|---|
| Wert | Tatsächlicher Wert des Attributs. Geben Sie Daten zum Wert ein, die darauf basieren, was für den ausgewählten Attributtyp gültig ist. Beispiel: Für ein Attribut vom Typ ip-src (Quell-IP-Adresse) ist 11.11.11.11 ein gültiger Wert.<br>**Hinweis:** Sie können nur Attribute oder erkennbare Elemente auswählen, die den Kontext mit dem Event teilen. Die erkennbaren Elemente dürfen nicht bereits ein Attribut in MISPhaben. |
| Kategorie | Kategorie des Attributs. Die Kategorie beschreibt den Aspekt der Malware für dieses Attribut. Ein Beispiel wären die Persistenzmechanismen der Malware- oder Netzwerkaktivität. |
| Typ | Typ, der die Kategorie erläutert. Wenn ein Angreifer beispielsweise eine IP-Adresse für einen Angriff verwendet, kann eine Quell-E-Mail-Adresse oder eine über einen Anhang gesendete Datei die Nutzlastbereitstellung einer Malware beschreiben. Diese Arten von Attributen haben die Kategorie der Nutzlastlieferung. |
| Verteilung | Benutzer, die dieses Attribut anzeigen können. Die Verteilung wird von Attributen geerbt. Die restriktivste Einstellung hat Vorrang. |
| Attribut als IDS-Signatur verwenden | Erkennbares Element, das in SIRals schädlich markiert ist. Das entsprechende Attribut in MISP wird ebenfalls als „true“ markiert. |
| Kommentare | Kommentare, die Sie für die Attribute hinzufügen. |

Das folgende Beispiel zeigt, dass Sie durch Navigieren aus der Liste Zugeordnete MISP-Ereignisse den Ereignisdatensatz 5627 anzeigen und dem Ereignis Attribute hinzufügen können. Die Attribute umfassen den Wert (testdomain.com), die Kategorie als externe Analyse und den Typ als Domäne. Sie können auch IDS aktivieren. Die Erfolgsmeldung im Event-Datensatz zeigt, dass das Attribut dem Event hinzugefügt wurde, wie im folgenden Beispiel gezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Fügen Sie einem MISP-Ereignis ein Attribut hinzu




5. Klicken **Sie auf Attribut zu MISP-Ereignis hinzufügen**.

## Ergebnisse

Sie können das hinzugefügte Attribut im Abschnitt Attribute anzeigen.

### Fügen Sie einem MISP -Ereignis Tags hinzu

Fügen Sie Tags in Now Platform MISP hinzu, um Events oder Attribute zu klassifizieren. Sie können Tagging global verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn MISP Events während der Klassifizierung nicht geändert werden sollen.

## Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen für die Verwendung der bidirektionalen Funktionen von MISP.
- Vergewissern Sie sich, dass das Event, das Sie bearbeiten, zu derselben Organisation gehört wie der Benutzer MISP.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf der Quelle MISP und ihren Verteilungsberechtigungen basieren.
- Erforderliche Rolle: sn_sec_misp.write

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, der das Event enthält, für das Sie Tags hinzufügen möchten.
3. Klicken Sie auf **Alle zugehörigen Listen** anzeigen und die zugehörige Liste MISP-Ergänzungsergebnisse anzeigen.
4. Klicken Sie in der Liste der Ergänzungsergebnisse auf die Event-ID.
   Sie können auch über navigieren **MISP** > **Zugeordnete MISP-Ereignisse** -Modul.
5. Überprüfen Sie den MISP-Ereignisdatensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### MISP-Ereignisformularansicht

| Feld | Beschreibung |
|---|---|
| Event-ID | Event-ID, die von MISP zugewiesen wurde, als das Event zuerst erstellt oder auf den Server MISP importiert wurde. |
| UUID | ID, die Events und Attribute eindeutig identifiziert |
| Erstellerorganisation | Organisation, die das Event in der Instanz MISP erstellt hat. |
| Besitzerorganisation | Organisation, die das Event in der Instanz MISP besitzt. Dieses Feld ist nur für Administratoren sichtbar. |
| Erstelleranwender | Benutzer, der das Event in MISPerstellt hat. |
| Letzter Change | Datum, an dem das Event zuletzt geändert wurde. |
| MISP-Quelle | MISP Quelle, in der das Event erstellt wird. |
| Erstellungsdatum (in MISP) | Datum, an dem das Event erstellt oder erstmals auf dem Server MISP importiert wurde. |
| Bedrohungsstufe | Risikostufe des Ereignisse. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, mittel, hoch) eingeteilt werden. Dieses Feld kann als undefiniert belassen werden. Im Folgenden sind die Optionen aufgeführt:<br>○ Niedrig: Allgemeine Massen-Malware<br>○ Mittel: Advanced Persistent Threats (APT)<br>○ Hoch: Ausgereifte APTs und 0-Tage-Angriffe |
| Analyse | Aktuelle Phase der Analyse für das Event mit den folgenden möglichen Optionen:<br>○ Anfänglich: Die Analyse beginnt gerade<br>○ Laufend: Die Analyse wird ausgeführt<br>○ Abgeschlossen: Die Analyse ist abgeschlossen |
| Verteilung | Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene als das Event haben. |
| Veröffentlicht | Status, ob das Event veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Events für alle berechtigten Exporte verwendet werden. Außerdem werden Benutzer benachrichtigt, die die Event-Warnungen abonniert haben. |
| MISP-Ereignis-Hyperlink | Link zum Ereignis MISP, das auf dem Server MISP gespeichert ist. |
| Info | Kurzbeschreibung des Events. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Tags (lokal) | Tags, die in der Instanz MISP der Hostorganisation verfügbar sind, um Tagging für die Synchronisierung und Exportfilterung zu aktivieren. MISP Events werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden immer entfernt, bevor sie mit anderen MISP Instanzen und Communitys synchronisiert werden. |
| Tags (global) | Tags, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie MISP -Instanzen globale Tags hinzufügen, können Sie Events ändern. |
| Galaxien (lokal) | Galaxien, die in der Instanz MISP der Hostorganisation für Synchronisierung und Exportfilterung verfügbar sind. MISP Events werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen MISP -Instanzen und Community-Freigaben synchronisiert werden. |
| Galaxien (global) | Galaxien, die global verfügbar sind, um mit anderen MISP Instanzen und Sharing-Communities geteilt und synchronisiert zu werden. Wenn Sie globale Galaxien hinzufügen, MISP können Sie Events ändern. |

6. Um ein lokales oder globales Tag zu bearbeiten, klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen:

   - **Tags (lokal)**
   - **Tags (global)**

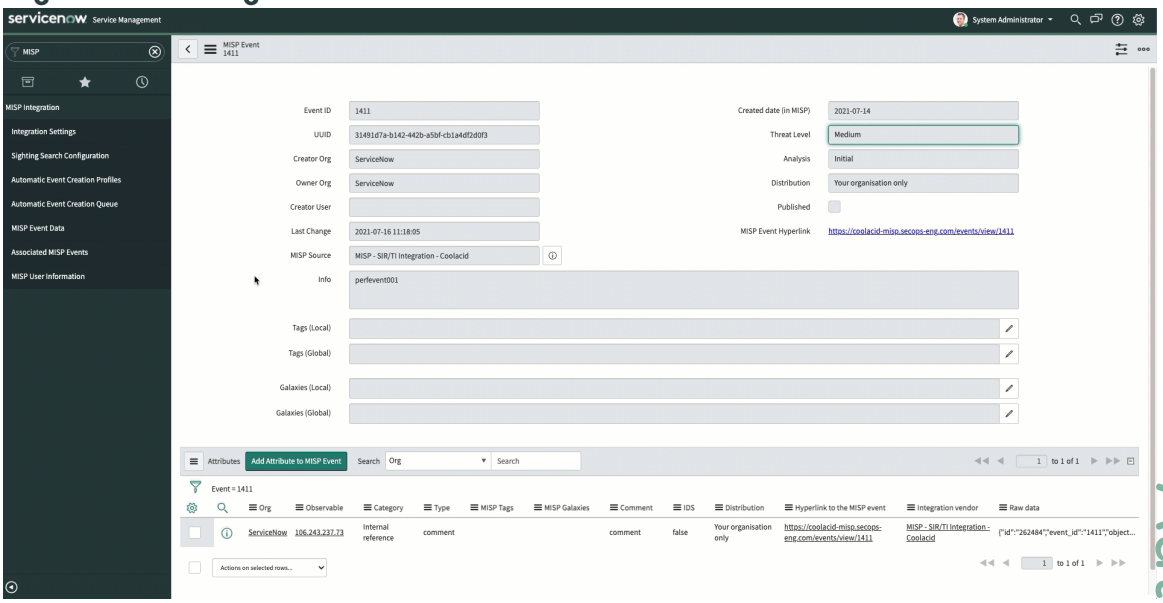
7. Geben Sie im Dialogfeld „MISP-Event-Tags“ den Tag-Namen ein, um die Tags zu suchen und hinzuzufügen.
8. Klicken Sie **auf Tags für MISP-Ereignis aktualisieren**.

   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen und hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsmeldung zeigt an, dass alle Tags in MISPaktualisiert wurden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Tags für MISP-Ereignis werden aktualisiert**




**9.** Klicken Sie in der Erfolgsmeldung auf **Formular** neu laden, um die Änderungen im Datensatz anzuzeigen.

## Ergebnisse

Die Tags wurden erfolgreich auf dem Server MISP aktualisiert.

### Aktualisiert Galaxien für ein MISP -Ereignis oder -Attribut

Fügen Sie Galaxien in Now Platform MISP hinzu, oder entfernen Sie sie, damit Sie diese Objekte als Cluster in der Instanz MISP klassifizieren und an MISP Events oder Attribute anhängen können.

## Vorbereitungen

- Überprüfen Sie die MISP Benutzerrolle und Berechtigungen ist für die Verwendung der bidirektionalen Funktionen von MISP erforderlich.
- Um lokale Galaxien hinzuzufügen, muss der Benutzer, der die Integration konfiguriert hat, zur Hostorganisation des entsprechenden MISP -Servers gehören.
- Die für Sie verfügbaren Tags und Galaxien basieren auf der Quelle MISP und ihren Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

## Prozedur

**1.** Klicken Sie auf das Bearbeitungssymbol in einer der folgenden Optionen.

- **Galaxien (lokal)**
- **Galaxien (global)**

**2.** Geben Sie im Dialogfeld MISP-Event-Galaxien ein, und suchen Sie, um die Tags hinzuzufügen.

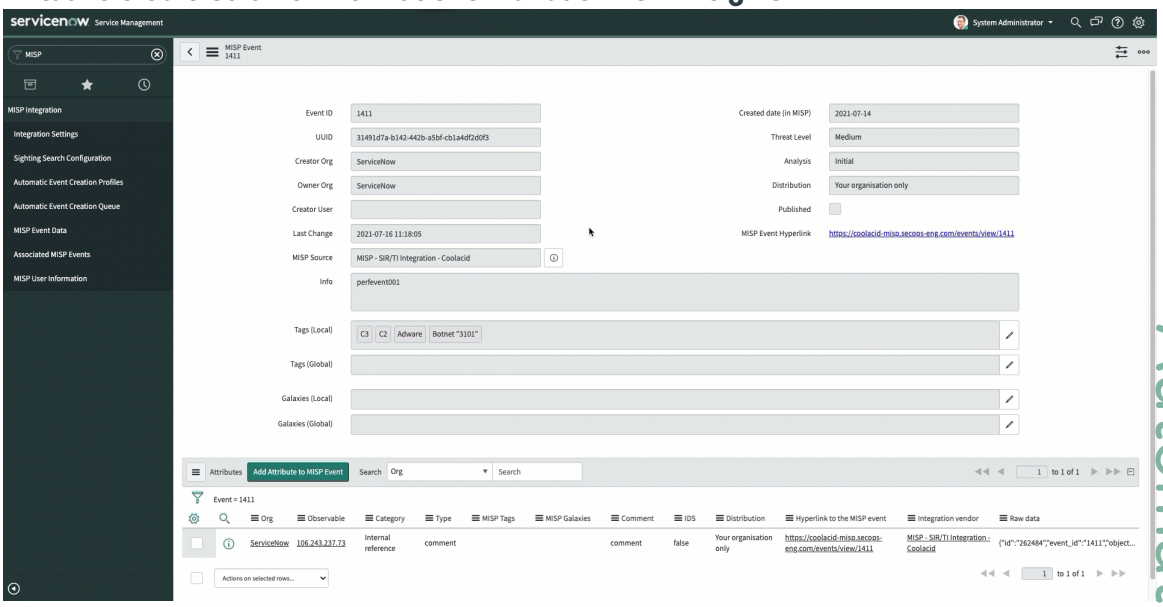
**3.** Klicken Sie **auf Galaxien für MISP-Ereignis aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt, wie Sie auf das Bearbeitungssymbol für die lokalen Galaxien klicken, den veralteten Namespace auswählen, die Galaxie Enterprise Attack - Attack Pattern auswählen und Clusterinformationen hinzufügen. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

**Aktualisiert die Galaxie-Informationen für das MISP-Ereignis**




Die Galaxien wurden auf dem Server MISP erfolgreich aktualisiert.

4. Klicken Sie in der Erfolgsmeldung auf **Formular** neu laden, um die Änderungen im Datensatz anzuzeigen.

## Führen Sie einen Rollup für MITRE-ATT&CK Informationen mithilfe von MISP Ergänzungsergebnissen durch

Führen Sie ein manuelles Rollup der MISP-Ergänzungsergebnisse durch, wenn Sie das automatische Rollup von MISP Informationen nicht aktiviert haben.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um die MITRE-ATT&CK -Informationen aus der MISP -Integration zu importieren. Mit MISP integration for Security Operations werden zwei Extraktionsregeln für die Basissystem-[ MITRE-ATT&CK -Technik für die Tags MISP - MISP Galaxien und MISP eingeführt. Weitere Informationen zu Regeln für die automatische Extraktion in MITRE-ATT&CKfinden Sie unter Technikregeln für automatische Extraktion zum Importieren von MITRE-ATT&CK-Informationen.

Wenn Sie aktiviert haben automatisches Rollup von MITRE-ATT&CK Informationen mit MISP Ergänzungsergebnisse zu einem Security Incident wird für die Informationen automatisch ein Rollup durchgeführt. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie diese Aufgabe manuell ausführen.

### Prozedur

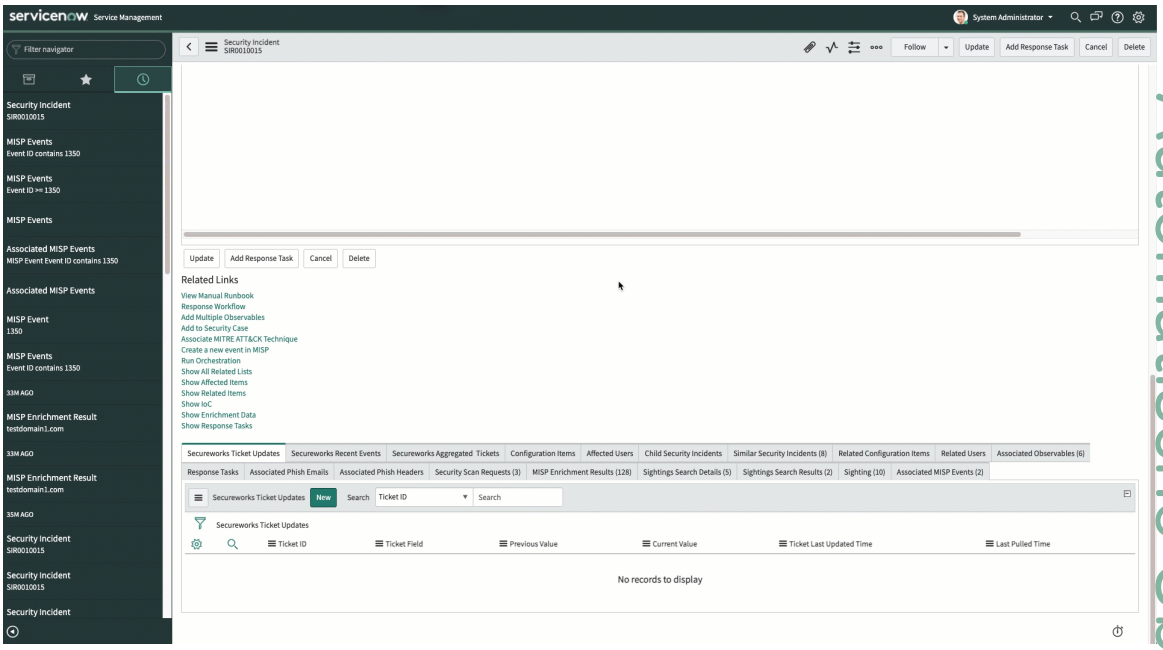
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie den Security Incident aus, den Sie mit den MITRE-ATT&CK -Informationen anreichern möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie **auf Alle zugehörigen Listen** anzeigen und die Registerkarte **MISP-Ergänzungsergebnisse** anzeigen.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü „Aktionen“ **auf MITRE ATT&CK-Informationen für SI zusammenfassen**.
   Sie können mehrere erkennbare Elemente auswählen und dann die Informationen zusammenfassen.
5. Um die Änderungen zu bestätigen, klicken Sie auf **Neu laden**.
   Das folgende Beispiel zeigt, wie Sie ein erkennbares Element auswählen und für die Ergänzungsergebnisse MISP einen Rollup zum Security Incident durchführen.

**Führen Sie einen Rollup für MITRE-Informationen zu einem Security Incident durch**




## Ergebnisse

Sie können die Karte MITRE-ATT&CK anzeigen, um zu bestätigen, dass für die MISP-Ergänzungsergebnisse ein Rollup zum Security Incident durchgeführt wurde.

## OPSWAT Metadefender-Integration

OPSWAT Metadefender ermöglicht das Herunterladen von Bedrohungsdaten, die vom Drittanbieter-Scanner Metadefender erkannt wurden, in die Anwendung Threat Intelligence, um sie nachzuverfolgen, zu priorisieren und zu beheben.

| | |
|---|---|
| Erkunden<br>• Integrationsüberblick OPSWAT Metadefender<br>• Threat Intelligence-Integrationen | Einrichtung<br>Aktivieren und konfigurieren Sie die OPSWAT Metadefender -Integration |
| Verwenden<br>• Suchvorgänge für erkennbare Elemente durchführen<br>• Bedrohungssuche – OPSWAT Metadefender-Workflow | Entwickeln<br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| | • Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und Hilfe<br><br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### Integrationsüberblick OPSWAT Metadefender

OPSWAT Metadefender ist eine Sicherheitslösung, die Zugriff auf mehrere Anti-Malware-Computer bietet und sich problemlos in Security Operationsintegrieren lässt.

Bevor Sie die OPSWAT Metadefender -Integration verwenden können, müssen Sie das Plugin aktivieren und die Integration konfigurieren. Bei Bedarf können Sie auch Ihre X509 SSL-Zertifizierung aktualisieren.

### Aktivieren und konfigurieren Sie die OPSWAT Metadefender -Integration

Bevor Sie die OPSWAT Metadefender -Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

#### Vorbereitungen
Erforderliche Rolle: admin

#### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Greifen Sie nach Abschluss der Integration auf das OPSWAT-Portal zu, und rufen Sie den Metadefender-Cloud-API-Schlüssel ab
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte „OPSWAT Metadefender“ auf **Konfigurieren**.
5. Geben Sie den **API-Schlüssel** ein, den Sie aus dem OPSWAT-Portal bezogen haben, oder fügen Sie ihn ein.
6. Klicken Sie auf **Absenden**.

#### Ergebnisse
Nach der Konfiguration kann OPSWAT Metadefender für Suchvorgänge für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

**Zugehörige Informationen**

Suchvorgänge für erkennbare Elemente durchführen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie für die Integration eine SSL-Verbindung benötigen, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie in der Adresszeile auf das Sperrsymbol.

   c. Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
   Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu**, und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   b. Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   d. Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

**Hinweis:**
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

### Bedrohungssuche – OPSWAT Metadefender-Workflow

Der Workflow „Bedrohungssuche – OPSWAT Metadefender“ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen

Automatische Übersetzung

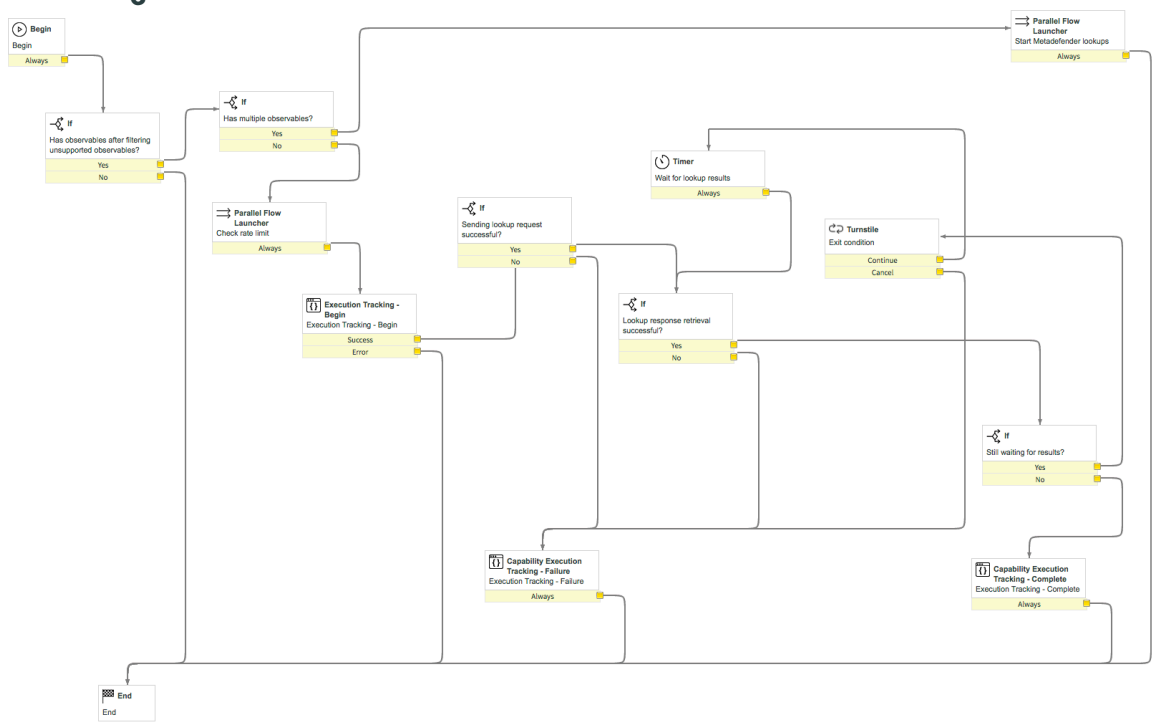
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um einen von OPSWAT Metadefender erkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

### Vorbereitungen
Erforderliche Rolle: sn_si.admin

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von Security Operations-Integration – Funktion „Bedrohungssuche“. ausgelöst, wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen und die Implementierung von OPSWAT Metadefender ausgewählt ist. Weitere Informationen finden Sie unter Suchvorgänge für erkennbare Elemente durchführen.

**Bedrohungssuche – OPSWAT Metadefender-Workflow**




Weitere Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## Integration mit VirusTotal

Mit der VirusTotal -Integration können Sie die Analyse verdächtiger IP-Adressen, Dateien, Datei-Hashes und URL-Adressen anfordern, um festzustellen, ob sie böswillig sind.

| | |
|---|---|
| Erkunden<br><br>Threat Intelligence-Integrationen | Einrichten<br><br>• VirusTotal Integrationen-Setup<br>• Aktivieren und konfigurieren Sie die VirusTotal-Integration |
| Verwenden | Entwickeln |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| | |
|---|---|
| • Suchvorgänge für erkennbare Elemente durchführen<br>• Workflow „Bedrohungssuche – VirusTotal“. | • ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und Hilfe | |
| • Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community<br>• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen<br>• Kontakt Kundenservice und Support | |

### VirusTotal Integrationen-Setup

VirusTotal ist ein kostenlosen Service, der verdächtige Dateien und URLs analysiert und die schnelle Erkennung von Viren, Worms, Trojanern und allen Arten von Malware ermöglicht. Die Integration mit Security Operationsist problemlos möglich.

Bevor Sie die VirusTotal -Integration verwenden können, müssen Sie das Plugin aktivieren und den entsprechenden API-Schlüssel hinzufügen. Bei Bedarf können Sie auch Ihre X509 SSL-Zertifizierung aktualisieren.

Wenn die Suchquelle VirusTotal verwendet wird und Malware gefunden wird, wird ein erkennbares Element erstellt. Für IP-Suchen wird eine zusätzliche Liste von URLs erstellt, die die IP-Adresse gemeinsam nutzen, und für jede der URLs werden erkennbare Elemente erstellt.

**Hinweis:**

- Das Threat Intelligence -Plugin ist erforderlich, um die VirusTotal -Integration zu implementieren.
- Die VirusTotal -Integration wurde auf APIs der Version 3 aktualisiert.

### Aktivieren und konfigurieren Sie die VirusTotal-Integration

Bevor Sie die VirusTotal-Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen.

#### Vorbereitungen

Erforderliche Rolle: admin

Threat Intelligence muss installiert und aktiviert sein, bevor Sie VirusTotal verwenden können. Die VirusTotal -Integration wurde auf APIs der Version 3 aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf VirusTotal zu, und rufen Sie den API-Schlüssel unter Ihrem VirusTotal-Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
4. Klicken Sie auf der VirusTotal-Karte auf **Konfigurieren**.

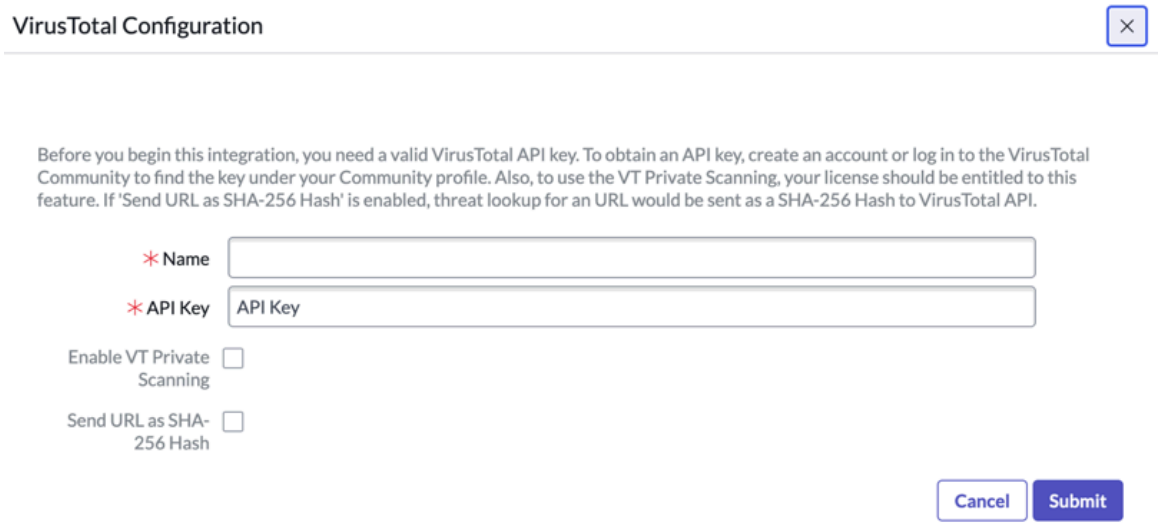
#### VirusTotal-Konfiguration

| Feld | Beschreibung |
|---|---|
| Name | Name der Integration Beispiel: VirusTotal. |
| API-Schlüssel | Geben Sie den **API-Schlüssel** ein (oder fügen Sie ihn ein), den Sie von der VirusTotal-Website erhalten haben. |
| VT Private Scanning aktivieren | Aktivieren Sie dieses Kontrollkästchen, um Dateien mit VirusTotal datenschutzkonform zu analysieren. Die über dieses Angebot hochgeladenen Dateien werden nicht für andere Personen als Ihre Organisation freigegeben und verbleiben nur für kurze Zeit in VirusTotal.<br><br>Die resultierenden Analysen sind ebenfalls flüchtig und nur für Ihre VirusTotal-Gruppe sichtbar.<br><br>**Wichtig:**<br>Um VT Private Scanning zu verwenden, muss Ihre VirusTotal-Lizenz für diese Funktion berechtigt sein. |
| URL als SHA-256-Hash senden | Aktivieren Sie dieses Kontrollkästchen, um die URLs als Hashes für die Bedrohungssuche zu senden und die Privatsphäre der Benutzer bei der Integration zu schützen.<br><br>**Hinweis:**<br>Wenn diese Option deaktiviert ist, wird die URL als Base64-Codierung an die VirusTotal-API gesendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.




## Ergebnisse

Nach der Konfiguration kann VirusTotal für Suchvorgänge für erkennbare Elemente in Threat Intelligence und für erkennbare Elemente in Security Incidents ausgewählt werden.

### Zugehörige Informationen

Suchvorgänge für erkennbare Elemente durchführen

### Workflow „Bedrohungssuche – VirusTotal“.

Der Workflow „Bedrohungssuche – VirusTotal “ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn es sich bei den erkennbaren Elementen um einen von VirusTotalerkannten Typ handelt, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

## Vorbereitungen

Erforderliche Rolle: admin

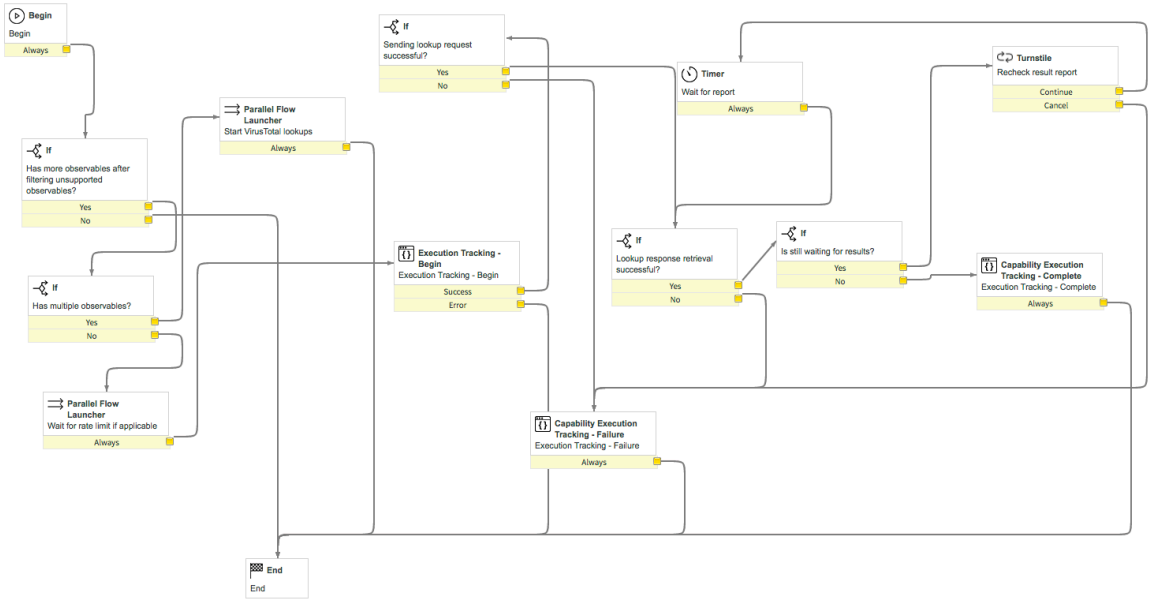
## Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird von Security Operations-Integration – Funktion „Bedrohungssuche“. ausgelöst, wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen und die Implementierung von VirusTotal ausgewählt ist. Weitere Informationen finden Sie unter Suchvorgänge für erkennbare Elemente durchführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow „Bedrohungssuche – VirusTotal“.**




Weitere Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

## WhoisXML-API-Integration

Mit der WhoisXML-API-Integration können Sie Whois-Suchen für Domänennamen und URLs übermitteln, um Kontext für erkennbare URL-Elemente zu erhalten und Bedrohungen besser zu bestimmen.

| | |
|---|---|
| Erkunden<br><br>Threat Intelligence-Integrationen | Einrichten<br><br>• WhoisXML-API-Integrationssetup<br>• Aktivieren und konfigurieren Sie die Security Operations Whois-Integration |
| Verwenden<br><br>Threat Intelligence IoC-Such-Workflow ausführen | Entwickeln<br><br>• ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen<br>• Tipps zum Schreiben von Integrationen<br>• Entwicklerschulungen<br>• Entwicklerdokumentation<br>• Suchen Sie nach Komponenten, die mit einer Anwendung installiert wurden |
| Problembehandlung und Hilfe<br><br>• Fehlerbehebung bei der Integration<br>• Stellen oder beantworten Sie Fragen in der Security Operations-Community | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

### WhoisXML-API-Integrationssetup

Bevor Sie die Whois-Integration verwenden können, müssen Sie das Plugin aktivieren und die Anmeldeinformationen hinzufügen. Bei Bedarf können Sie auch Ihre X509 SSL-Zertifizierung aktualisieren.

Die Plugins Threat Intelligence und WhoisXML API Integration sind erforderlich, um die WhoisXML-API-Integration zu implementieren.

### Aktivieren und konfigurieren Sie die Security Operations Whois-Integration

Mit der Funktion „Integrationskonfiguration“ können Sie Sicherheitsintegrationen von Drittanbietern, einschließlich der Whois-Integration von Security Operations, schnell aktivieren und einrichten. Bevor Sie die Security Operations Whois-Integration verwenden können, müssen Sie sie aus dem ServiceNow Storeherunterladen und über ein gültiges Konto in der WhoisXML-API verfügen.

#### Vorbereitungen

Threat Intelligence muss installiert und aktiviert sein, bevor Sie die Whois-Integration von Security Operations verwenden können.

Erforderliche Rolle: admin

#### Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Store.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt.
3. Klicken Sie in der Whois-API-Karte auf **Konfigurieren**.
4. Geben Sie den Benutzernamen und das Passwort aus Ihrem WhoisXML-API-Konto ein.
5. Klicken Sie auf **Absenden**.

### Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie für die Integration eine SSL-Verbindung benötigen, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Diese Aufgabe ist optional.

#### Vorbereitungen

Erforderliche Rolle: admin

#### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
      Beispiel: https://<3rdparty>/.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**b.** Klicken Sie in der Adresszeile auf das Sperrsymbol.

**c.** Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.

**d.** Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.

**e.** Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.

**f.** Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu**, und erstellen Sie einen neuen Datensatz für die Integration.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   **a.** Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**.
   **b.** Wählen Sie den aktiven Standardidentitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   **c.** Scrollen Sie nach unten zur zugehörigen Liste **X.509-Zertifikate**, und klicken Sie auf **Bearbeiten**.
   **d.** Verschieben Sie das neu erstellte Zertifikat in die Spalte **Ausgewählt**.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

> **Hinweis:**
> Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 Ablaufendes SAML-Zertifikat ersetzen .

### Workflow „Erkennbares WhoIs anreichern“.

Der Workflow **„Erkennbares WhoIs anreichern“** führt eine Ergänzung für ausgewählte erkennbare Elemente durch. Wenn die erkennbaren Elemente von einem Typ sind, der von WhoisXML-API-Integrationerkannt wird, werden die erkennbaren Elemente angereichert.

### Vorbereitungen

Erforderliche Rolle: admin

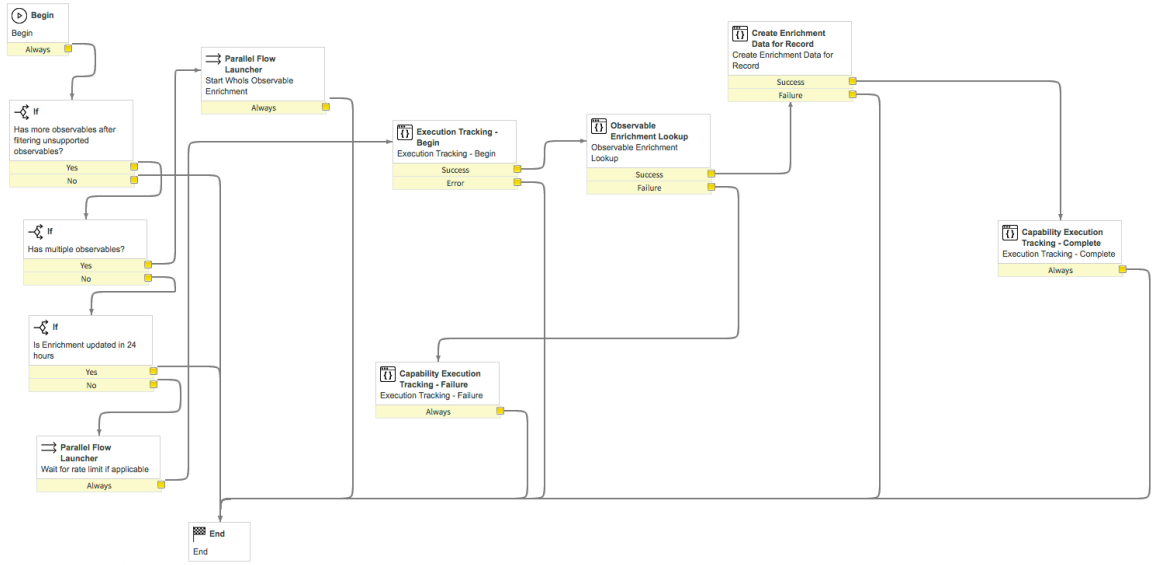
### Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird von Integration von Sicherheitsvorgängen – Fähigkeit „Erkennbares Element anreichern“. ausgelöst, wenn Sie eine Ergänzung für ein oder mehrere erkennbare Elemente durchführen und die WhoIs-Implementierung ausgewählt ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Workflow „Erkennbares WhoIs anreichern“.**




Spezifische Aktivitäten für diese Integration werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Anreicherung erkennbarer Elemente“

Die Workflow-Aktivität **„Anreicherung erkennbarer** Elemente“ initiiert den Ergänzungsprozess für erkennbare Elemente.

Die Aktivität „ **Anreicherung** erkennbarer Elemente“ kann mit jedem Workflow für erkennbare Elemente verwendet werden, um mit der Ergänzung zu beginnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Die Suche ist erfolgreich. |
| Fehlgeschlagen | Beim Versuch, die Suche durchzuführen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| „implementierung_id“. | Systembezeichner der Implementierung, die für die Suche verwendet wird. |
| domain_id | Der Domänenbezeichner für die Domäne, in der die Suche ausgeführt wird. |
| observable_ids | Ein oder mehrere erkennbare Elemente, für die die gewünschte Aktion ausgeführt werden soll. Die IDs werden als Workflow-Eingabe verwendet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityExcutionId | Systembezeichner der Fähigkeit, die den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows von Integration Capability wie Splunk, Elasticsearch erforderlich. |
| task_sys_id | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response_data | Rohdaten, die vom API-Endpunkt der Implementierung für die angegebene Domäne zurückgegeben werden. |
| „mapping_id“ | Der Bezeichner für die Ergänzungszuordnung. Beispielsweise gibt die WhoIs-Integration Daten in zwei verschiedenen Formaten zurück, IP und URL, mit jeweils einer Zuordnungs-ID. |

## Orchestration für Threat Intelligence

Threat Intelligence Orchestration Mit -Aktivitäten können Benutzer mithilfe der Workflow-Orchestrierung feststellen, ob eine Bedrohung zuvor in anderen Security Incidents oder auf anderen Systemen erkannt wurde.

Weitere Informationen zum Bearbeiten von Security Incident Response Orchestration -Workflows oder zum Erstellen benutzerdefinierter Workflows finden Sie unter Erste Schritte mit Workflows und Workflow-Editor Workflow-Editor .

### Richten Sie Threat Intelligence Orchestration ein

Führen Sie vor der Verwendung von Threat Intelligence OrchestrationSchritte zum Einrichten verschiedener Teile des Systems aus, einschließlich Ausfüllen der CMDB, Konfigurieren des MID Servers und Konfigurieren der Anmeldeinformationen.

#### Vorbereitungen

Erforderliche Rolle: admin

Zur Verwendung von Threat Intelligence Orchestration benötigen Sie eine vollständig mit Domänennamen ausgefüllte CMDB. Weitere Informationen finden Sie unter Discovery .

#### Warum und wann dieser Vorgang ausgeführt wird

#### Prozedur

1. Aktivieren Sie das Threat Intelligence-Plugin.
2. Konfigurieren Sie den MID Server
3. Konfigurieren Sie Anmeldeinformationen für den MID Server-Service
   Sie können jetzt Threat Intelligence Orchestration Aktivitäten in einem Workflow verwenden.

### Workflows und Aktivitäten von Threat Intelligence Orchestration

Das Basissystem enthält Workflows und Workflow-Aktivitäten, mit denen Sie Aktionen in Ihrer Instanz automatisieren können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Threat Intelligence IoC-Such-Workflow ausführen

Der Workflow „ **Threat Intelligence – IoC** -Suche ausführen“ überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf **Abgeschlossen** gesetzt und mit den Daten aus dem erkennbaren Element aktualisiert.

**Vorbereitungen**
Erforderliche Rolle: sn_si.basic

**Hinweis:**
Dieser Workflow ersetzt Threat Intelligence Orchestration Geschäftsregeln (**Mit vorhandenen IoC-Tabellen ausfüllen**, Suche in **die Warteschlange stellen**und **Erkennbares Element aktualisieren**) durch Aktivitäten.

Wenn eine Suche eingefügt oder aktualisiert wird und die Bedingungen erfüllt, löst die Business Rule Suche diesen Workflow aus.

**Warum und wann dieser Vorgang ausgeführt wird**
Der Workflow „ **Threat Intelligence – IoC** -Suche ausführen“ überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf **Abgeschlossen** gesetzt und mit den Daten aus dem erkennbaren Element aktualisiert. Alle mit dem erkennbaren Element verknüpften Indikatoren werden erneut aktiviert.

Wenn das erkennbare Element abgelaufen ist, führt der Workflow die Suchvorgänge aus und erhöht die **Sichtungsanzahl** im vorhandenen, abgelaufenen erkennbaren Element.

Wenn kein korrelierendes erkennbares Element vorhanden ist, wird ein neues erkennbares Element mit Indikator erstellt.

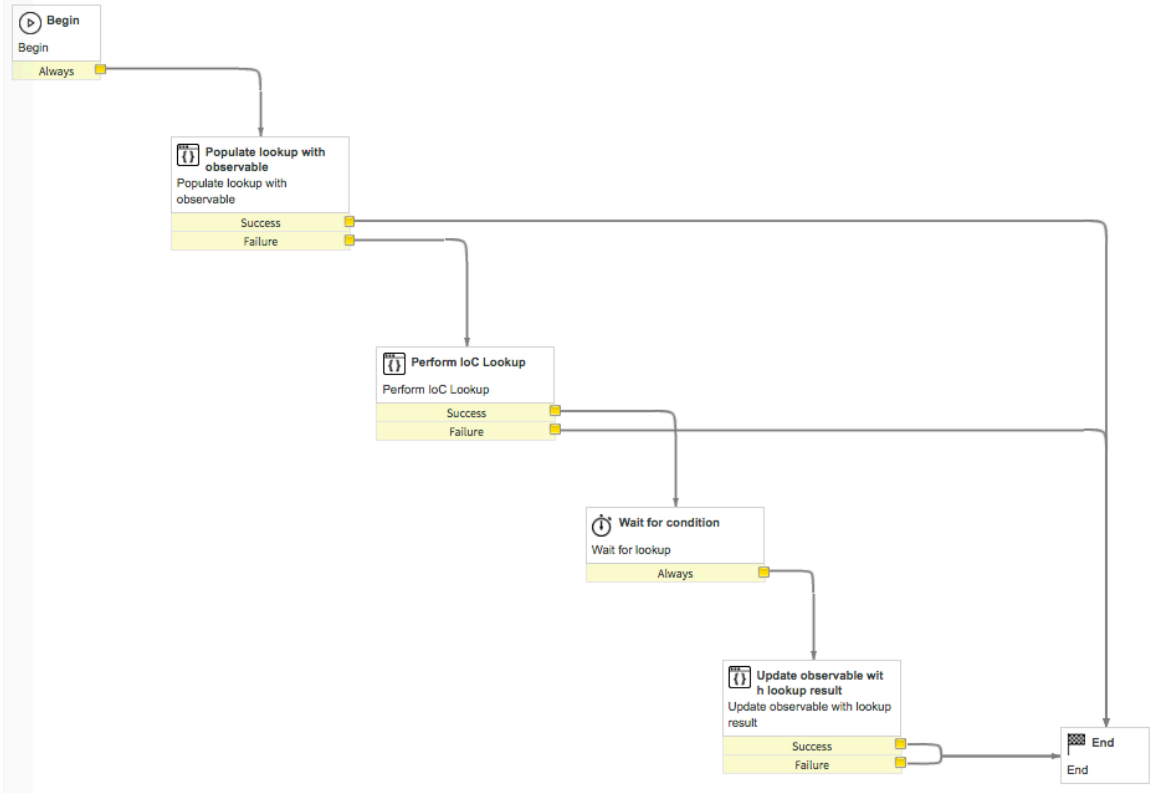
Workflow-Prozessaktivitäten umfassen:

- Füllen Sie die Suche mit der Aktivität „Erkennbares Element“ aus
- IoC-Suchaktivität ausführen
- Warten auf Suche (Kernaktivität)
- Erkennbares Element mit Suchergebnisaktivität aktualisieren



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Threat Intelligence – IoC-Such-Workflow ausführen




### Füllen Sie die Suche mit der Aktivität „Erkennbares Element“ aus

Wenn ein nicht abgelaufenes erkennbares Element gefunden wird, stellt die Workflow-Aktivität **Threat Intelligence Orchestration – Suche mit erkennbarem Element ausfüllen** Daten aus einem vorhandenen erkennbaren Element für eine Suche bereit. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Wenn durch einen Workflow **„Suche mit erkennbarem Element ausfüllen** “ ausgelöst, wird versucht, ein vorhandenes erkennbares Element für eine Suche zu finden, die dem **Wert** und **Typ** der Suche entspricht, die der Aktivität als Eingabe bereitgestellt wurde.

Wenn das erkennbare Element vorhanden und nicht abgelaufen ist, wird diese Aktivität:

- Aktualisiert die Suche mit den im erkennbaren Element gefundenen Informationen
- Reaktiviert einen Indikator, wenn er inaktiv ist, erhöht die **Anzahl**der erkannten Fälle und aktualisiert das **Zuletzt gesehen** -Datum
- **Legt** den Status auf „Abgeschlossen“ fest.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Eingabevariablen | Beschreibung |
|---|---|
| scanID[Zeichenfolge] | Suchbezeichner |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

| Ausgabevariablen | Beschreibung |
|---|---|
| Wahr | Gültiges erkennbares Element gefunden und Suche aktualisiert. |
| Falsch | Es wurde kein gültiges erkennbares Element gefunden. Erkennbares Element fehlt oder ist abgelaufen. |

### IoC-Suchaktivität ausführen

Die Workflow-Aktivität **Threat Intelligence Orchestration – IoC-** Suche durchführen führt eine bestimmte Suche aus. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Wenn **IoC** -Suche durchgeführt durch einen Workflow ausgelöst wird, wird eine scanID verwendet, der Suchdatensatz wird durchsucht, und die Suche wird der Warteschlange hinzugefügt, indem ein Suchwarteschlangeneintrag erstellt wird.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| scanID[Zeichenfolge] | Suchbezeichner |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Wahr | Die Suche wurde ausgelöst. |
| Falsch | Die Suche wurde nicht ausgelöst. |

### Erkennbares Element mit Suchergebnisaktivität aktualisieren

Die Workflow-Aktivität **Threat Intelligence Orchestration - Update erkennbares Element mit Suchergebnis** aktualisiert den Datensatz des erkennbaren Elements. Wenn keines vorhanden ist, wird ein neues erkennbares Element erstellt. Diese Aktivität ist nützlich für die Protokollierung von Informationen.

Bei Auslösung durch einen Workflow „ **Erkennbares Element mit Suchergebnis** aktualisieren“ wird ein vorhandenes erkennbares Element mit der neuen **Sichtungsanzahl**aktualisiert, eine Notiz hinzugefügt und, falls inaktiv, alle Indikatoren erneut aktiviert. Die **Anzahl** der Konsultationen und das Datum der **letzten** Anzeige im Indikator werden ebenfalls aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn kein korrelierendes erkennbares Element vorhanden ist, erstellt der Workflow wie folgt ein neues erkennbares Element mit Indikator:

- Führt die IoC-Suchen aus
- Erstellt ein neues erkennbares Element
- Erstellt einen Indikator für das erkennbare Element
- Fügt dem erkennbaren Element eine **Sichtungsanzahl** hinzu
- Fügt dem Indikator die **Anzahl** „Erkannt“ und das Datum „ **Zuletzt** angezeigt“ hinzu
- Fügt eine Meldung hinzu, die angibt, aus welcher Suche sie erstellt wurde

.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| scanID[Zeichenfolge] | Suchbezeichner. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Wahr | Aktualisierung oder Erstellung des erkennbaren Elements war erfolgreich. |
| Falsch | Fehler beim Aktualisieren oder Erstellen des erkennbaren Elements. |

### Führen Sie die Aktivität „Standard-IoC-Suchquellen“ aus

Bei Auslösung durch einen Workflow nimmt Threat Intelligence - **Standard-IoC-Suchquellen ausführen** eine Suchanforderungs-ID auf und erstellt abhängig von den eingegebenen Datenwerten mehrere Suchvorgänge.

Für jeden Datentyp wird die **Scan-Spalte include_in_bulk** der unterstützten Suchtyptabelle jeder Suchquelle ausgewertet. Bei „true“ wird der Suchanforderung eine Suche hinzugefügt.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| scan_request_id | Systembezeichner der Suchanforderung |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Anzahl der erstellten Scans | Ganzzahl |

## Security Case Management

Security Case Management bietet Sicherheitsanalysten, die an der Bedrohungssuche beteiligt sind, die Möglichkeit, Informationen über verdächtige Aktivitäten in ihrer Umgebung zu sammeln. Fallbezogene Datensätze wie Security Incidents, erkennbare Elemente, CIs und betroffene Benutzer können Fällen hinzugefügt werden, um eine umfassende und spezifische Analyse zu ermöglichen.

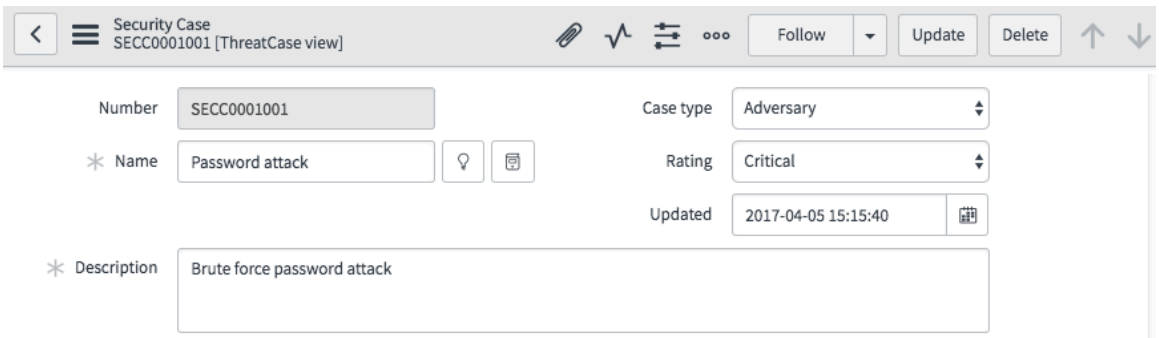
Mit der Möglichkeit, einfach durch die Datensätze und zugehörigen Informationen zu navigieren, können Analysten beurteilen, ob sie einer gezielten Kampagne, einer erweiterten persistenten Bedrohung usw. ausgesetzt sind.

Sicherheitsfälle können aus verschiedenen Quellen in Ihrer Instanz erstellt werden, einschließlich Security Case Management, Security Incident Responseund Threat Intelligence. Sie können Fälle auch aus Konfigurationselementen und betroffenen Benutzern in den Tabellen „Konfigurationselemente“ [cmdb.ci] und „Benutzer“ [sys.user] erstellen. Nachdem Fälle erstellt wurden, kann jede dieser Quellen auch verwendet werden, um vorhandenen Fällen wertvolle Analyseressourcen hinzuzufügen.

Jeder Sicherheitsfall besteht aus drei Hauptabschnitten, einem Header-Abschnitt, einem Abschnitt mit zusätzlichen Falldetails und einem Abschnitt mit Fallartefakten, der eine Sammlung von Datensätzen enthält, die beim Erstellen eines Arguments für die Identifizierung und Behandlung bestimmter Bedrohungen helfen.

### Fall-Header

**Fall-Header-Abschnitt**



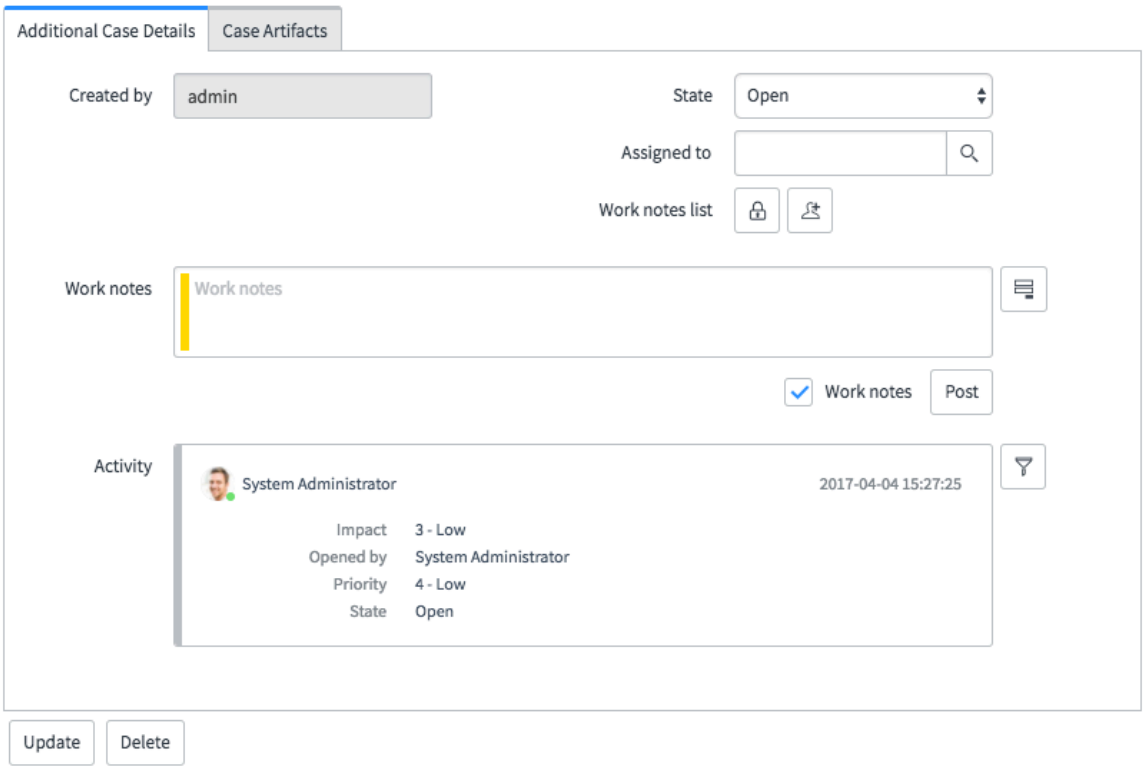

Der Fall-Header enthält grundlegende Informationen zum Identifizieren und Klassifizieren des Sicherheitsfalls. Die Fallnummer verwendet das SECC-Präfix.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zusätzliche Falldetails

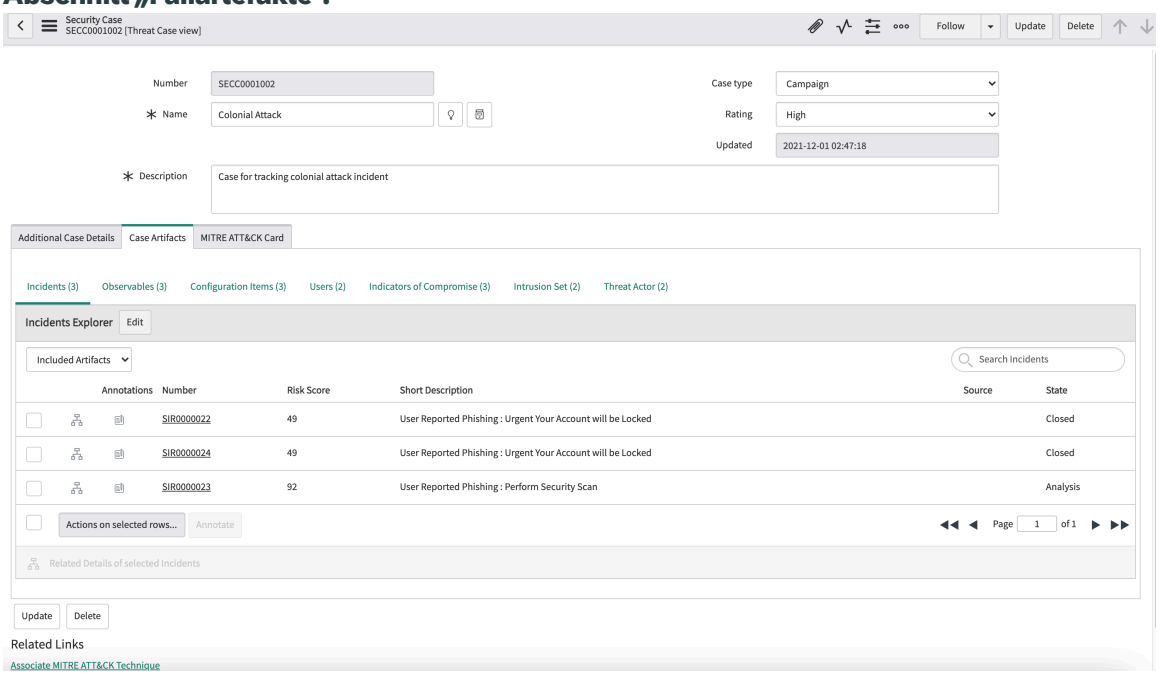
### Abschnitt „Zusätzliche Falldetails“.




Der Abschnitt „ **Zusätzliche Falldetails** “ enthält spezifische Informationen für die Analyse, die bereits für den Fall durchgeführt wurde, einschließlich des aktuellen Status sowie der für den Fall aufgezeichneten Arbeitsnotizen und Aktivitäten.

## Fallartefakte

### Abschnitt „Fallartefakte“.



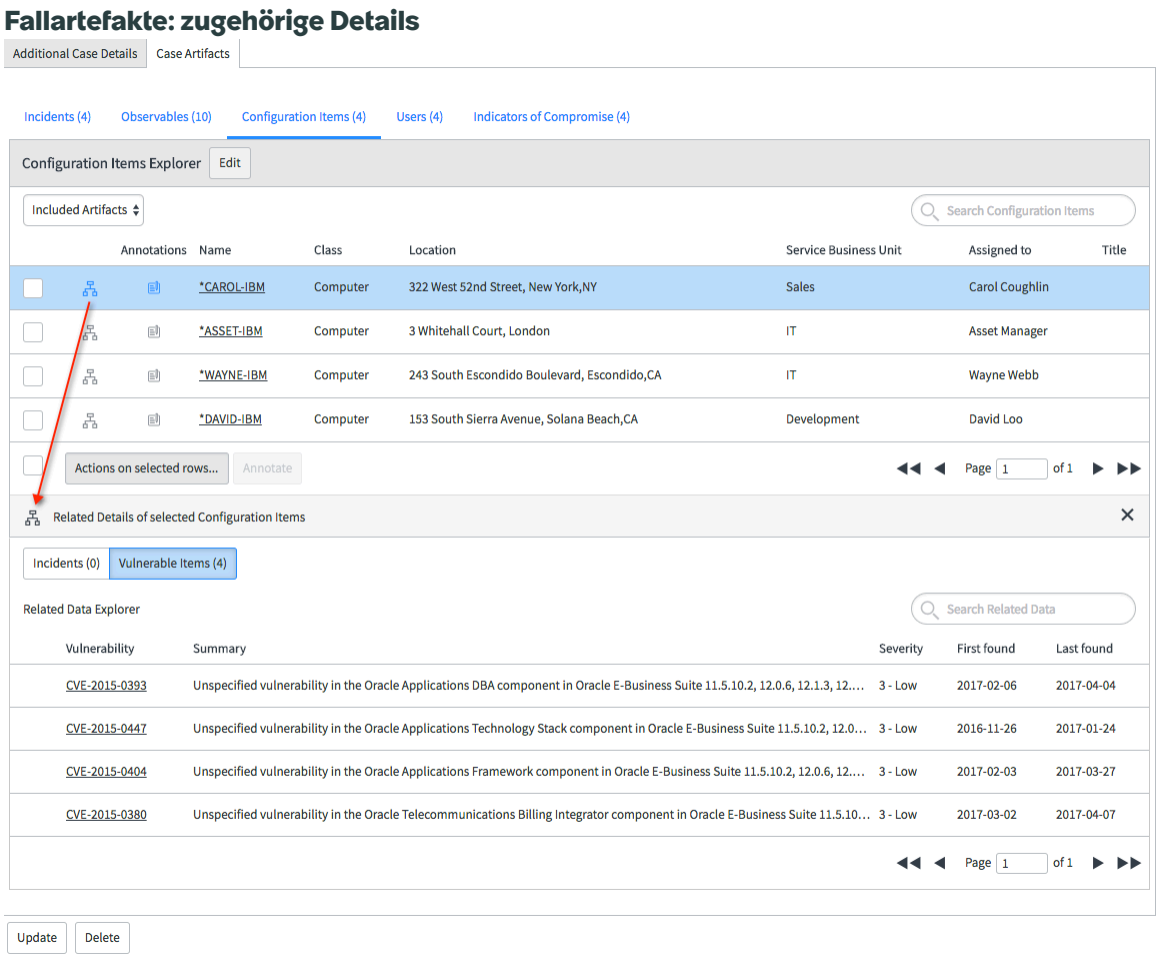

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abschnitt „ **Fallartefakte** “ enthält eine Reihe von Registerkarten mit Informationen, die im Sicherheitsfall enthalten sind.

Sie können den Inhalt jeder Registerkarte durchsuchen. Sie können auch bestimmte Datensätze ausschließen, die Sie bereits als sicher eingestuft haben oder die für Ihre Untersuchung keinen Wert haben. Die ausgeschlossenen Datensätze werden nicht gelöscht, sondern in der Ansicht ausgeblendet. Bei Bedarf können Sie ausgeschlossene Datensätze anzeigen und wieder hinzufügen.

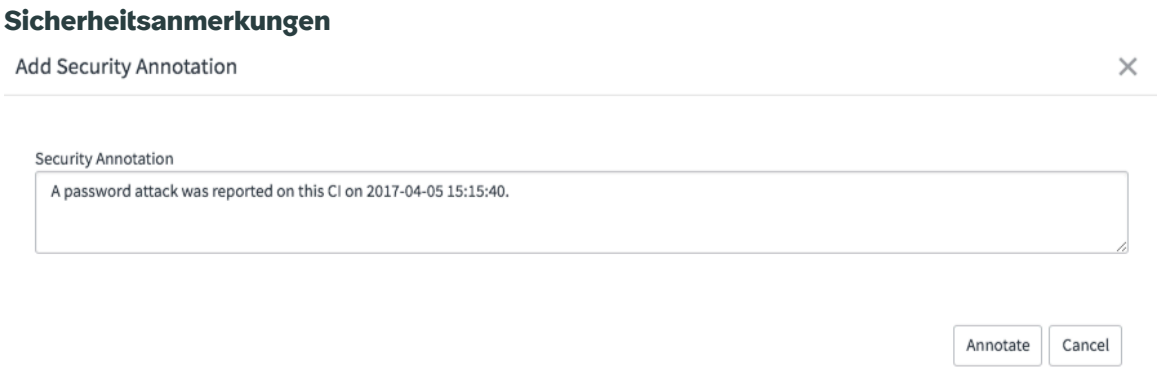
Auf jeder Registerkarte können Sie auf das Symbol Zusätzliche Details klicken, um zugehörige Informationen für den ausgewählten Datensatz anzuzeigen. Wenn Sie beispielsweise auf die Registerkarte **Konfigurationselemente** klicken, um den Explorer für Konfigurationselemente anzuzeigen, und für ein bestimmtes CI auf Zusätzliche Details klicken, können Sie Incidents, angreifbare Elemente und Anmerkungen anzeigen, die diesem CI zugeordnet sind.




Sie können auch einen Datensatz auswählen und auf die Schaltfläche **Kommentieren** für ein fallbezogenes Artefakt klicken, um dem Datensatz Anmerkungen hinzuzufügen. Anmerkungen sind einfach Notizen, die jeder Analyst zu einem bestimmten Artefakt machen kann.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Andere Tools, die der Analyst zur Untersuchung von Fällen verwenden kann:

- Führen Sie eine Sichtungssuche für erkennbare Elemente in einem Fall aus
- Suchen Sie nach Sicherheitsartefakten

## Erstellen Sie Fälle in Security Case Management

Fälle werden verwendet, um Informationen über eine Kampagne oder einen staatlichen Akteur nachzuverfolgen, die Ihre Organisation bedrohen. Nachdem ein Fall erstellt wurde, können Sie Artefakte hinzufügen, mit denen Sie alle zugehörigen Informationen in einem einzelnen Falldatensatz überprüfen und analysieren können.

### Vorbereitungen

Erforderliche Rolle: sn_ti.case_use

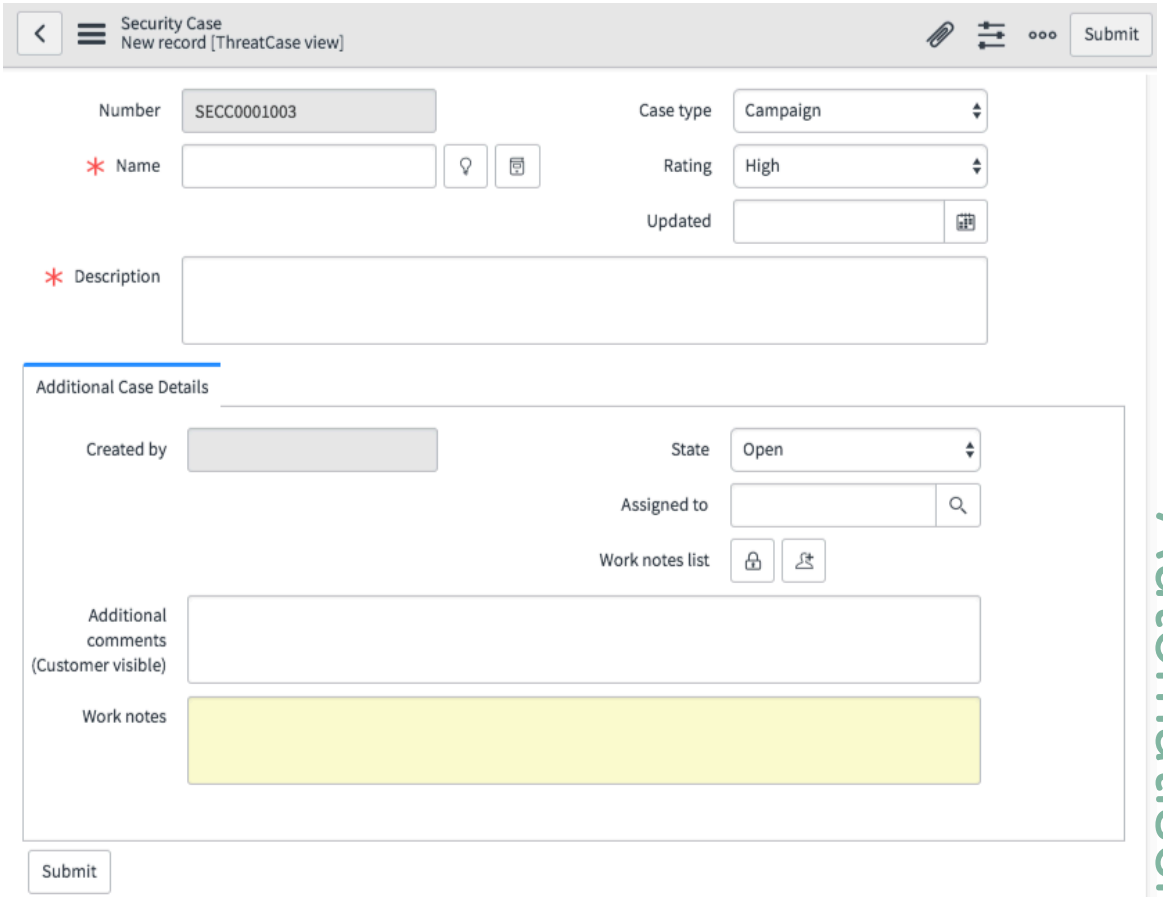
r

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallverwaltung** > **Alle Fälle**.
   Die Liste „Sicherheitsfälle“ wird geöffnet.
2. Klicken Sie auf **Neu**.
   Der Bildschirm „Sicherheitsfälle“ wird geöffnet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



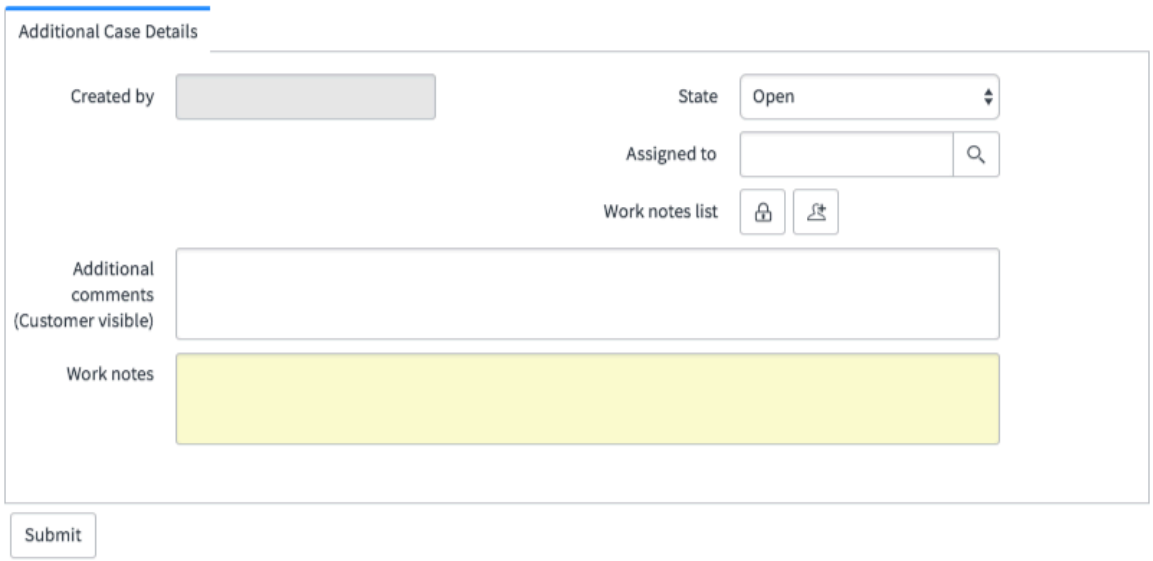

**3.** Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Fallnummer | [Nur Lesen] Die Fallnummer. |
| Fallname | Geben Sie einen beschreibenden Namen für den Fall ein. |
| Falltyp | Wählen Sie die Art des untersuchten Falls aus. |
| Bewertung | Wählen Sie die Wichtigkeit dieses Falls aus (von „Kritisch“ bis „Niedrig“). |
| Letztes Update | [Nur Lesen] Datum und Uhrzeit der letzten Aktualisierung des Falls. |
| Kurzbeschreibung | Eine kurze Beschreibung des Falls. |

**4.** Klicken Sie auf die Registerkarte **Zusätzliche** Falldetails.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Erstellt von | [Schreibgeschützt] Der Name des Benutzers, der diesen Fall erstellt hat. |
| Status | Aktueller Status des Falls. Bei der Fallerstellung wird der Status standardmäßig auf Entwurf gesetzt. |
| Zugewiesen an | Klicken Sie auf das Suchsymbol, und weisen Sie den Fall einem Analysten zu. |
| Arbeitsnotizenliste | Klicken Sie auf das Sperrsymbol, und fügen Sie interne Benutzer hinzu, die Arbeitsnotizen anzeigen können. |
| Zusätzliche Anmerkungen | Geben Sie nach Bedarf Notizen zum Fall ein, die für den Kunden sichtbar sind. |
| Arbeitsnotizen | Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein. |

6. Klicken Sie auf **Absenden**.
   Nachdem der Datensatz gespeichert wurde, können Sie auf die Registerkarte Fallartefakte klicken und dem **Fall Artefakte**hinzufügen.

### Fügen Sie einem Fall Artefakte hinzu

Nachdem Sie einen Fall erstellt haben, können Sie dem Fall Artefakte hinzufügen, z. B. Security Incidents, CIs und Gefährdungsindikatoren. Diese Artefakte dienen als Anhaltspunkte bei der Lösung des Falls.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

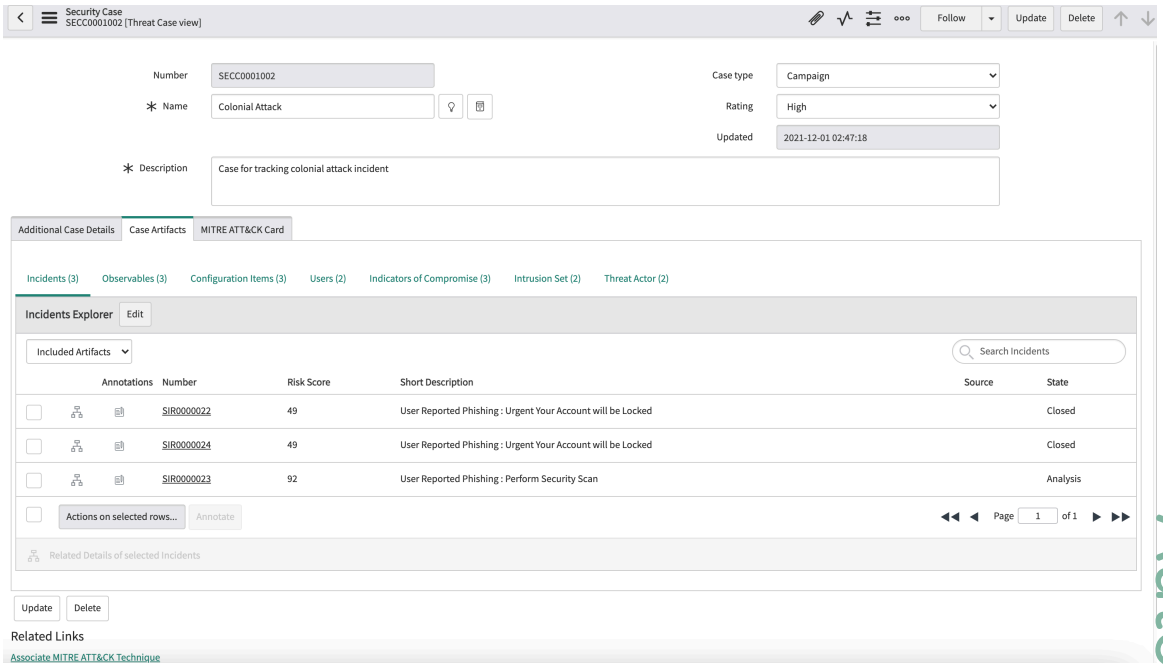
Erforderliche Rolle: sn_ti.case_user_write

#### Prozedur

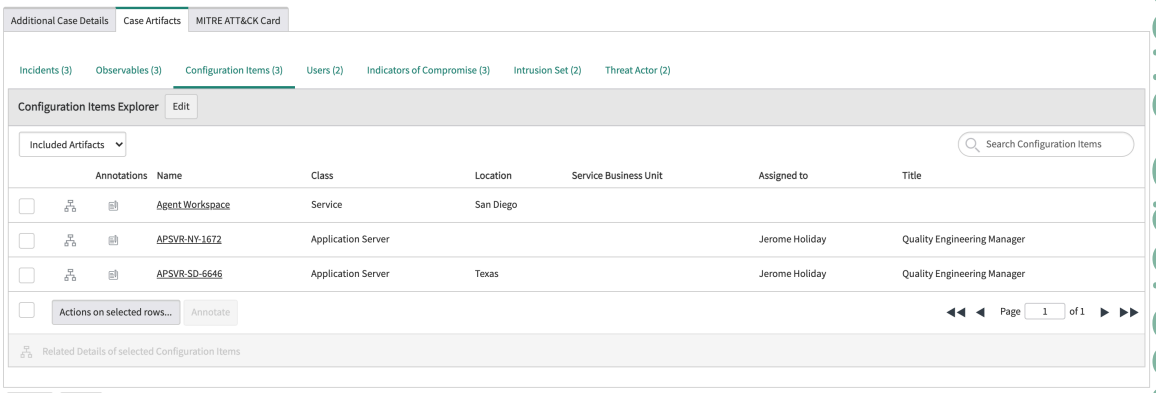
1. Öffnen Sie einen Fall, dem Sie Artefakte hinzufügen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



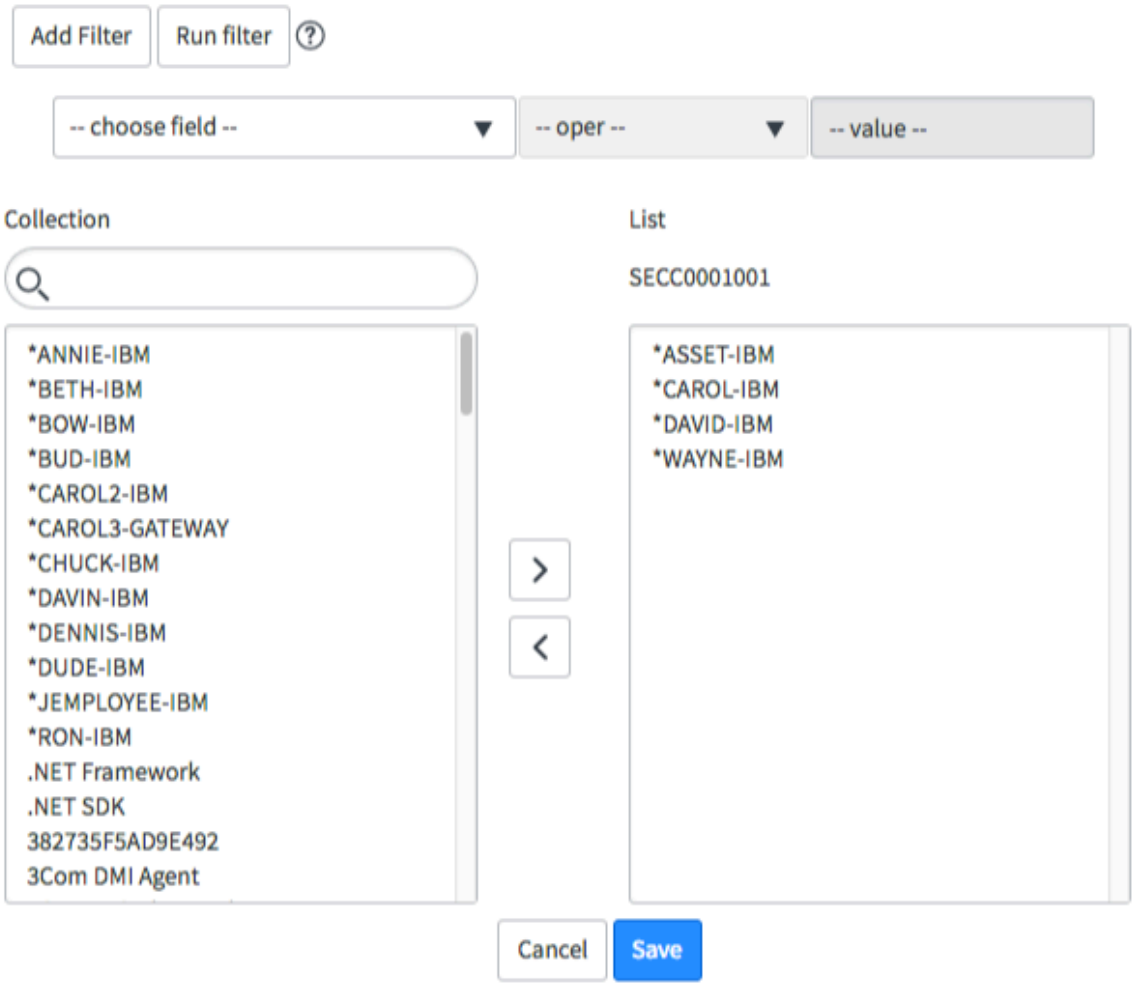

**3.** Klicken Sie auf die Registerkarte, die dem Artefakttyp zugeordnet ist, den Sie dem Fall hinzufügen möchten. Klicken Sie beispielsweise auf **Konfigurationselemente**, um dem Fall ein oder mehrere CIs hinzuzufügen.




**4.** Klicken Sie auf **Bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Suchen Sie mithilfe des Slushbuckets und der Filter nach den Artefaktdatensätzen, die Sie dem Fall hinzufügen möchten, verschieben Sie sie aus dem Bucket „Sammlung“ in den Bucket „Liste“ und klicken Sie auf **Speichern**.
   Die Liste wird auf der ausgewählten Registerkarte angezeigt, und die ausgewählten Artefakte werden der Liste hinzugefügt.

**Zugehörige Informationen**

Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Fügen Sie Security Incidents zu einem vorhandenen Fall hinzu

Fügen Sie CIs zu vorhandenen Fällen hinzu

Fügen Sie betroffene Benutzer zu vorhandenen Fällen hinzu

## Ordnen MITRE-ATT&CK Sie Informationen dem Sicherheitsfall zu

Ordnen Sie MITRE-ATT&CK Taktiken und Techniken einem Sicherheitsfall zu, um die Verwaltung von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene zu verbessern.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

Automatische Übersetzung

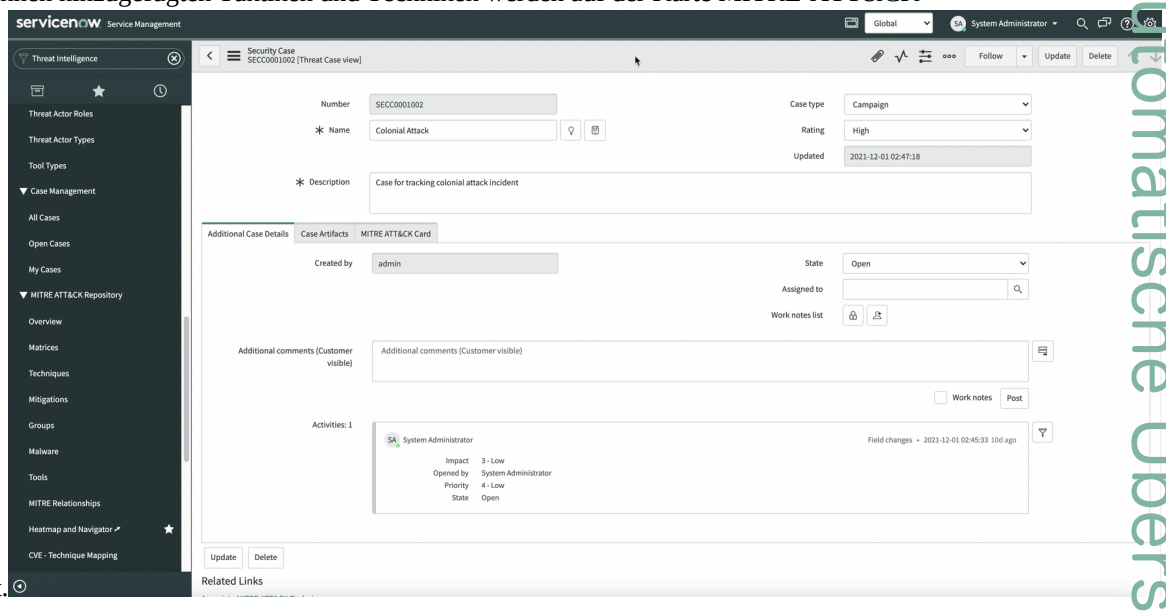
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallverwaltung** > **Alle Fälle**.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.
3. Klicken Sie in der zugehörigen Liste auf **MITRE ATT&CK-Technik zuordnen**.

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu **MITRE ATT&CK-Technik zuordnen**navigieren, die Quelle überprüfen und eine Taktik und Technik hinzufügen.

4. Überprüfen Sie in den Quelllisten die **Quelle**.
5. Überprüfen Sie die **Taktik** und **Techniken**, und fügen Sie sie basierend auf der Relevanz für den Fall hinzu oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die von Ihnen hinzugefügten Taktiken und Techniken werden auf der Karte MITRE-ATT&CK angezeigt.




## Fallerstellung aus Sicherheitsartefakten

Sie können Fälle nicht nur manuell über Security Case Managementerstellen, sondern auch Fälle aus Sicherheitsartefakten erstellen, z. B. aus Security Incidents, Gefährdungsindikatoren, betroffenen Benutzern und Konfigurationselementen.

### IoCs und erkennbare Elemente in Fällen

In Threat Intelligencekönnen Sie Fälle aus IoCs und erkennbaren Elementen erstellen sowie vorhandenen Fällen IoCs und erkennbare Elemente hinzufügen. Sie können erkennbare Elemente auch direkt aus einem Fall erstellen.

### Erstellen Sie einen Fall aus IoCs oder erkennbaren Elementen

In Threat Intelligencekönnen Sie einen Fall aus Artefakten (IoCs oder erkennbaren Elementen) erstellen. Nachdem die IoCs oder erkennbaren Elemente zum Erstellen eines Falls verwendet wurden, können Sie die Daten mit Security Case Management analysieren.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

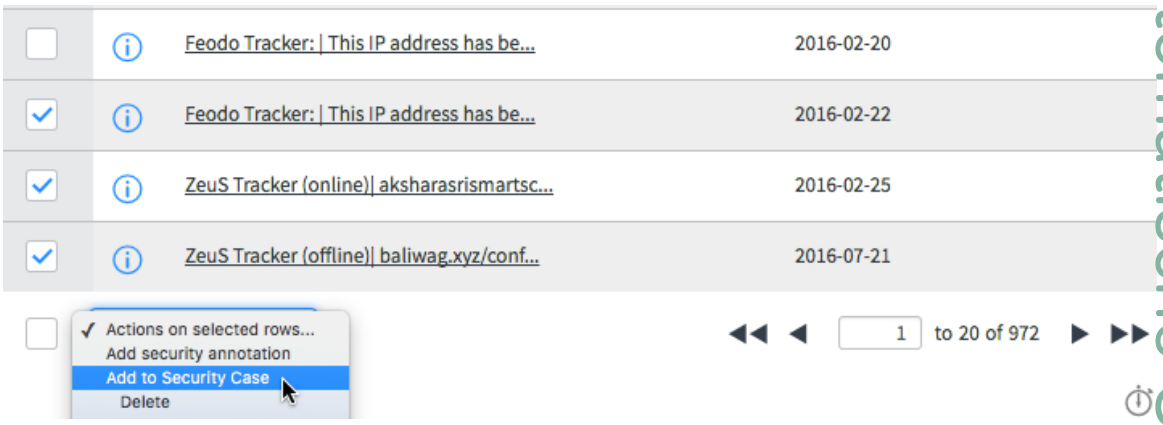
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

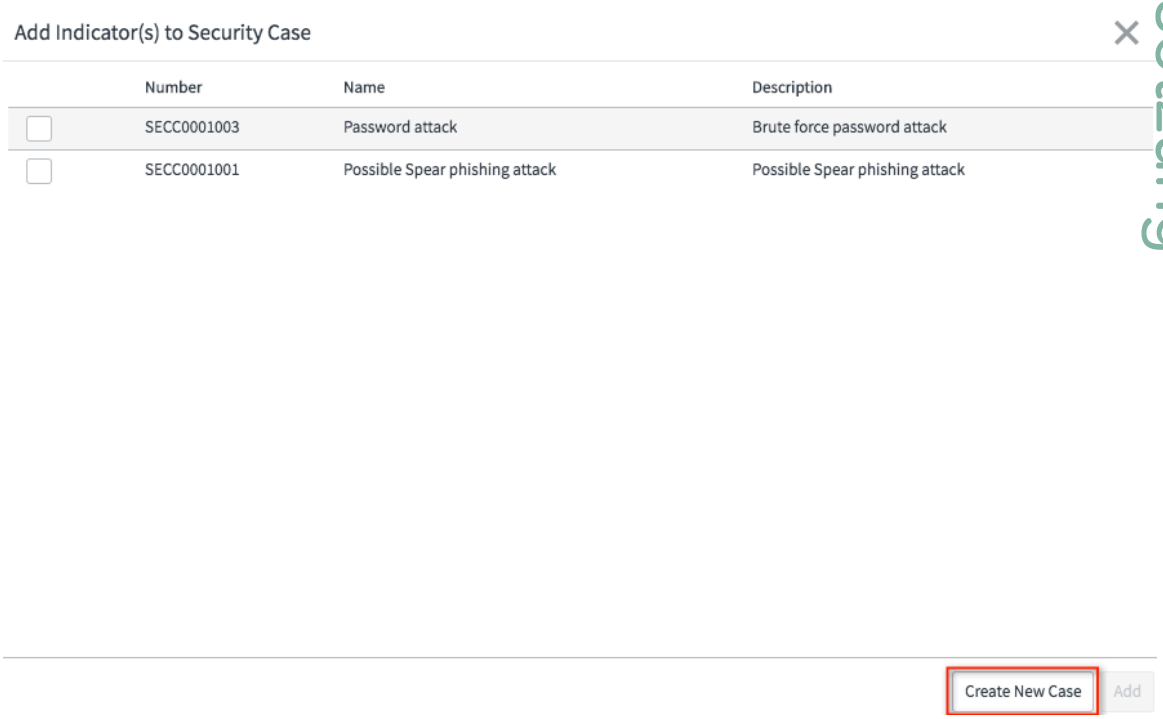
1. Navigieren Sie zu den Artefakten (IoCs oder erkennbaren Elemente), die Sie zum Erstellen eines Falls verwenden möchten.
   - Um einen Fall aus IoCs zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   - Um einen Fall aus erkennbaren Elementen zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Wählen Sie in der Liste die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.

   **Hinweis:**
   Wenn Sie mehrere IoCs oder erkennbare Elemente auswählen, werden sie alle dem Fall hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.




Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden diese in der Liste angezeigt.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken **Sie auf Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Fallname | Geben Sie einen Namen für diesen Fall ein. |
| Beschreibung | Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte. |

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zu dem Fall in Security Case Management.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

### Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Sie können vorhandenen Fällen IoCs und erkennbare Elemente hinzufügen. Nachdem die Security Incidents den Fällen hinzugefügt wurden, können Sie die Daten mit Security Case Management analysieren.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

#### Prozedur

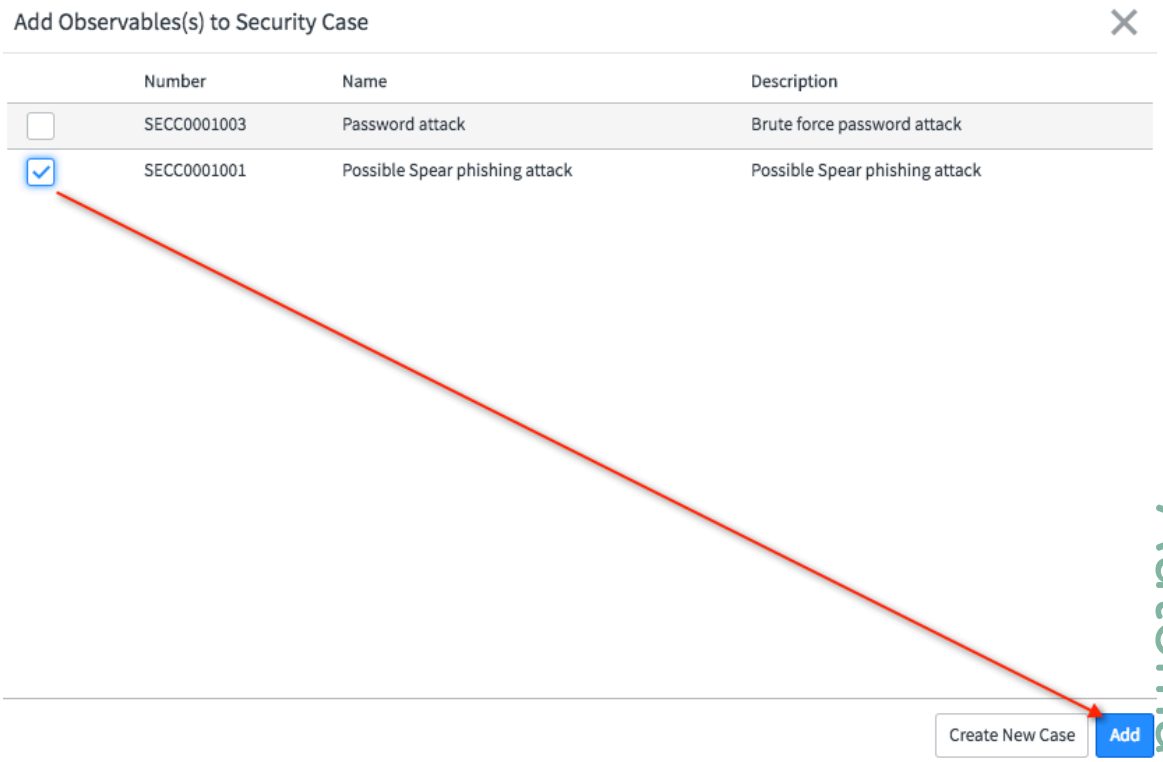
1. Navigieren Sie zu den Artefakten (IoCs oder erkennbaren Elemente), die Sie vorhandenen Fällen hinzufügen möchten.
   - Um einem oder mehreren Fällen IoCs hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**.
   - Um einem oder mehreren Fällen erkennbare Elemente hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**.
2. Wählen Sie in der Liste die Artefaktdatensätze aus, die Sie vorhandenen Fällen hinzufügen möchten.

   **Hinweis:**
   Wenn Sie mehrere Fälle auswählen, werden die ausgewählten IoCs oder erkennbaren Elemente jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.
   Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden diese in der Liste angezeigt.
4. Wählen Sie die Fälle aus, denen Sie die ausgewählten IoCs oder erkennbaren Elemente hinzufügen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht weist darauf hin, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Security Case Management.

### Erstellen Sie ein erkennbares Element aus einem Fall

Neue erkennbare Elemente können aus Fällen in Security Case Managementerstellt werden.

### Vorbereitungen

Erforderliche Rolle: sn_ti.case_user

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallverwaltung** > **Alle Fälle**.
   Die Liste „Sicherheitsfälle“ wird geöffnet.
2. Öffnen Sie entweder einen vorhandenen Fall, oder klicken Sie auf **Neu**, um einen neuen Fallzu erstellen.
3. Klicken Sie auf den zugehörigen Link **Fallartefakte**, und klicken Sie auf die Registerkarte **Erkennbare** Elemente.
4. Klicken Sie auf **Neu**, und geben Sie die angeforderten Informationen ein.

| Feld | Beschreibung |
|---|---|
| Wert | [Nur Lesen] Die Fallnummer. |
| Erkennbarer Typ | Geben Sie einen beschreibenden Namen für den Fall ein. |
| Kategorie des erkennbaren Typs | Wählen Sie die Art des untersuchten Falls aus. |
| Incident-Anzahl | Wählen Sie die Wichtigkeit dieses Falls aus (von „Kritisch“ bis „Niedrig“). |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Ergebnis | [Nur Lesen] Datum und Uhrzeit der letzten Aktualisierung des Falls. |
| Notizen | Eine kurze Beschreibung des Falls. |

5. Klicken Sie auf die Registerkarte **Zusätzliche** Falldetails.
6. Füllen Sie die Felder entsprechend aus.

| Feld | Beschreibung |
|---|---|
| Erstellt von | [Schreibgeschützt] Der Name des Benutzers, der diesen Fall erstellt hat. |
| Status | Aktueller Status des Falls. Bei der Fallerstellung wird der Status standardmäßig auf Entwurf gesetzt. |
| Arbeitsnotizenliste | Klicken Sie auf das Kontrollkästchen, um die Arbeitsnotizen im Abschnitt „Zusätzliche Falldetails“ des Falldatensatzes anzuzeigen. |
| Arbeitsnotizen | Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein. Wenn die **Liste** Arbeitsnotizen ausgewählt ist, wird die Arbeitsnotiz im Abschnitt „Zusätzliche Falldetails“ des Falldatensatzes angezeigt. |

7. Klicken Sie auf **Absenden**.
   Bei Bedarf können Sie auf die Registerkarte Fallartefakte klicken und dem **Fall Artefakte**hinzufügen.

### Führen Sie eine Sichtungssuche für erkennbare Elemente in einem Fall aus

Sie können mit der Sichtungssuchfunktion nach erkennbaren Elementen suchen, um zu bestimmen, wie oft sie vorkommen. Jedes Vorkommen wird als *Sichtung*betrachtet. Sie können die Suche auf die Anzahl der Sichtungen innerhalb einer ausgewählten Anzahl von Tagen oder innerhalb eines Datumsbereichs beschränken.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

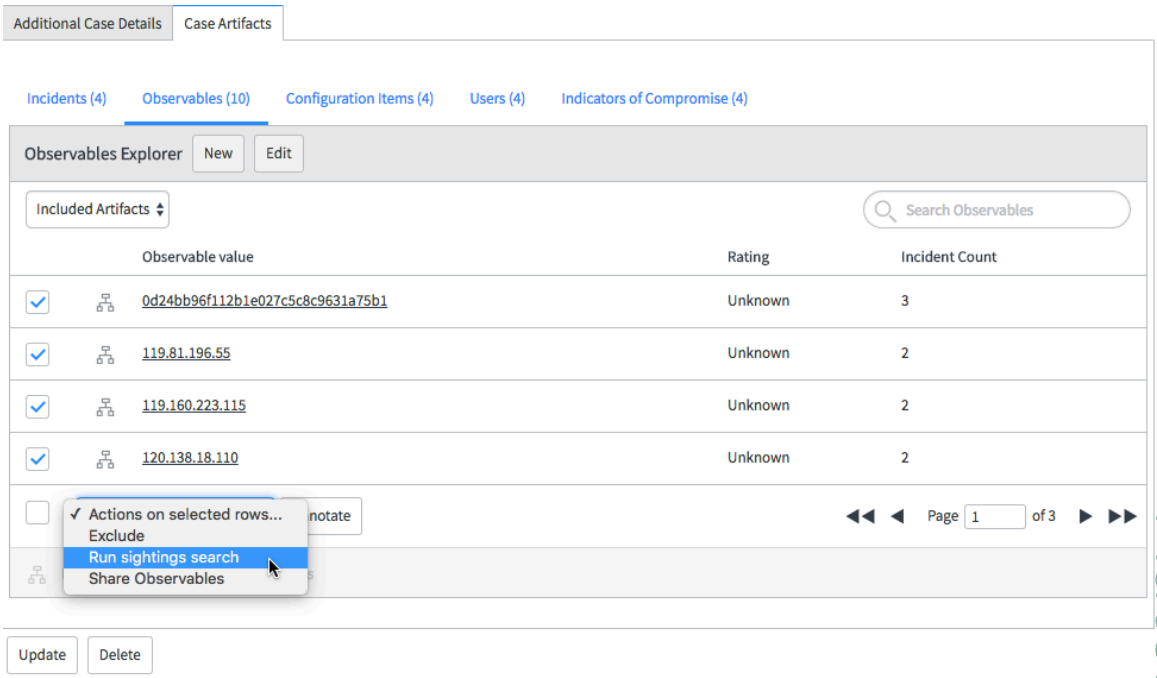
Erforderliche Rolle: sn_ti.case_user_write

#### Prozedur

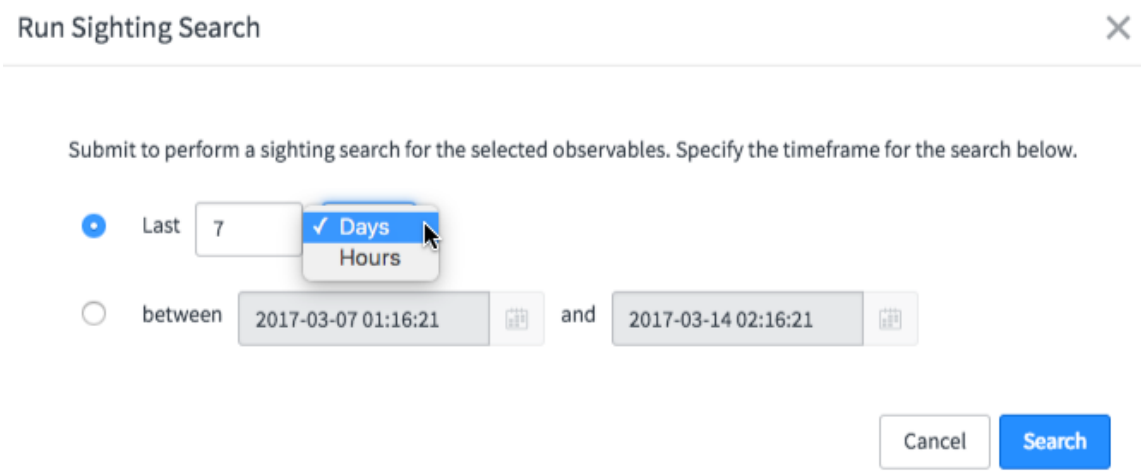
1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallverwaltung** > **Alle Fälle**.
2. Öffnen Sie den Fall, der erkennbare Elemente enthält, für die Sie eine Sichtungssuche ausführen möchten.
3. Klicken Sie auf den zugehörigen Link **Fallartefakte**.
4. Klicken Sie auf die Registerkarte **Erkennbare** Elemente.
5. Wählen Sie ein oder mehrere erkennbare Elemente aus, für die Sie nach Sichtungen suchen möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die **Option Sichtungssuche ausführen**aus.
   Das Dialogfeld „ **Sichtungssuche** ausführen“ wird angezeigt.




7. Geben Sie entweder die Anzahl der Tage oder Stunden ein, nach denen Sie nach Sichtungen der ausgewählten erkennbaren Elemente suchen möchten, oder wählen Sie einen Datumsbereich aus.
8. Klicken Sie auf **Suche**.

### Security Incidents in Fällen

In Security Incident Responsekönnen Sie Fälle aus Security Incidents, CIs und betroffenen Benutzern erstellen und diese Artefakte zu vorhandenen Fällen hinzufügen.

### Erstellen Sie einen Fall aus Security Incidents

In Security Incident Responsekönnen Sie Fälle aus Security Incidents erstellen. Nachdem die Security Incidents zum Erstellen eines neuen Falls verwendet wurden, können Sie die Daten mit Security Case Management analysieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

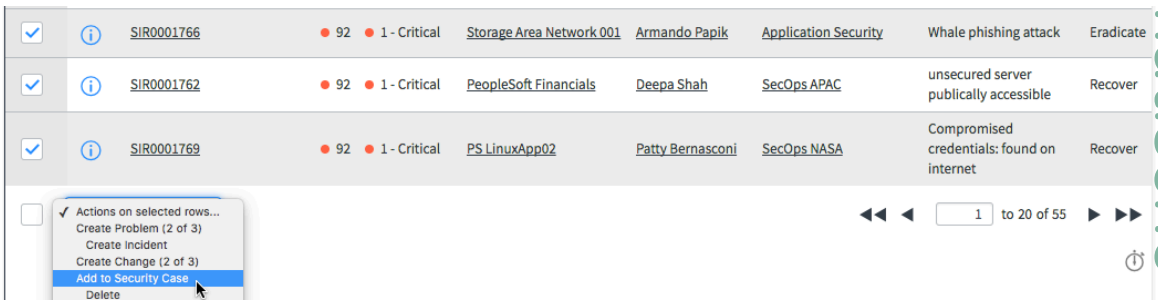
Erforderliche Rolle: sn_ti.case_user_write

## Warum und wann dieser Vorgang ausgeführt wird

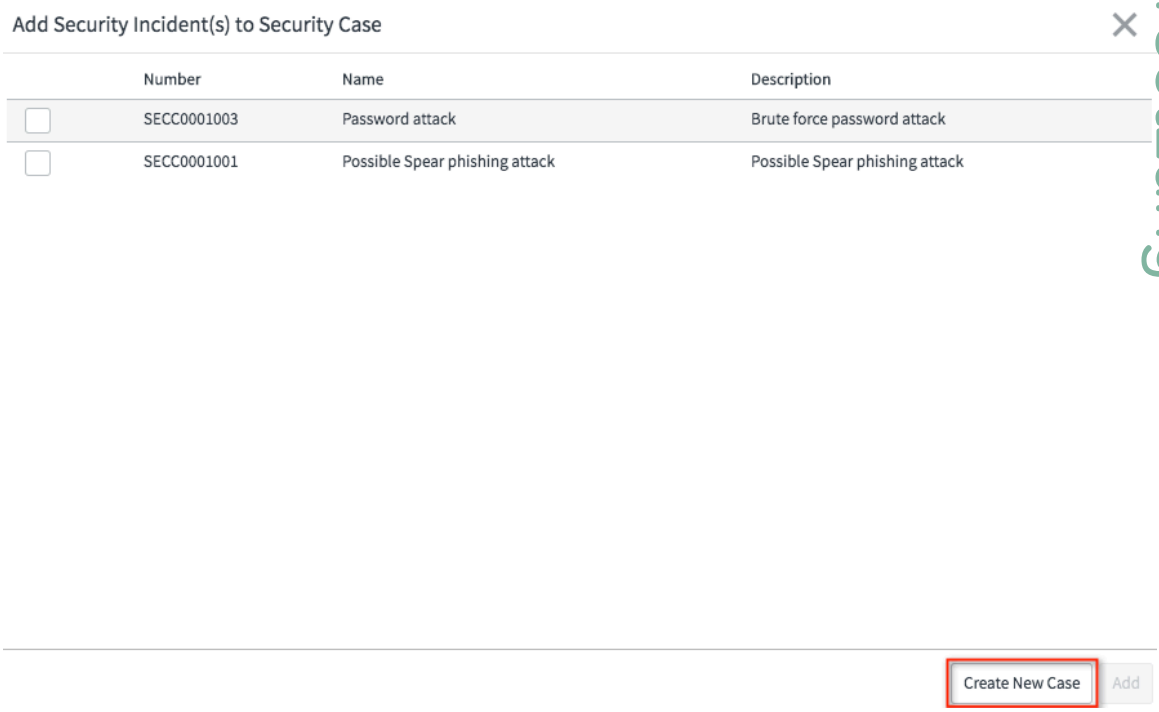
Sie müssen zu den Security Incidents navigieren, die Sie zum Erstellen von Fällen verwenden möchten.

## Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
   Die Liste Security Incidents wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Security Incidents erstellen, oder Sie können einen bestimmten Security Incident auswählen und einen neuen Fall aus dem Formular erstellen.
2. Um einen Fall aus der Liste zu erstellen, wählen Sie die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.




Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden diese in der Liste angezeigt.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken **Sie auf Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Fallname | Geben Sie einen Namen für diesen Fall ein. |
| Beschreibung | Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte. |

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zu dem Fall in Security Case Management.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

### Fügen Sie Security Incidents zu einem vorhandenen Fall hinzu

Sie können Security Incidents zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die Security Incidents den Fällen hinzugefügt wurden, können Sie die Daten mit Security Case Management analysieren.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

#### Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Security Incidents navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

#### Prozedur

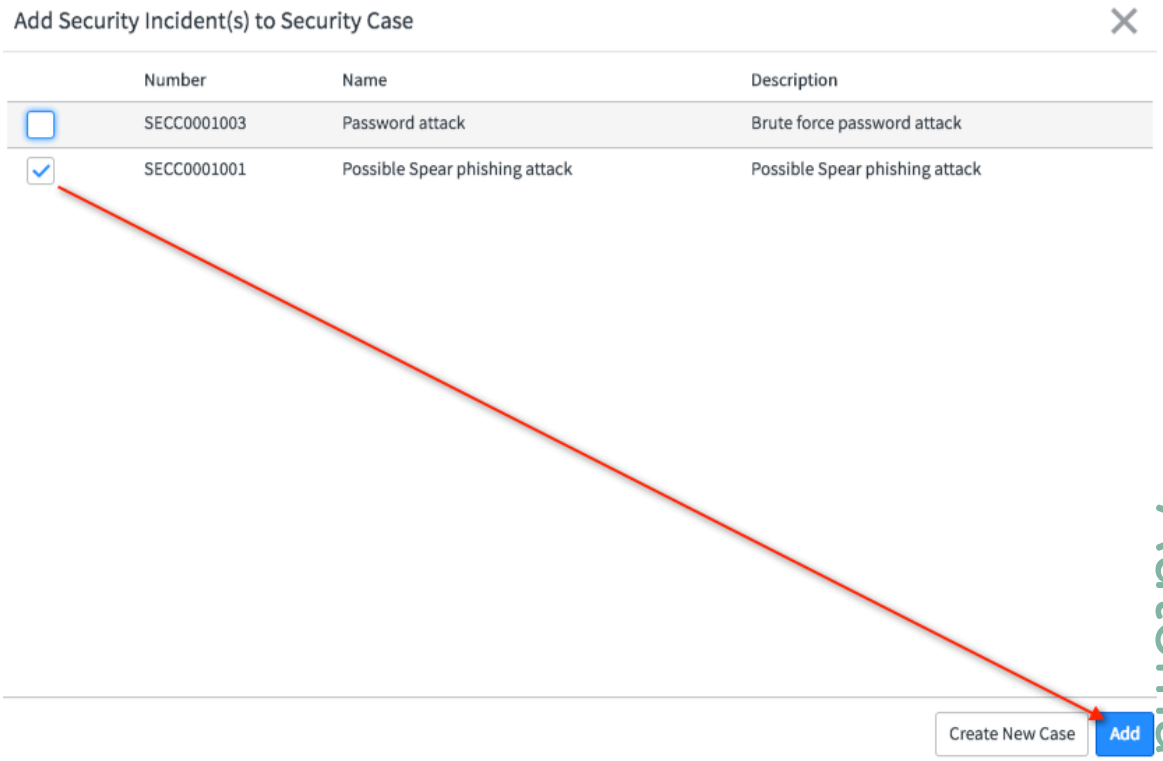
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**.
   Die Liste Security Incidents wird geöffnet.
2. Wählen Sie in der Liste einen oder mehrere Security Incidents aus, die Sie zu vorhandenen Fällen hinzufügen möchten.

   **Hinweis:**
   Wenn Sie mehrere Security Incidents auswählen, werden die ausgewählten Security Incidents jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.
   Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Security Incidents hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht weist darauf hin, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Security Case Management.

### Konfigurationselemente in Fällen

Sie können einen neuen Fall aus einem oder mehreren Konfigurationselementen (CI) in der Tabelle „Konfigurationselement“ [cmdb_ci] erstellen. Sie können auch vorhandenen Fällen CIs hinzufügen.

### Erstellen Sie einen Fall aus CIs

Sie können einen Sicherheitsfall aus Konfigurationselementen in der Tabelle „Konfigurationselement“ [cmdb_ci] erstellen. Nachdem die CIs zum Erstellen eines neuen Falls verwendet wurden, können Sie die Daten mit Security Case Management analysieren.

## Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

## Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Konfigurationselementen navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

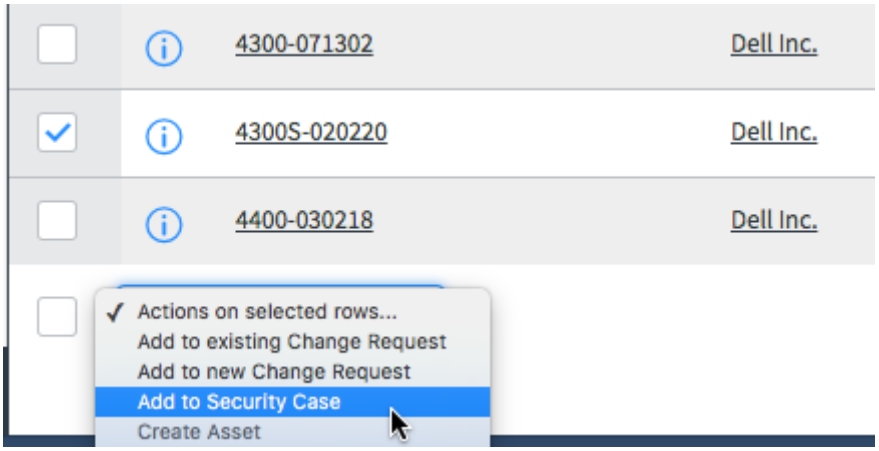
## Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** , um CIs für Computer anzuzeigen.
   Die Liste für den ausgewählten CI-Typ wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren CIs erstellen, oder Sie können ein bestimmtes CI auswählen und einen neuen Fall aus dem Formular erstellen.

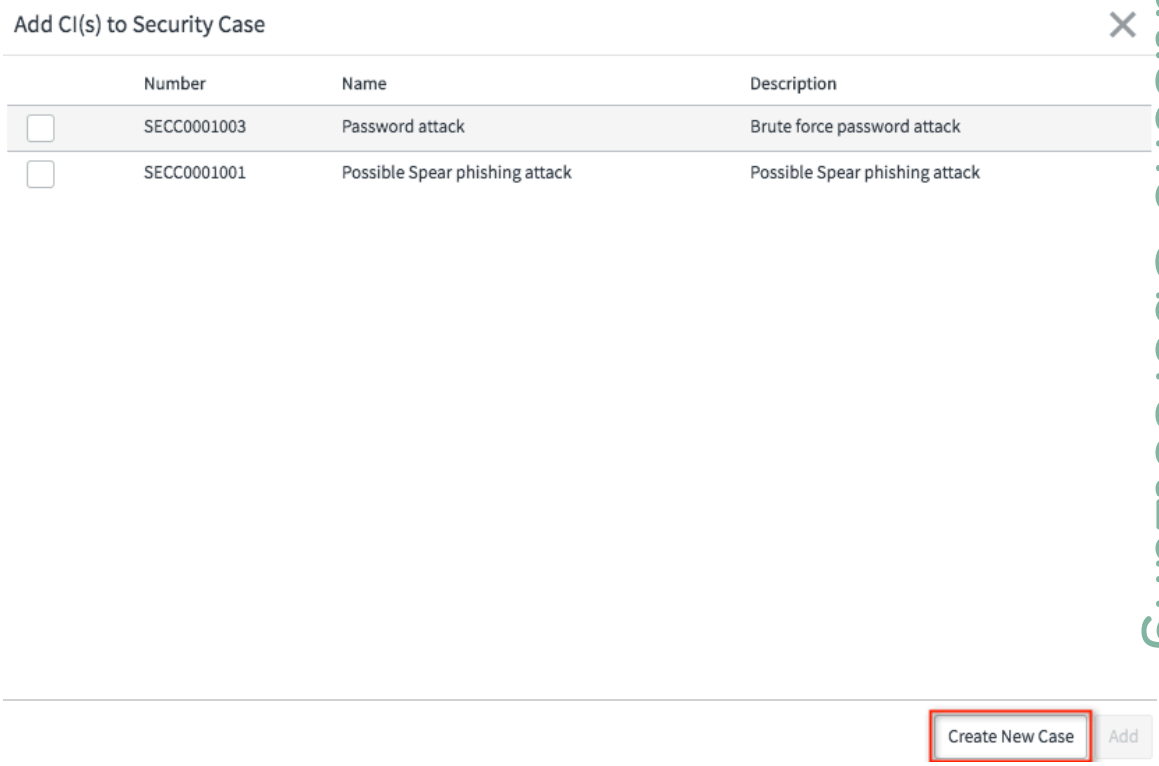
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie in der Liste die CIs aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.




Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden diese in der Liste angezeigt.




4. Klicken **Sie auf Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Fallname | Geben Sie einen Namen für diesen Fall ein. |
| Beschreibung | Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zu dem Fall in Security Case Management.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

### Fügen Sie CIs zu vorhandenen Fällen hinzu

Sie können Konfigurationselemente zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die CIs den Fällen hinzugefügt wurden, können Sie die Daten mit Security Case Management analysieren.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

#### Warum und wann dieser Vorgang ausgeführt wird

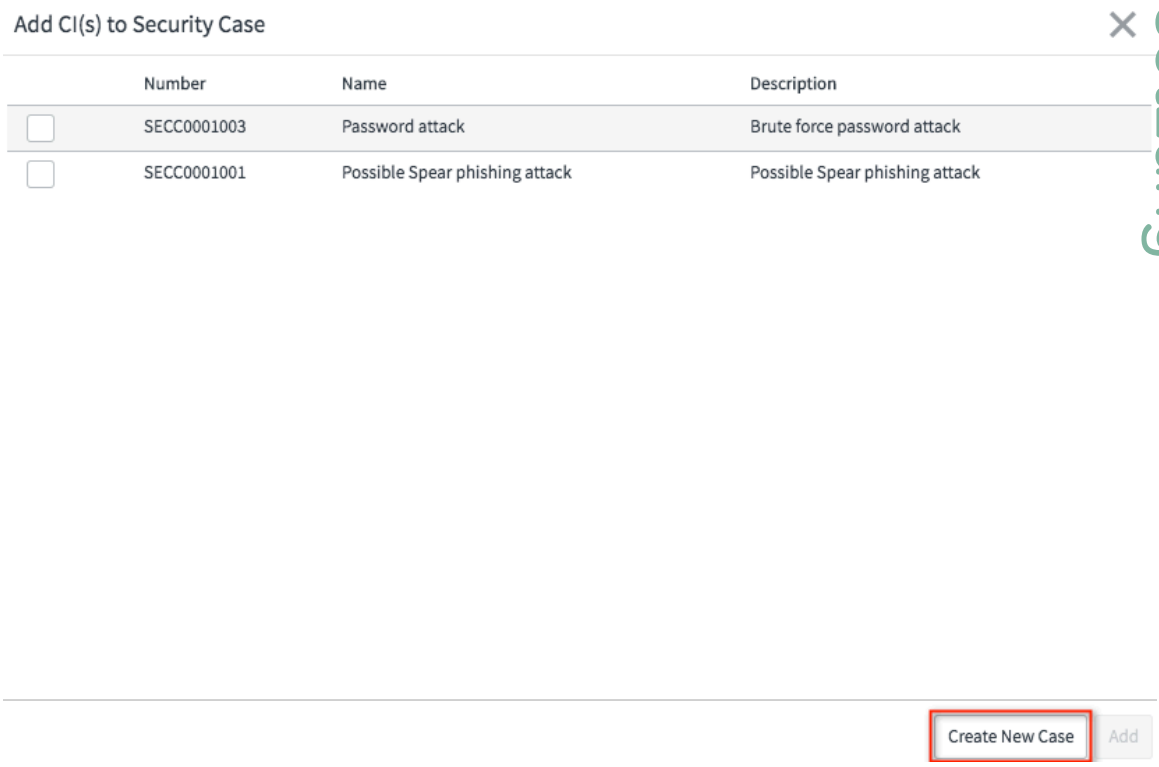
Sie müssen zu den CIs navigieren, die Sie den vorhandenen Fällen hinzufügen möchten.

#### Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** , um CIs für Computer anzuzeigen.
   Die Liste der ausgewählten CIs wird geöffnet.
2. Wählen Sie in der Liste mindestens ein CI aus, das Sie vorhandenen Fällen hinzufügen möchten.

   **Hinweis:**
   Wenn Sie mehrere CIs auswählen, werden die ausgewählten CIs jedem der ausgewählten Fälle hinzugefügt.

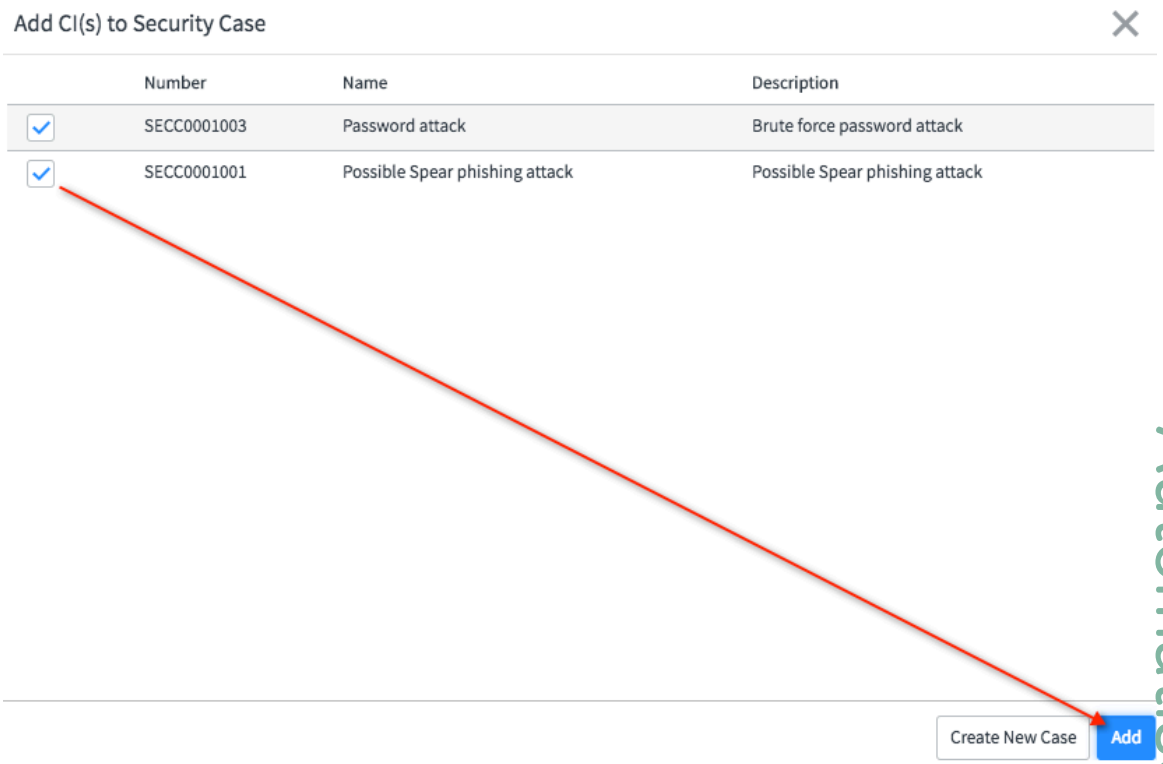
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.
   Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie die Fälle aus, denen Sie die ausgewählten CIs hinzufügen möchten.




5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht weist darauf hin, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Security Case Management.

### Betroffene Benutzer in Fällen

Sie können einen neuen Fall aus einem oder mehreren betroffenen Benutzern in der Benutzertabelle [sys_user] erstellen. Sie können Benutzer auch zu vorhandenen Fällen hinzufügen.

### Erstellen Sie einen Fall aus betroffenen Benutzern

Sie können einen Sicherheitsfall aus betroffenen Benutzern in der Benutzertabelle [sys_user] erstellen. Nachdem die betroffenen Benutzer zum Erstellen eines neuen Falls verwendet wurden, können Sie Security Case Management verwenden, um die Daten zu analysieren.

## Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

## Warum und wann dieser Vorgang ausgeführt wird

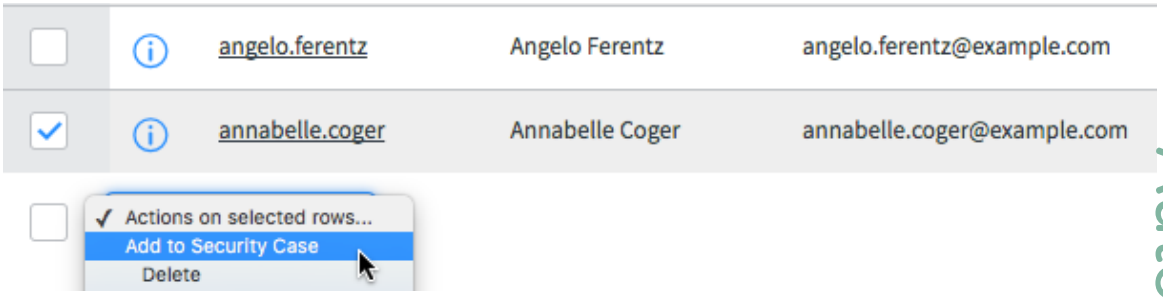
Sie müssen zu den Benutzern navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

Automatische Übersetzung

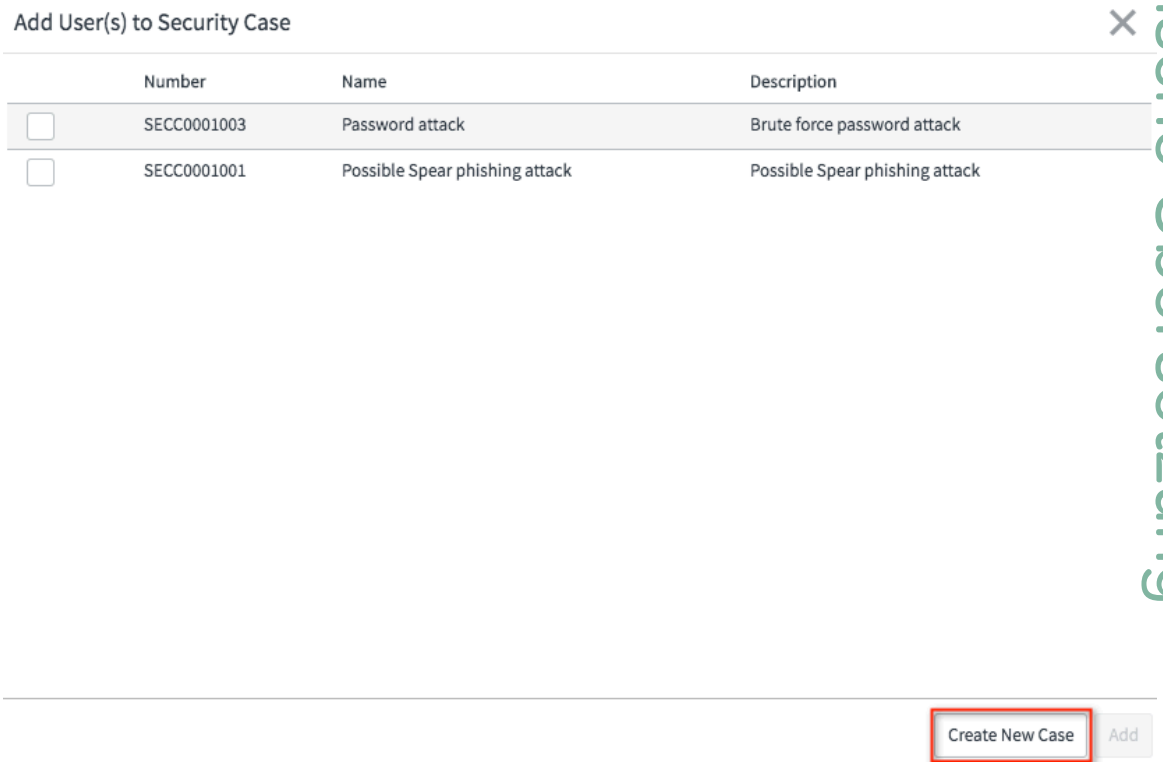
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Anwender**.
   Die Liste für die ausgewählten Benutzer wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Benutzerdatensätzen erstellen, oder Sie können einen bestimmten Benutzerdatensatz auswählen und einen neuen Fall aus dem Formular erstellen.
2. Wählen Sie in der Liste die Benutzer aus, die Sie einem neuen Fall hinzufügen möchten.
3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.




Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden diese in der Liste angezeigt.




4. Klicken **Sie auf Neuen Fall erstellen**.
5. Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Fallname | Geben Sie einen Namen für diesen Fall ein. |
| Beschreibung | Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert sein könnte. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zu dem Fall in Security Case Management.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

### Fügen Sie betroffene Benutzer zu vorhandenen Fällen hinzu

Sie können betroffene Benutzer zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die Benutzerdatensätze zu Fällen hinzugefügt wurden, können Sie die Daten mit Security Case Management analysieren.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

#### Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Benutzerdatensätzen navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

#### Prozedur

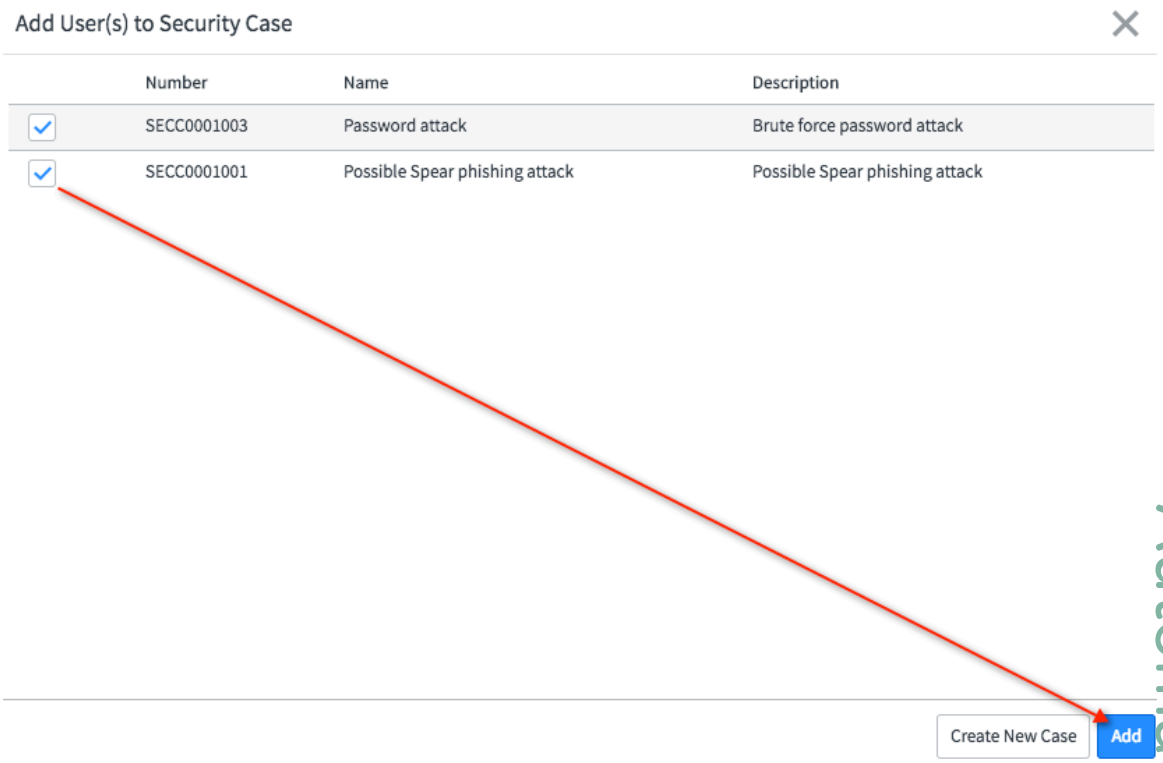
1. Navigieren zu **Alle** > **Benutzeradministration** > **Anwender**.
   Die Liste der Benutzerdatensätze wird geöffnet.
2. Wählen Sie in der Liste einen oder mehrere Benutzer aus, die Sie zu vorhandenen Fällen hinzufügen möchten.

   **Hinweis:**
   Wenn Sie mehrere Benutzer auswählen, werden die ausgewählten Benutzerdatensätze jedem der ausgewählten Fälle hinzugefügt.

3. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die Option **Add to Security Case**(Zu Sicherheitsfall hinzufügen) aus.
   Das Dialogfeld **Zu Sicherheitsfall** hinzufügen wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Benutzer hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht weist darauf hin, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Security Case Management.

## Analyse von Sicherheitsartefakten

Nachdem Sie Fälle erstellt haben, entweder mit Security Case Managementoder aus Artefakten wie IoCs, erkennbaren Elementen, Security Incidents usw., können Sie weitere Artefakte hinzufügen, um die Analyse der identifizierten Bedrohungen zu unterstützen.

### Zugehörige Details für Fallartefakte

Wenn Sie einem Fall Artefakte hinzufügen, können zusätzliche zugehörige Details für jedes Artefakt automatisch hinzugefügt werden. Wenn Sie beispielsweise einen Security Incident hinzufügen, kann dieser betroffene CIs und Benutzerdatensätze enthalten. Sie können die zugehörigen Details für ein ausgewähltes Artefakt schnell anzeigen, ohne die Liste der Artefakte zu verlassen.

### Zeigen Sie zugehörige Details für ein Security Incident-Artefakt an

Wenn Ihr Fall Security Incident-Artefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem Security Incident enthalten sind, auf den der Fall verweist.

#### Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

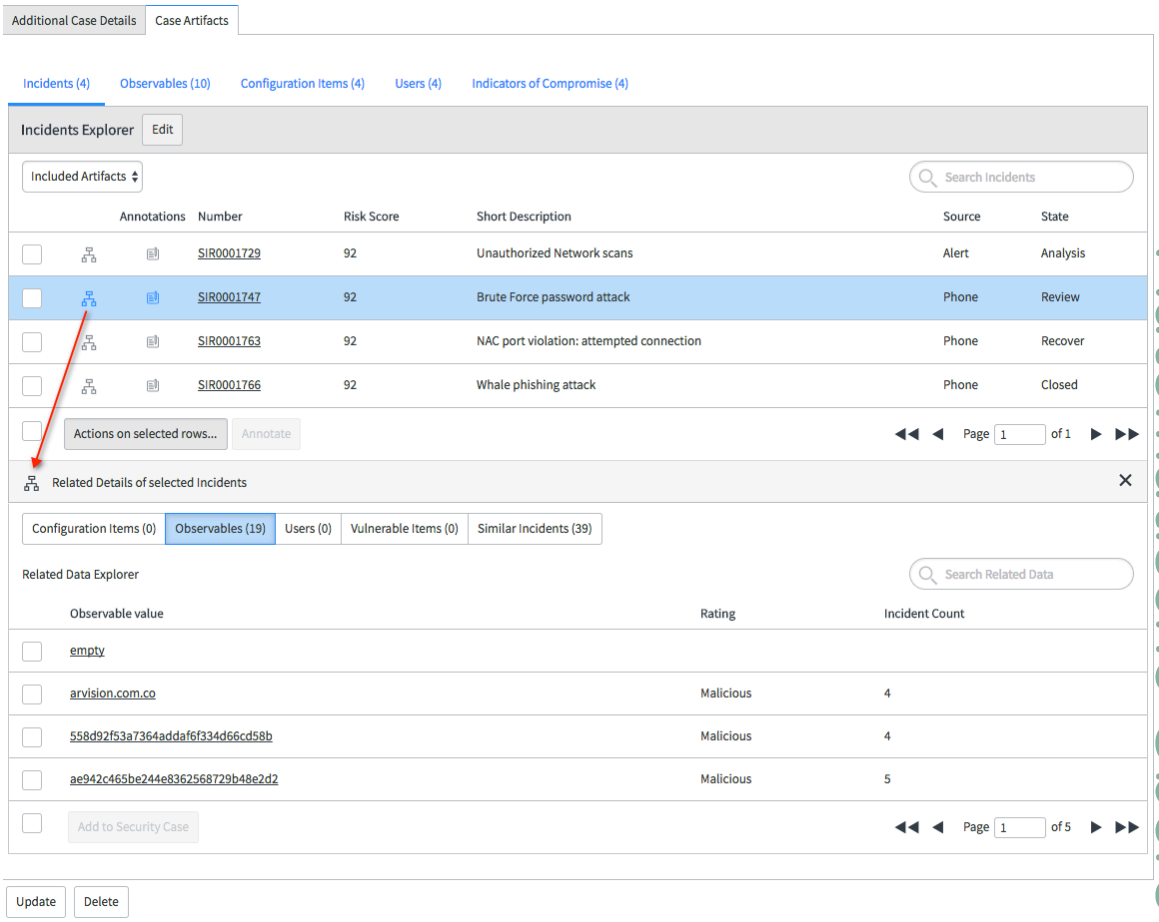
Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Öffnen Sie einen Fall, der Security Incident-Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Incidents**.
3. Klicken Sie auf das Symbol Zusätzliche Details für den Security Incident, für den Sie zugehörige Details anzeigen möchten.




4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

## Zeigen Sie zugehörige Details für ein Konfigurationselement-Artefakt an

Wenn Ihr Fall Konfigurationselementartefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem vom Fall referenzierten CI enthalten sind.

### Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

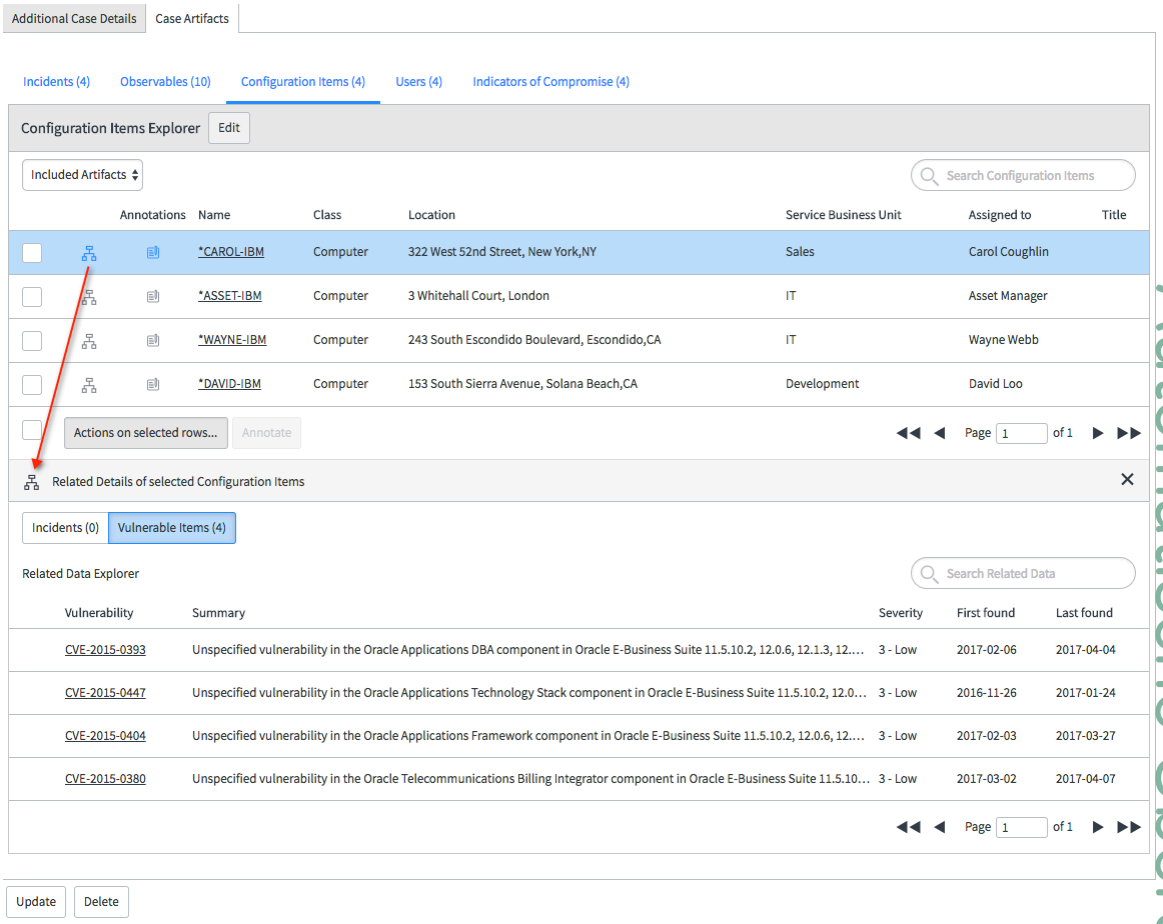
Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Öffnen Sie einen Fall, der CI-Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Konfigurationselemente**.
3. Klicken Sie auf Zusätzliche Details für das CI-Artefakt, für das Sie zugehörige Details anzeigen möchten.




4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

### Zeigen Sie zugehörige Details für ein IoC-Artefakt an

Wenn Ihr Fall IoC-Artefakte (Indicators of Compromise) enthält, können Sie alle zugehörigen Details anzeigen, die in jedem vom Fall referenzierten IoC enthalten sind.

## Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

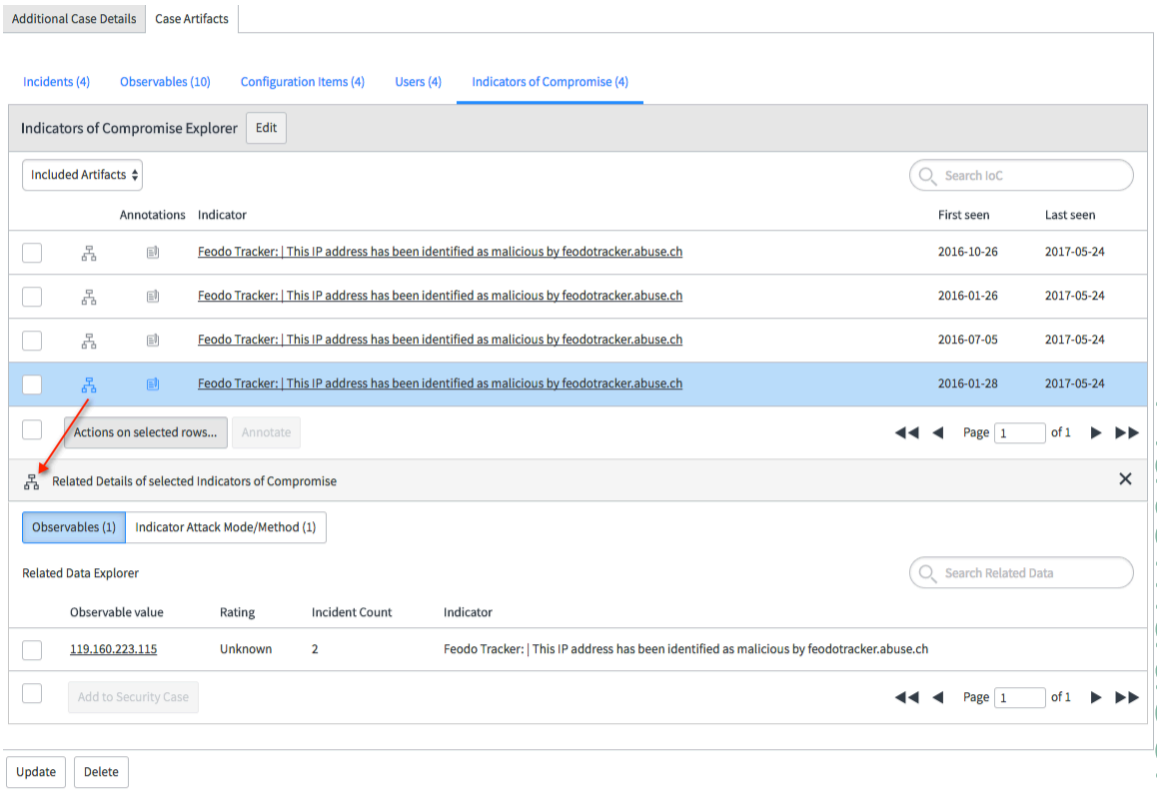
## Prozedur

1. Öffnen Sie einen Fall, der IoC-Artefakte enthält.
2. **Klicken Sie auf** die Registerkarte Gefährdungsindikatoren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf das Symbol „Zusätzliche Details“ für das IoC-Artefakt, für das Sie zugehörige Details anzeigen möchten.




4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

### Zeigen Sie zugehörige Details für ein betroffenes Benutzerartefakt an

Wenn Ihr Fall betroffene Benutzerartefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem betroffenen Benutzer enthalten sind, auf den der Fall verweist.

### Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

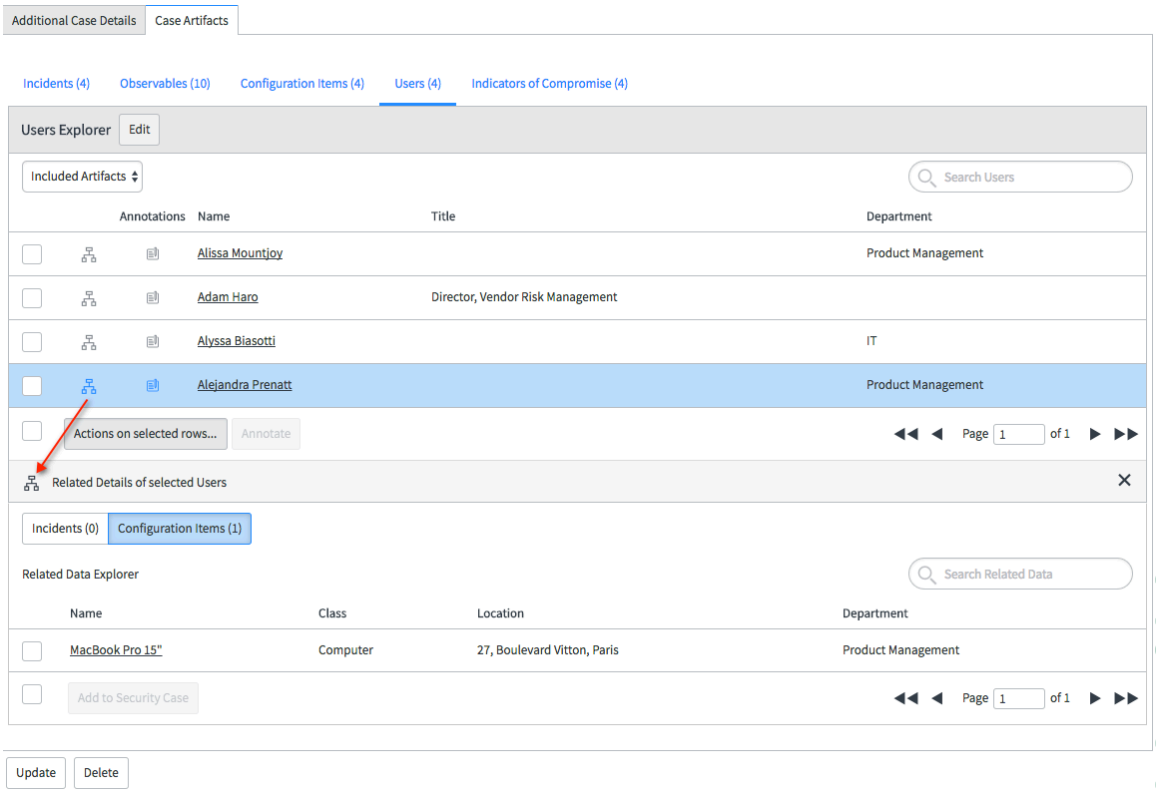
Erforderliche Rolle: sn_ti.case_user_write

### Prozedur

1. Öffnen Sie einen Fall, der betroffene Benutzerartefakte enthält.
2. Klicken Sie auf die Registerkarte **Benutzer**.
3. Klicken Sie auf Zugehörige Details für das betroffene Benutzerartefakt, für das Sie zugehörige Details anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

### Zeigen Sie zugehörige Details für ein erkennbares Artefakt an

Wenn Ihr Fall Artefakte erkennbarer Elemente enthält, können Sie alle zugehörigen Details anzeigen, die in jedem erkennbaren Element enthalten sind, auf das der Fall verweist.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

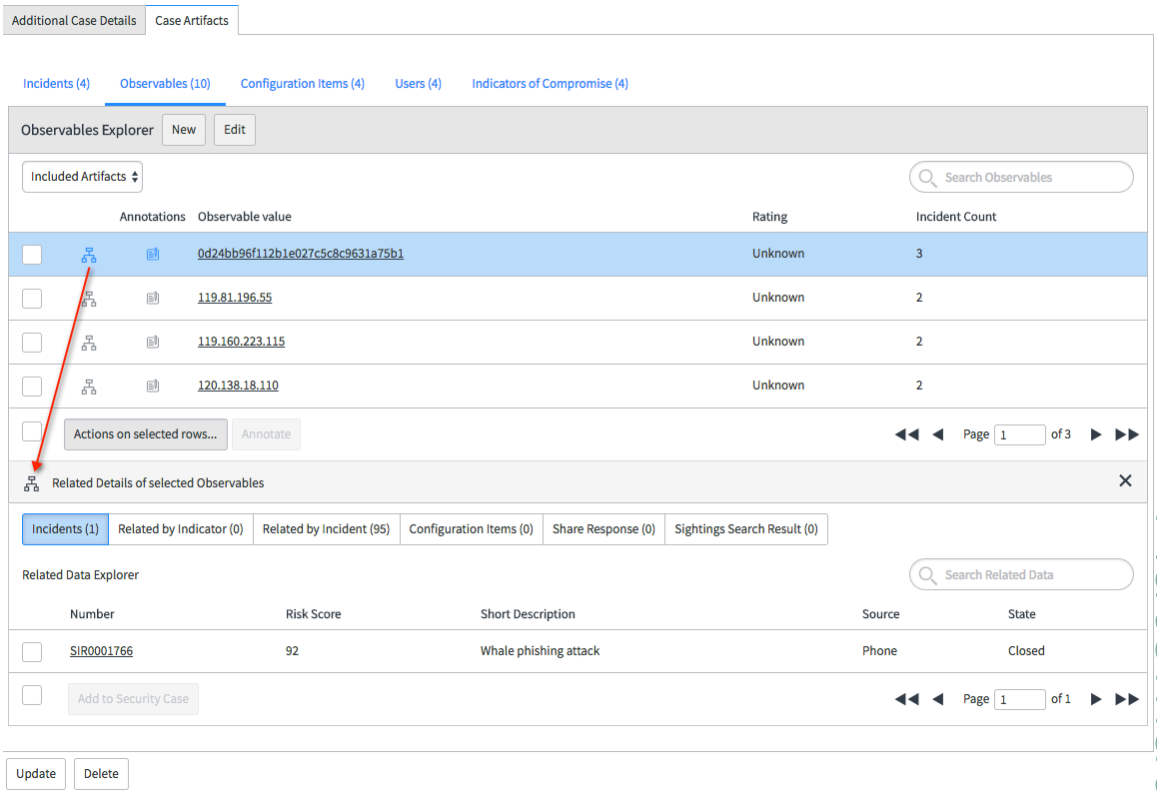
Erforderliche Rolle: sn_ti.case_user_write

#### Prozedur

1. Öffnen Sie einen Fall, der erkennbare Artefakte enthält.
2. Klicken Sie auf die Registerkarte **Erkennbare** Elemente.
3. Klicken Sie auf das Symbol Zusätzliche Details für das erkennbare Artefakt, für das Sie zugehörige Details anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf die Registerkarte **Sicherheitsanmerkung** klicken, um Anmerkungen für das ausgewählte Artefakt anzuzeigen.

### Ausschluss und Einschluss von Sicherheitsartefakten

Die Listen der unterstützenden Artefakte, die einem Fall zugewiesen sind, können manchmal lang werden, und es kann Fälle geben, in denen Sie bestimmte Artefakte aus einer Liste entfernen möchten. Anstatt die Artefakte dauerhaft zu entfernen, können Sie sie aus der Liste ausschließen und sie bei Bedarf zu einem späteren Zeitpunkt wieder in die Liste aufnehmen.

### Schließen Sie Sicherheitsartefakte aus einem Fall aus

Sie können Artefakte aus den Listen der unterstützenden Artefakte entfernen. Sie werden nicht dauerhaft entfernt und können bei Bedarf an den Fall zurückgegeben werden.

#### Vorbereitungen

- Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

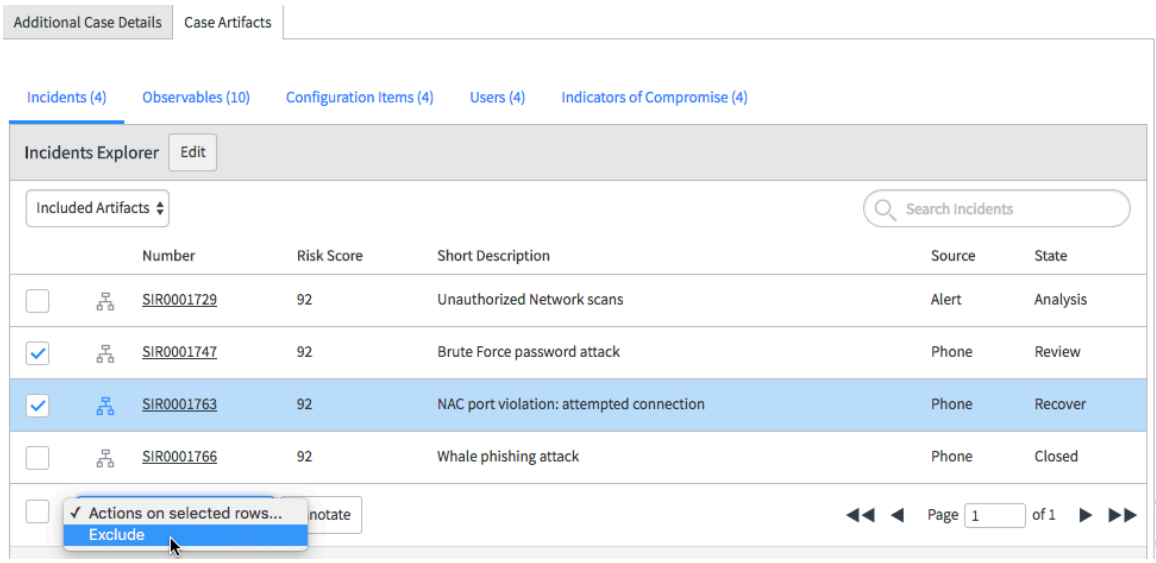
#### Prozedur

1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie aus einer Liste ausschließen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie ausschließen möchten. Klicken Sie beispielsweise auf **Incidents**, um Security Incidents aus der Liste auszuschließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie mindestens einen Artefaktdatensatz aus, den Sie ausschließen möchten.




5. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die **Option Ausschließen**aus.

6. Klicken Sie im Bestätigungsfeld auf **Ausschließen**.
Die ausgewählten Artefakte werden aus der Liste entfernt.

## Ausgeschlossene Sicherheitsartefakte an einen Fall zurückgeben

Nachdem Sie Artefakte aus einer Liste in einem Fall ausgeschlossen haben, können Sie sie an den Fall zurückgeben, um weiter an ihnen zu arbeiten.

### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

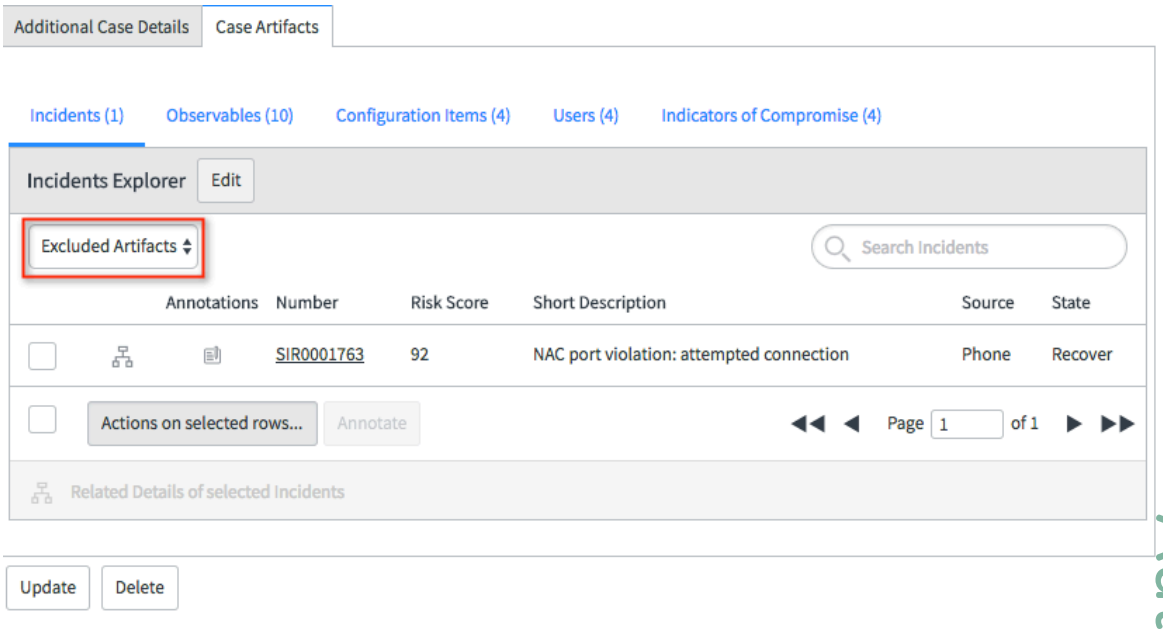
Erforderliche Rolle: sn_ti.case_user_write

### Prozedur

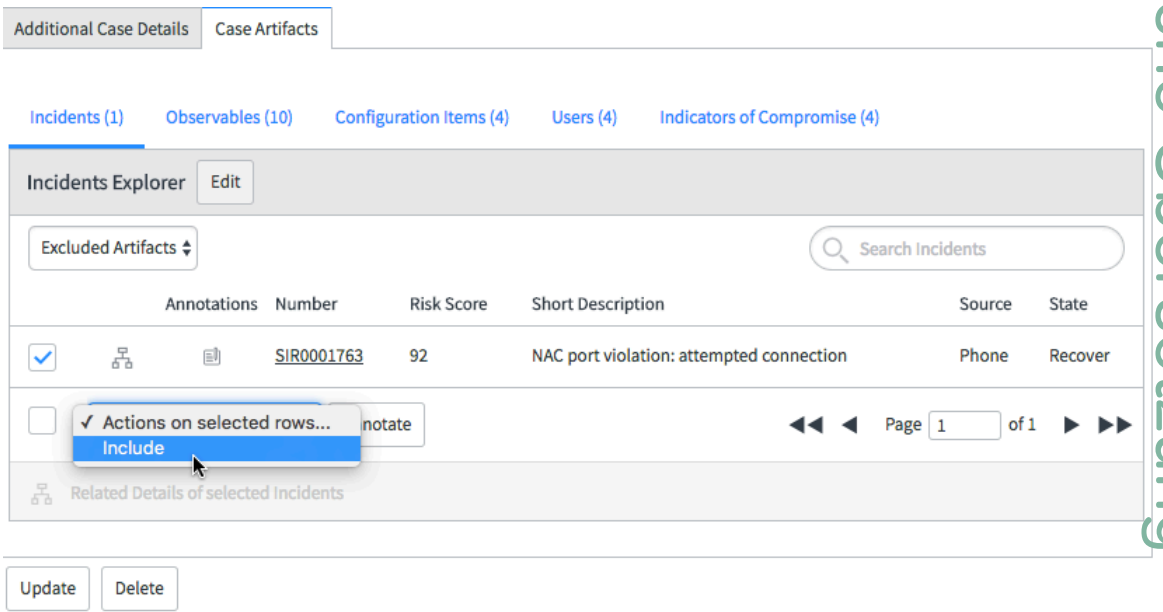
1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie zuvor aus einer Liste ausgeschlossen haben, die Sie in die Liste zurückgeben möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie an die Liste zurückgeben möchten.
4. Klicken Sie auf die Dropdown-Liste Artefaktfilter und wählen Sie **Ausgeschlossene Artefakte**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Wählen Sie einen oder mehrere Artefaktdatensätze aus, die Sie an die Liste Einbeziehen zurückgeben möchten.
6. Wählen Sie in der Dropdown-Liste **Aktionen für ausgewählte Elemente** die **Option Einbeziehen**aus.




7. **Klicken** Sie im Bestätigungsfeld auf Einbeziehen.
   Die ausgewählten Artefakte werden aus der Liste der ausgeschlossenen Artefakte entfernt und an die Liste der im Fall enthaltenen Artefakte zurückgegeben.

### Versehen Sie Sicherheitsartefakte mit Anmerkungen

Während Sie einen Fall analysieren, können Sie jedem Artefakt Anmerkungen hinzufügen.

### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle:

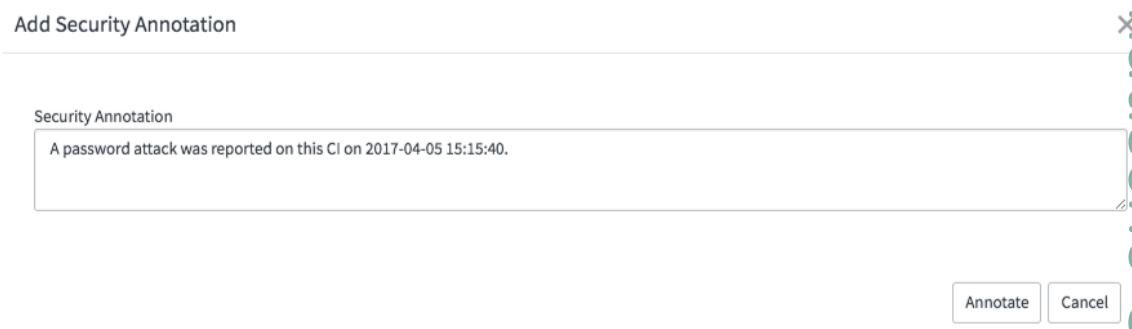
- sn_ti.case_user_write zum Hinzufügen von Anmerkungen
- sn_ti.case_user_read, um Anmerkungen anzuzeigen

### Prozedur

1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie mit Anmerkungen versehen möchten.
2. Klicken Sie auf die zugehörige Liste **Fallartefakte**.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie mit Anmerkungen versehen möchten.
   Klicken Sie beispielsweise **auf Kompromittierungsindikatoren**, um IoCs Anmerkungen hinzuzufügen.
4. Führen Sie die folgenden Schritte aus, um einem oder mehreren Artefakten eine Anmerkung hinzuzufügen:

   a. Wählen Sie die Artefakte aus, denen Sie eine Anmerkung hinzufügen möchten.

   b. Klicken Sie **auf Annotieren**.

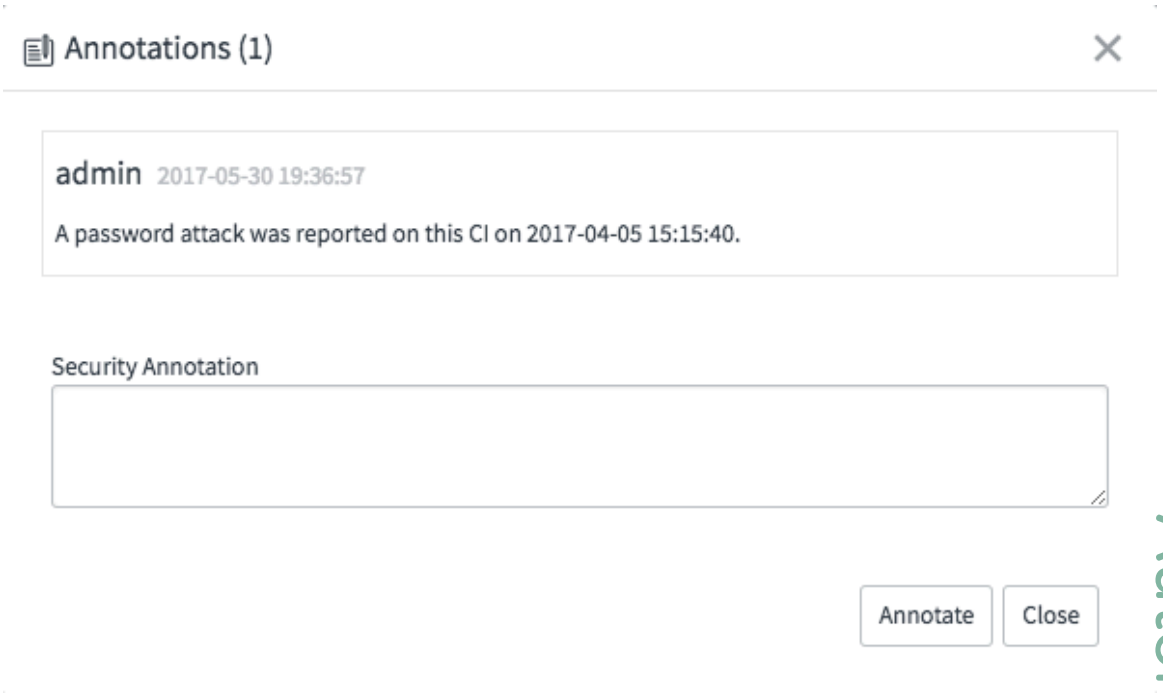



   c. Geben Sie die Anmerkung ein, und klicken Sie auf **Annotieren**.
   Die Anmerkung wird den ausgewählten Artefakten hinzugefügt.

5. Um Anmerkungen für ein Artefakt anzuzeigen, klicken Sie auf das Symbol Anmerkungen anzeigen ( anzeigen).
   Die vorhandenen Anmerkungen werden im Dialogfeld Anmerkungen angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Sie können auch eine neue Anmerkung für das Artefakt in das Feld **Sicherheitsanmerkung** eingeben und auf **Annotieren**klicken.

### Suchen Sie nach Sicherheitsartefakten

Sie können eine Stichwortsuche in jeder Sicherheitsartefaktliste durchführen.

#### Vorbereitungen

Das Plugin Threat Intelligence muss aktiviert sein, um Security Case Managementverwenden zu können.

Erforderliche Rolle: sn_ti.case_user_write

#### Prozedur

1. Öffnen Sie einen Fall, der Sicherheitsartefakte enthält.
2. Klicken Sie auf die Registerkarte für die Sicherheitsartefakte, für die Sie eine Stichwortsuche durchführen möchten.
3. Beginnen Sie im Feld **Stichwortsuche mit der Eingabe des Namens des Artefakts, das Sie suchen** möchten.
   Wenn Artefakte gefunden werden, die Ihrem Eintrag entsprechen, werden sie angezeigt.

## Security Operations allgemeine Funktionalität

Immer wenn eines der Plugins für die Hauptanwendungen von Security Operations (Security Incident Response, Vulnerability Response, Threat Intelligenceoder Configuration Compliance) aktiviert wird, wird das Plugin Security Support Common aktiviert. Dieses Plugin lädt verschiedene Module, die Funktionen bereitstellen, die allen Security Operations -Anwendungen gemeinsam sind.

**Hinweis:**
Nur Benutzer mit [sn_sec_cmn.admin] können das Modul Security Operations ] anzeigen und verwenden. Diese Rolle wird geerbt, wenn Ihnen eine Administratorrolle in einer der Anwendungen von Security Operations zugewiesen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Security Operations-Module

| Funktion | Beschreibung |
|---|---|
| Referenzen zur Integration mit Security Operations, Threat Intelligence-Integrationen, Vulnerability Response-Integrationen | Mehrere Integrationen sind in den Security Operations -Anwendungen enthalten (Security Incident Response, Threat Intelligenceund Vulnerability Response). Dieser Abschnitt enthält Anweisungen zum Aktivieren der Plugins und zum Konfigurieren von ServiceNow und Integrationen von Drittanbietern. Außerdem sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen enthalten, die im Basissystem enthalten sind. |
| Security Operations E-Mail-Verarbeitung | Sie können die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Datensätzen zu Sicherheitsvorgängen bereitstellen, nicht abgeglichene E-Mails behandeln und die Duplizierung von Datensätzen mit E-Mail-Verarbeitungverhindern. |
| Gruppen | • **Filtergruppen**<br><br>Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer Instanz zu suchen. Sie können beispielsweise eine Gruppe aller Computer desselben Herstellers erstellen. Sie können auch Konfigurationselemente (CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten Subnetz-IP-Adressbereich fallen.<br><br>• **Eskalationen**<br><br>Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachkenntnisse erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird für jeden Security Incident in dieser Gruppe eine Schaltfläche angezeigt. |
| Sicherheits-Tags | **Tags**: Sicherheits-Tag-Regeln bieten Filterung für den Zugriff auf Sicherheits-Tags. |
| Workflows | • **Sicherheitsworkflows anzeigen**<br><br>Sie können die vielen Workflows anzeigen, die in den Security Operations-Anwendungen enthalten sind. Sie können Workflows aus Vorlagen und im Workflow-Editor erstellen.<br><br>• **Workflow-Auslöser** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Funktion | Beschreibung |
| --- | --- |
| | Security Operations Workflow-Auslöser enthalten eine Bedingung für eine Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist. |
| Dienstprogramme | • **Ergänzungsdatenzuordnung**<br><br>Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaften -Dateien in ServiceNow -Datensätze um. Security Operations -Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit.<br><br>• **Feldwertumwandlungen**<br><br>Wandelt eindeutige Kundenfeldwerte in Feldwerte um, die von Security Operations E-Mail-Analyse, Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen erkannt werden. Unterstützt Auswahlfelder, Referenzen und richtet externe Daten in der Standardterminologie und im Standardformat für Ihren neuen Datensatz aus.<br><br>• **Feldzuordnung**<br><br>Security Operations -Tabellen können anderen Tabellen zugeordnet werden und aus anderen Tabellen, wodurch ein Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen des Security Operations -Systems verknüpft wird. Sie können beispielsweise ein Plugin in eine Security Incident Response -Aufgabe integrieren.<br><br>• **Orchestration bei Bedarf**<br><br>Während der Analyse Security Incident Response möchte ein Sicherheitsanalyst möglicherweise eine Aufgabe ausführen, die von einem Security Incident-Workflow gesteuert wird. Führen Sie beispielsweise eine Prozesssicherung für ein bestimmtes CI aus. Dies kann mit On-Demand-Orchestration erreicht werden.<br><br>• **Betriebssystemgruppen**<br><br>N/V |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Funktion | Beschreibung |
|---|---|
| | • **SecOps-Applikationsregistrierung**<br>N/V |
| CMDB | **CI**-Bezeichnerregeln: CI-Bezeichner sind Regeln, die zum Suchen eines Konfigurationselements (CI) in der CMDB verwendet werden, das übereinstimmende Informationen aus einer Drittanbieterintegration enthält. Diese Regeln definieren die Felder, die übereinstimmende Daten enthalten, und die Rangfolge, nach der sie ausgewertet werden. Der niedrigste Wert für die **Reihenfolge** wird zuerst ausgewertet. |

## Erstellen und definieren Sie Filtergruppen in Security Operations

Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer Instanz zu suchen. Sie können beispielsweise eine Gruppe aller Computer desselben Herstellers erstellen. Sie können auch Konfigurationselemente (CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten Subnetz-IP-Adressbereich fallen.

### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

### Warum und wann dieser Vorgang ausgeführt wird

Filtergruppen können dynamisch aktualisierte Datensätze, eine Reihe von statischen Datensätzen, die nicht anhand von Bedingungen gefiltert werden, oder eine Kombination aus dynamisch aktualisierten und statischen Datensätzen enthalten. Einige Filtergruppen sind im Basissystem enthalten, z. B. CI-Ausschlüsse.

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Filtergruppen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Filtergruppe. |
| Aktiv | Feld zum Aktivieren der Gruppe. |
| Beschreibung | Beschreibung für die Filtergruppe. |
| IP-Adresse für Netzwerk | Die Netzwerk-IP-Adresse, die die IP-Adressen der CIs enthält, die Sie der Gruppe hinzufügen möchten.<br>Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das Konfigurationselement im Feld **Tabelle** erweitert. |
| Subnetzmaske | Das Subnetz, das die IP-Adressen der CIs enthält, die Sie der Gruppe hinzufügen möchten, z. B. 255.255.255.0. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das Konfigurationselement im Feld **Tabelle** erweitert. |
| Tabelle | Die Tabelle, nach der gefiltert werden soll. |
| Bedingung | Verwenden Sie den Bedingungsgenerator, um die zu filternden Kriterien zu definieren. |

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarte **Erweiterte Bedingungen** wird angezeigt.

   Je nach Tabellentyp, den Sie im Feld **Tabelle** angegeben haben, werden weitere Registerkarten angezeigt:

| Tabelle | Angezeigte Registerkarten |
|---|---|
| Konfigurationselement [cmdb_ci] oder eine Tabelle, die die Konfigurationselementtabelle erweitert | **Manuell hinzugefügte CIs** und **übereinstimmende CIs** |
| Aufgabe [Aufgabe] oder eine Tabelle, die die Aufgabentabelle erweitert | **Manuell hinzugefügte Aufgaben** und **übereinstimmende Aufgaben** |
| Eine Tabelle, die nicht zu einem CI oder einer Aufgabe gehört | **Manuell hinzugefügter Datensatz** |

5. So definieren Sie weitere Bedingungen für Ihre Filtergruppe:

   a. Klicken Sie auf **Erweiterte Bedingungen**.

   b. Fügen Sie eine neue Zeile in die eingebettete Liste **Zusätzliche** Filtergruppenbedingungen ein, um andere vordefinierte Filtergruppen auszuwählen, die Sie mit der zu aktualisierenden Filtergruppe kombinieren möchten.
   Wenn die ausgewählte Filtergruppe Datensätze basierend auf einem Referenzfeld filtern soll, wird beim Speichern des aktuellen Datensatzes automatisch ein zugeordnetes Feld ausgewählt.

   **Hinweis:**
   Der **Feldwert „Zugeordnet** “ kann nicht in der eingebetteten Liste **„Zusätzliche Filtergruppenbedingungen“** bearbeitet werden. Um das Feld zu ändern, klicken Sie auf das Informationssymbol, um den Datensatz zu öffnen.

   c. Klicken Sie auf **Aktualisieren**.

6. So fügen Sie der Filtergruppe manuell weitere CIs oder Aufgaben hinzu:

   a. Klicken Sie auf die Registerkarte **Manuell hinzugefügte CIs** oder **Manuell hinzugefügte Aufgaben**.

   b. Klicken Sie auf **Bearbeiten**.

   c. Wählen Sie die CIs oder Aufgaben aus, die Sie hinzufügen möchten.

   d. Klicken Sie auf **Speichern**.

7. So zeigen Sie die CIs oder Aufgaben an, die Ihren Auswahlkriterien entsprechen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie auf die Registerkarte **Übereinstimmende CIs** oder **Übereinstimmende Aufgaben**.

**b.** Wenn Sie die Kriterien geändert haben, aktualisieren Sie die Liste, indem Sie mit der rechten Maustaste in den Formular-Header klicken und **Liste aktualisieren**auswählen.

## Transformation freigegebener Daten

Die Plugins Security Incident Response, Vulnerability Responseund Threat Intelligence verwenden gemeinsame Funktionen für Beziehungsdaten und Duplizierungsregeln, die zum Importieren externer und interner Informationen in Security Operationsverwendet werden.

E-Mail-Analyse, Duplizierungsregelnund Feldzuordnung nehmen Eingabedaten (eine E-Mail, eine JSON- oder XML-Datei oder einen Datensatz) und wandeln diese Daten in das richtige Format um, um einen neuen Datensatz zu erstellen. Jede dieser Funktionen ruft Daten auf ihre eigene Weise ab, sie werden jedoch mit vielen der gleichen Prozesse in den neuen Datensatz umgewandelt.

### Beziehungsdaten

Wenn Sie einer zugehörigen Liste Informationen hinzufügen (z. B. ein zugeordnetes erkennbares Element in einem Security Incident), können Sie einen Beziehungsdatensatz erstellen, der aus einer m2m-Tabelle besteht. Manchmal gibt es zusätzliche Daten in diesem Beziehungsdatensatz, die festgelegt werden müssen. Zum Beispiel, wenn ein erkennbares Element eine Quell-IP ist (im Gegensatz zu einer Ziel-IP). Diese Informationen werden in das **FeldBeziehungsdaten** im Formular „Feldtransformation“ eingefügt, das von der E-**Mail** -Analyse verwendet wird, oder in eine zugehörige Liste „ **Feldzuordnungsfelder** “ im Formular „ **Feldzuordnung** “.

Das Feld „ **Beziehungsdaten“** ist normalerweise leer. Es wird am häufigsten für IP-Adressen für erkennbare Elemente in der **E-Mail-Analyse**verwendet.

Sie können Daten aus einem beliebigen ServiceNow -Datensatz in einen anderen ServiceNow -Datensatz mithilfe von **Feldzuordnungsfeldern** in der **Feldzuordnungsfunktion umwandeln**. Zum Beispiel, um Daten aus einem Incident in einen Security Incident oder einen Security Incident in einen PRB umzuwandeln.

### Duplizierungsregeln für Security Operations

Verwenden Sie Duplizierungsregeln, um doppelte Datensätze für Sicherheit, Schwachstelle, IoCs usw. zu verarbeiten.

Duplizierungsregeln haben zwei Zwecke. Sie verhindern, dass zu viele doppelte Datensätze erstellt werden, und geben an, welche Felder im Datensatz aktualisiert werden, wenn ein Duplikat erkannt wird. Es wird nur nach aktiven Duplikaten gesucht. Wenn der Datensatz nicht aktiv ist, z. B. wenn der Incident geschlossen wird, wird jedes neue identische Problem zu einem neuen Incident.

Duplizierungsregeln werden von **E**-Mail-Analyse, **Feldzuordnung**und **Ergänzungsdatenzuordnung**verwendet.

**Zugehörige Informationen**

Erstellen Sie E-Mail-Parser in Security Operations

Ordnen Sie Tabellen Tabellen mit Security Operations-Feldzuordnung zu



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erstellen Sie Duplizierungsregeln in Security Operations

Sie können Duplizierungsregeln verwenden, um neue E-Mail-Adressen, Ergänzungsdaten oder Feldzuordnungen mit aktiven doppelten Datensätzen zu identifizieren und entsprechend zu verarbeiten.

### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Duplizierungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus:

#### Duplizierungsregel

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Duplizierungsregel. |
| Tabelle | Tabelle, in der Datensätze erstellt und zur Bestimmung der Duplizierung verwendet werden. |
| Identifizierende Felder | Wählen Sie eine Reihe von Feldern aus, die auf einen doppelten Security Incident, ein erkennbares Element, eine Schwachstelle usw. hinweisen, wenn die Werte in diesen Feldern identisch sind. |
| Duplikataktion | Steuert den Umgang mit doppelten E-Mails. Die Auswahlmöglichkeiten lauten wie folgt:<br>**Als untergeordnet erstellen**<br>Erstellt einen Datensatz als untergeordnetes Element des Originals. Das Feld, das das untergeordnete Element mit dem übergeordneten Element verknüpft, ist das Feld **Übergeordnet**.<br>**Datensätze nicht erstellen oder aktualisieren**<br>(Standard) Tut nichts. Ignoriert Duplikate.<br>**Duplizierten Datensatz aktualisieren**<br>Aktualisiert die Felder im vorhandenen Datensatz wie in **Duplizierungsaktionen angegeben.**<br>**Hinweis:** Wenn Sie **Doppelten Datensatz**aktualisieren wählen, wird die zugehörige Liste **Duplizierungsaktionen** angezeigt. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Regel zu aktivieren. |
| Beschreibung | Beschreibt den Zweck und die Anwendung dieser Duplizierungsregel. wann sie verwendet werden soll, z. B. eine Regel für IP-basierte erkennbare Elemente oder Security Incidents von der Firewall. |

4. Klicken Sie mit der rechten Maustaste auf den Datensatz-Header, und wählen **Sie Speichern**, oder klicken Sie auf **Aktualisieren**.
5. Um Duplizierungsaktionen festzulegen, klicken Sie auf **Neu**, wenn Sie **Doppelten Datensatz** aktualisieren ausgewählt haben, um Duplizierungsaktionen für jedes Feld zu erstellen, das Sie im Incident aktualisieren möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

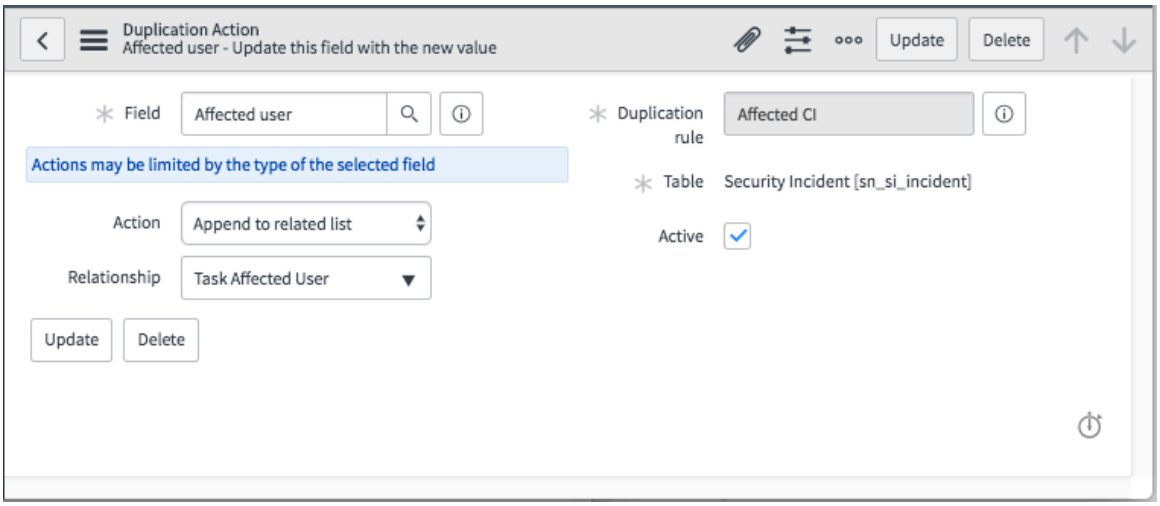
6. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie, um zu beschreiben, wie das Feld aktualisiert wird:

### Duplizierungsaktionen

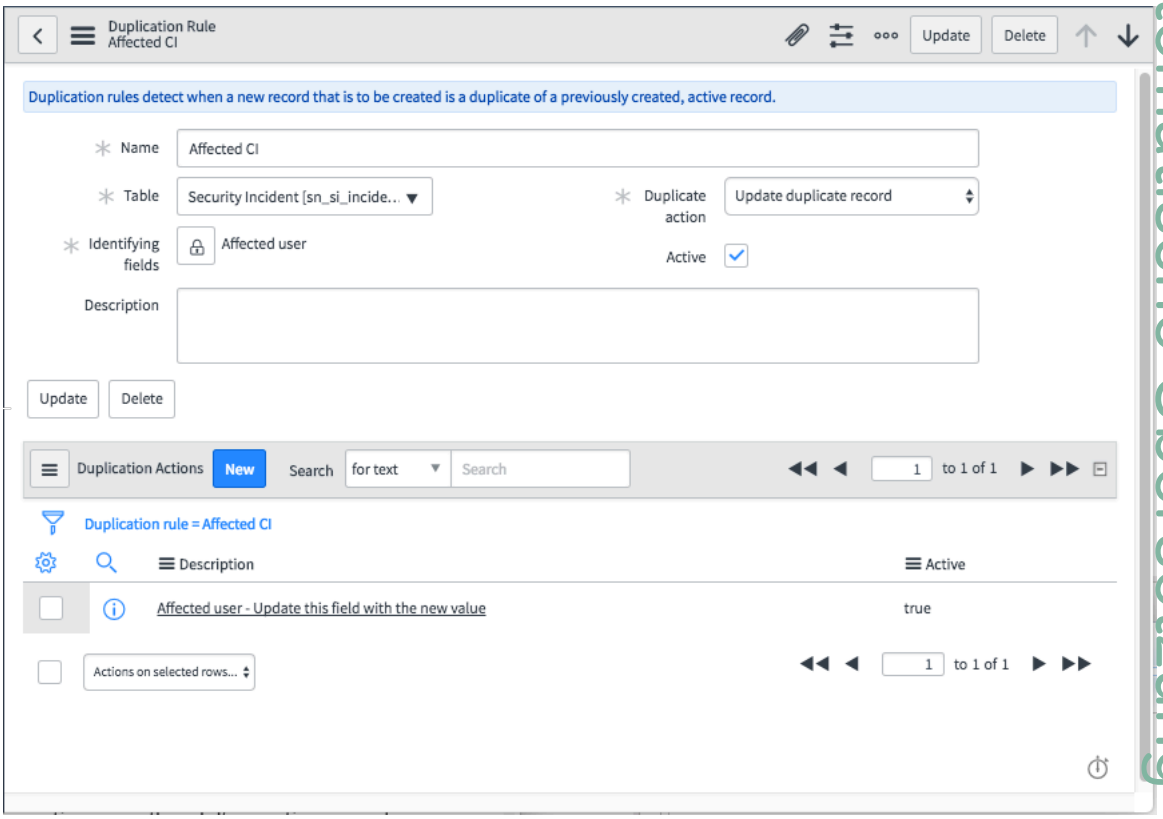
| Feld | Beschreibung |
|---|---|
| Feld | Der Name des Felds, das für die Duplizierungsaktion verwendet werden soll. |
| Aktion | Die unterstützten Aktionen variieren je nach Feldtyp.<br>Die Auswahlmöglichkeiten lauten wie folgt:<br>**Dieses Feld mit dem neuen Wert aktualisieren**<br>Ersetzt den vorherigen Wert im vorhandenen Datensatz durch diesen Wert.<br>**Neuen Wert an eine kommagetrennte Liste anhängen, falls einzigartig**<br>Behandelt den Wert als Eintrag in einer durch Kommas getrennten Liste und fügt die neuen Daten (falls vorhanden) als neuen Eintrag in dieser Liste hinzu. Wenn sich die Daten bereits in der Liste befinden, werden sie nicht zweimal hinzugefügt.<br>**Neuen Wert an dieses Feld anhängen**<br>Hängt den neuen Wert an das Ende des vorhandenen Texts im Feld an.<br>**Einmal zu einem Zählerfeld hinzufügen**<br>Fügt dem numerischen Feld eins hinzu.<br>**Feld auf heute einstellen**<br>Legt das Feld auf das aktuelle Datum und die aktuelle Uhrzeit fest.<br>**An zugehörige Liste anhängen**<br>Fügt den zugehörigen Datensatz mit diesem Wert der zugehörigen Liste des aktuellen Datensatzes hinzu. Wird angezeigt, wenn eine m:n-Tabelle mit einer Spalte desselben Typs vorhanden ist, die mit der zu aktualisierenden Tabelle verknüpft ist.<br>Beispiel: **Betroffenes CI** oder **Betroffener Benutzer**. |
| Beziehung | [Optional] Dieses Feld wird nur angezeigt, wenn die Aktion **An zugehörige Liste** anfügen ausgewählt ist. Dies ist der Name der zugehörigen Liste, die Sie dieser Regel zuordnen möchten. |
| Duplizierungsregel | Regel, zu der diese Aktion gehört. |
| Tabelle | Tabelle, in der Datensätze erstellt werden. Wird nur als Information angezeigt. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Aktion zu aktivieren. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**7.** Klicken Sie auf **Absenden**.




Automatische Übersetzung

## Security Operations E-Mail-Verarbeitung

Sie können die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Datensätzen zu Sicherheitsvorgängen bereitstellen, nicht abgeglichene E-Mails behandeln und die Duplizierung von Datensätzen mit E-Mail-Verarbeitungverhindern.

E-Mail-Verarbeitung besteht aus den folgenden Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Funktion | Beschreibung |
|---|---|
| E-Mail-Analyse | Generiert neue Security Operations Datensätze aus externen System-E-Mails. |
| Duplizierungsregeln | Identifiziert neue E-Mails mit bekannten Incidents und verarbeitet sie entsprechend. |
| Eigenschaften | Gibt Accounts an, die als Eingabe in E-Mail-Analyse für Sicherheit, Schwachstelle und IoCs verwendet werden. Ermöglicht die Granularität bei der Verarbeitung von Security Operations Datensätzen. |
| Nicht übereinstimmende E-Mails | Listet E-Mails auf, die keinem Security Operations -Datensatz entsprechen. |

## E-Mail-Eigenschaften für Security Operations

E-Mail Eigenschaften Geben Sie an, welche Posteingänge als Eingabe in E-Mail-Analyse verwendet werden, um Informationen aus externen Erkennungssystemen zu importieren und Datensätze für Sicherheit, Schwachstelle und IoCs zu erstellen. Sie können ein allgemeines Konto für alle zu verwendenden externen Erkennungssysteme oder einzelne E-Mail-Konten für Security Incident Response, Threat Intelligenceoder Vulnerability Responseeinrichten.

### Erstellen Sie Security Operations E-Mail-Eigenschaften

Sie können E-Mail-Adressen für Berichte angeben und das automatische E-Mail-Verhalten über E-Mail Eigenschaftensteuern.

#### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Richten Sie externe Erkennungstools ein, um E-Mails an Ihren Posteingang zur E-Mail-Analyse zu senden.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften**.
2. Geben Sie die entsprechenden Empfängerpostfächer ein:
   Dies sind eingehende E-Mail-Adressen, die von der E- **Mail-Analyse**und nicht von **eingehenden Aktionen**verarbeitet werden sollen.

**E-Mail-Analyseeigenschaften**

| Feld | Beschreibung |
|---|---|
| Posteingang für Security Operations Tools | Vollständige E-Mail-Adresse für Security Operations. Beispiel: secops_support@yourcompany.com. |
| Postfach für Sicherheits-Incident-Tools | Vollständige E-Mail-Adresse für Security Incident Response. Beispiel: sir_support@your.company.com. |
| Posteingang für Vulnerability Response Tools | Vollständige E-Mail-Adresse für Vulnerability Response. Beispiel: vuln_resp@yourcompany.com. |
| Posteingang für Threat Intelligence Tools | Vollständige E-Mail-Adresse für Threat Intelligence. Beispiel: Threat_intel@yourcompany.com. |

3. Klicken Sie auf **Speichern**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Security Operations E-Mail-Analyse

Generieren Sie neue Security Operations Datensätze aus externen Erkennungssystemen mit E-Mail-Analyse. Diese Funktion bietet eine Methode zur Integration von Informationen aus externen Tools wie Malware-Erkennung, Schwachstellenerkennung, Firewalls, Threat Intelligence und mehr.

### Wie E-Mails analysiert werden

Jedes System, das eine E-Mail senden kann, kann Security Operations Datensätze erstellen, z. B. Security Incidents, Anforderungen, angreifbare Elemente, Schwachstellen, erkennbare Elemente von Security Incidents, Angriffsmethoden und mehr.

Alle Security Operations -Plugins (Security Incident Response, Threat Intelligenceund Vulnerability Response) haben eine Eigenschaft (**email_to**), die die E-Mail-Adresse definiert, an die externe Integrationen E-Mails senden sollen, die von den E-Mail-Parsern analysiert werden sollen. Siehe **E-Mail-Verarbeitung** > **Eigenschaften** für weitere Informationen.

E-Mails, die an eine der Security Operations E-Mail-Adressen gesendet werden, werden in einer E-Mail-Ereignistabelle gespeichert. Diese E-Mails werden verarbeitet, um festzustellen, ob sie mit einem E-Mail-Parser übereinstimmen.

E-Mails mit einer Übereinstimmung werden gekennzeichnet, und die Transformations- und Duplizierungsregeln erstellen oder aktualisieren einen Security Operations -Datensatz. Die E-Mail wird mit diesem Datensatz verknüpft und als abgeglichen gekennzeichnet.

E-Mails, die nicht übereinstimmen, werden in Nicht übereinstimmende E-Mails als Datensatz Security Operations ] aufgelistet. Sie können überprüft werden, um E-Mail-Parser für die Verarbeitung dieser E-Mails zu erstellen. Mit einer Aktion „Erneut verarbeiten“ können Sie die nicht abgeglichene E-Mail erneut durch die Parser ausführen. Das ursprüngliche E-Mail-Protokoll ist mit diesem Datensatz verknüpft.

Die Duplizierungsregeln für die E-Mail-Transformation verwalten mehrere E-Mails, die sich auf dasselbe Problem beziehen. Diese Regeln definieren, was einen doppelten Datensatz ausmacht, und können verhindern, dass doppelte Datensätze erstellt werden. Wenn ein Duplikat erkannt wird, gibt die Regel an, welche Aktion ausgeführt werden soll: keine Aktion (keinen neuen Datensatz erstellen), den neuen Datensatz als untergeordneten Datensatz des vorhandenen Datensatzes erstellen oder den vorhandenen Datensatz aktualisieren. Beim Aktualisieren gibt die Duplikatregel an, welche Felder im vorhandenen Datensatz aktualisiert werden.

**Hinweis:**
Ein Security Operations E-Mail-Parser funktioniert in Verbindung mit eingehenden Plattformaktionen und ersetzt diese nicht. Das Festlegen von Werten für indirekte Felder, z. B. **sys_journal_field-**Einträge, wird nicht unterstützt.

Standardmäßig werden E-Mail-Events nach 30 Tagen gelöscht.

### Mehrere Datensätze

Externe Erkennungssysteme (Malware-Detektoren, Schwachstellen usw.) können E-Mails senden, die mehrere Elemente gleichzeitig melden. Der E-Mail-Parser unterstützt Trennzeichen innerhalb der E-Mail.

Zum Beispiel könnte ein Malware-Erkenner Ihnen einen E-Mail-Bericht über alle Systeme in Ihrem Netzwerk senden, die mit einer bestimmten Malware infiziert sind, wobei zuerst Informationen zur Malware angezeigt werden, gefolgt von einer Liste der betroffenen Systeme.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Beispiel für schädliche E-Mail**

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
============================
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
============================
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
============================
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

In diesem Beispiel wird die E-Mail in vier Abschnitte aufgeteilt, wenn die **Datensatztrennung** in Ihrer E- **Mail-Transformation**als ========== **nicht** Dadurch wird für jedes der drei betroffenen Systeme ein Security Incident erstellt.

**Hinweis:**
Der Header-Abschnitt wird erkannt, weist jedoch keine betroffenen Systeme auf. Daher wird er in allen drei Datensätzen verwendet und erstellt keinen vierten Datensatz.

**Feldtransformationen** rufen Daten aus jedem Abschnitt ab. Wenn etwas in der Kopf- oder Fußzeile der E-Mail für alle Datensätze gilt, z. B. Malware-Hash, Malware-Name und Typ in diesem Beispiel, sollte die Feldtransformation für sie **Wert für Suche** auf einen Wert festlegen, der den E-Mail-Text durchsucht, entweder **At der Beginn einer Zeile im E-Mail-Text** oder **an beliebiger Stelle im E-Mail-Text**.

**Feldtransformationen**müssen so festgelegt werden, dass sie **am Anfang einer Zeile innerhalb des Datensatzabschnitts oder Abschnittsnach** Daten suchen, die in jedem Abschnitt definiert sind, z. B. System, IP-Adresse oder Status. Die Optionen für Datensatzabschnitte sind nur verfügbar, wenn in der E-Mail-Transformation ein Datensatztrennzeichen definiert ist.

Beim Analysieren einer E-Mail mit definiertem Trennzeichen werden Datensätze nur für Abschnitte mit mindestens einem abschnittsspezifischen Datenelement erstellt.

In diesem Beispiel werden drei Datensätze erstellt, obwohl vier Abschnitte definiert sind. Der erste Abschnitt ist ein Header, und es fehlt etwas, das nur für ein System spezifisch ist. Wenn eines der Felder im ersten Abschnitt ausgefüllt wurde (System, IP oder Status), wird auch für diesen Abschnitt ein Datensatz erstellt.

**Zugehörige Informationen**

- Erstellen Sie E-Mail-Parser in Security Operations
- Security Operations -Ergänzungsdatenzuordnung
- Security Operations Feldzuordnung

## Erstellen Sie E-Mail-Parser in Security Operations

E-Mail-Analyse erstellt Security Operations Datensätze aus Ihrer E-Mail für Sicherheit, Schwachstelle und erkennbare Elemente, um die Reaktion auf Bedrohungen und die Behebung von Bedrohungen zu beschleunigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

- Richten Sie externe Erkennungstools ein, um E-Mails an eine zentrale E-Mail-Adresse zu senden.
- Legen Sie die E-Mail-Adresse in Security Operations Eigenschaften fest. Weitere Informationen finden Sie unter Erstellen Sie Security Operations E-Mail-Eigenschaften.
- Weisen Sie dieser E-Mail-Adresse ein Benutzerkonto zu, und geben Sie diesem Benutzer Sicherheitszugriffskontrollen, um die E-Mail-Ereignisdatensätze zu erstellen und zu aktualisieren.
- Halten Sie eine Kopie der relevanten E-Mail von Ihrem externen Erkennungstool bereit.
- Entscheiden Sie, welche Art von Datensatz Sie erstellen möchten: Security Incident, Schwachstellendatensatz, Aufgabe usw. Diese Auswahl bestimmt die Tabelle, die Sie auswählen.

Erforderliche Rolle: sn_sec_cmn.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Hinweis:**
Wenn mehr als ein Feld angegeben ist, müssen alle Felder mit der E-Mail übereinstimmen, um einen Datensatz zu erstellen.

#### E-Mail-Parser

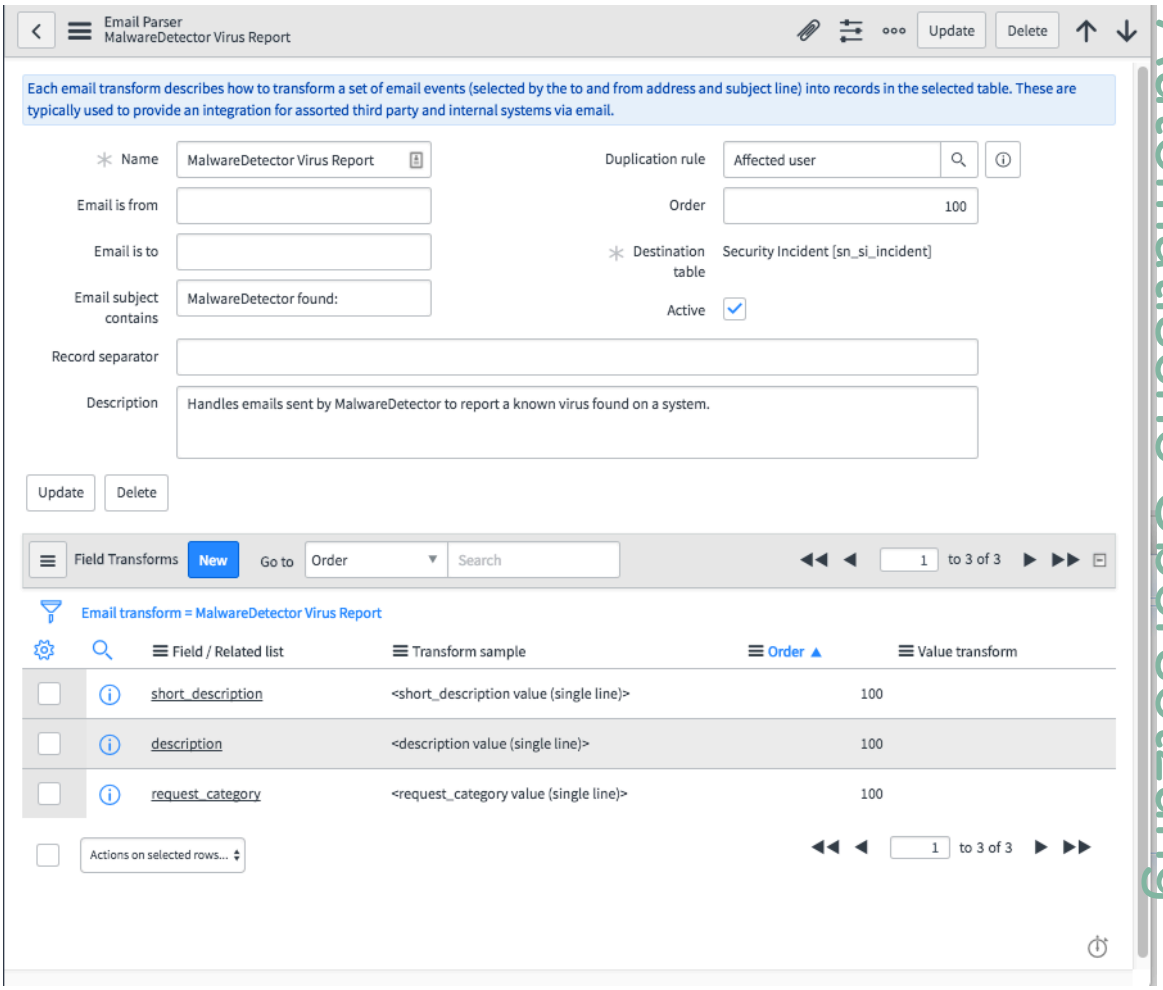
| Feld | Beschreibung |
|---|---|
| Name | Der Name des E-Mail-Parsers. |
| E-Mail ist von | Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt. |
| E-Mail an | Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt. |
| E-Mail Betreff enthält | Wenn ausgefüllt, werden nur E-Mails, deren Betreff diesen Ausdruck enthält, von diesem E-Mail-Parser umgewandelt. |
| Duplizierungsregel | Steuert die Behandlung doppelter E-Mails für alle E-Mails, die diese Transformation behandelt. Weitere Informationen finden Sie unter Transformation freigegebener Daten. |
| Bestellung | In welcher Reihenfolge die Transformationen berücksichtigt werden sollen. Die erste übereinstimmende E-Mail-Transformation wird verwendet. Normalerweise möchten Sie die spezifischsten E-Mail-Parser in den niedrigeren Nummern mit etwas Fallback einrichten. Geben Sie Catchall-E-Mail-Parsern höhere **Reihenfolgennummern**, damit sie ausgeführt werden, wenn nichts anderes übereinstimmt. Der Standardwert ist 100. Wenn alles übereinstimmt, wird der spezifischste E-Mail-Parser (entspricht **von**, **bis**und **Betreff**) verwendet. |
| Zieltabelle | Die Tabelle, in der Sie Datensätze erstellen möchten. |
| Aktiv | Gibt an, ob diese Transformation aktiv ist, verwendet wird oder nicht aktiv ist. Wenn diese Option deaktiviert ist, werden keine E-Mails mit diesem Code umgewandelt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Datensatztrennung | Wenn von diesem E-Mail-Parser verarbeitete E-Mails mehrere Datensätze erstellen, enthält dieses Feld das Trennzeichen zwischen den Informationen für diese Datensätze. Weitere Informationen finden Sie unter Security Operations E-Mail-Analyse. |
| Beschreibung | Beschreibung dieses E-Mail-Parsers, das Tool, mit dem er funktioniert, der Zweck usw. |

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formular-Header, und wählen **Sie Speichern**aus.
Eine Registerkarte **Feldtransformationen** wird angezeigt. Diese Registerkarte zeigt, wie einzelne Felder in der Zieltabelle basierend auf dem E-Mail-Inhalt festgelegt werden.




5. Führen Sie die folgenden Schritte aus, um **Feldtransformationen**hinzuzufügen.

   a. **Klicken** Sie auf der Registerkarte Feldtransformationen auf **Neu**.

   b. Füllen Sie die entsprechenden Felder im Formular aus.

| Option | Bezeichnung |
|---|---|
| **Feld** | **Beschreibung** |
| **Wert in einem Feld oder einer zugehörigen Liste speichern** | Wählen Sie aus, wo der Wert zu finden ist. Zur Auswahl stehen: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | ○ Speichern Sie den Wert in einem Feld im neuen Datensatz<br>○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen<br>○ Verknüpfung mit diesem Wert erstellen und neuen Datensatz erstellen, wenn kein übereinstimmender Datensatz vorhanden ist<br>**Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt. |
| **Feld** | Wählen Sie das Feld aus, das mit diesem Wert ausgefüllt werden soll.<br>**Hinweis:**<br>Bei Auswahlfeldern werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten anhand der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Auswahlwerts vorgenommen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, der Auswahlliste wird jedoch kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten.<br>Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert gefunden wird, der dem Anzeigenamen des Datensatzes oder einer gültigen `sys_id` entspricht. Weitere Informationen finden Sie unter Referenzfelder. |
| **Zugehörige Liste** | Wenn **Wert in einem Feld oder einer zugehörigen Listespeichern auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit **diesem Wert verknüpfen festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhande**nist. In diesem Feld wird die zugehörige Liste angegeben, der Informationen hinzugefügt werden sollen. |
| **Wertfeld** | Wenn **Store value in a field or related list** (Wert in einem Feld oder einer zugehörigen Liste speichern) **auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit diesem Wert verknüpfen festgelegt **ist,** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | **wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhande n**ist. In diesem Feld wird das Feld in der Tabelle angegeben, die im zugehörigen an– gezeigt wird Liste. Es wird verwendet, um einen vorhandenen Datensatz zu suchen und zu finden. Wenn Ihre zugehörige Lis– te beispielsweise **„Betroffene CIs“**ist, kann dieses Feld „ **Name** “ oder „ **Vollständig qualifizierter Domänenname**“ oder ein an– deres Feld im CI-Datensatz enthalten, das für die Suche nach dem CI verwendet wer– den soll, das der Liste „ **Betroffene CIs** “ hinzugefügt wurde. |
| **Beziehungsdaten** | Wenn **Wert in einem Feld oder einer zugehö rigen Listespeichern auf Mit diesem Wert in einer zugehörigen Liste verknüpfen**fest– gelegt ist, wird ein Datensatz erstellt, um diesen Datensatz (z. B. einen Security In– cident) mit dem Wert (einem CI, einem er– kennbaren Element usw.) zu verknüpfen. ). Dieses Feld gibt zusätzliche Informationen (Feld- und Wertpaare) an, die dem Ver– knüpfungsdatensatz hinzugefügt werden sollen. Wenn Sie beispielsweise ein erkenn– bares Element für eine Quell-IP hinzufü– gen, geben Sie an, dass diese IP die Quell- und nicht die Ziel-IP ist. Verwenden Sie für mehrere Werte das Trennzeichen ^, z. B. type= Source IP^Active=true. |
| **Neue Datensatzdaten** | Wenn **Wert in einem Feld oder einer zugehö rigen Listespeichern auf Mit diesem Wert verknüpfen festgelegt ist, wird ein neuer Da tensatz erstellt, wenn kein übereinstimmen der Datensatz vorhanden**ist. Wenn kein zu– gehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein Datensatz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sollen. Wenn für **betrof fene CIs**keine übereinstimmenden CIs ge– funden werden, wird ein CI-Datensatz er– stellt. In diesem Fall wird der in der E-Mail gefundene Wert auf das Feld **Wert** im CI-Datensatz festgelegt. Sie können zusätz– liche Daten festlegen – eine Notiz, die an– gibt, warum das CI erstellt wurde, eini– ge Informationen darüber, mit welcher Art von CIs Sie arbeiten usw. Ein Beispiel wä– |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | re: description=Created by Malware Scan–ner email parser^type=autodetect. |
| **Suche nach Wert** | Wählen Sie die zu durchsuchende Stelle in der E-Mail aus. Zur Auswahl stehen:<br>○ **Am Anfang einer Zeile im E-Mail-Text**<br>○ **Irgendwo im E-Mail-Text**<br>○ **In der E-Mail-Betreffzeile**<br>○ **Immer der statistische Wert**<br><br>Wenn Sie eine **Datensatztrennung**definiert haben, können Sie mit weiteren Optionen (**Überall im Datensatzabschnitt** und **Am An fang einer Zeile innerhalb des Datensatzab schnitts)** nur im aktuellen Abschnitt anstatt im gesamten E-Mail-Text suchen (weitere Informationen finden Sie unter Security Ope-rations E-Mail-Analyse. Informationen.<br><br>Informationen, die sich in einer Kopf- oder Fußzeile befinden und für alle Datensät–ze gelten, werden im gesamten E-Mail-Text durchsucht. Die Informationen, die sich zwischen Datensätzen unterscheiden, wer–den nur innerhalb des Abschnitts gesucht. |
| **Werttrennzeichen** | Wenn **Wert in einem Feld oder einer zugehö rigen Listespeichern auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit **diesem Wert verknüpfen festgelegt ist, neuen Datensatz erstellen, wenn kein über einstimmender Datensatz vorhanden ist**, gibt dieses Feld das für Listen von Ele–menten zu verwendende Trennzeichen an. Zum Beispiel ein Komma oder ein Semi–kolon, wenn die Daten aus der E-Mail eine Liste von IP-Adressen sind. |
| **Wertepräfix** | Der Text, der immer vor dem in diesem Feld platzierten Wert steht, um zu extra–hieren. |
| **Ende des Werts** | Wählen Sie aus, was das Ende des Werts angibt. Auswahlmöglichkeiten: **Zeilenende**, E- **Mail-Ende** (führt den gesamten ver–bleibenden Text in die E-Mail ein) oder **Bis** (wird angehalten, wenn der angegebene Text gefunden wird) oder **Bis** (wird ange– |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | halten, wenn der angegebene Text gefunden wird). |
| **Wertesuffix** | Wenn das **Ende des Werts** auf **Bis**festgelegt ist, gibt dieses Feld an, welcher Text immer auf den in diesem Feld platzierten Wert folgt.<br><br>Suchen Sie beispielsweise nach einem Wert, der nach „Der betroffene Computer ist“ und vor „“ kommt. analysiert „AB123“ aus „Der dementierte Häschen-Virus wurde gefunden“. Der betroffene Computer ist AB123. Geschätzte Zeit der Infektion war 15:45 Uhr“ in einer E-Mail. |
| **Wertumwandlung** | Wählen Sie den anzuwendenden Feldtransformationseintrag aus. Konvertiert den in der E-Mail gefundenen Wert in einen anderen Wert, der zum Ausfüllen von Auswahlfeldern, gelegentlichen Referenzen und anderen Feldern verwendet wird. |
| **Bestellung** | Die Reihenfolge, in der die Feldtransformationen ausgeführt werden, von der niedrigsten zur höchsten. Zuerst wird eine Feldtransformation mit einem Reihenfolgeneintrag von 100 versucht. Nur wenn diese Feldtransformation keinen Wert findet, wird eine Feldtransformation mit einer höheren Reihenfolge (200) für dasselbe Feld ausgeführt. |
| **E-Mail-Transformation** | Die Transformation, zu der diese Feldtransformation gehört. |
| **Zieltabelle** | Zieltabelle der E-Mail-Transformation. Sie enthält Informationsdaten aus der E-Mail-Transformation. |
| **Aktiv** | Der Standardwert ist aktiviert. Wenn diese Option aktiviert ist, ist die Feldtransformation aktiviert. Deaktivieren Sie dieses Kontrollkästchen, um die Feldtransformation zu deaktivieren. |

**a.** Klicken Sie auf **Absenden**.
Der neue Datensatz wird verwendet, um die Informationen in der E-Mail in einen neuen Datensatz zu analysieren.

**Zugehörige Informationen**

Erstellen Sie Duplizierungsregeln in Security Operations

Erstellen Sie Security Operations Feldwerttransformationen

Definieren Sie Vulnerability Response E-Mail-Benachrichtigungen

### Bearbeiten Sie E-Mail-Datensätze in Security Operations

Fügen Sie Transformationen in Ihren vorhandenen E-Mail-Ereignisdatensätzen hinzu, oder erstellen Sie sie.



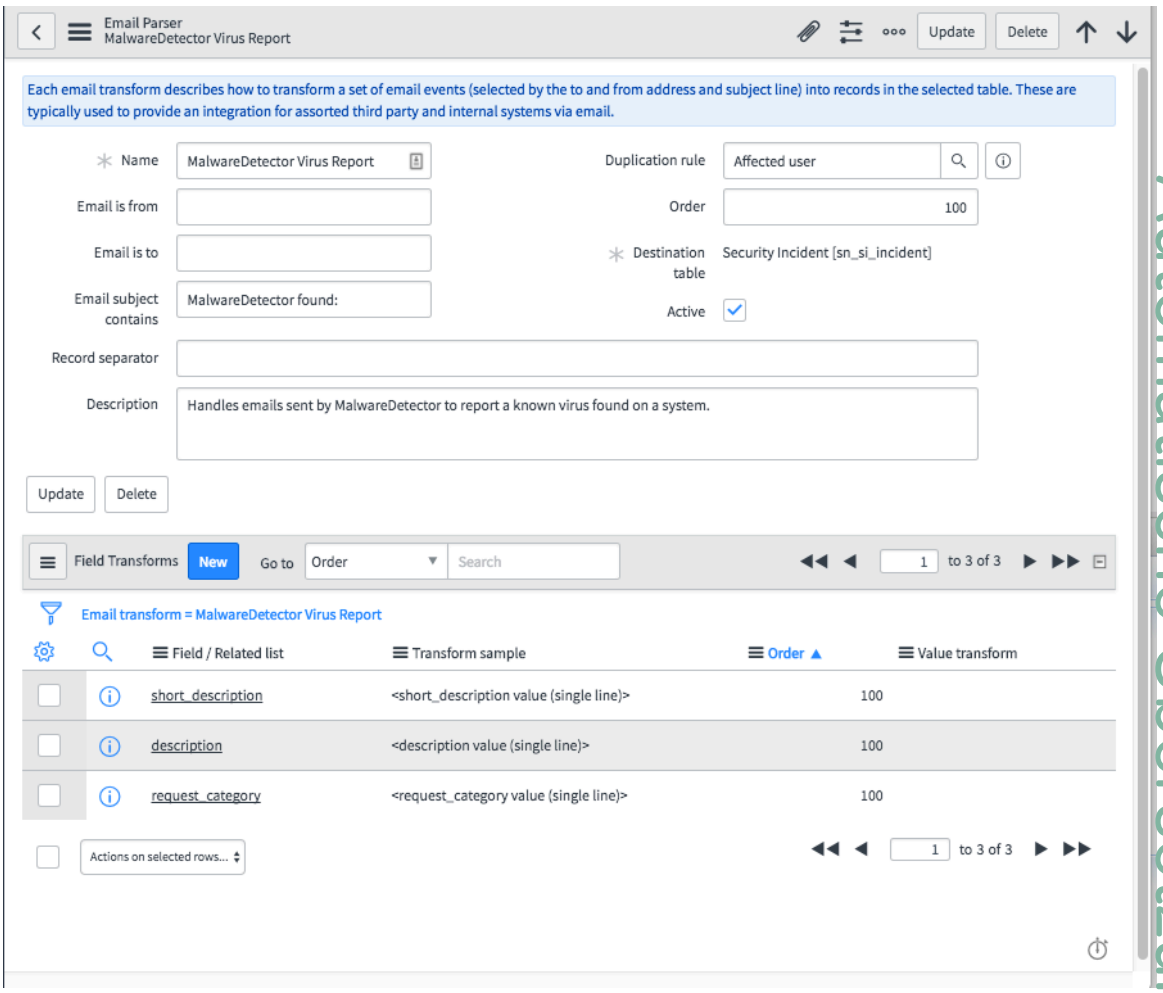
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**.
2. Klicken Sie auf den E-Mail-Parser, um ihn zu bearbeiten.
   Wenn der Datensatz schreibgeschützt ist, klicken Sie in der Header-Nachricht auf den Link hier.
   Sie gelangen zum bearbeitbaren Formular der Transformation.




3. Bearbeiten Sie die Felder nach Bedarf.
4. Um Feldtransformationen zu bearbeiten, klicken Sie in das **Feld**, und ändern Sie die entsprechenden Änderungen.
5. Klicken Sie auf **Aktualisieren.**

## Nicht abgeglichene Security Operations E-Mail-Ereignisse

Bei E-Mail-Events, die nicht mit einem E-Mail-Parser übereinstimmen, wird die Kennzeichnung „Abgestimmt“ aufgehoben. Sie können diese E-Mail-Ereignisdatensätze aus der Liste Nicht übereinstimmende E-Mails anzeigen, um externe Erkennungssysteme anzuzeigen, deren E-Mails noch nicht analysiert wurden.

Beim Erstellen von E-Mail-Parsern können Sie versuchen, das E-Mail-Ereignis (aus dem Formular oder der Liste) erneut zu verarbeiten, um einen neuen E-Mail-Parser zu validieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nicht abgeglichene Security Operations-E-Mails anzeigen und erneut verarbeiten

Sie können Nicht übereinstimmende E-Mails für eingestellte Filter oder als Kandidaten für einen neuen Filter überprüfen, um die Rate, mit der Sie E-Mail-Bedrohungen erkennen, beizubehalten oder zu verbessern.

#### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.read

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Nicht übereinstimmende E-Mails**.
   Wenn nicht abgeglichene E-Mails gefunden wurden, werden sie aufgelistet.
2. Die Felder im Formular lauten wie folgt:

**Sicherheits-E-Mail-Ereignisse**

| Feld | Beschreibung |
|---|---|
| Von | E-Mail-Adresse des Absenders. |
| Bis | E-Mail-Adresse der Empfänger. |
| Betreff | Betreffzeile in der E-Mail. |
| Textkörper | Inhalt des E-Mail-Texts. |
| Abgleich | Gibt an, ob dieses E-Mail-Ereignis abgeglichen wurde. |

3. Um diese E-Mail erneut zu verarbeiten, erstellen Sie einen E-Mail-Datensatz, oder bearbeiten Sie einen vorhandenen E-Mail-Datensatz, um die Informationen in dieser E-Mail abzugleichen.
   Weitere Informationen finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
4. Navigieren Sie zurück zu **Security Operations** > **Nicht übereinstimmende E-Mails**.
5. Klicken Sie auf E- **Mail-Ereignis erneut** verarbeiten, um zu versuchen, diese E-Mail zu verarbeiten.
   Sie kehren zur Hauptliste Nicht übereinstimmende E-Mails zurück. Wenn der neue E-Mail-Datensatz übereinstimmt, befindet sich das E-Mail-Event nicht mehr in der Liste. Eine Nachricht gibt an, ob eine Übereinstimmung gefunden wurde oder nicht.

## Security Operations Feldzuordnung

Security Operations -Tabellen können anderen Tabellen zugeordnet werden und aus anderen Tabellen, wodurch ein Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen des Security Operations -Systems verknüpft wird.

**Die Feldzuordnung** definiert die Zuordnung, die verwendet wird, wenn ein Datensatz aus der Quelltabelle zum Erstellen eines neuen Datensatzes in der Zieltabelle verwendet wird. Diese Zuordnungen werden normalerweise verwendet, um einen Security Incident aus einem anderen Datensatz zu erstellen. Sie definieren, welche Felder in einem Security Incident in ein neues Problem eingefügt werden oder welche Felder aus einem vorhandenen Kunden-Incident einen neuen Security Incident ausfüllen.

### Ordnen Sie Tabellen Tabellen mit Security Operations-Feldzuordnung zu

Security Operations bietet Ihnen eine feinere Granularität der Feldzuordnung, sodass Sie eine Tabelle Security Operations einer anderen Tabelle zuordnen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:sec_cmn.write

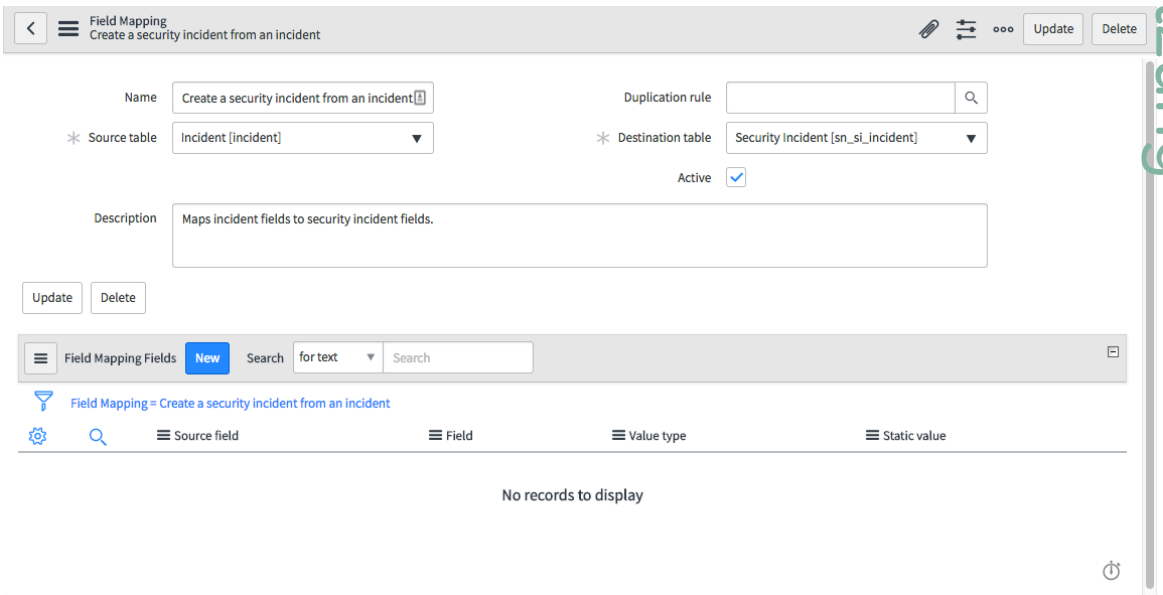
### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

**Feldzuordnung**

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Feldzuordnung. |
| Quelltabelle | Die Tabelle, die die Daten bereitstellt, die zum Erstellen eines Datensatzes in der Zieltabelle verwendet werden sollen. |
| Duplizierungsregel | Steuert den Umgang mit Quelldatensätzen, die einen doppelten Datensatz generieren würden. Weitere Informationen finden Sie unter Transformation freigegebener Daten. |
| Zieltabelle | Die Tabelle, in der neue Datensätze erstellt werden. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Zuordnung zu aktivieren.<br>**Hinweis:**<br>Es kann jeweils nur eine Zuordnung zwischen Tabellen aktiv sein. Wenn zwei Zuordnungen dieselben Tabellen enthalten, wird die ältere Version automatisch deaktiviert. |
| Beschreibung | Beschreibung für die Feldzuordnung. |

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formular-Header, und wählen **Sie Speichern**aus.
   Die Registerkarte**Feldzuordnungsfelder** wird angezeigt. Dieser Datensatz definiert, welche Daten im Zielfeld in Datensätzen platziert werden, die von dieser Feldtransformation erstellt werden.




5. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**6.** Füllen Sie die entsprechenden Felder im Formular aus.

| Option | Bezeichnung |
|---|---|
| **Feld** | **Beschreibung** |
| **Wert in einem Feld oder einer zugehörigen Liste speichern** | Wählen Sie aus, wo der Wert zu finden ist. Zur Auswahl stehen:<br>○ Neuen Wert in einem Feld im Datensatz hinzufügen<br>○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen<br>○ Verknüpfen Sie mit diesem Wert, und erstellen Sie einen Datensatz, wenn kein übereinstimmender Datensatz vorhanden ist<br>**Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt. |
| **Feld** | Wenn **Wert in einem Feld oder einer zugehörigen Listespeichern im Datensatz auf Neuen Wert in einem Feld** hinzufügen festgelegt ist, gibt dieses Feld das auszufüllende Feld an.<br>**Hinweis:**<br>Bei Auswahlfeldern werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten anhand der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Auswahlwerts vorgenommen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, der Auswahlliste wird jedoch kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten.<br>Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert gefunden wird, der dem Anzeigenamen des Datensatzes oder einer gültigen`sys_id` `entspricht`. Weitere Informationen finden Sie unter Referenzfelder. |
| **Zugehörige Liste** | Wenn **Wert in einem Feld oder einer zugehörigen Listespeichern auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit **diesem Wert verknüpfen festgelegt ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhande**nist. In diesem Feld wird die zugehörige |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | Liste angegeben, der Informationen hinzugefügt werden sollen. |
| **Wertfeld** | Wenn **Store value in a field or related list** (Wert in einem Feld oder einer zugehörigen Liste speichern) **auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit diesem Wert verknüpfen festgelegt **ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhande n**ist. In diesem Feld wird das Feld in der Tabelle angegeben, die im zugehörigen angezeigt wird -Liste, die zum Suchen und Finden eines vorhandenen Datensatzes verwendet wird. Wenn Ihre zugehörige Liste beispielsweise **„Betroffene CIs“**ist, kann dieses Feld „ **Name** “ oder „ **Vollständig qualifizierter Domänenname**“ enthalten, oder ein beliebiges anderes Feld im CI-Datensatz, das für die Suche nach dem CI verwendet werden soll, wird der Liste „ **Be troffene CIs** “ hinzugefügt. |
| **Beziehungsdaten** | Wenn **Wert in einem Feld oder einer zugehö rigen Listespeichern auf Mit diesem Wert in einer zugehörigen Liste verknüpfen**festgelegt ist, wird ein neuer Datensatz erstellt, um diesen Datensatz (z. B. einen Security Incident) mit dem Wert (einem CI, einem erkennbaren Element usw.) zu verknüpfen ). Dieses Feld gibt zusätzliche Informationen (Feld- und Wertepaare) an, die diesem Verknüpfungsdatensatz hinzugefügt werden sollen. Wenn Sie beispielsweise ein erkennbares Element für eine Quell-IP hinzufügen, können Sie angeben, dass diese IP die Quell- und nicht die Ziel-IP ist. Verwenden Sie für mehrere Werte das Trennzeichen ^, z. B. type= Source IP^active=true. |
| **Neue Datensatzdaten** | **Wenn Wert in einem Feld oder einer zugehö rigen Listespeichern auf Mit diesem Wert verknüpfen festgelegt ist, wird ein neuer Da tensatz erstellt, wenn kein übereinstimmen der Datensatz vorhanden**ist. Wenn kein zugehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein neuer Datensatz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sollen. Beispiel: Wenn das CI für **Betroffene CIs**nicht gefunden werden kann, gibt diese Einstellung an, dass ein neu- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
| --- | --- |
| | es CI erstellt wird. Der im Quelldatensatz gefundene Wert wird auf das Feld **Wert** im CI-Datensatz festgelegt. Sie können zusätzliche Daten festlegen – eine Notiz, die angibt, warum dieses CI erstellt wurde, und einige Informationen darüber, mit welcher Art von CIs Sie arbeiten. Ein Beispiel wäre: `description=Created byMalware Incident report^type=autodetect` |
| **Werttrennzeichen** | Wenn **Wert in einem Feld oder einer zugehörigen Listespeichern auf Mit diesem Wert verknüpfen in einer zugehörigen Liste** oder Mit diesem Wert verknüpfen festgelegt **ist, wird ein neuer Datensatz erstellt, wenn kein übereinstimmender Datensatz vorhanden ist**. In diesem Feld wird das für Listen von Elementen zu verwendende Trennzeichen angegeben. üblicherweise ein Komma oder Semikolon. |
| **Werttyp** | Wenn **Wert in einem Feld oder einer zugehörigen Listespeichern im Datensatz auf Neuen Wert in einem Feld** hinzufügen festgelegt ist, gibt dieses Feld den Typ des Werts an. Zur Auswahl stehen:<br>○ **Quellfeld-Datensatz**<br>○ **Dem Feld als neue Zeile anfügen**<br>○ **Statischer Wert**<br>○ **Statischer Wert plus Quelldatensatz-Feld wert** |
| **Quellenfeld** | Wählen Sie das Quellfeld aus, das den Wert enthält, der im Zielfeld oder in der ausgewählten zugehörigen Liste platziert werden soll. |
| **Statisches Feld** | Statischer Wert für das Feld. |
| **Wertumwandlung** | Wählen Sie den anzuwendenden Feldwert-Transformationseintrag aus. Es wird verwendet, um Auswahlfelder zwischen Datensätzen zuzuordnen, z. B. um den Satz der **Kategorieauswahlmöglichkeiten** für einen Security Incident in das entsprechende **Typfeld** für eine Change-Anforderung zu konvertieren. |
| **Zieltabelle** | Wird automatisch mit der Zieltabelle ausgefüllt. |
| **Feldzuordnung** | Wird automatisch mit der übergeordneten Feldzuordnung ausgefüllt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Bezeichnung |
|---|---|
| **Quelltabelle** | Wird automatisch mit der Quelltabelle ausgefüllt. |

**7.** Klicken Sie auf **Absenden**.

## Security Operations Feldwerttransformationen

Wandelt eindeutige Kundenfeldwerte in Feldwerte um, die von Security Operations E-Mail-Analyse, Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen erkannt werden. Unterstützt Auswahlfelder, Referenzen und richtet externe Daten in der Standardterminologie und im Standardformat für Ihren neuen Datensatz aus.

Sie können Daten für Felder wie Kategorie, Status oder Zuweisungsgruppe den Werten zuordnen, die in der Tabelle „Sicherheitsvorgänge“ verwendet werden. Ordnen Sie beispielsweise „In Analyse“ zu „In Arbeit“ zu.

### Erstellen Sie Security Operations Feldwerttransformationen

**Feldwerttransformationen** definiert eine Transformation zwischen den bereitgestellten Quelldaten und dem zu verwendenden Ersatzwert.

#### Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.basic oder sn_si.basic

#### Warum und wann dieser Vorgang ausgeführt wird
Definieren Sie jeden Transformationseintrag, der angewendet werden soll, wenn eine Übereinstimmung mit dem Suchwert vorliegt oder wenn der Suchwert in den bereitgestellten Quelldaten enthalten ist oder wenn keine Übereinstimmungen gefunden werden. Legen Sie einen Standardwert fest, wenn keine Übereinstimmung gefunden wird. Wenn kein Standardwert festgelegt ist und keine Übereinstimmungen gefunden werden, werden die ursprünglichen Quelldaten verwendet.

#### Prozedur

**1.** Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldwertumwandlungen**.

**2.** Klicken Sie auf **Neu**.

**3.** Füllen Sie die entsprechenden Felder im Formular aus.

**Feldwerttransformationen**

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Feldwerttransformation. |
| Beschreibung | Beschreibung für die Feldzuordnung. |
| Feldwert-Umwandlungseinträge | Die Tabellenliste der Einträge.<br>**a.** Doppelklicken Sie unter „ **Daten ersetzen**“ auf „Neue Zeile einfügen“.<br>**b.** Wählen Sie eine der folgenden Optionen: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Wann das Datum für dieses Feld übereinstimmt<br>Wenn die Daten für dieses Feld Folgendes enthalten<br>Wenn kein anderer Transform-Eintrag mit den Daten (Standard) übereinstimmt<br>**c.** Klicken Sie auf das grüne Häkchen.<br>**d.** Doppelklicken Sie unter **Suchwert**, und fügen Sie Ihren Suchwert hinzu.<br>**e.** Klicken Sie auf das grüne Häkchen.<br>**f.** Doppelklicken Sie unter **Ersatzwert auf** den entsprechenden Wert ServiceNow.<br>**g.** Wiederholen Sie den Vorgang bei Bedarf. |
| Aktiv | Aktivieren Sie dieses Kontrollkästchen, um die Transformation zu aktivieren. |
| Anwendung | Umfang der Anwendung. |

4. Klicken Sie auf **Absenden**.

## Security Operations -Ergänzungsdatenzuordnung

Ergänzungsdatenzuordnung wandelt Daten aus XML-, JSON- oder Eigenschaften -Dateien in ServiceNow -Datensätze um. Security Operations -Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit.

Security Operations enthält mehrere Ergänzungsdatenzuordnungen, die durch verschiedene Workflows ausgelöst werden, z. B. Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“. und Workflow „Security Operations System Command Integration – Laufende Prozesse abrufen“.. Die Ausgabe der Ergänzungsdatenzuordnung von Security Operations**-Workflows** wird auf der Registerkarte Ergänzungsdaten im Security Incident-Formular angezeigt.

### Erstellen Sie eine Security Operations -Ergänzungsdatenzuordnung

Transformieren Sie Daten aus dem JSON-, XML- oder Eigenschaften -Dateiformat mithilfe von Ergänzungsdatenzuordnungen in ServiceNow -Datensätze.

#### Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.write

#### Warum und wann dieser Vorgang ausgeführt wird
Vorhandene Ergänzungsdatenzuordnungen werden von Workflows verwendet, die in Security Operationsbereitgestellt werden. Sie können die Liste unter **Ergänzungsdatenzuordnung**anzeigen. Um eine Zuordnung zu verwenden, benötigen Sie einen Auslöser, entweder eine Geschäftsregel oder einen Workflow.

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Ergänzungsdatenzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen einer Ergänzungsdatenzuordnung

| Feld | Beschreibung |
|---|---|
| Name | Name dieser Ergänzungsdatenzuordnung. |
| Eingabeformat | Wählen Sie ein Format aus der Liste aus:<br>JSON (Standard)<br>XML<br>Eigenschaften Dateiformat |
| Präfixschlüssel | Verwenden Sie diese Option, um den Eingabedatensatz auf einen angegebenen Schlüssel zu beschränken. Der Stamm des Eingabedatensatzes wird auf diesen Schlüssel festgelegt. Wenn Sie in diesem Beispiel file_info eingegeben haben, sind die Eingabewerte auf die Werte in file_info beschränkt.<br>`<?xml version="1.0" encoding="UTF-8"?>`<br>`<malware>`<br>`<version>2.0</version>`<br>`<file_info>`<br>`<malware>yes</malware>`<br>`<sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>`<br>`<filetype>PE</filetype>`<br>`<sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256>`<br>`<md5>ee8c91751b3010e38c479cf9ab09827a</md5>`<br>`<size>546304</size>`<br>`</file_info>`<br>`</malware>` |
| Anwendung | Umfang der Anwendung. |
| Duplizierungsregel | Regel, die definiert, wann ein Datensatz als Duplikat betrachtet wird und welche Aktionen mit doppelten Datensätzen ausgeführt werden sollen. |
| Zieltabelle | Wählen Sie eine Tabelle aus der Liste aus. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Zuordnung zu aktivieren. |
| Beschreibung | Geben Sie eine Beschreibung der Ergänzungsdatenzuordnung ein. |

4. Klicken Sie auf **Absenden**.
   Die Registerkarte Ergänzungsdatenzuordnungsfelder wird angezeigt.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergänzungsdatenzuordnungsfelder

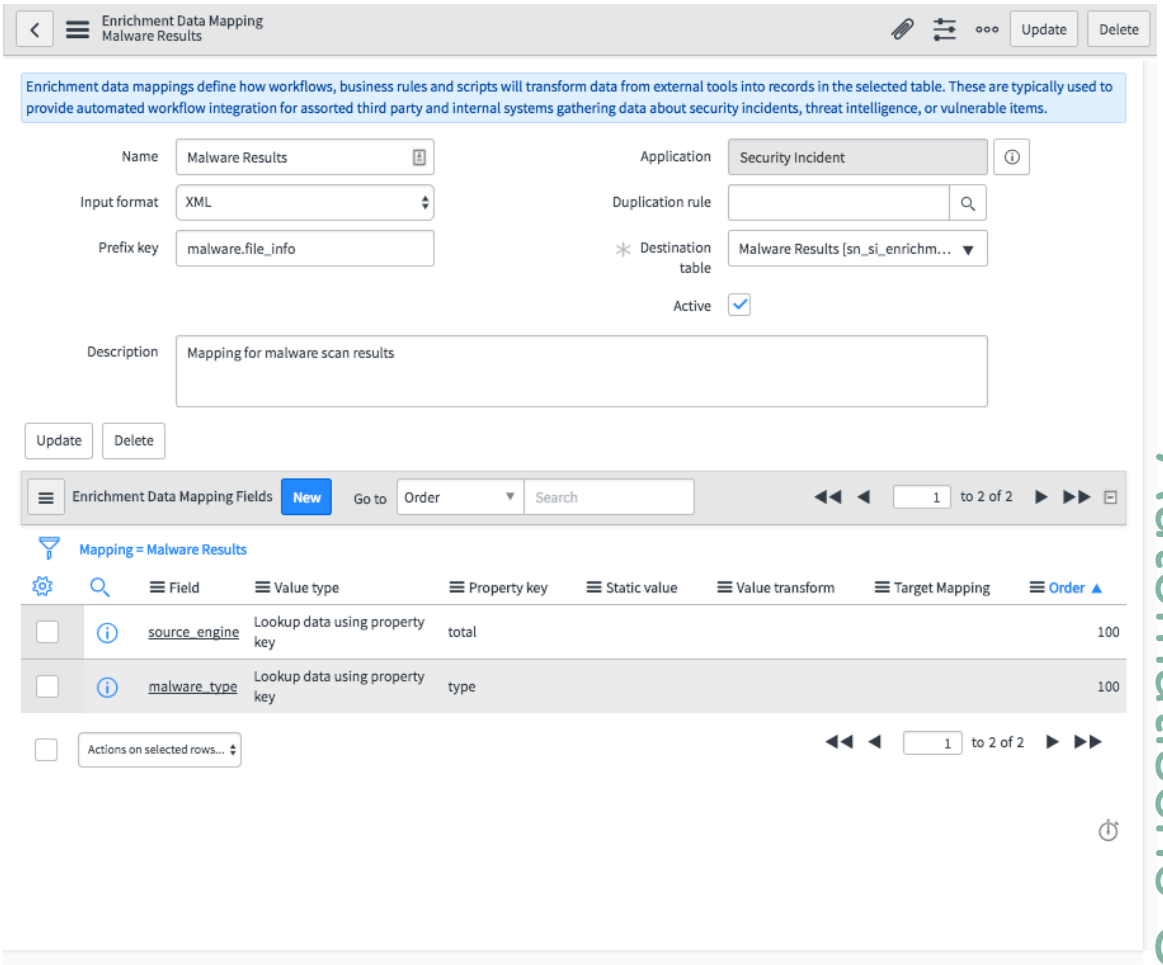
| Feld | Beschreibung |
|---|---|
| Feld | Name der Ergänzungsdatenzuordnung. |
| Werttyp | Wählen Sie aus der Liste:<br>Suchdaten, die einen Eigenschaftsschlüssel verwenden<br>Statischer Wert<br>Statischer Wert plus Daten aus dem Eigenschaftsschlüssel<br>Feld ist ein Array oder Objekt (Rohdatenschachtelung)<br>Jede Auswahl hat unterschiedliche Einträge. Feldwerte und Arrays oder Objekte erfordern einen Eigenschaftsschlüssel. |
| Eigenschaftsschlüssel | Bestimmt den Schlüssel für die Eingabedatensuche und den in das Zielfeld geschriebenen Wert. |
| Wertumwandlung | Die Feldwerttransformation, die einen Wert einem anderen zuordnet. |
| Anwendung | Umfang der Anwendung. |
| Bestellung | In welcher Reihenfolge die Zuordnung berücksichtigt werden soll. Die erste Übereinstimmung wird verwendet. Der Standardwert ist 100. |
| Zuordnung | Name der Ergänzungsdatenzuordnung. |
| Zieltabelle | Die Tabelle, der die zuzuordnenden Felder zugeordnet werden. |

7. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt eine Ergänzungsdatenzuordnung.




## Security Operations benutzerdefinierte Eskalation

Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachkenntnisse erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird für jeden Security Incident in dieser Gruppe eine Schaltfläche angezeigt.

### Erstellen Sie eine Security Operations benutzerdefinierte Eskalationsgruppe

Eskalieren Sie einen Security Incident mithilfe von Eskalationen an eine beliebige Gruppe, die mit dem Incident verknüpft ist.

#### Vorbereitungen

Erforderliche Rolle: sn_si.admin

#### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Eskalationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

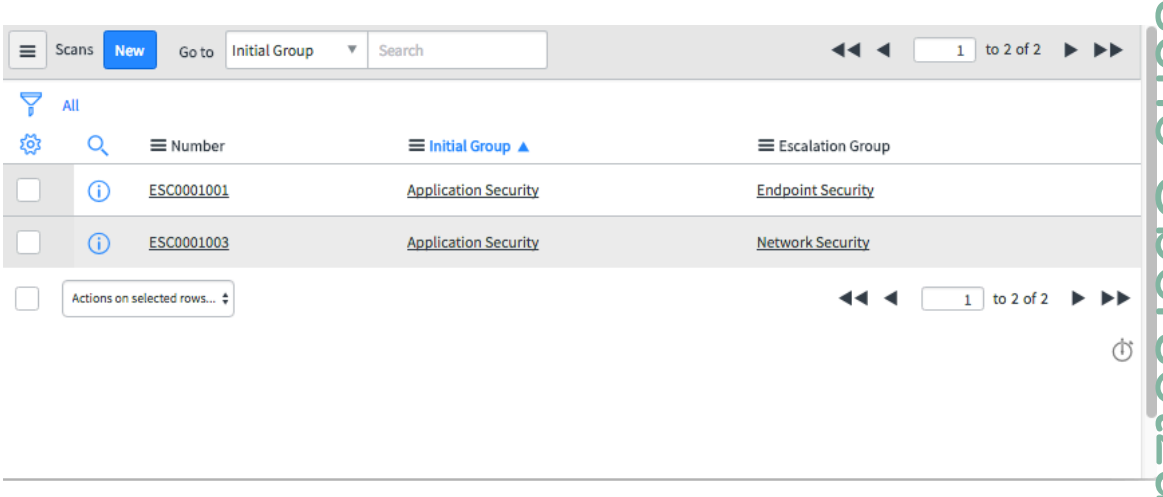
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eskalationen

| Feld | Beschreibung |
|---|---|
| Nummer | Nummer des Eskalations-Incidents (Feld wird automatisch generiert). |
| Ursprungsgruppe | Wählen Sie die Gruppe aus, zu der dieser Security Incident gehört. |
| Eskalationsgruppe | Wählen Sie die Gruppe aus, an die der Security Incident eskaliert werden soll. |

4. Klicken Sie auf **Absenden**.
   Eine Eskalationsgruppe ist für alle Security Incidents in der ursprünglichen Gruppe verfügbar. Sie können mehrere Gruppen erstellen.




## Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen

Wenn Sie die Domänentrennung verwenden, können Sie Überschreibungen für vorhandene Security Operations-Eigenschaften erstellen, mit denen Sie die Funktionen der Anwendungen in jeder Ihrer Domänen anpassen können.

### Vorbereitungen

Erfordert die Aktivierung von Domänen-Support – Domänenerweiterungen . Sie können auch mehr über den Domänenüberschreibungs-Viewer erfahren.

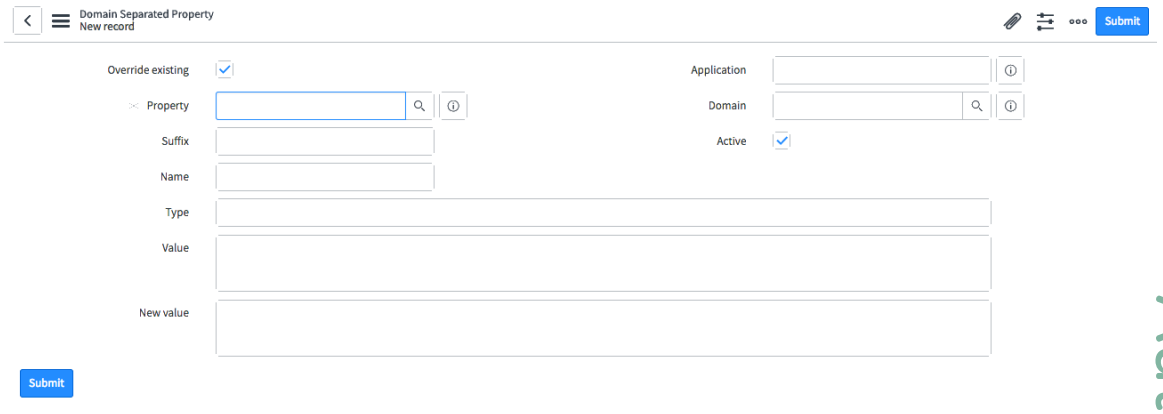
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Nach Domäne getrennte Eigenschaften**.
2. Klicken Sie auf **Neu**.




3. Füllen Sie die Felder des Formulars aus.

### Formular „Domain Separation-Eigenschaft“

| Feld | Beschreibung |
|---|---|
| Vorhandene überschreiben | Aktivieren Sie diese Checkbox, um einen domänenspezifischen Wert für eine vorhandene Eigenschaft zu erstellen. |
| Anwendung | Wählen Sie die Anwendung aus, die die Eigenschaft enthält, die Sie überschreiben möchten. |
| Eigenschaft | Wählen Sie die Eigenschaft für die ausgewählte Anwendung aus, für die Sie eine domänenspezifische Überschreibung erstellen möchten. |
| Domäne | Wählen Sie die Domäne aus, für die Sie diese Eigenschaftsüberschreibung erstellen. |
| Aktiv | Aktivieren oder deaktivieren Sie die Überschreibung. |
| Suffix | Zeigt das Eigenschaftssuffix an. |
| Name | Zeigt den Eigenschaftsnamen an. |
| Typ | Zeigt den Eigenschaftstyp an. |
| Wert | Zeigt den aktuellen Wert an, der für die Eigenschaft festgelegt wurde. |
| Neuer Wert | Geben Sie einen neuen Wert für die Eigenschaft ein, die auf diese Domäne angewendet werden soll. |

4. Klicken Sie auf **Absenden**.
   Die Eigenschaftsüberschreibung wird auf die ausgewählte Eigenschaft in der angegebenen Domäne angewendet. Wenn die Logik für diese Eigenschaft ausgelöst wird, sucht das System nach domänengetrennten Eigenschaftsüberschreibungen. Wenn eine Überschreibung für die Domäne gefunden wird, wird der neue Wert verwendet. Andernfalls wird der Wert für die Standarddomäne verwendet.

### Zugehörige Informationen

Domänentrennung verstehen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Erstellen Sie eine Betriebssystemgruppe

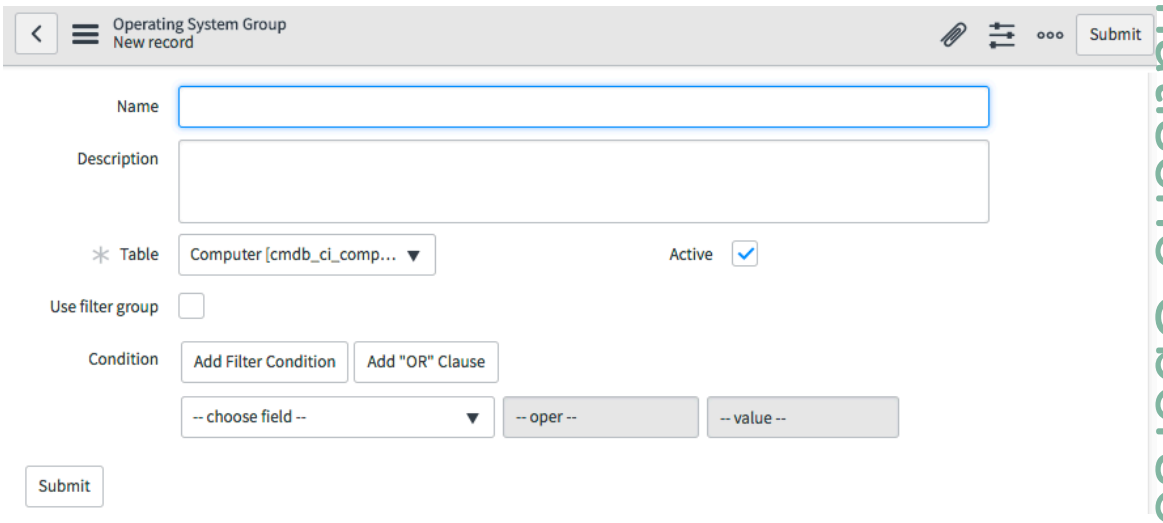
Betriebssystemgruppen werden verwendet, um ein Betriebssystem bestimmten Prozesstypen und Skripts in Security Incident Response -Workflows zuzuordnen. Die Skripts definieren, wie laufende Prozesse für die definierten Betriebssystemgruppen abgerufen werden. Neue Betriebssysteme können nach Bedarf hinzugefügt werden.

## Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Betriebssystemgruppen**.
   Das Basissystem enthält Skripts für drei Betriebssysteme:
   - BSD-basiertes Betriebssystem
   - POSIX-basiertes Betriebssystem
   - Betriebssystem Windows
2. Klicken Sie auf **Neu**.



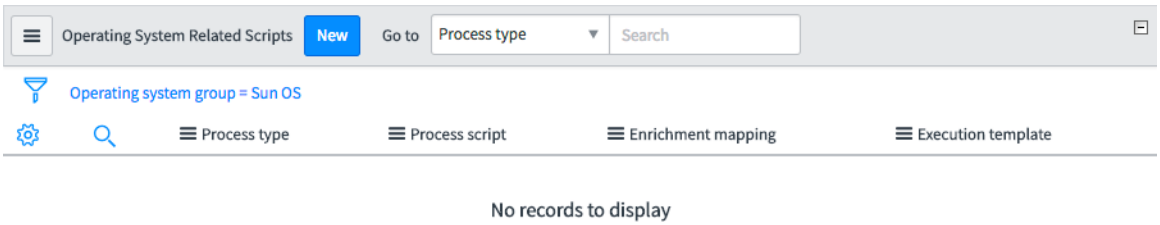

3. Füllen Sie die Felder nach Bedarf aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Betriebssystemgruppe. |
| Beschreibung | Eine Beschreibung für die Betriebssystemgruppe. |
| Tabelle | Die betroffene Tabelle. |
| Aktiv | Aktivieren Sie diese Checkbox, um die Betriebssystemgruppe zu aktivieren. |
| Filtergruppe verwenden | Aktivieren Sie diese Checkbox, um eine Filtergruppe für die Suche nach übereinstimmenden Datensätzen in der ausgewählten Tabelle zu verwenden. |
| Filtergruppe | Wählen Sie die Filtergruppe für die Suche nach übereinstimmenden Datensätzen in der ausgewählten Tabelle aus. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert haben. |
| Bedingung | Die zugehörigen Listen namens Bedingungsgeneratorfelder werden nur angezeigt, wenn Sie das Kontrollkästchen **Filtergruppe verwenden** nicht aktiviert haben. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.
   Die zugehörige Liste Betriebssystem Zugehörige Skripts wird geöffnet.




5. Klicken Sie auf **Neu**.
6. Wählen Sie Skripts aus, die den Workflows entsprechen, die Sie verwenden, um laufende Prozesse, Services und/oder Netzwerkstatistiken abzurufen.
7. Klicken Sie auf **Absenden**.

### Zugehörige Informationen

Hängen Sie eine Skriptdatei an einen mit der Datei synchronisierten MID Server an

## Sicherheits-Tag-Gruppen und -Tags einrichten

Sie können Security Incidents, Reaktionsaufgaben, angreifbaren Elemente, erkennbaren Elemente, IoCs und Sicherheitsfälle Tags zuweisen, um Metadaten für den antwortenden Datensatz zu erstellen und zu definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll. Die Tags können Sicherheitsgruppen hinzugefügt werden, um sie zu organisieren.

### Vorbereitungen

Erforderliche Rolle: sn_si.admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Gruppen**.
   Im Basissystem sind drei Standardklassifizierungsgruppen enthalten.
   - Ergänzungs-**Allow-Liste/Deny-Liste**: Diese Gruppe definiert, ob ein Datensatz als Allow-Listen- oder Deny-Listen-Datensatz behandelt werden soll. Allow-Listen-Datensätze sind im Allgemeinen von geringerer Bedeutung, daher können sie ignoriert werden. Deny-Listen-Datensätze sind im Allgemeinen von höherem Interesse.
   - **Metatag**: Diese Gruppe wird als Demodaten bereitgestellt. Sie können damit benutzerdefinierte Klassifizierungs-Tags erstellen, die von Anwendungen für Sicherheitsvorgänge verwendet werden.
   - **Traffic Light-Protokoll**: Diese Gruppe wird verwendet, um sicherzustellen, dass vertrauliche Informationen für die richtige Zielgruppe freigegeben werden.
     Es verwendet vier Farben (weiß, grün, gelb und rot), um unterschiedliche Empfindlichkeitsgrade anzuzeigen. Für jede Farbe können Sie die entsprechenden Lese-/Schreibzugriffsrollen zuweisen. Bei der Freigabe von erkennbaren Elementen für einen vertrauenswürdigen Sicherheitskreis bestimmt das dem vertrauenswürdigen Sicherheitskreisprofil zugewiesene Tag, welche mit TLP gekennzeichneten erkennbaren Elemente für den Kreis freigegeben werden können:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **TLP: WEISS:** Nur erkennbare Elemente mit TLP: WEISS können für ein TLP: WEISS-Profil freigegeben werden.
- **TLP: GREEN:** Erkennbare Elemente mit TLP: GREEN und TLP: WEISS können für ein TLP: GREEN-Profil freigegeben werden.
- **TLP: AMBER:** Erkennbare Elemente mit TLP: AMBER, TLP: GREEN und TLP: WEISS können für ein TLP: AMBER-Profil freigegeben werden.
- **TLP: ROT:**Alle erkennbaren Elemente können unabhängig von ihrem TLP-Tag für ein TLP: ROT-Profil freigegeben werden, da TLP: ROT das TLP-Tag mit dem höchsten Rang ist.

**Hinweis:**
Sie können weitere TLP-Farben hinzufügen, aber alle zusätzlichen Farben werden vom Forum für Reaktion auf Incidents und Sicherheitsteams (FIRST ) als nicht gültig angesehen.

2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie den Namen der Sicherheitsgruppe ein. |
| Mehrfachauswahl zulassen | Aktivieren Sie dieses Kontrollkästchen, wenn Sie einem Datensatz, der eine Gruppe freigibt, mehrere Sicherheits-Tags zuweisen möchten. |
| Aktiv | Aktivieren oder deaktivieren Sie die Gruppe. |
| Beschreibung | Geben Sie eine Beschreibung für diese Gruppe ein. |

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
Die zugehörige Liste Sicherheits-Tags wird angezeigt.
5. Klicken Sie in der zugehörigen Liste Sicherheits-Tags auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Klassifizierungs-Tags. |
| Sicherheits-Tag-Gruppe | Wenn das Tag mithilfe der Schaltfläche **Neu** in der zugehörigen Gruppenliste erstellt wurde, wird dieses Feld standardmäßig auf die aktuelle Gruppe gesetzt. Bei Bedarf können Sie das Tag einer anderen Gruppe hinzufügen. Dies ist jedoch optional. |
| Bestellung | Geben Sie die Reihenfolge an, in der das Tag in Formularen oder innerhalb einer Liste angezeigt wird. |
| Farbe | Wählen Sie die Farbe für dieses Tag aus. |
| Eingeschränkten Zugriff erzwingen | Aktivieren Sie dieses Kontrollkästchen, um Lese- und/oder Schreibrollen zuzuweisen, die Benutzer zum Lesen oder Schreiben in Datensätzen mit diesem Sicherheits-Tag benötigen. |
| Aktiv | Aktivieren oder deaktivieren Sie das Tag. |
| Beschreibung | Eine Beschreibung dieses Tags. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Rollen (Lesezugriff) | Um einem Sicherheits-Tag Lesezugriff zuzuweisen, klicken Sie auf das Schlosssymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Schlosssymbol. Dieses Feld wird nur angezeigt, wenn Sie das **Kontrollkästchen Eingeschränkten Zugriff erzwingen aktiviert haben**. |
| Rollen (Schreibzugriff) | Um einem Sicherheits-Tag Schreibzugriff zuzuweisen, klicken Sie auf das Schlosssymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Schlosssymbol. Dieses Feld wird nur angezeigt, wenn Sie das **Kontrollkästchen Eingeschränkten Zugriff erzwingen aktiviert haben**. |

7. Wiederholen Sie diese Schritte nach Bedarf, um weitere Sicherheits-Tags zu erstellen.
8. Klicken Sie auf **Aktualisieren**.

**Hinweis:**
Sie können auch neue Tags erstellen, indem Sie zu navigieren **Security Operations** > **Sicherheits-Tags** > **Tags**. Das Verfahren ist das gleiche.

## Sicherheits-Tag-Regeln erstellen

Sicherheits-Tag-Regeln bieten Filterung für den Zugriff auf Sicherheits-Tags.

### Vorbereitungen
Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**.
2. Wählen oder erstellen Sie ein Sicherheits-Tag.
3. Klicken Sie auf der zugehörigen Registerkarte **Sicherheits-Tag-Regeln** auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Sicherheits-Tag-Regel. |
| Sicherheits-Tag | Das Sicherheits-Tag, das an die Regel angehängt werden soll. |
| Aktiv | Aktivieren oder deaktivieren Sie das Sicherheits-Tag. |
| Beschreibung | Eine Beschreibung dieser Regel. |

5. Legen **Sie die Datensatzfilterung fest.**
6. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Filtergruppe verwenden | Ordnet der Regel eine Filtergruppe zu. |
| Tabelle | Die Tabelle, die die Regel enthalten soll. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Bedingung | Fügen Sie eine oder mehrere Filterbedingungen hinzu. |

7. Klicken Sie auf **Absenden**.

## Sicherheits-Tag-Regeln importieren

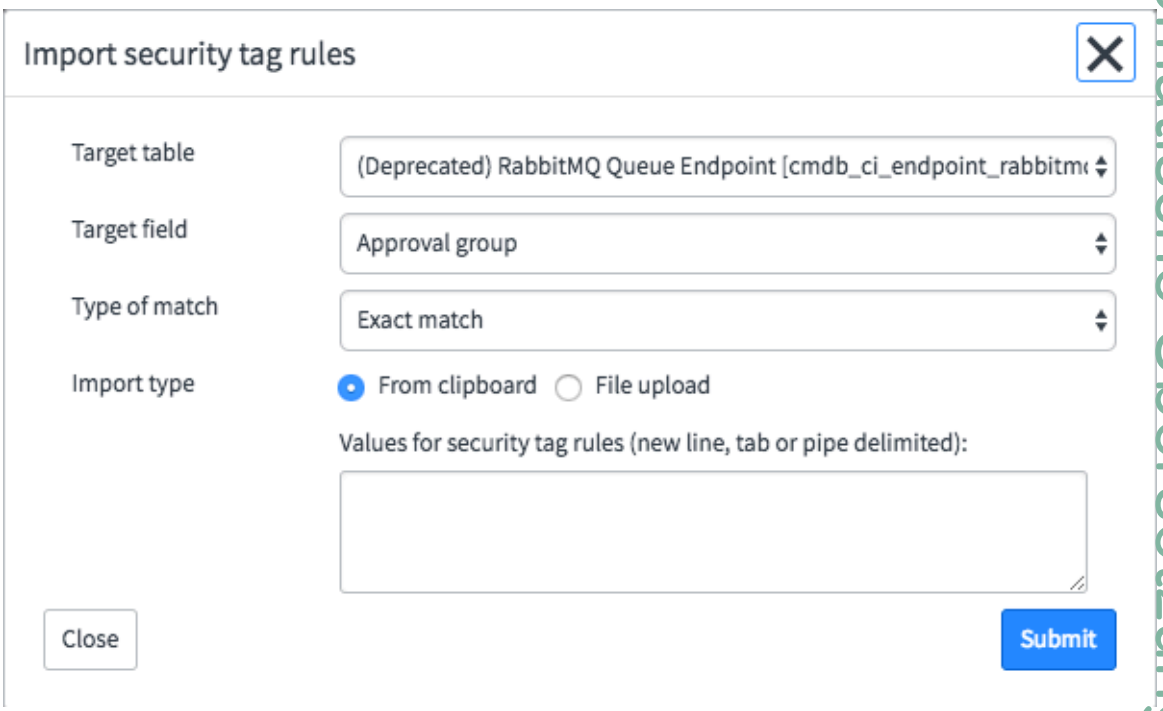
Sie können Sicherheits-Tag-Regeln aus anderen Tabellen in Ihrer Bereitstellung importieren.

### Vorbereitungen

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**.
2. Wählen oder erstellen Sie ein Sicherheits-Tag.
3. Klicken Sie auf den zugehörigen Link **Sicherheits-Tag-Regeln** importieren.




4. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Zieltabelle | Wählen Sie die Tabelle aus, die zum Importieren von Regeln verwendet werden soll. |
| Zielfeld | Wählen Sie das Feld aus, das zum Importieren von Regeln verwendet werden soll. |
| Typ der Übereinstimmung | Wählen Sie aus, wie die importierten Regeln mit **Sicherheits-Tags abgeglichen** werden sollen:<br>Genaue Übereinstimmung (Standard)<br>Enthält |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Beginnt mit<br>Endet mit<br>Regulärer Ausdruck |
| Importtyp | Wählen Sie:<br>**Aus Zwischenablage**<br>Kopieren Sie eine Liste der durch Trennzeichen getrennten Werte in den Textbereich. Die Werte werden in Sicherheits-Tags analysiert.<br>**Aus Datei-Upload**<br>Laden Sie eine Datei mit getrennten Werten hoch. Die Werte werden in Sicherheits-Tags analysiert.<br>Fügen Sie Werte für die Sicherheits-Tag-Regeln mithilfe von neuen Zeilen oder Pipeline-Begrenzern hinzu. |

5. Klicken Sie auf **Absenden**.

## Sicherheitsanmerkungen

Eine Sicherheitsanmerkung ist eine Erklärung oder Anmerkung, die einem Konfigurationselement, einem erkennbaren Element oder einer Verwendung für einen Security Incident hinzugefügt wird.

Mehrere Sicherheitsanmerkungen sind für Benutzer und erkennbare Elemente verfügbar (erfordert das Threat Intelligence -Plugin). Berichte zu Sicherheitsanmerkungen sind ebenfalls verfügbar.

### Erstellen Sie Sicherheitsanmerkungen für CIs

Mit Anmerkungen zu CIs können Sie Aktivitäten in Incidents nachverfolgen. Sie können einem einzelnen oder mehreren CIs Anmerkungen hinzufügen.

#### Vorbereitungen

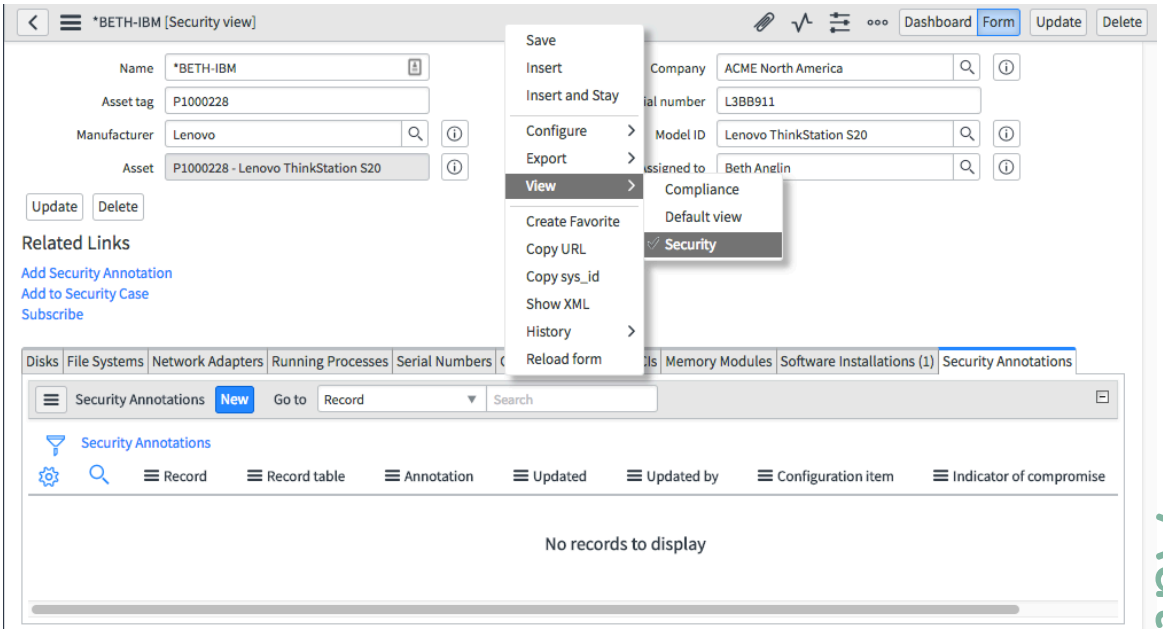
Erforderliche Rolle: admin

#### Prozedur

1. Öffnen Sie ein CI aus einem Security Incident oder der Tabelle „Configuration Item“.
2. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Ansicht** > **Sicherheit**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Klicken Sie auf der Registerkarte **„Sicherheitsanmerkungen“** auf **Neu**.
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Sie können dieselbe Anmerkung mehreren CIs hinzufügen, indem Sie CIs in der Liste auswählen, **Sicherheitsanmerkung**hinzufügen wählen, eine Anmerkung in einem beliebigen Textformat eingeben und auf **Absenden**klicken.

## Erstellen Sie Sicherheitsanmerkungen für erkennbare Elemente

Sie können ein einzelnes oder mehrere erkennbare Elemente auswählen und Sicherheitsanmerkungen auf sie anwenden, indem Sie das Auswahlmenü **Aktionen für ausgewählte Zeilen** verwenden.

### Vorbereitungen

- Erfordert das Plugin Threat Intelligence und die Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

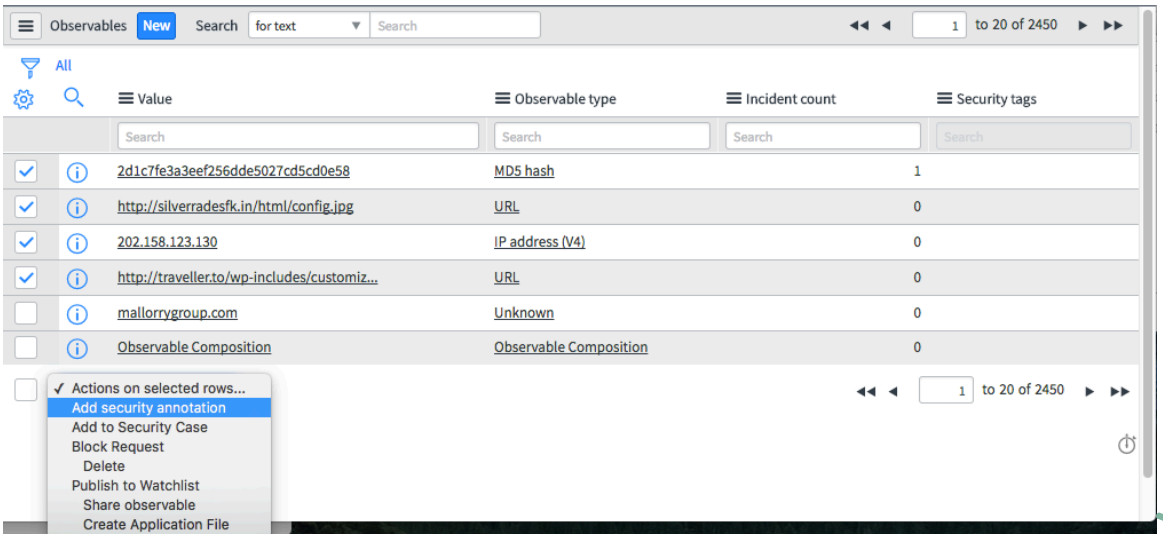
Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Erkennbare Elemente**
2. Wählen Sie ein oder mehrere erkennbare Elemente in der Liste aus.
3. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen** die **Option Sicherheitsanmerkung hinzufügen**aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

## Erstellen Sie Sicherheitsanmerkungen für Benutzer

Sie können einen einzelnen oder mehrere Benutzer auswählen und Sicherheitsanmerkungen auf sie anwenden, indem Sie das Auswahlmenü **Aktionen für ausgewählte Zeilen** verwenden.

### Vorbereitungen

Erfordert das Plugin Threat Intelligence und die Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

Erforderliche Rolle: admin

### Prozedur

1. Navigieren zu **Alle** > **Benutzeradministration** > **Anwender**
2. Wählen Sie einen oder mehrere Benutzer in der Liste aus.
3. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen** die **Option Sicherheitsanmerkung hinzufügen**aus.
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

## Zeigen Sie Berichte mit Sicherheitsanmerkungen an

Der Bericht „Sicherheitsanmerkungen“ enthält Details, die in der Tabelle „Sicherheitsanmerkungen“ [sn_sec_cmn_security_annotations] gespeichert sind. Sie können die Spalten im Bericht anpassen und die Daten nach Ihren Wünschen gruppieren.

### Vorbereitungen

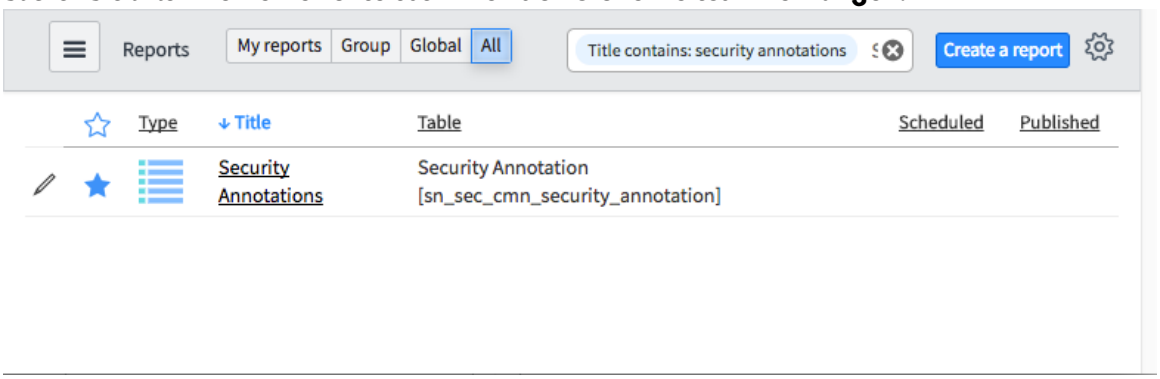
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Anzeigen/Ausführen**.
2. Suchen Sie unter **Meine Berichte** oder **Alle nach Sicherheitsanmerkungen.**




**Zugehörige Informationen**

Liste „Berichte“ anzeigen

## Mit Security Support Common installierte Komponenten

Mit Security Support Common werden verschiedene Arten von Komponenten installiert. Sie bieten allgemeine Funktionen zur Verwendung in den verschiedenen Sicherheitsanwendungen, z. B. Security Incident Response.

### Installierte Komponenten suchen und anzeigen

Weitere Informationen zum Suchen und Anzeigen installierter Komponenten finden Sie unter Zeigen Sie mit installierte Komponenten an Security Support Common.

### Zeigen Sie mit installierte Komponenten an Security Support Common

Wenn Sie das Plugin Security Support Common aktivieren, werden verschiedene Arten von Komponenten installiert, darunter Tabellen, Benutzerrollen und Module.

### Komponenten werden gesucht

**Hinweis:**
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Wenn Sie die Liste der installierten Komponenten auf Rollen, regelmäßige Aufgaben und Tabellen für die Anwendung Security Support Common beschränken möchten, führen Sie die folgenden Schritte aus:

### Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Anwendungsdateien-Tabelle, sodass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, muss so installiert sein, dass ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Befolgen Sie diese Schritte, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Geben Sie im **Filternavigator sys_metadata.list** ein, um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) und dann **Anwendung** > **ist** gefolgt vom Namen Ihrer Anwendung.
3. Um im Bedingungsgenerator einen zweiten Filter hinzuzufügen, klicken Sie auf **UND**und wählen Sie Folgendes aus: **Klasse** > **ist ein** und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle**, **Geplante Aufgabe**oder **Tabelle**.
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Security Operations-Anwendungen

Zeigen Sie für jede Anwendung die Menüelemente an, auf die eine bestimmte Rolle zugreifen kann.

[End]
[store-future: BEGIN review]

### Modulzugriff nach Rolle für Configuration Compliance

Informationen zu Configuration Compliance finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

### Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Übersicht | ✗ | ✓ | ✗ | ✗ |
| Richtlinien | ✗ | ✓ | ✗ | ✗ |
| Tests | ✗ | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

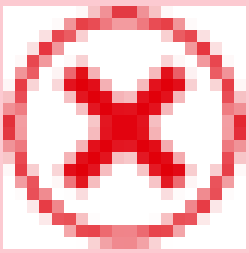
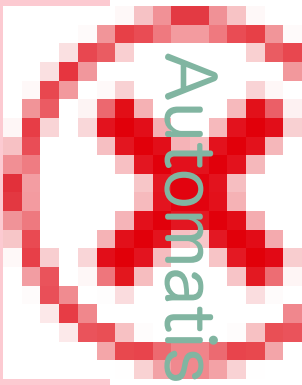
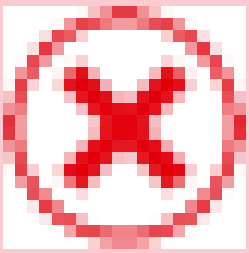
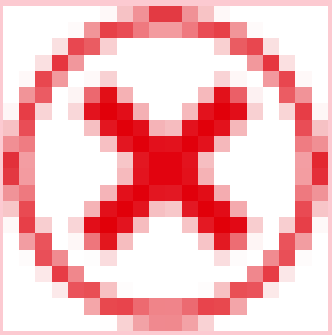
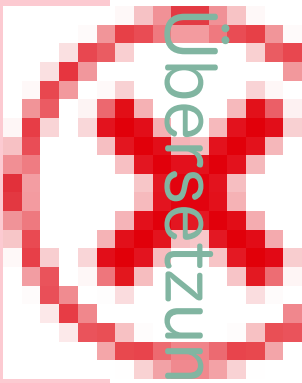
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Meine Freigaben |  | | |  |
| Testergebnisse | | | | |
| Nicht selektierte Testergebnisse |  | |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Meine offenen Testergebnisse | ✗ | ✓ | ✗ | ✗ |
| Offene Testergebnisse | ✗ | ✓ | ✗ | ✗ |
| Ziel rückt näher | ✗ | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

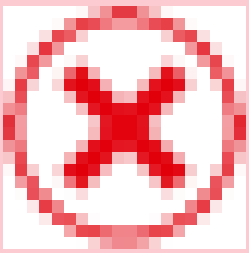
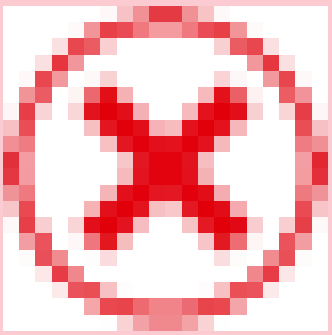
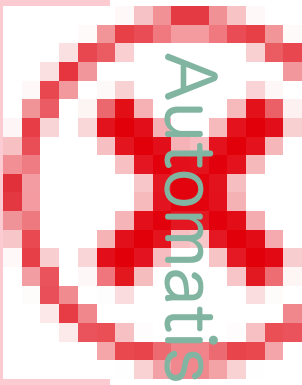
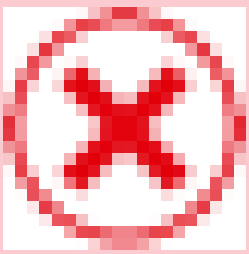
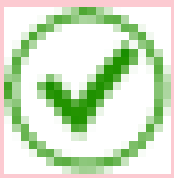
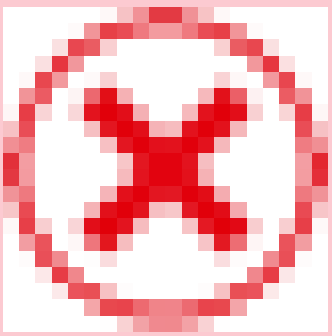
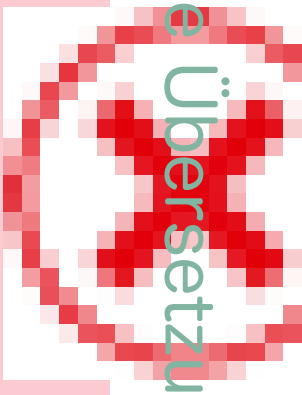
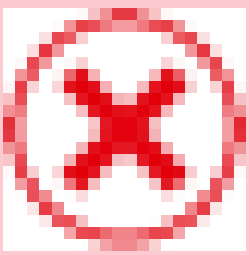
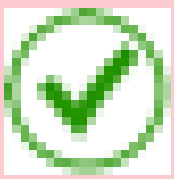
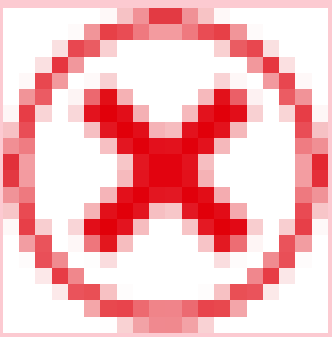
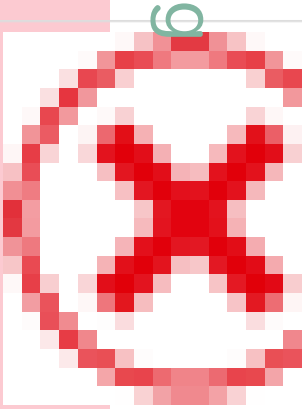
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Verfehltes Ziel |  | |  |  |
| Nicht zugewiesen |  |  |  |  |
| Mehrere Zurückstellungen |  |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

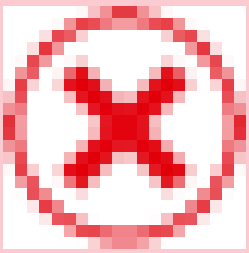
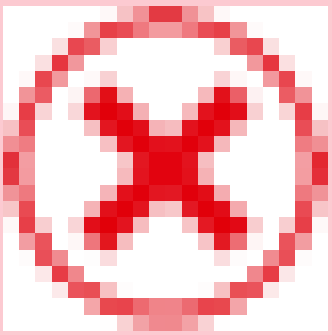
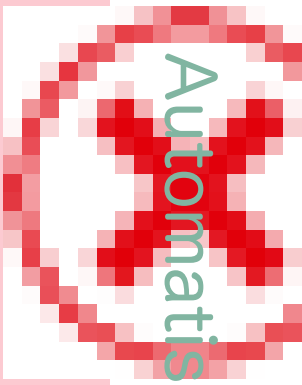
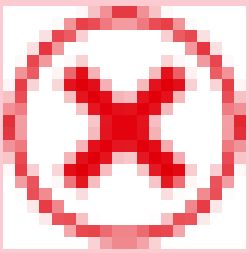
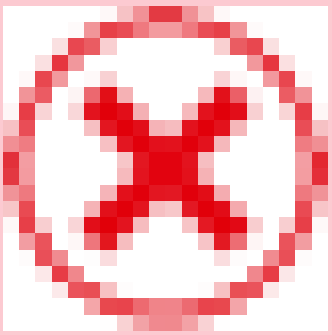
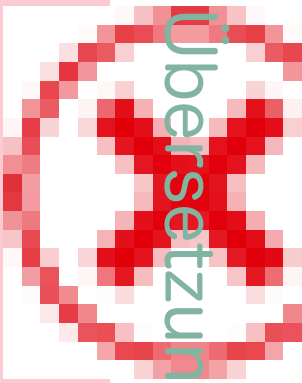
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Alle |  | |  |  |
| Testergebnisgruppen | | | | |
| Meine offenen Gruppen |  | |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

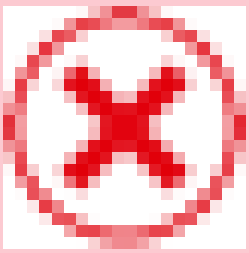
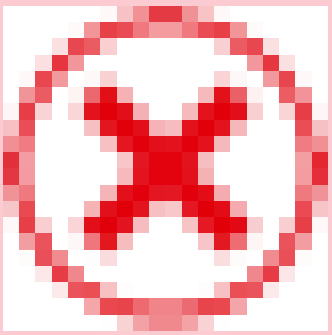
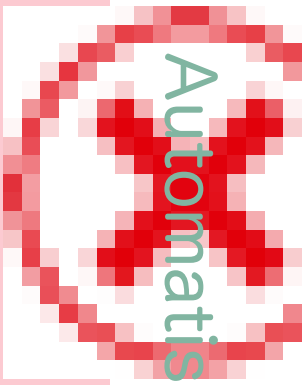
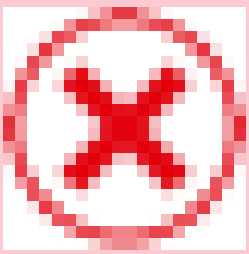
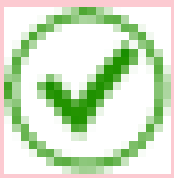
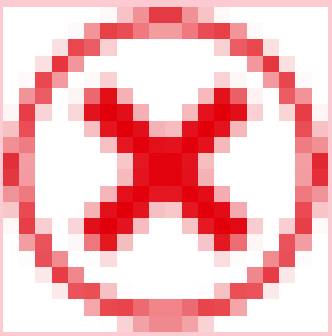
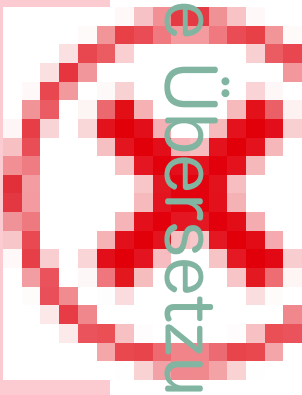
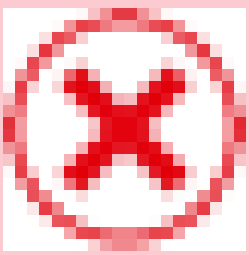
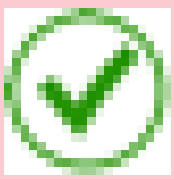
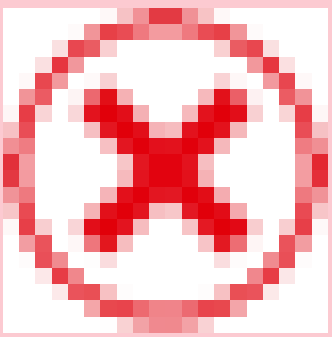
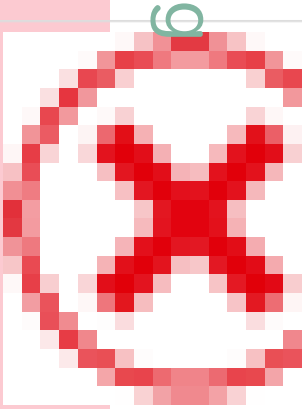
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Alle offenen Gruppen |  | |  |  |
| Mehrere Zurückstellungen |  |  |  |  |
| Alle Gruppen |  |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

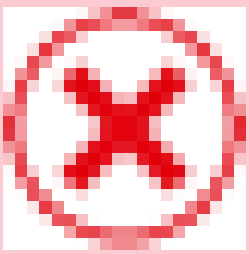
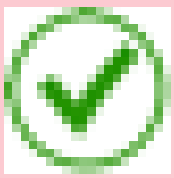
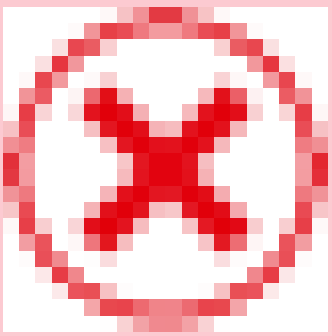
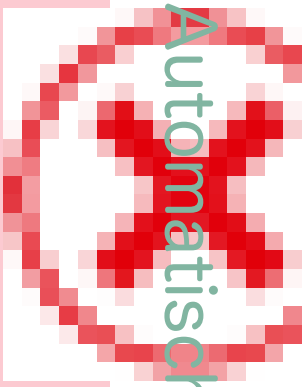
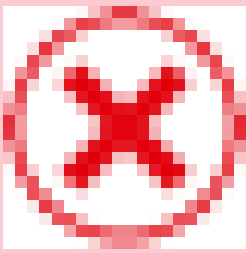
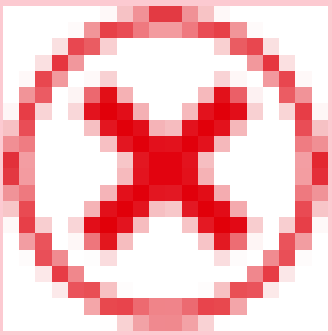
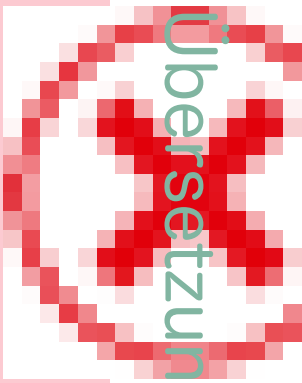
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Unterstützungsdaten | | | | |
| Autoritative Quellen |  |  |  |  |
| Technologien |  | |  |  |
| Administration | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

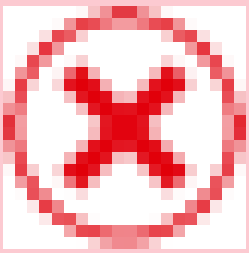
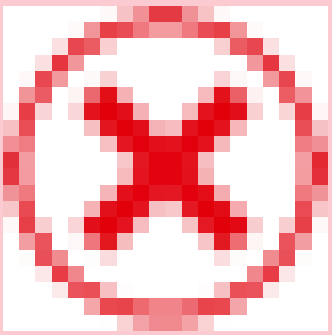
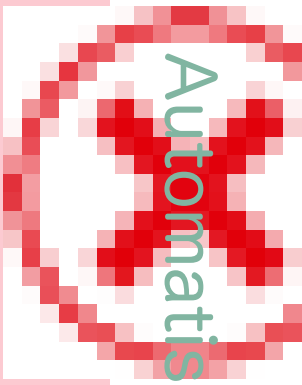
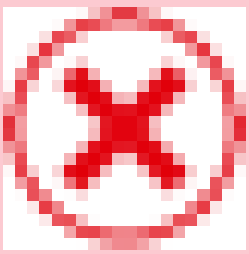
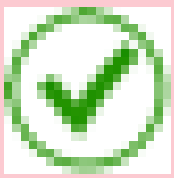
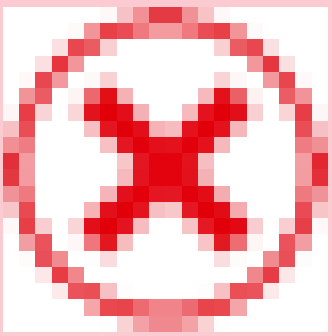
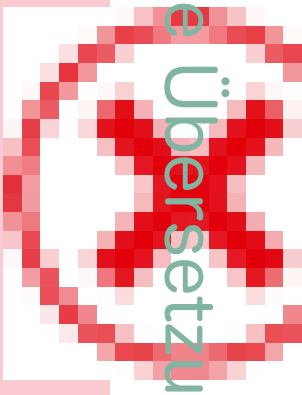
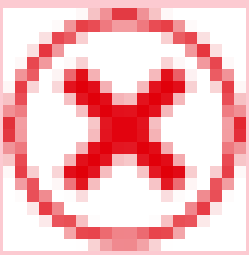
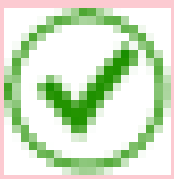
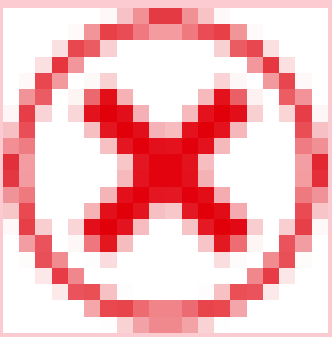
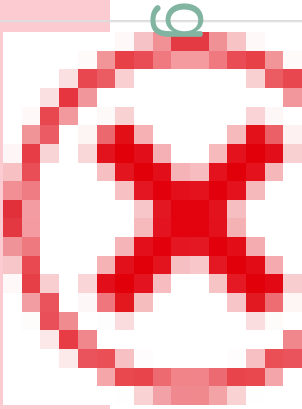
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Zuweisungsregeln |  | |  |  |
| Veraltete Testergebnisse automatisch schließen |  |  |  |  |
| Gruppenregeln |  |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Automatische Ausnahmeregel | ✗ | ✓ | ✗ | ✗ |
| Genehmigungsregeln | ✗ | ✓ | ✗ | ✓ |
| Risikorechner | ✗ | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Rollup-Rechner für Risikopunktzahl | ✗ | ✓ | ✗ | ✗ |
| Nachbesserungszielregeln | ✗ | ✓ | ✗ | ✗ |
| Relevanz-Zuordnung | ✓ | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

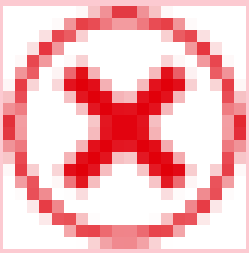
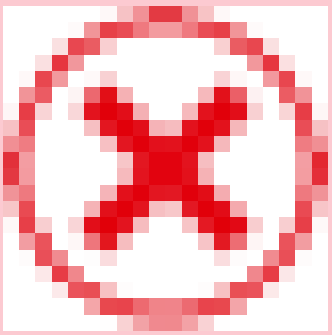
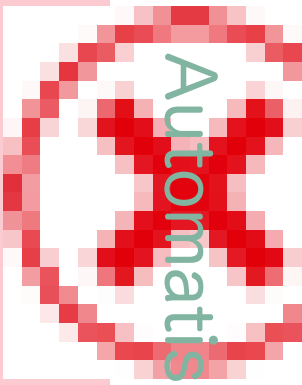
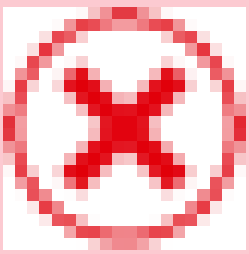
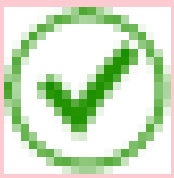
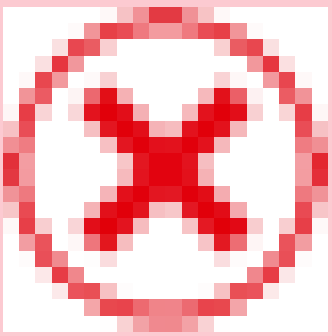
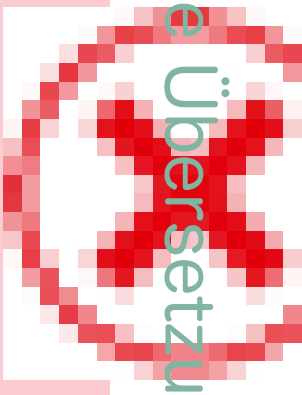
**Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vul_qualys.admin | sn_vulc.admin | sn_vulc.exception_approver | sn_vulc.manage_approval |
|---|---|---|---|---|
| Benachrichtigungen |  | |  |  |
| Ausnahmenverwaltung |  |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

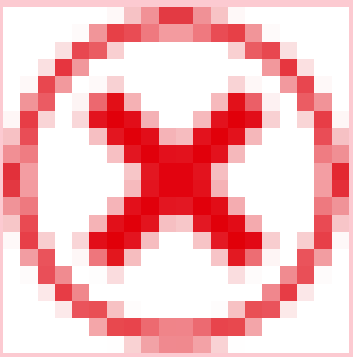
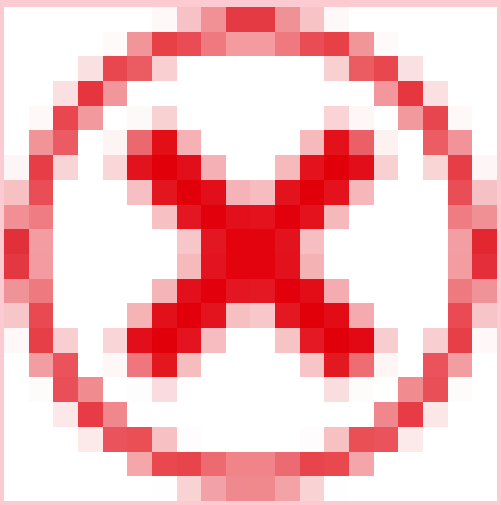
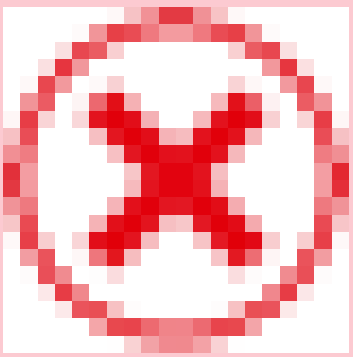
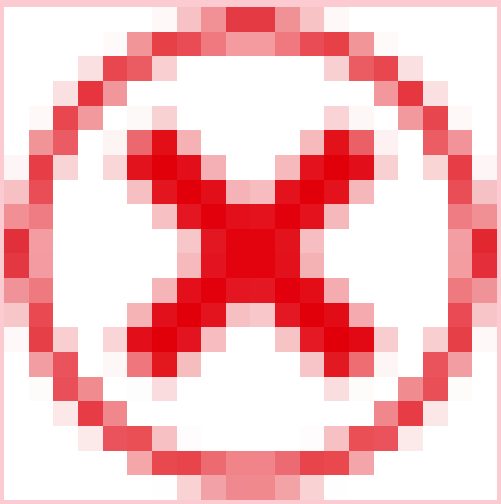
## Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.remediation_owner*

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |
| Übersicht |  |  | | |
| Richtlinien |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

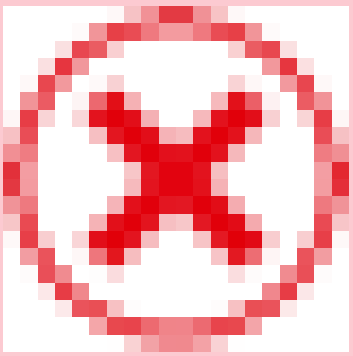
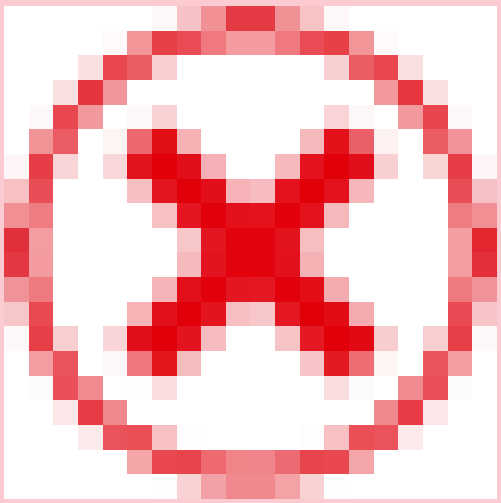
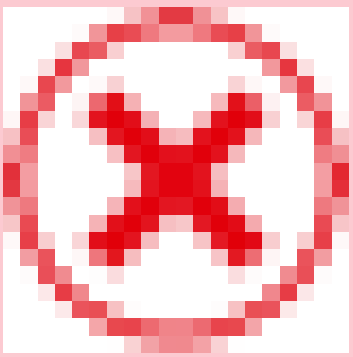
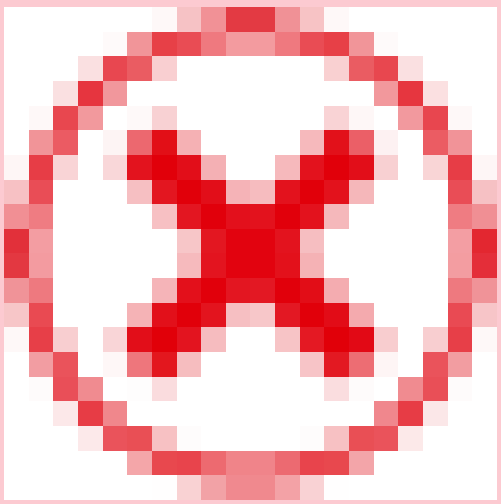
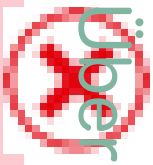
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Tests |  |  | | |
| Meine Freigaben |  |  |  | |
| Testergebnisse | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

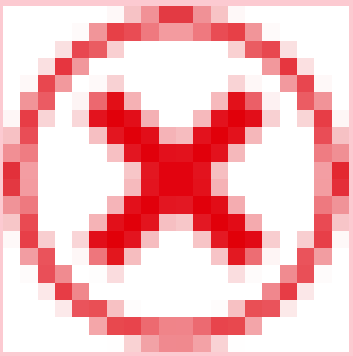
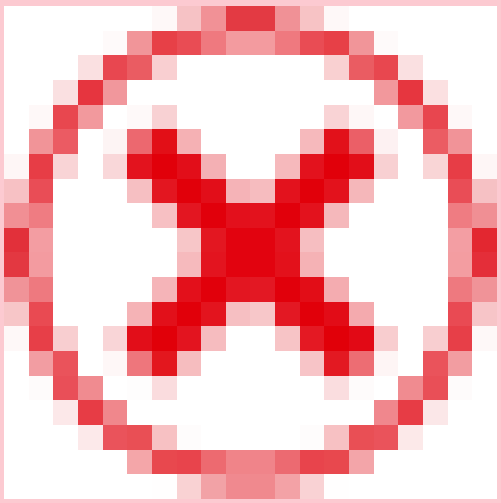
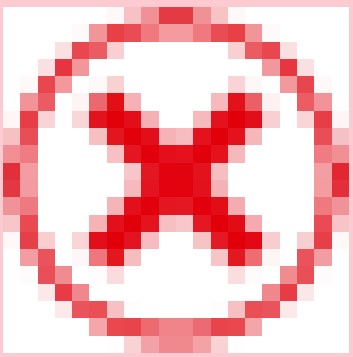
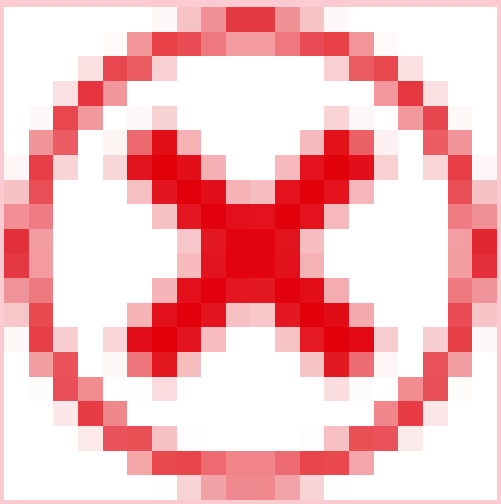
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Nicht selektierte Testergebnisse |  |  | | |
| Meine offenen Testergebnisse |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

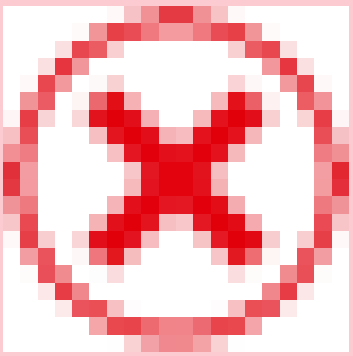
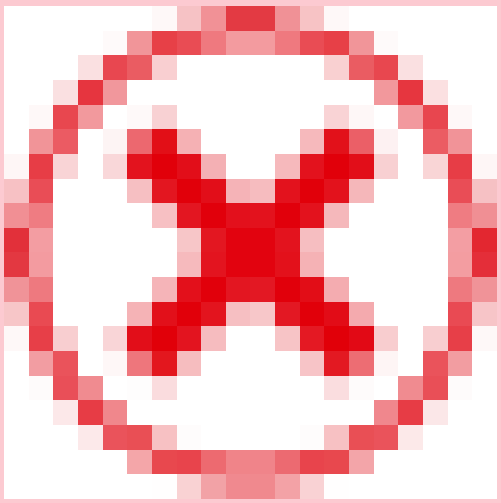
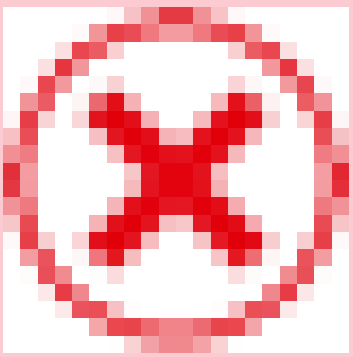
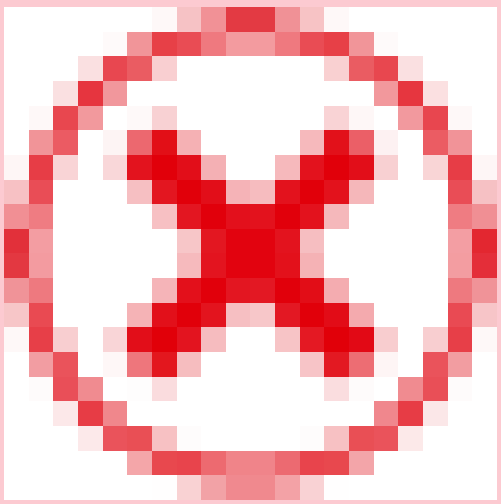
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Offene Testergebnisse |  |  | | |
| Ziel rückt näher |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

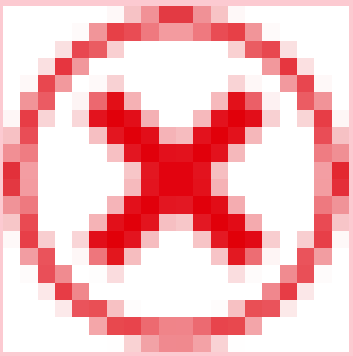
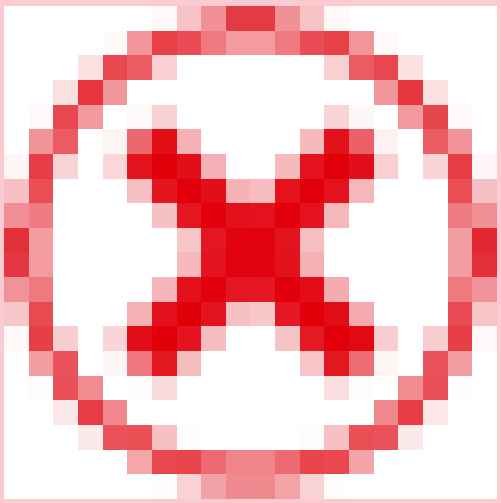
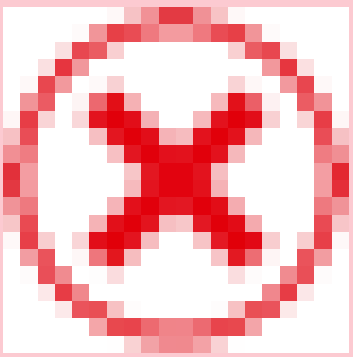
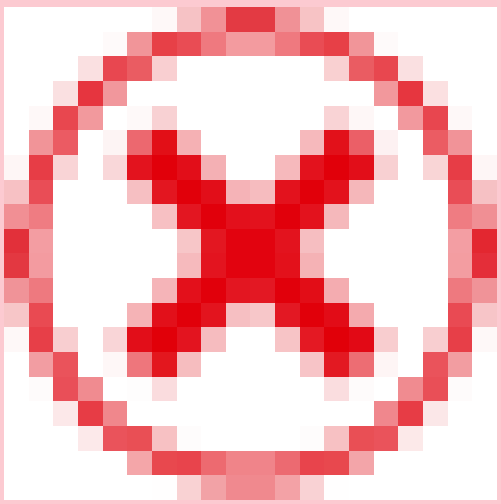
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Verfehltes Ziel |  |  | | |
| Nicht zugewiesen |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Mehrere Zurückstellungen | ✗ | ✗ | ✓ | |
| Alle | ✗ | ✗ | ✓ | |
| Testergebnisgruppen | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

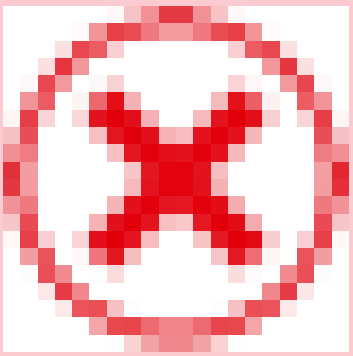
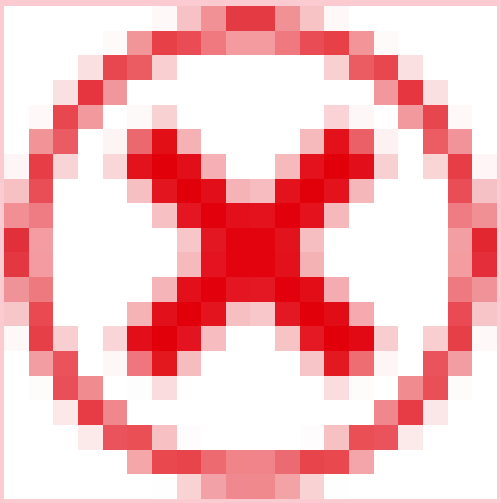
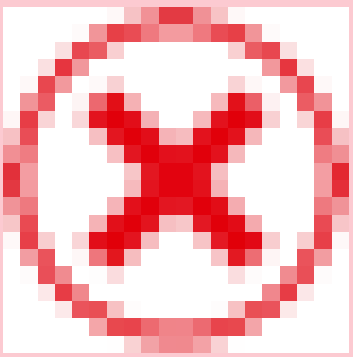
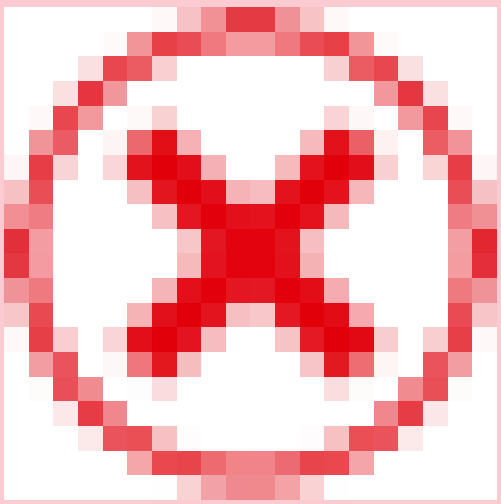
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Meine offenen Gruppen |  |  | | |
| Alle offenen Gruppen |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Mehrere Zurückstellungen | ✗ | ✗ | ✓ | |
| Alle Gruppen | ✗ | ✗ | ✓ | |
| Unterstützungsdaten | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Autoritative Quellen | ✗ | ✗ | ✓ | |
| Technologien | ✗ | ✗ | ✓ | |
| Administration | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

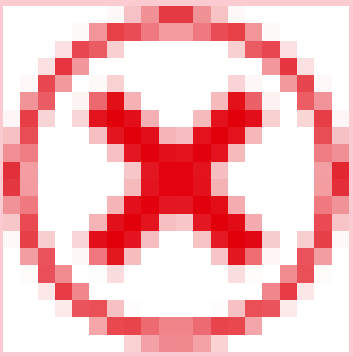
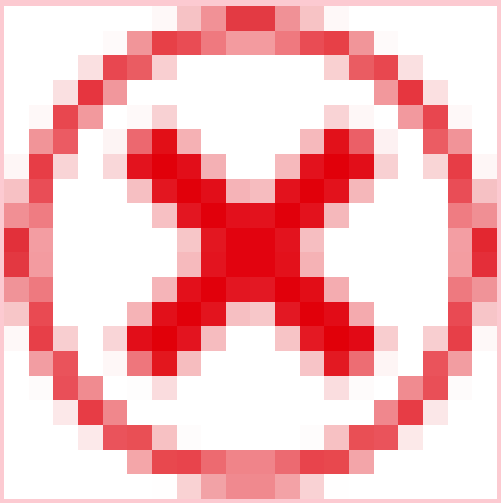
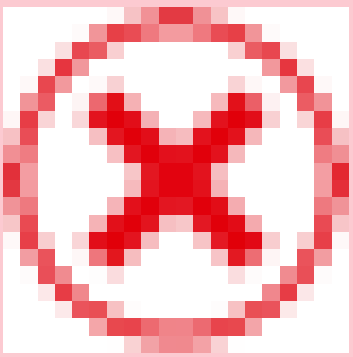
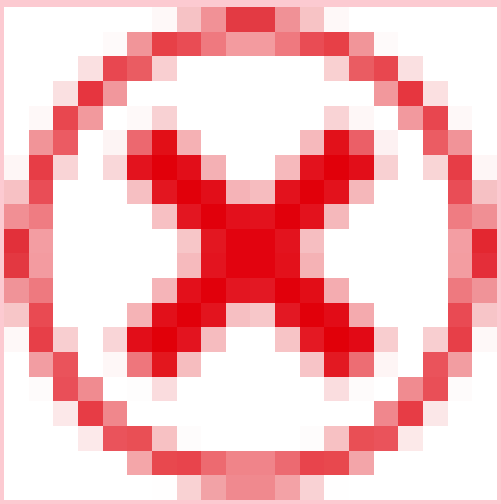
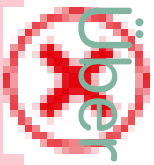
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Zuweisungsregeln |  |  | | |
| Veraltete Testergebnisse automatisch schließen |  |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

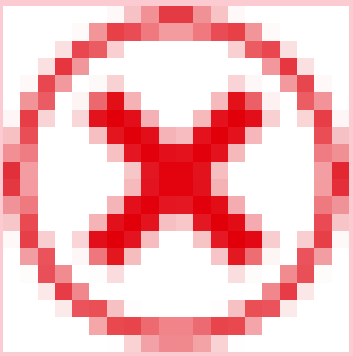
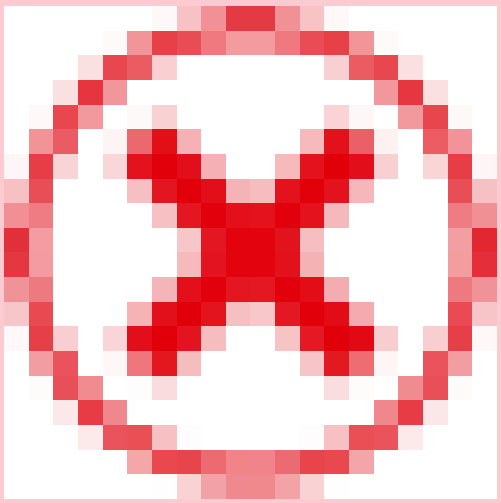
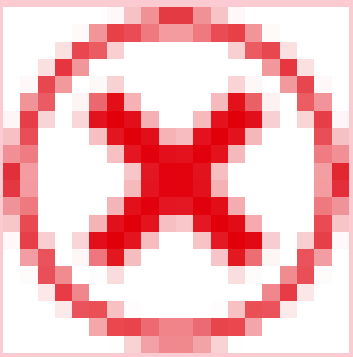
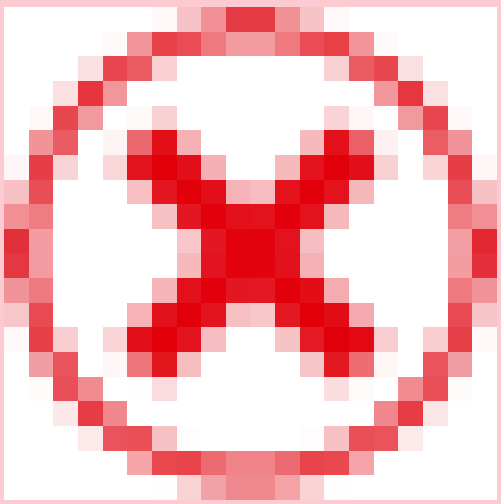
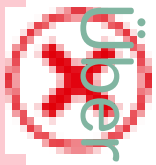
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Gruppenregeln |  |  | | |
| Automatische Ausnahmeregel |  |  |  | |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

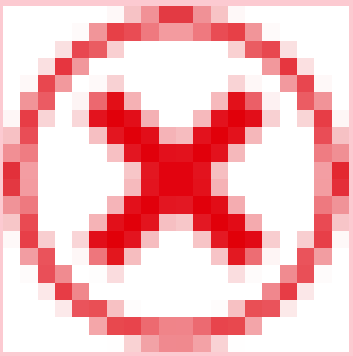
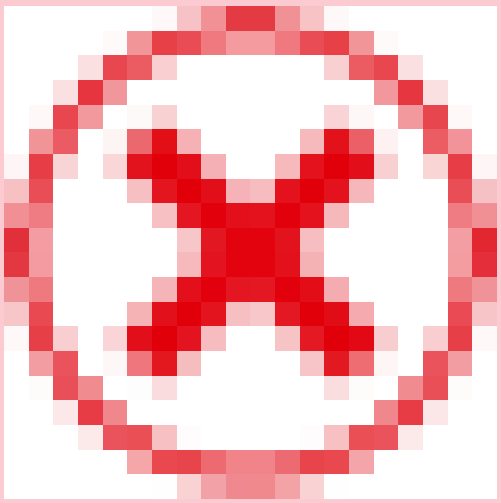
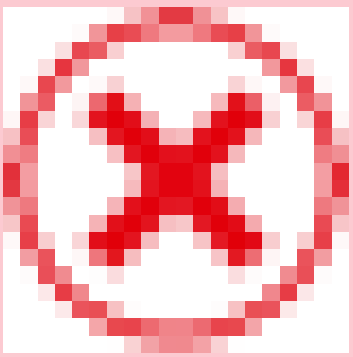
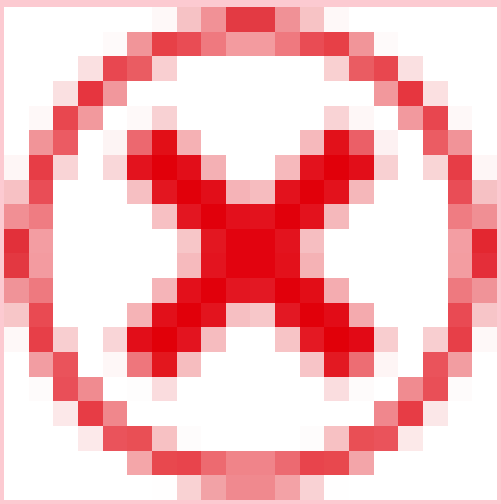
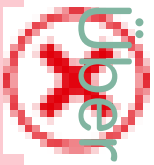
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Genehmigungsregeln |  |  | | |
| Risikorechner |  |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

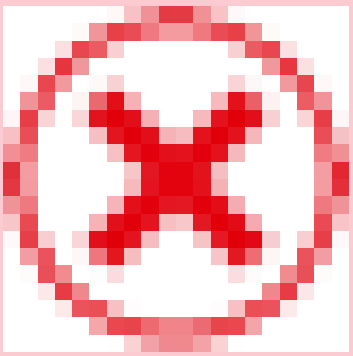
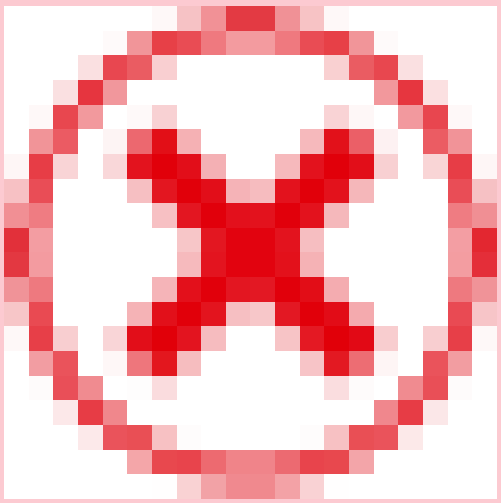
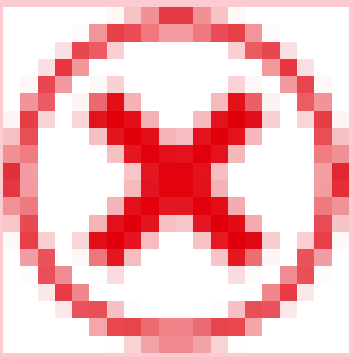
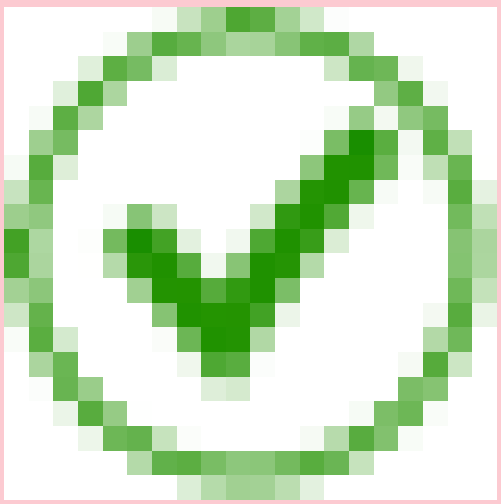
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Rollup-Rechner für Risikopunktzahl |  |  | | |
| Nachbesserungszielregeln |  |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

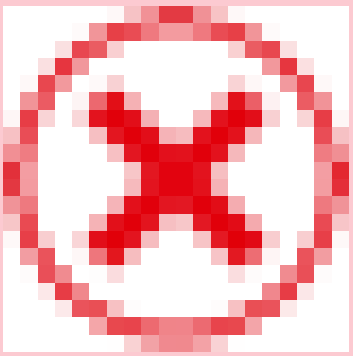
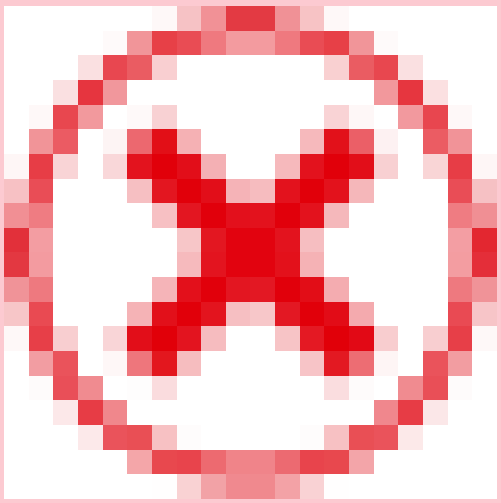
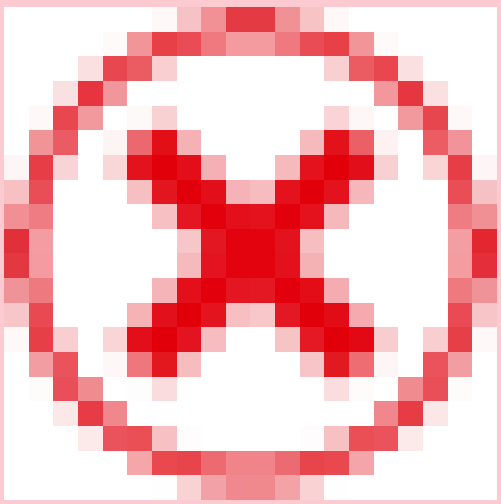
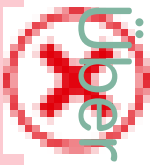
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Relevanz-Zuordnung |  |  | | |
| Benachrichtigungen | |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

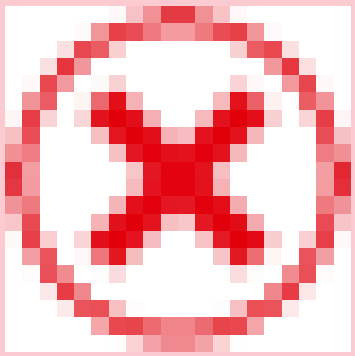
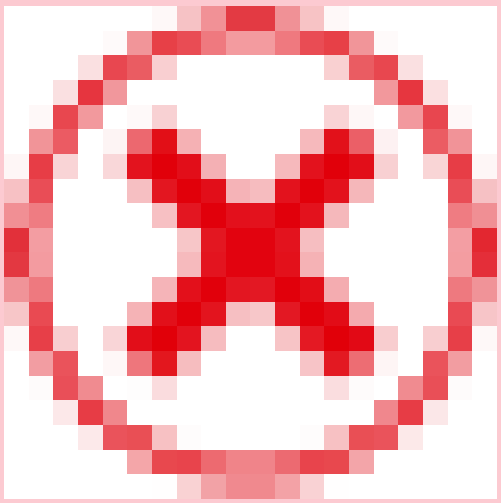
**Modulzugriff für: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.remediation_owner***

**(Fortsetzung)**

| Modul | sn_vulc.manage_notifications | sn_vulc.manage_remediation_target_rules | sn_vulc.read | sn_v |
|---|---|---|---|---|
| Ausnahmenverwaltung |  |  | | |

Automatische Übersetzung

## Modulzugriff für: sn_vulc.remediation_owner

**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

| Modul | sn_vulc.remediation_owner |
|---|---|
| (Haupt-App-Gruppe) | |

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

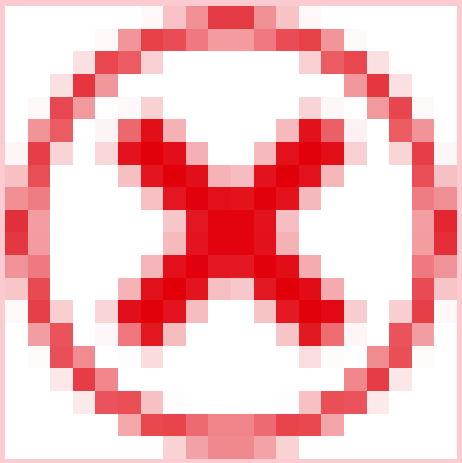
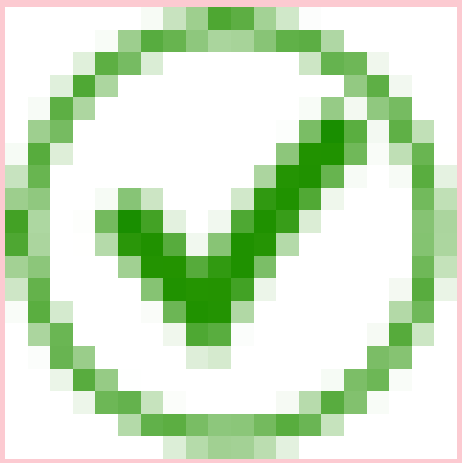
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Übersicht |  |
| Richtlinien |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

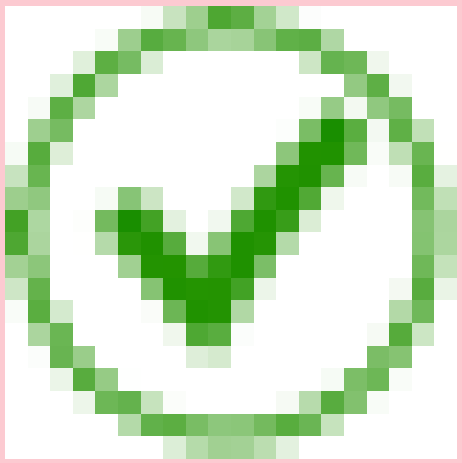
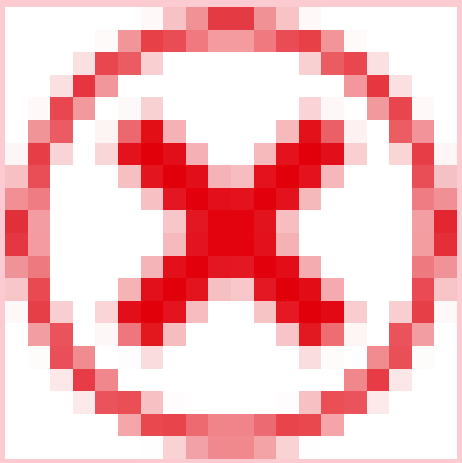
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Tests |  |
| Meine Freigaben |  |
| Testergebnisse | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

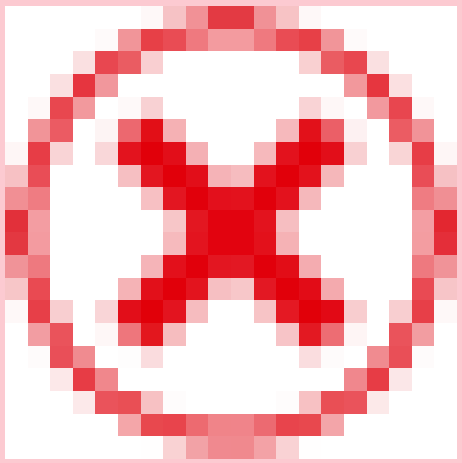
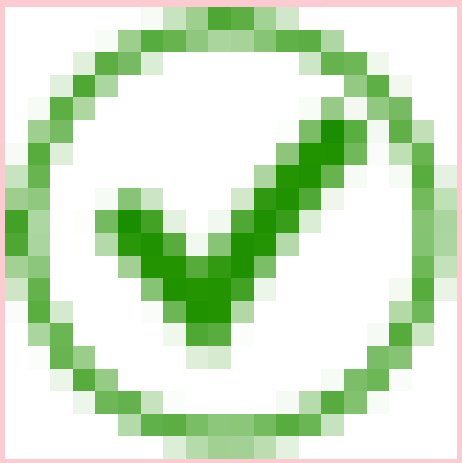
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Nicht selektierte Testergebnisse |  |
| Meine offenen Testergebnisse |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Offene Testergebnisse | ✗ |
| Ziel rückt näher | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Verfehltes Ziel | ✗ |
| Nicht zugewiesen | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

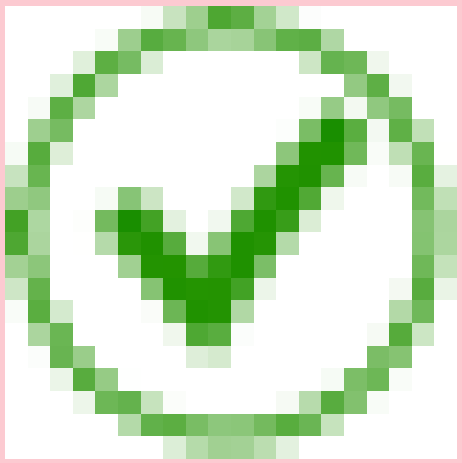
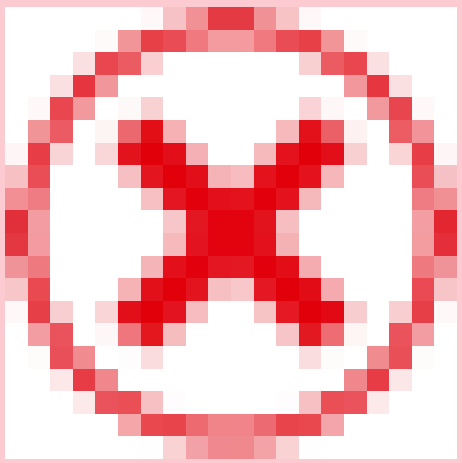
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Mehrere Zurückstellungen |  |
| Alle |  |
| Testergebnisgruppen | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

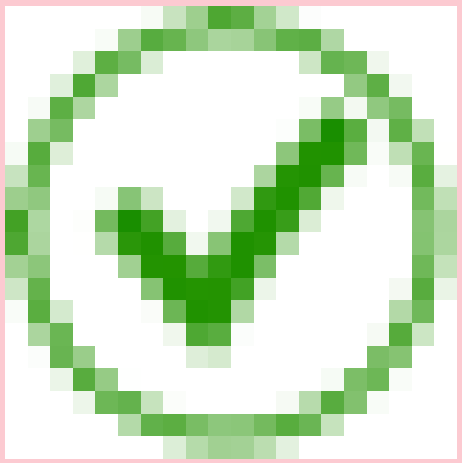
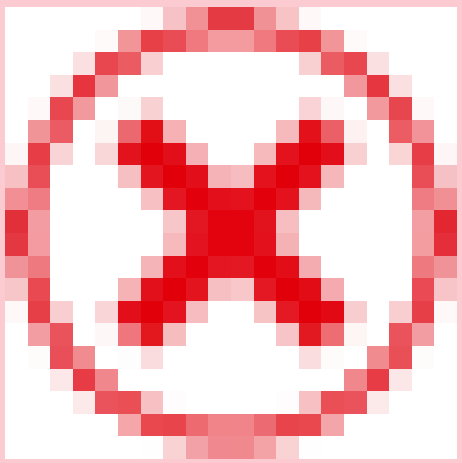
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Meine offenen Gruppen |  |
| Alle offenen Gruppen |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

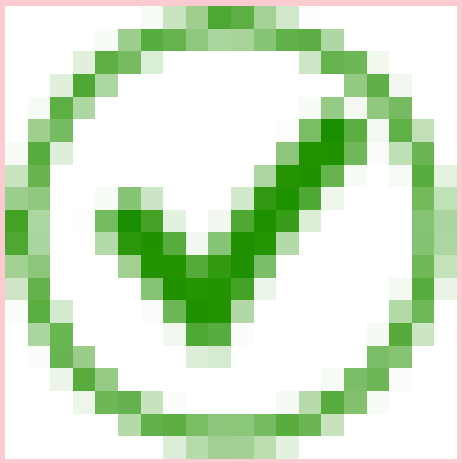
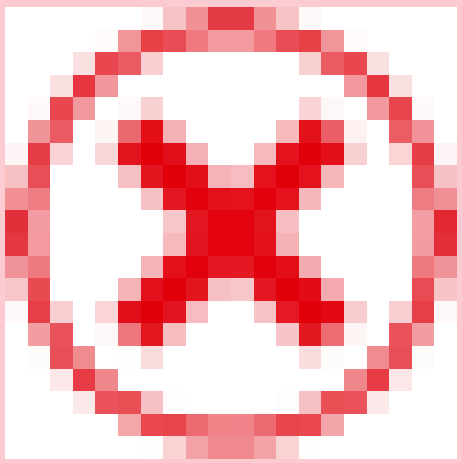
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Mehrere Zurückstellungen |  |
| Alle Gruppen |  |
| Unterstützungsdaten | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

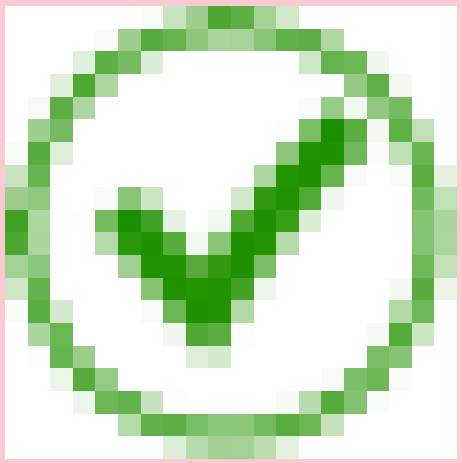
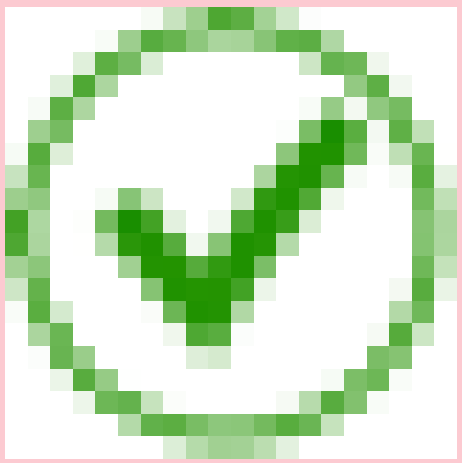
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Autoritative Quellen |  |
| Technologien |  |
| Administration | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

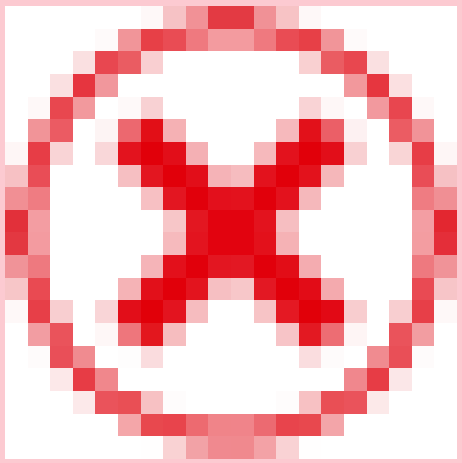
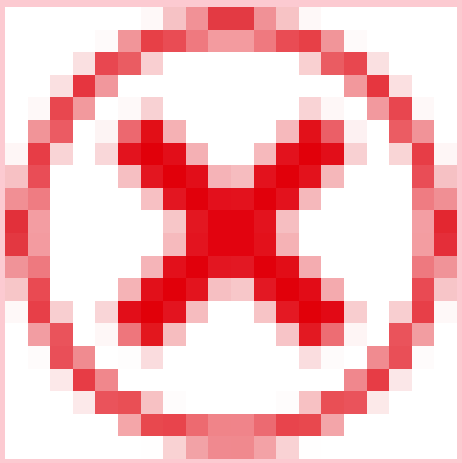
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Zuweisungsregeln |  |
| Veraltete Testergebnisse automatisch schließen |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

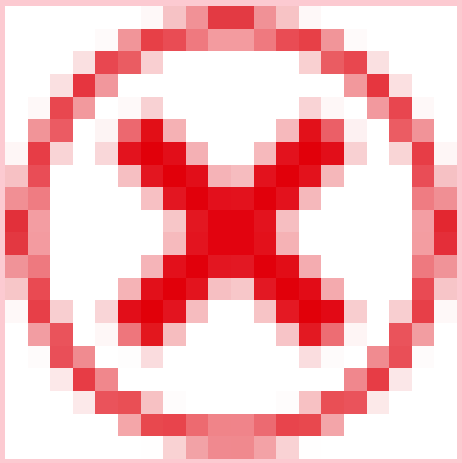
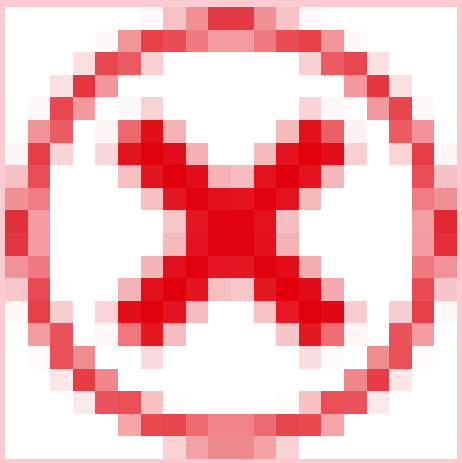
**Modulzugriff für: sn_vulc.remediation_owner**

***Informationen für andere Rollen:***

***sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule***

***sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules***

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Gruppenregeln |  |
| Automatische Ausnahmeregel |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

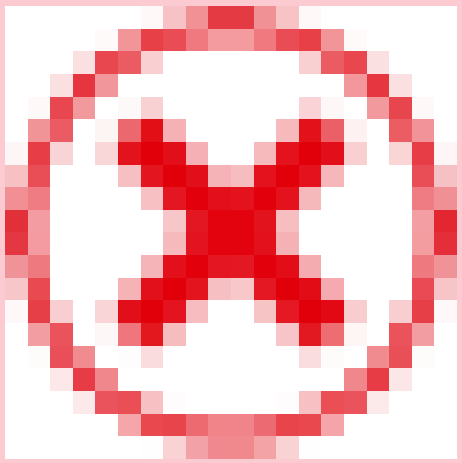
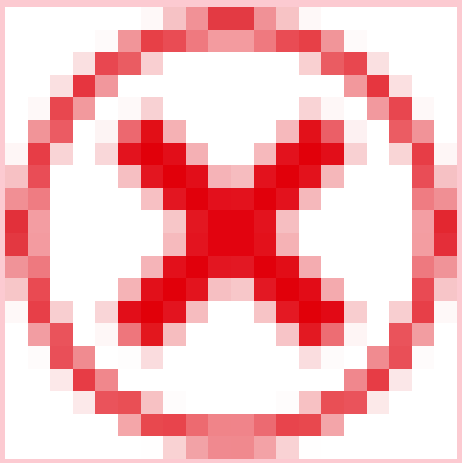
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Genehmigungsregeln |  |
| Risikorechner |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

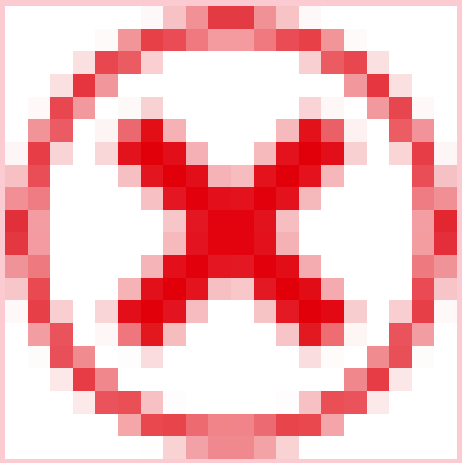
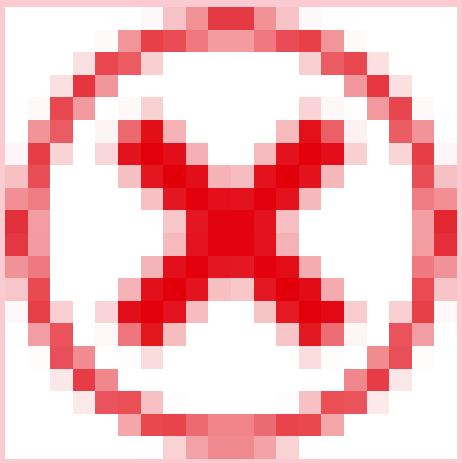
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Rollup-Rechner für Risikopunktzahl |  |
| Nachbesserungszielregeln |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

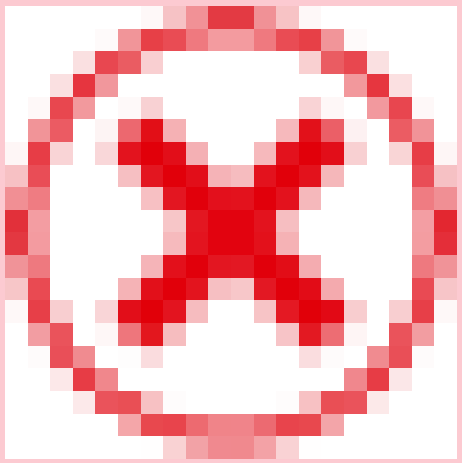
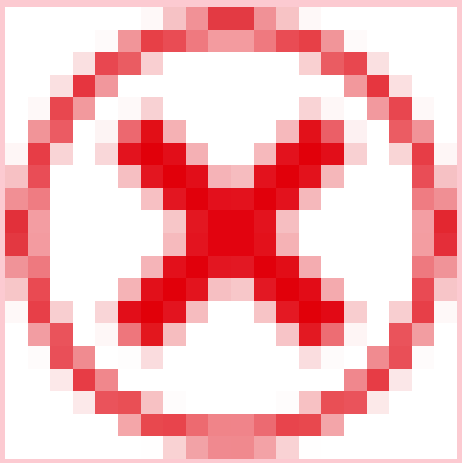
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
|---|---|
| Relevanz-Zuordnung |  |
| Benachrichtigungen |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

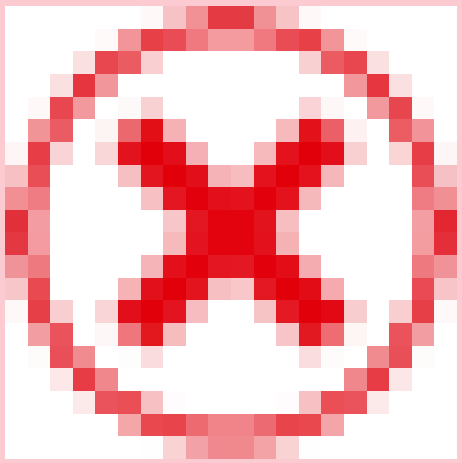
**Modulzugriff für: sn_vulc.remediation_owner**

*Informationen für andere Rollen:*

*sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule*

*sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules*

**(Fortsetzung)**

| Modul | sn_vulc.remediation_owner |
| --- | --- |
| Ausnahmenverwaltung |  |

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Container Vulnerability Response

Informationen zu Container Vulnerability Response finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

### Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

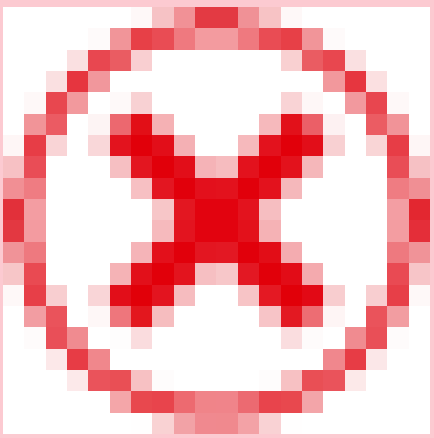
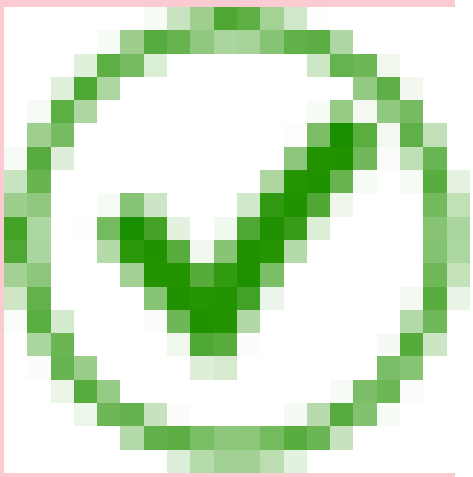
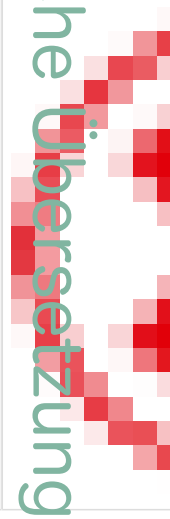
*Informationen für andere Rollen:*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| Übersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

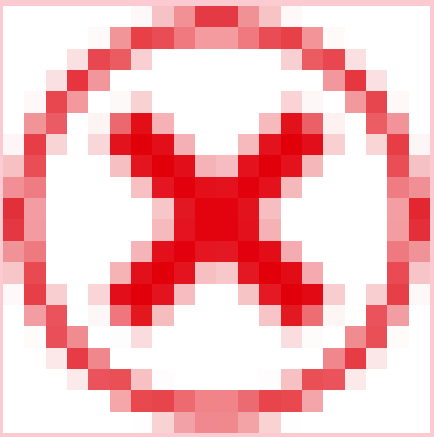
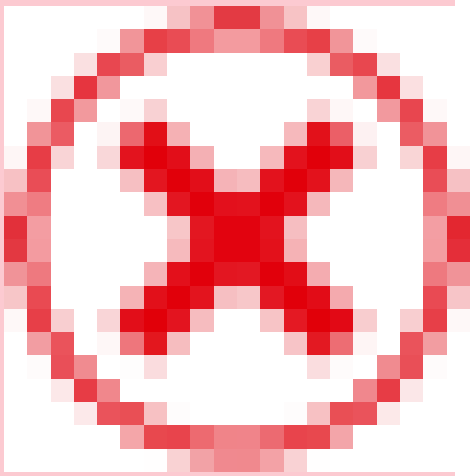
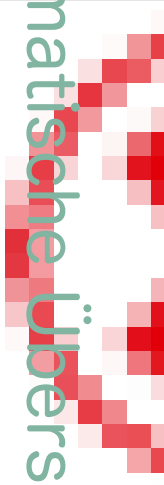
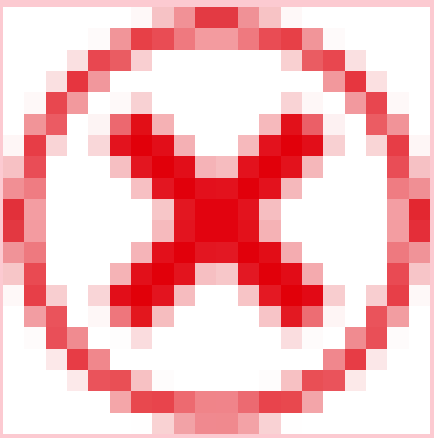
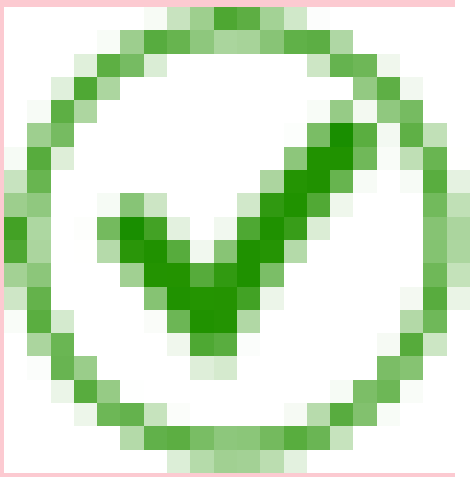
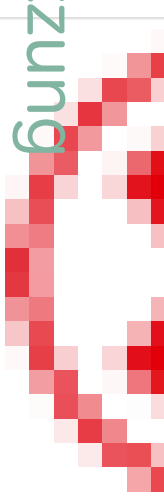
***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Meine Freigaben |  |  |  |
| Angreifbare Container-Elemente | | | |
| Mir zugewiesen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

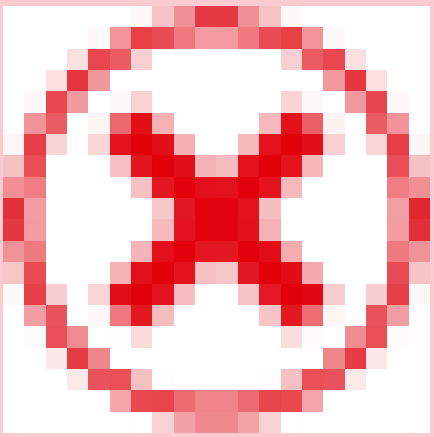
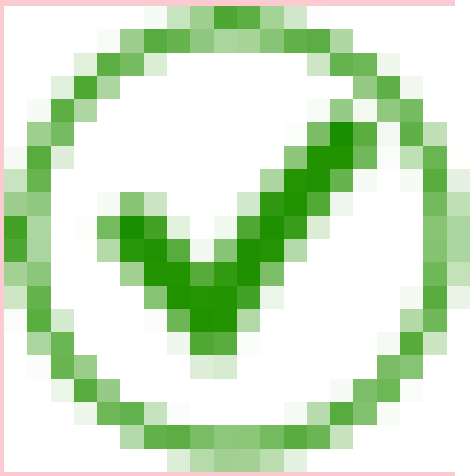
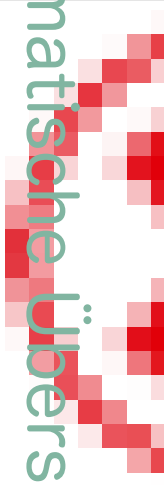
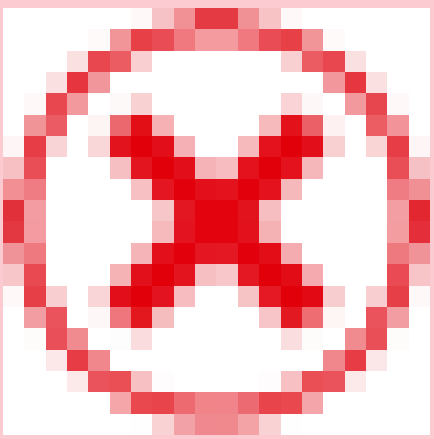
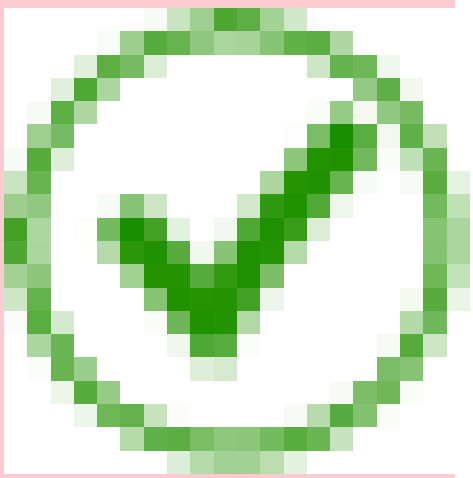
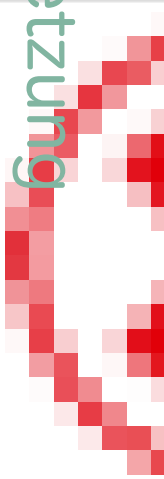
***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Meinen Gruppen zugewiesen |  |  |  |
| Kritisches und hohes Risiko |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Nutzbar | ✗ | ✓ | |
| Ziel rückt näher | ✗ | ✓ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Verfehltes Ziel | ✗ | ✓ | |
| Alle | ✗ | ✓ | |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

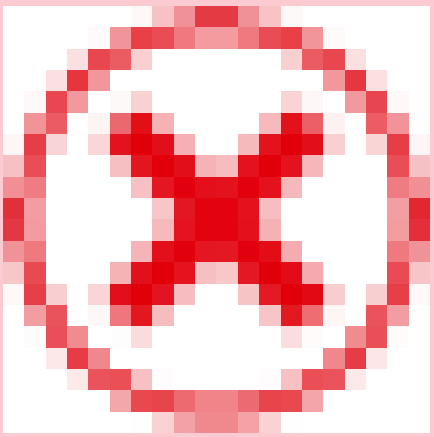
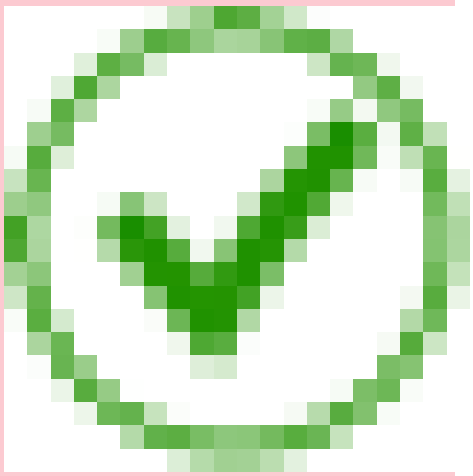
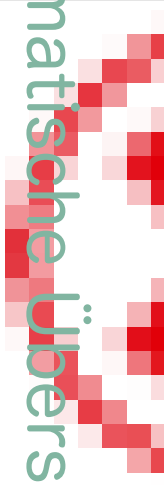
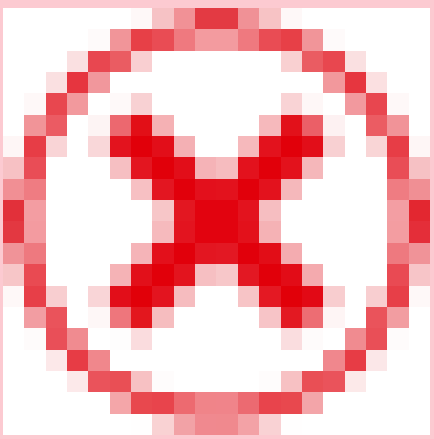
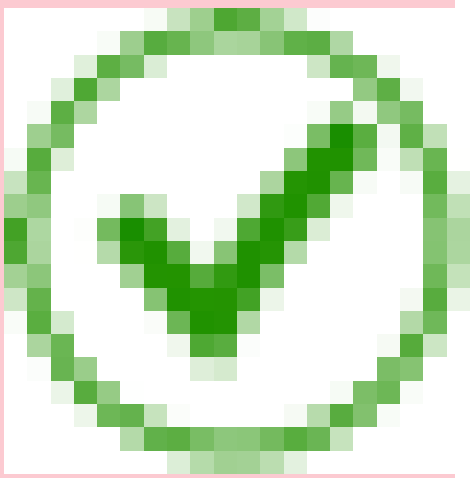
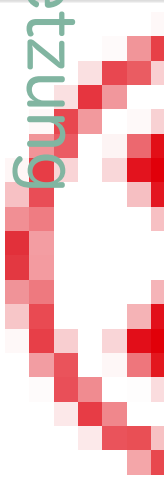
***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| NVD |  |  |  |
| Drittpartei |  |  |  |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

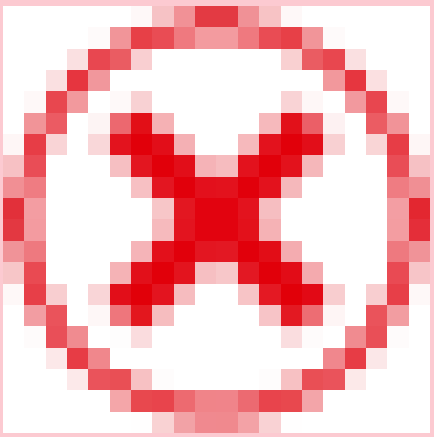
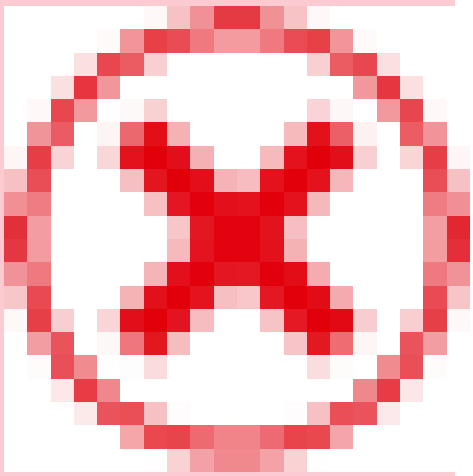
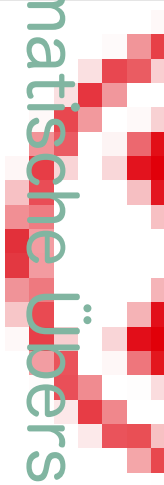
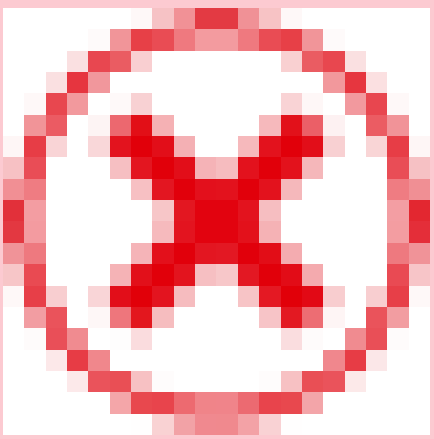
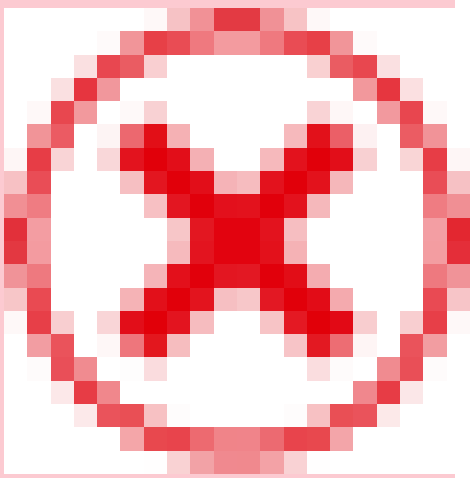
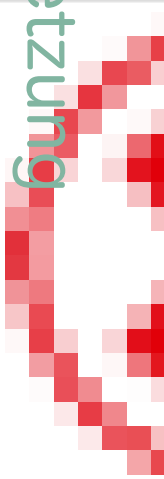
***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Zuweisungsregeln |  |  |  |
| Sicherheitsrisiko-Rechner |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✗ | ✗ |
| VI-Granularität konfigurieren | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

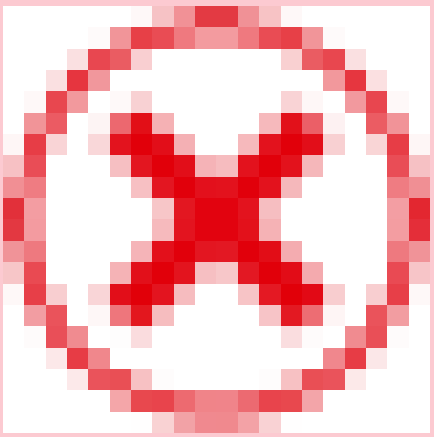
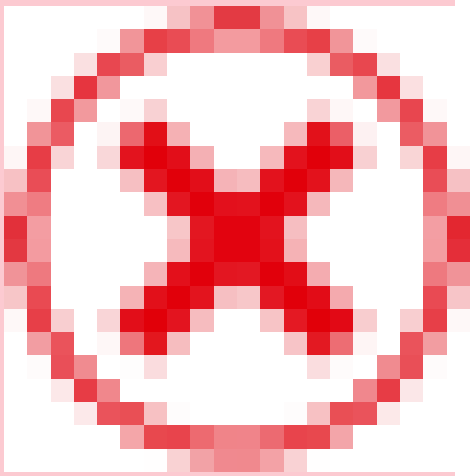
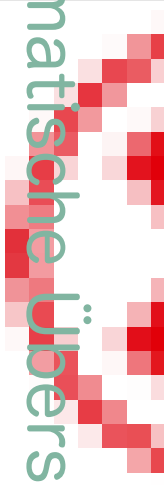
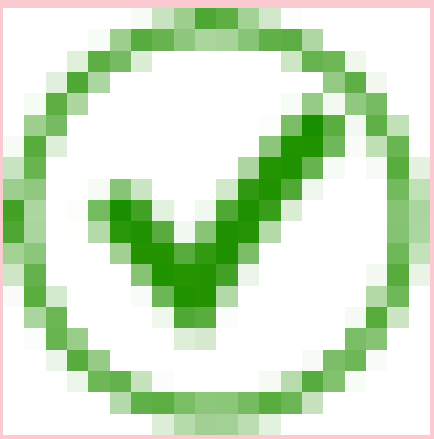
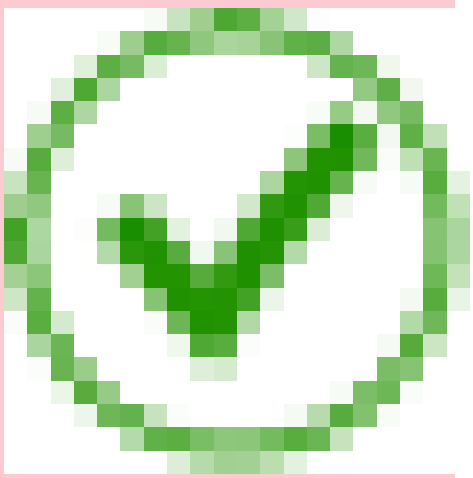
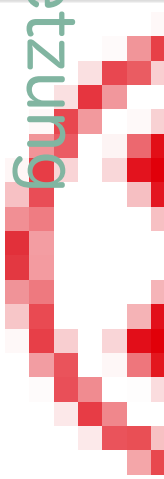
***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Ausnahmeregeln |  |  |  |
| Genehmigungsregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Container-Sicherheitsintegrationen | ✗ | ✓ | |
| Angreifbare Elemente automatisch schließen | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity**

***Informationen für andere Rollen:***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul_container.configure_integrations | sn_vul_contai |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

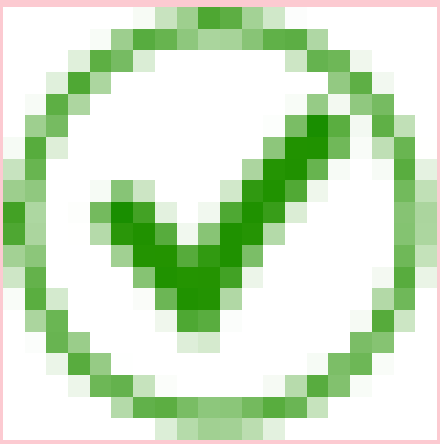
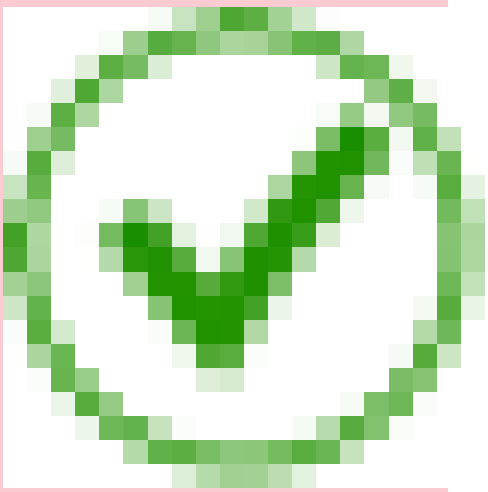
*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| Übersicht |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

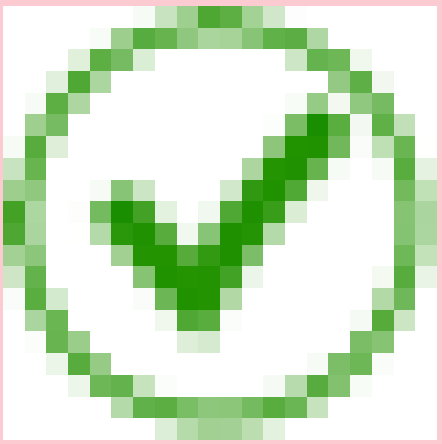
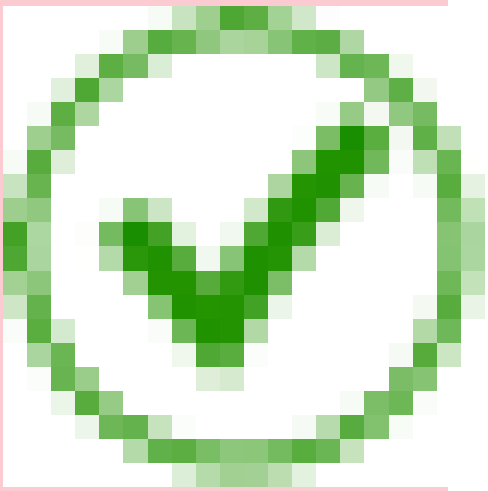
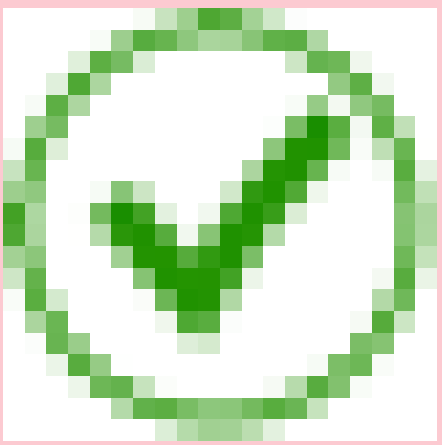
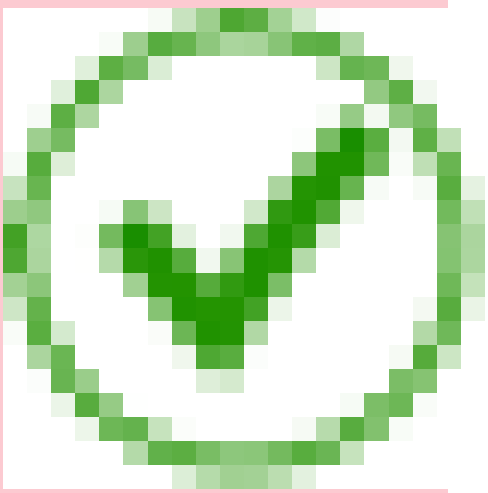
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Meine Freigaben |  |  | |
| Angreifbare Container-Elemente | | | |
| Mir zugewiesen |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

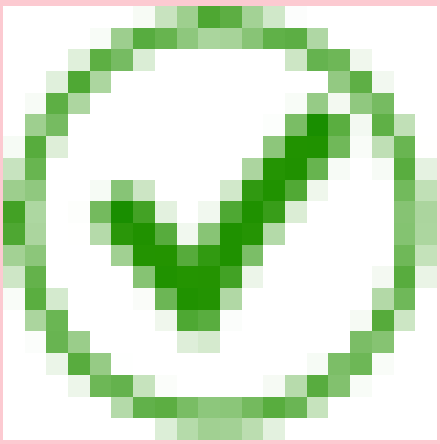
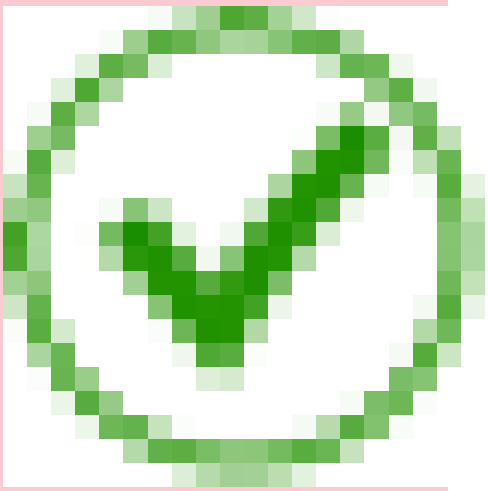
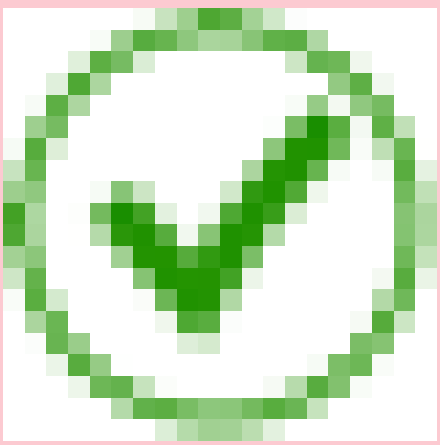
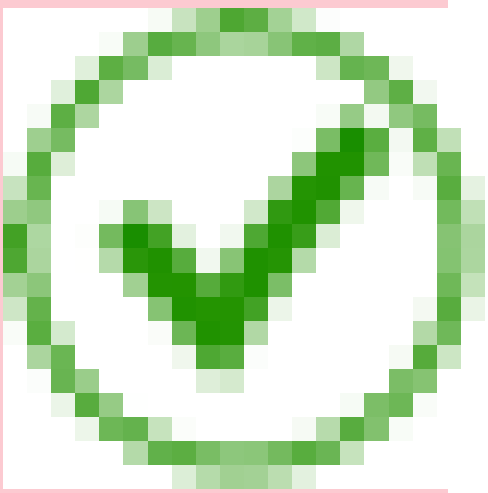
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Meinen Gruppen zugewiesen |  |  | |
| Kritisches und hohes Risiko |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

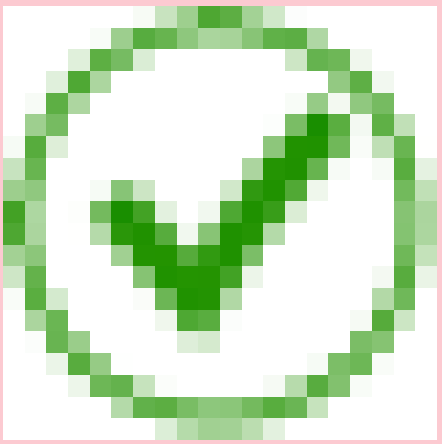
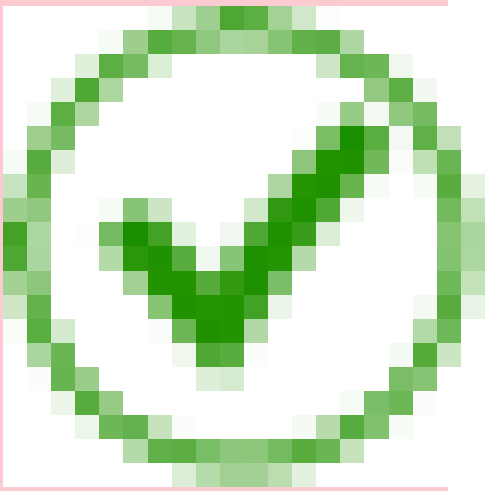
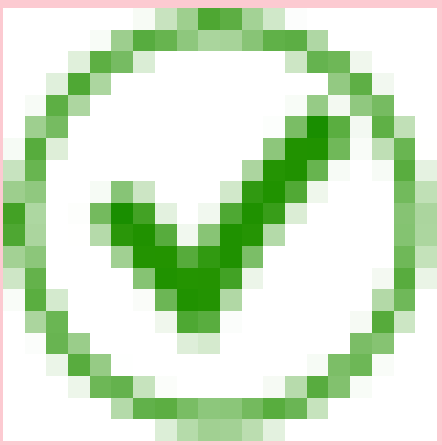
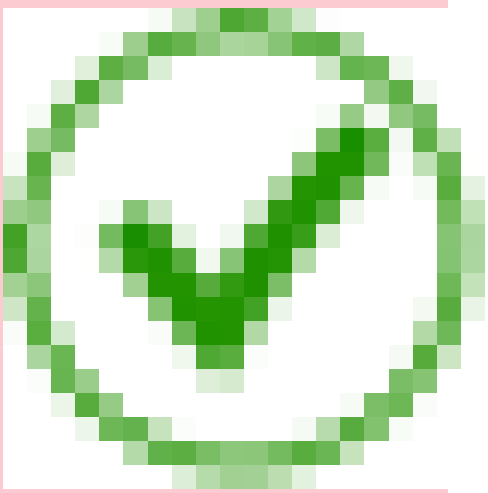
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Nutzbar |  |  | |
| Ziel rückt näher |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

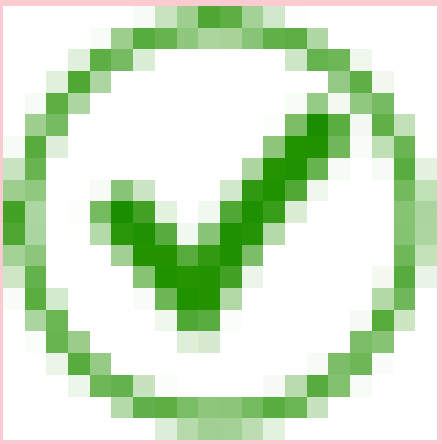
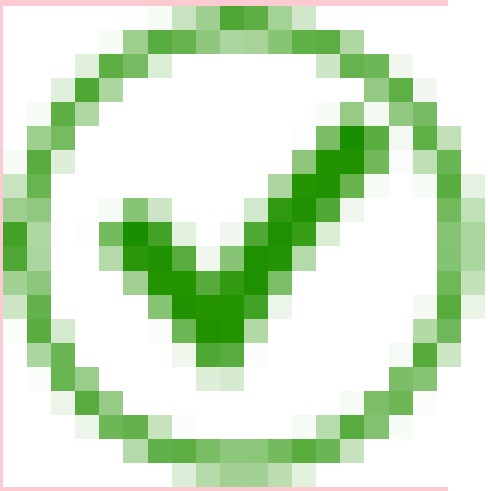
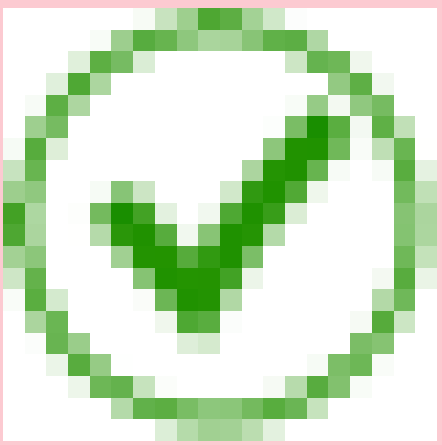
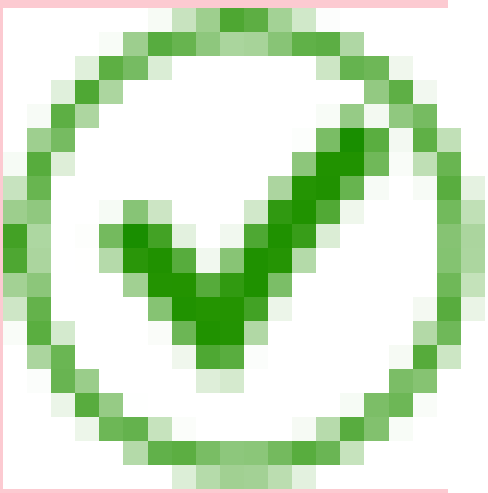
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Verfehltes Ziel |  |  | |
| Alle |  |  | |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

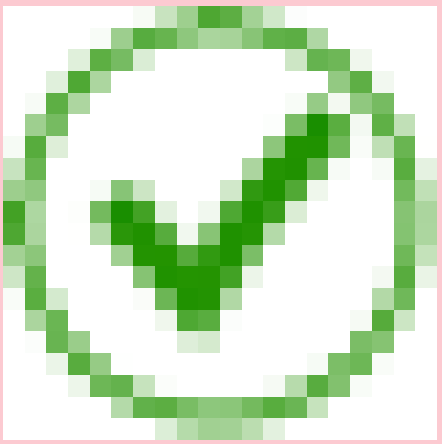
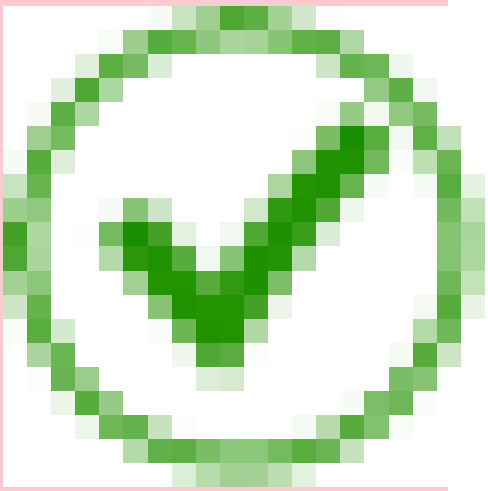
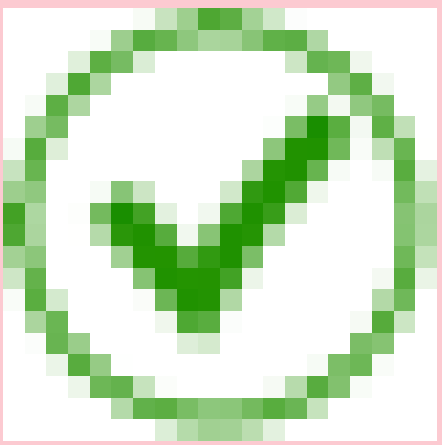
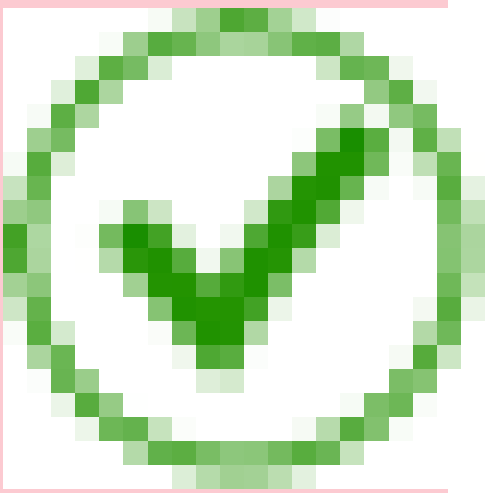
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| NVD |  |  | |
| Drittpartei |  |  | |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

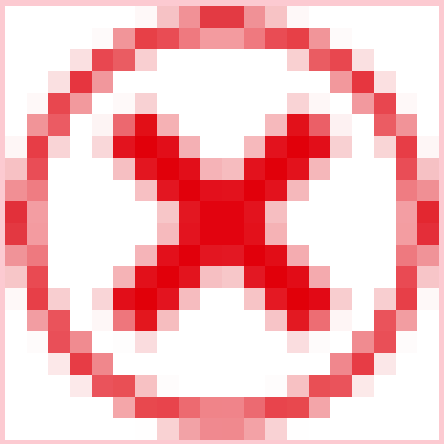
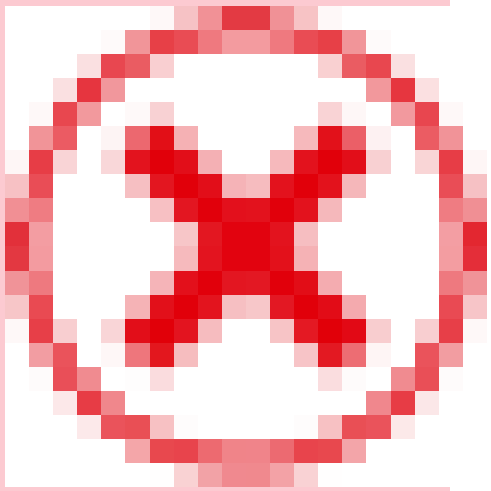
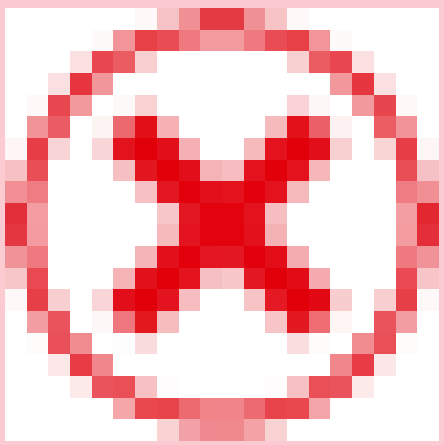
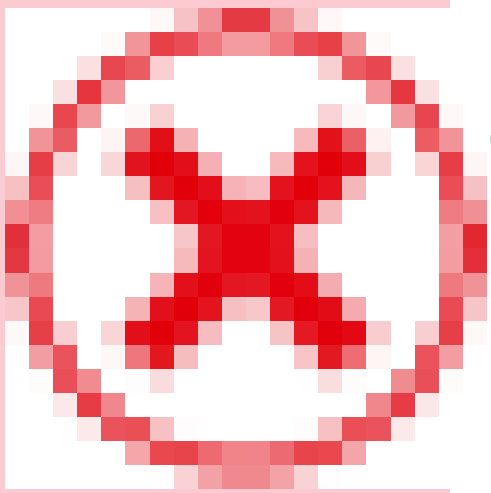
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Zuweisungsregeln |  |  | |
| Sicherheitsrisiko-Rechner |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

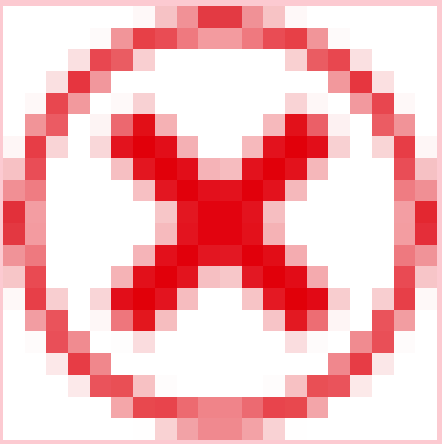
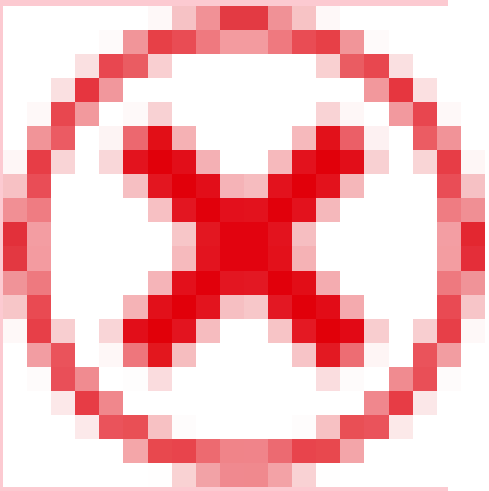
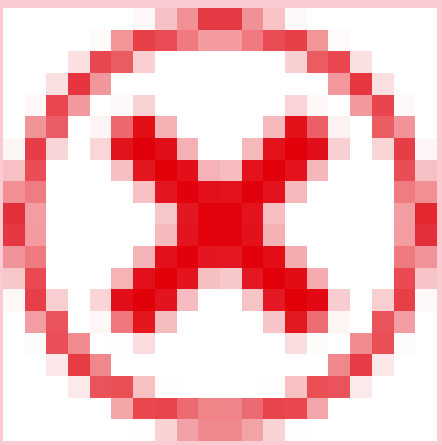
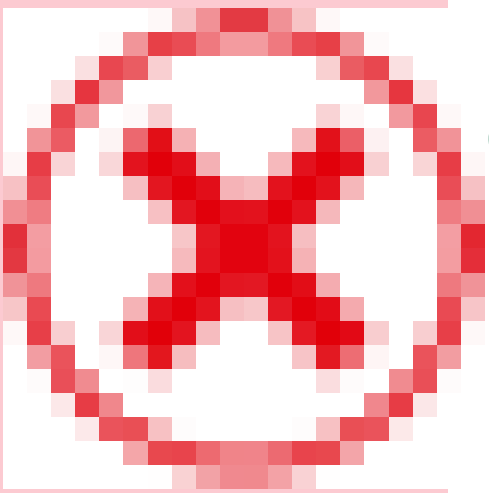
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Nachbesserungszielregeln |  |  | |
| VI-Granularität konfigurieren |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

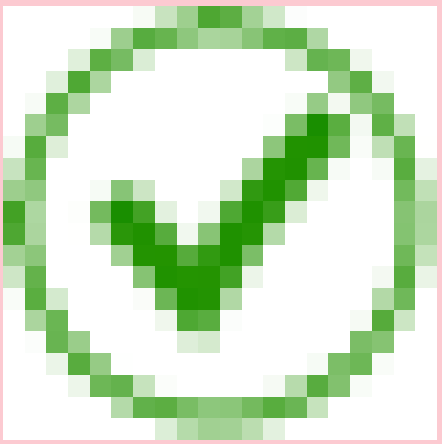
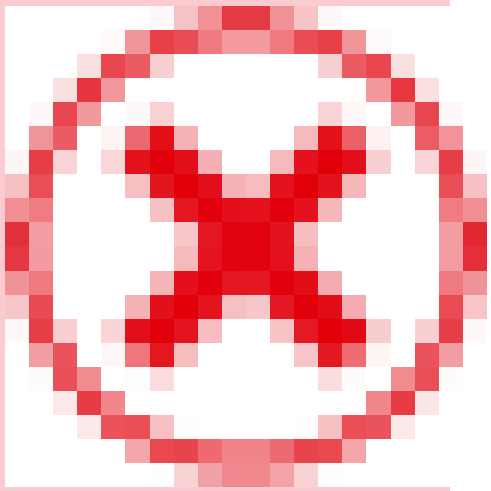
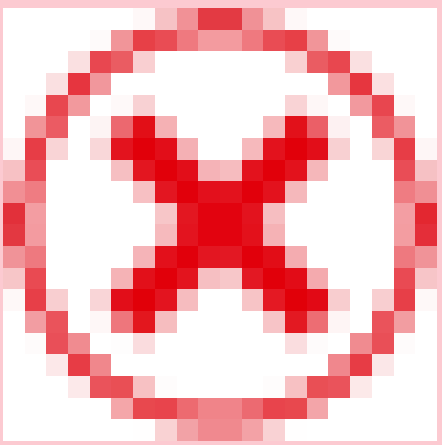
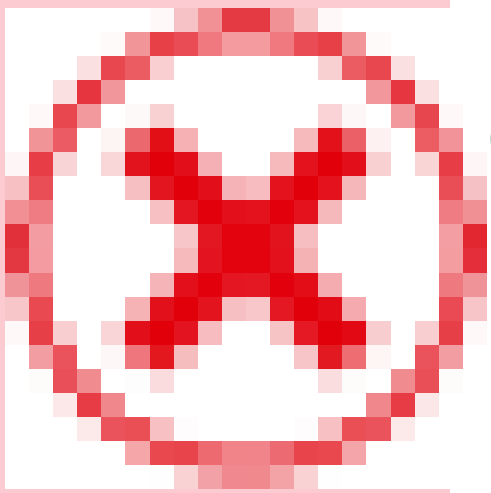
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Ausnahmeregeln |  |  | |
| Genehmigungsregeln |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

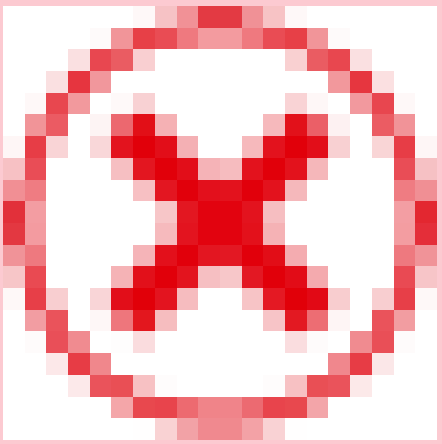
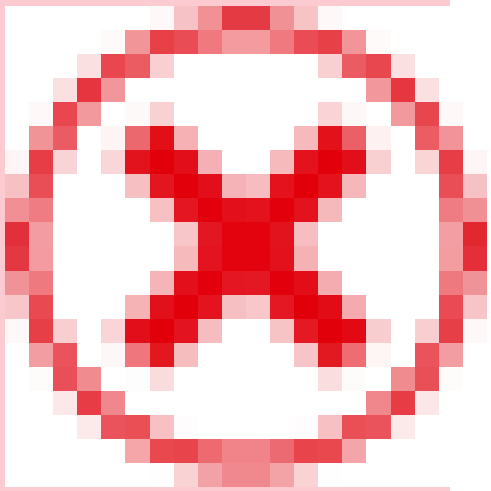
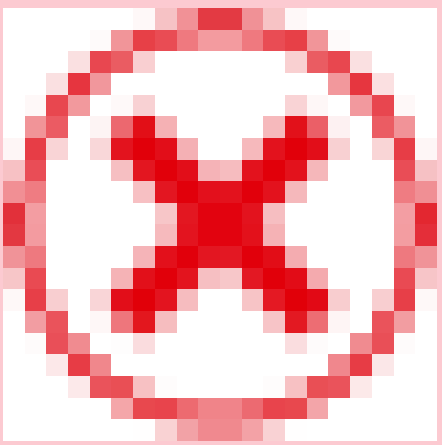
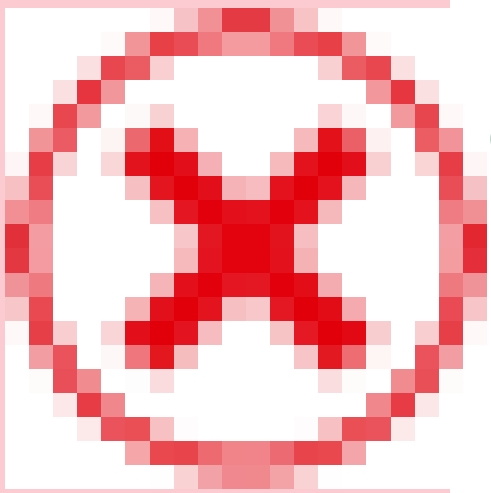
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Container-Sicherheitsintegrationen |  |  | |
| Angreifbare Elemente automatisch schließen |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules**

***Informationen für andere Rollen:***

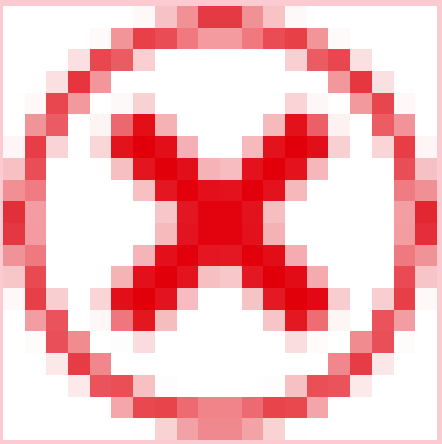
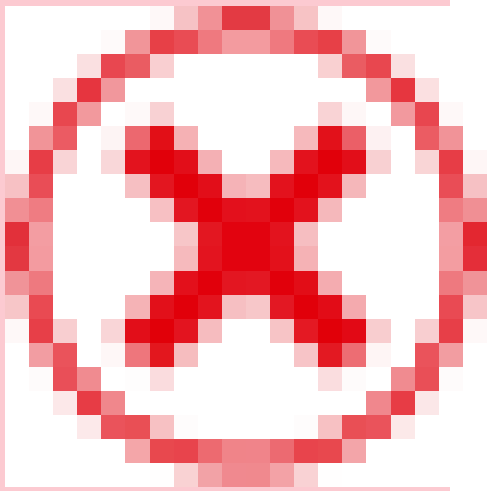
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.exception_approver | sn_vul_container.false_positive_approver | sn_vul_cont |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

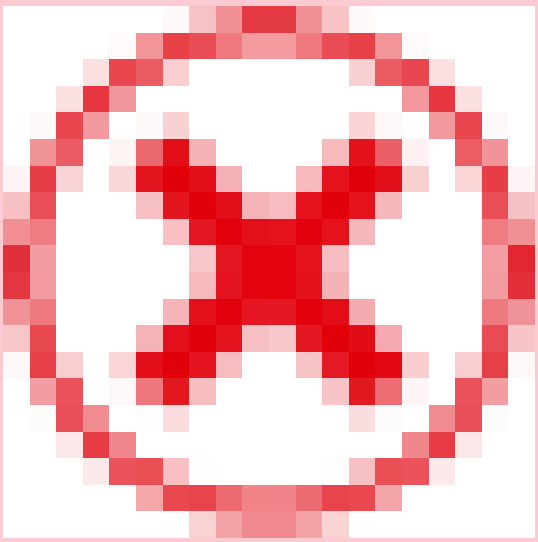
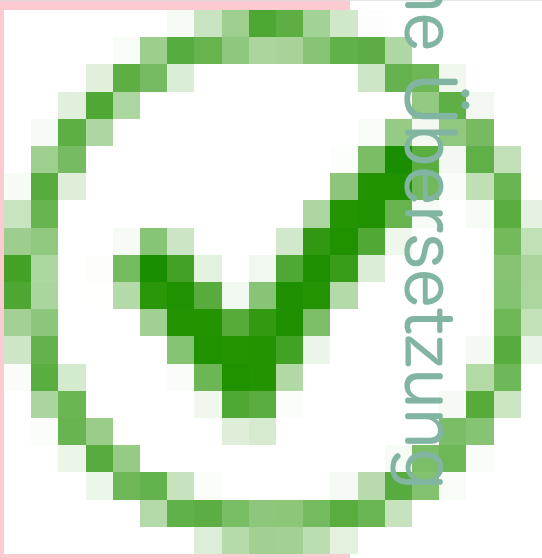
*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| Übersicht |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

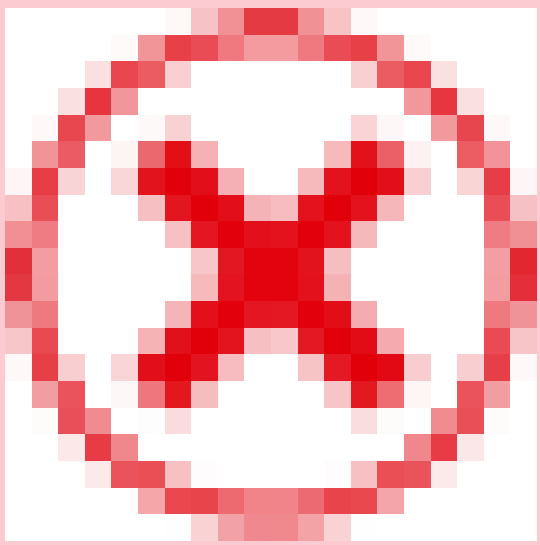
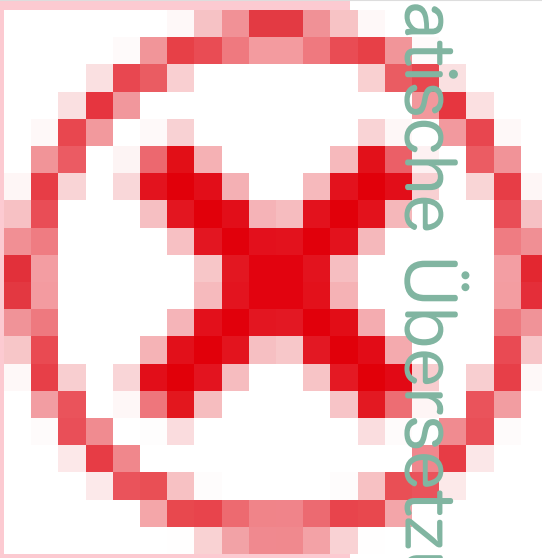
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Meine Freigaben |  |  |
| Angreifbare Container-Elemente | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

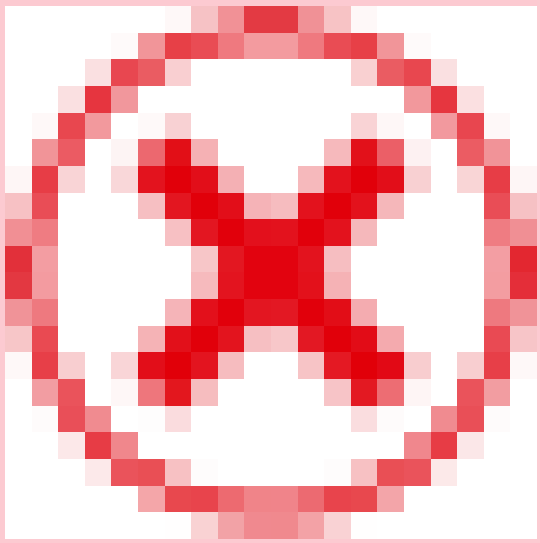
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Mir zugewiesen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

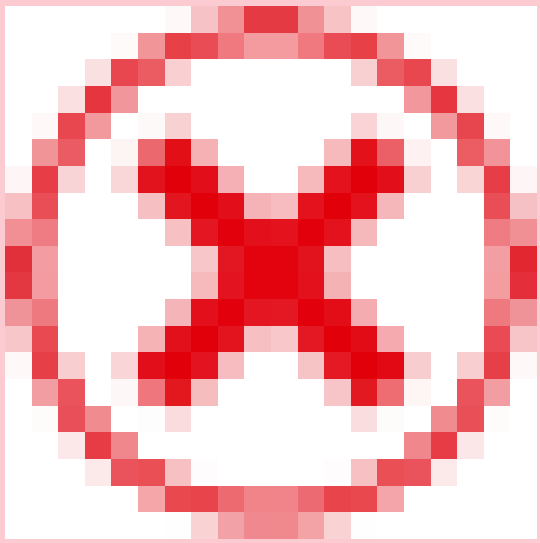
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Meinen Gruppen zugewiesen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

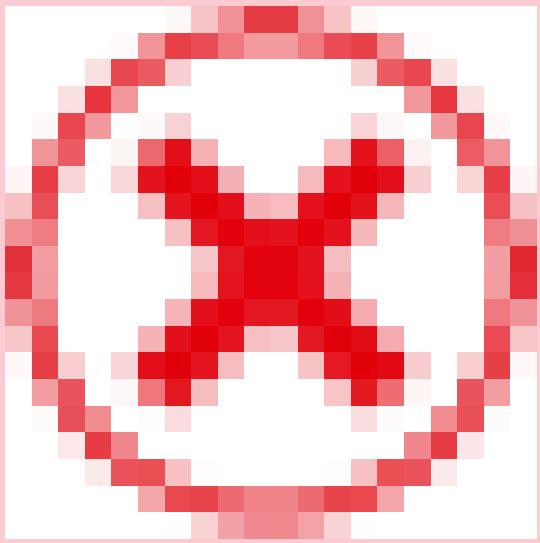
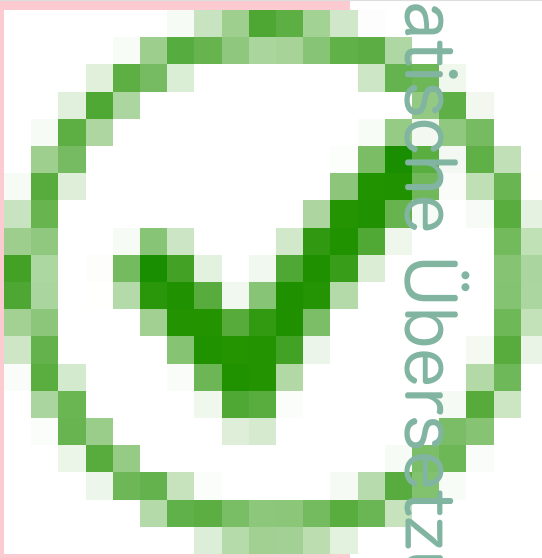
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Kritisches und hohes Risiko |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

***Informationen für andere Rollen:***

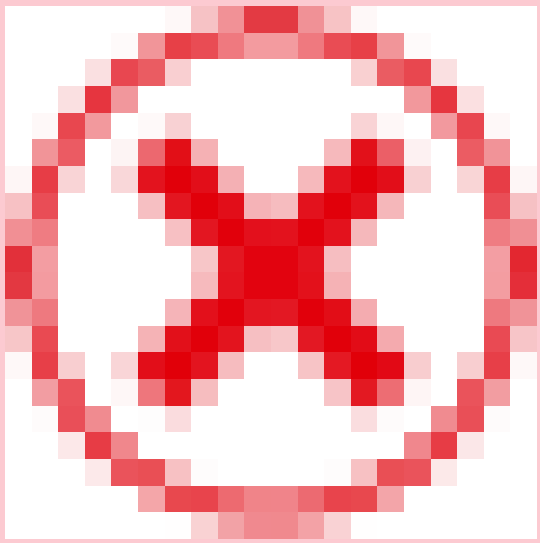
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Nutzbar |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

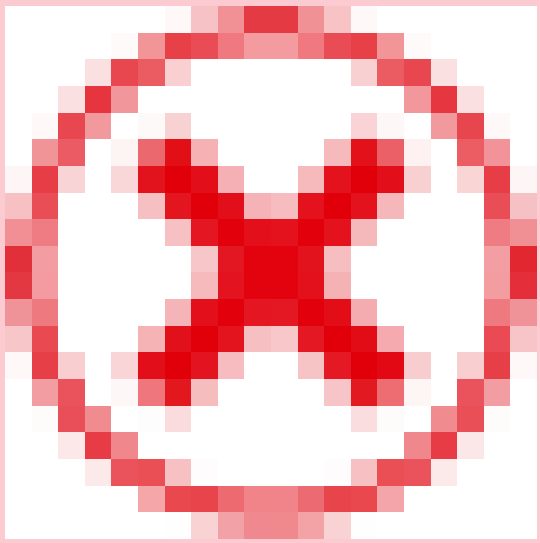
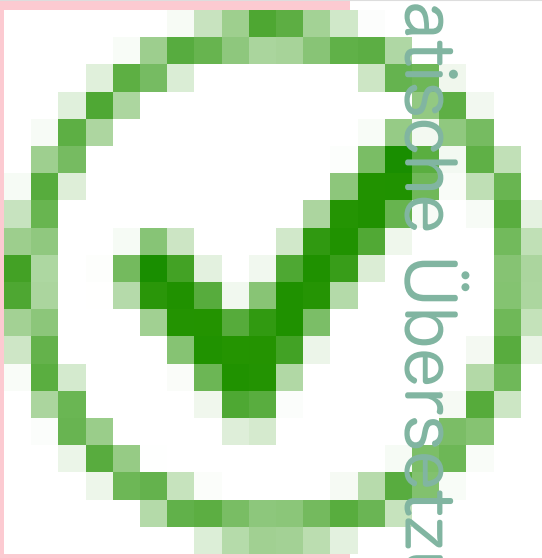
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Ziel rückt näher |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

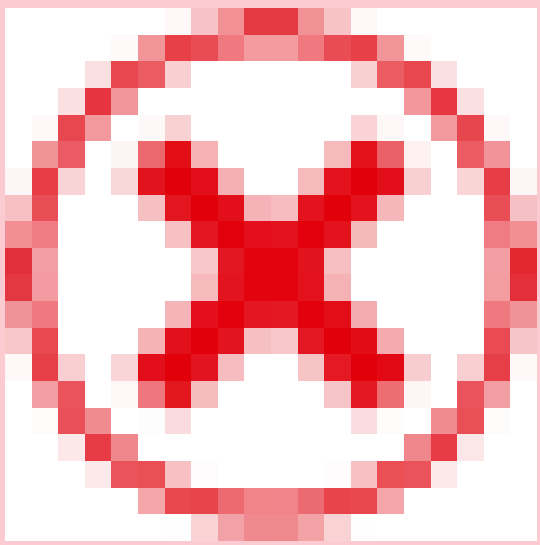
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Verfehltes Ziel |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

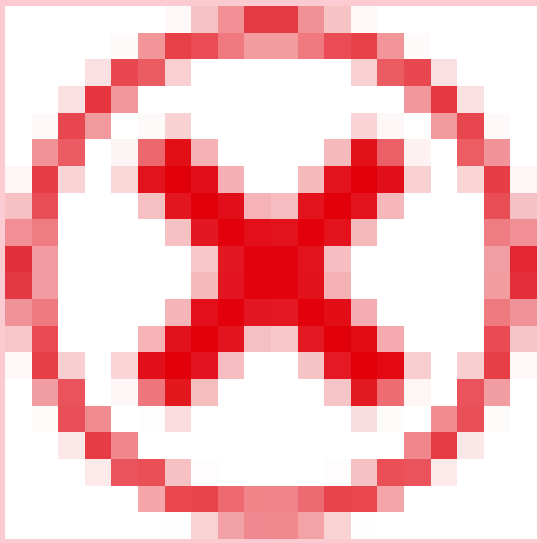
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Alle |  | |
| Bibliotheken | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

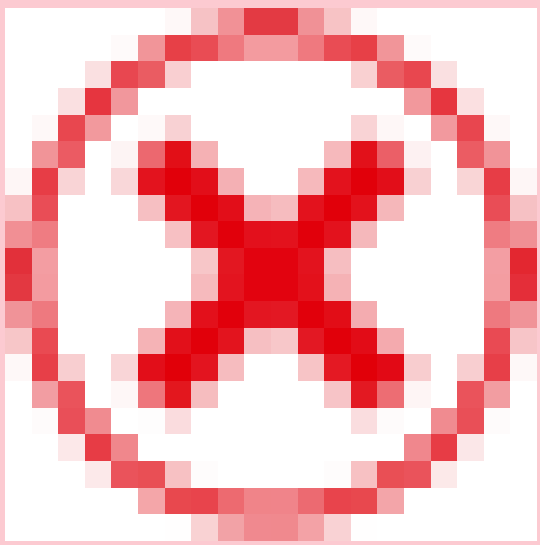
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| NVD |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

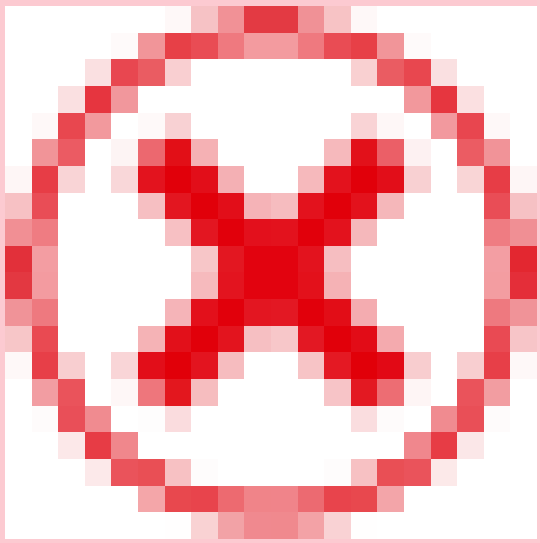
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Drittpartei |  | |
| Administration | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

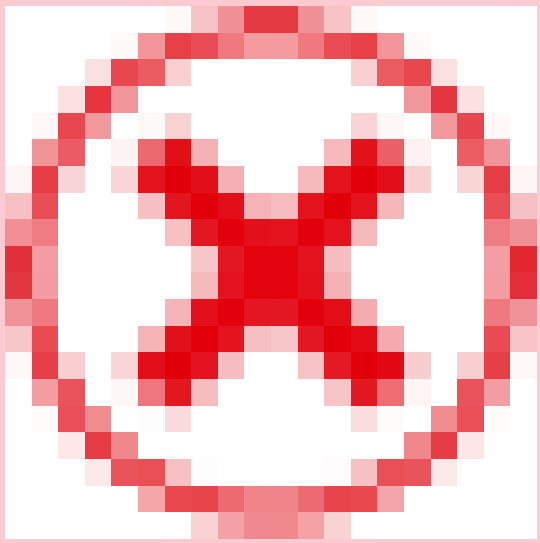
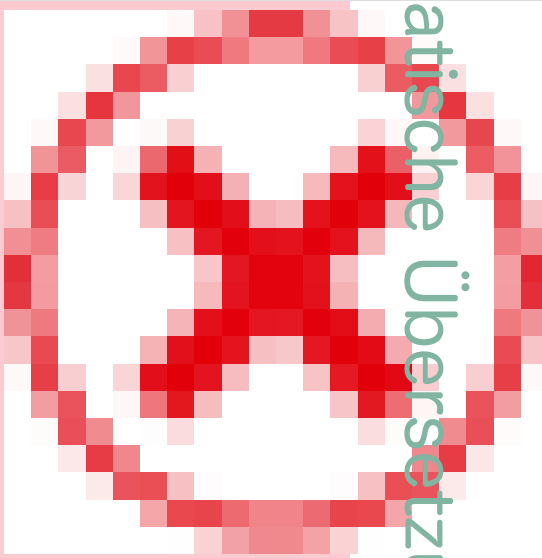
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Zuweisungsregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

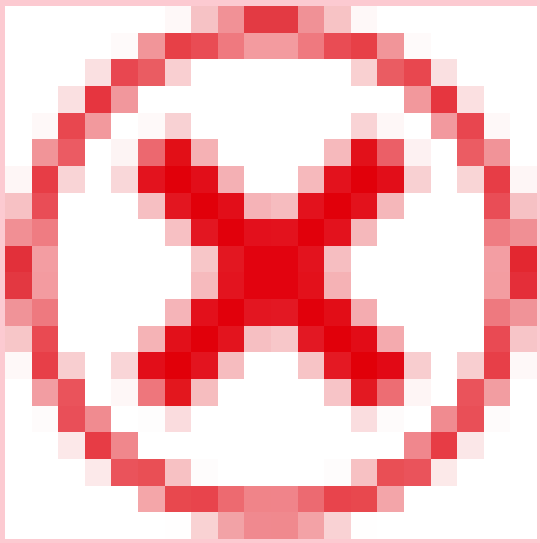
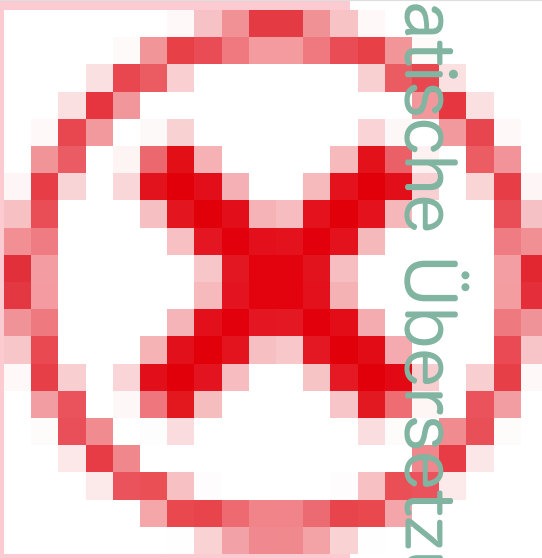
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Sicherheitsrisiko-Rechner |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

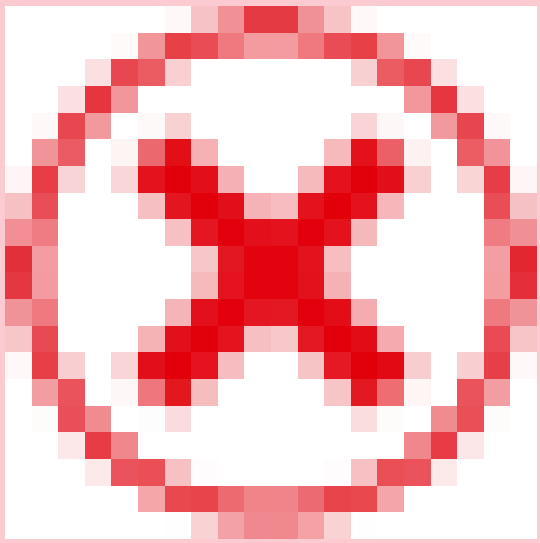
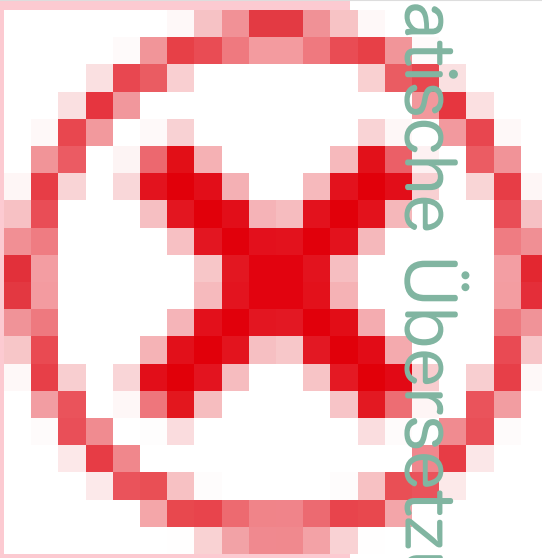
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Nachbesserungszielregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

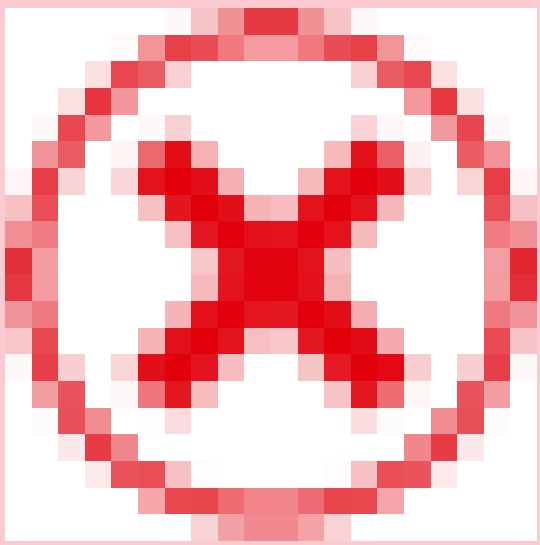
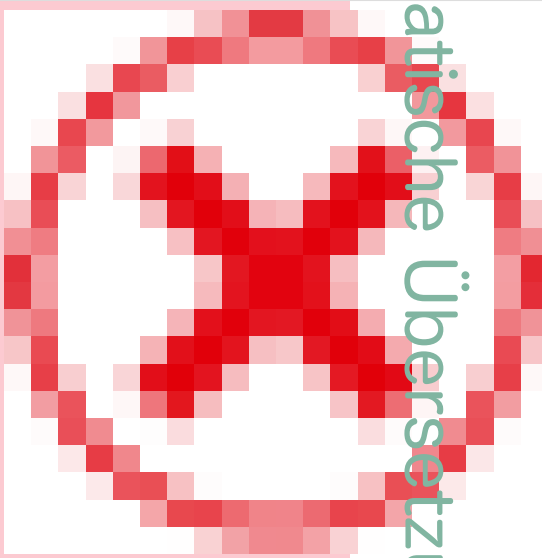
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| VI-Granularität konfigurieren |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

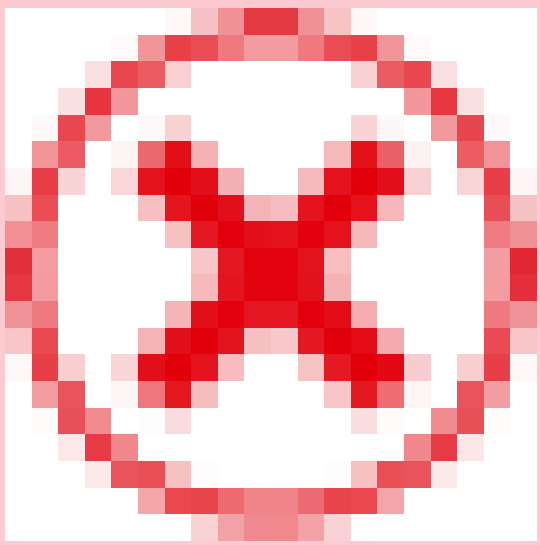
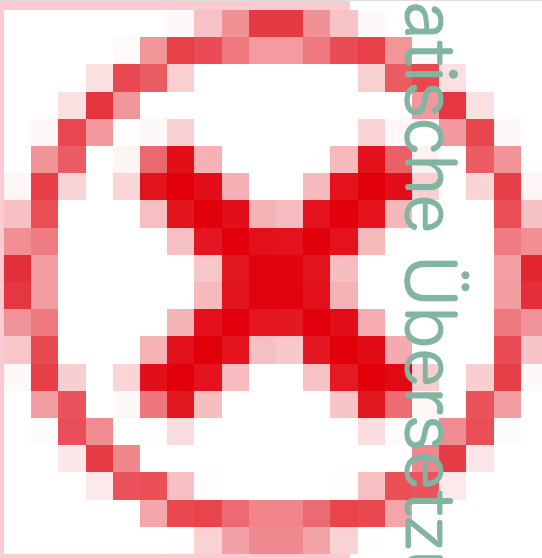
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Ausnahmeregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

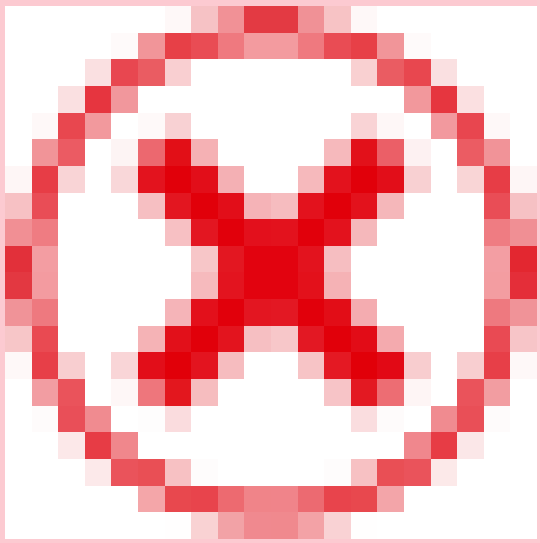
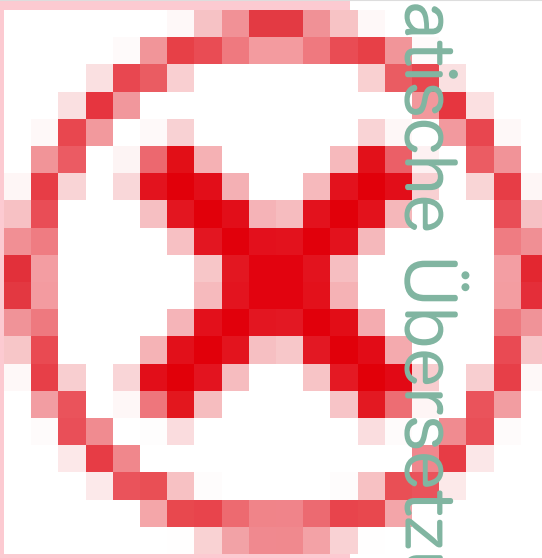
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Genehmigungsregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

***Informationen für andere Rollen:***

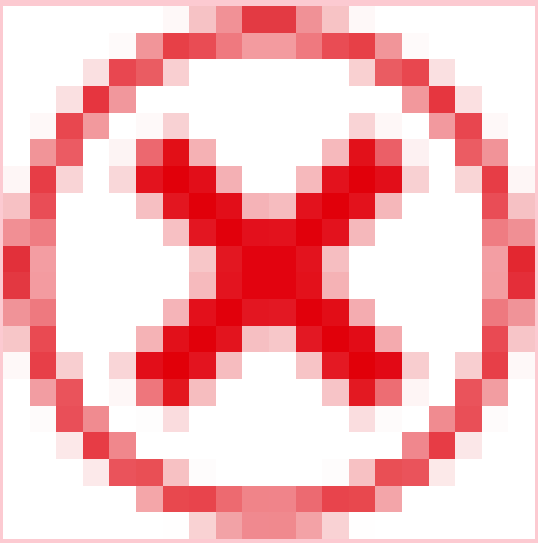
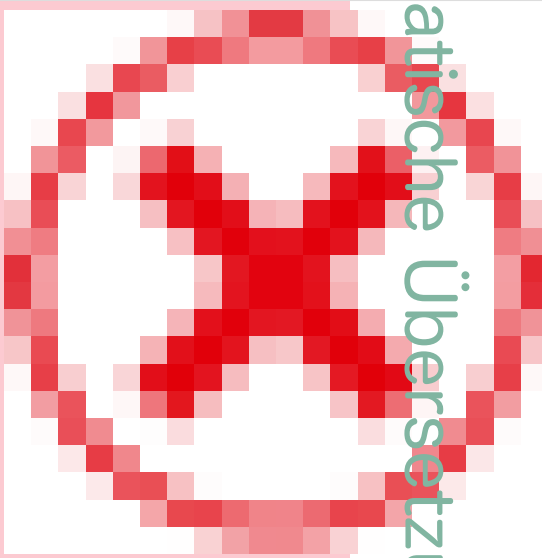
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Container-Sicherheitsintegrationen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

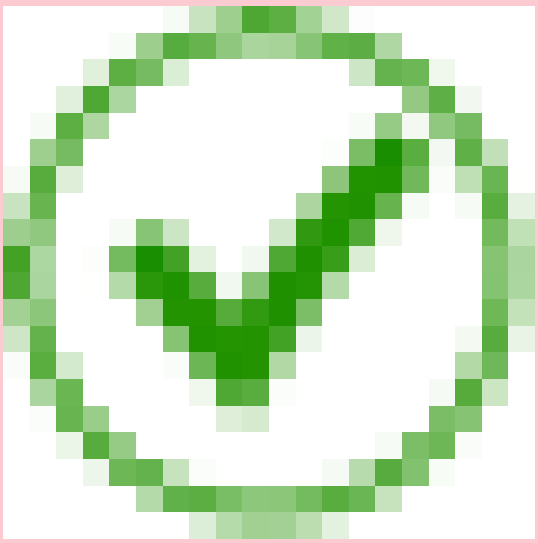
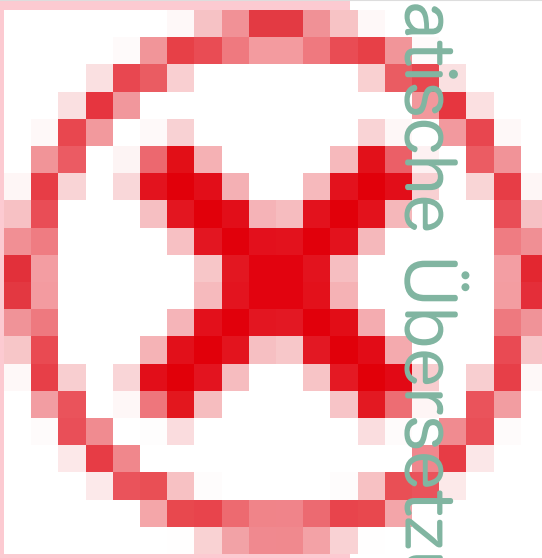
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Angreifbare Elemente automatisch schließen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules**

*Informationen für andere Rollen:*

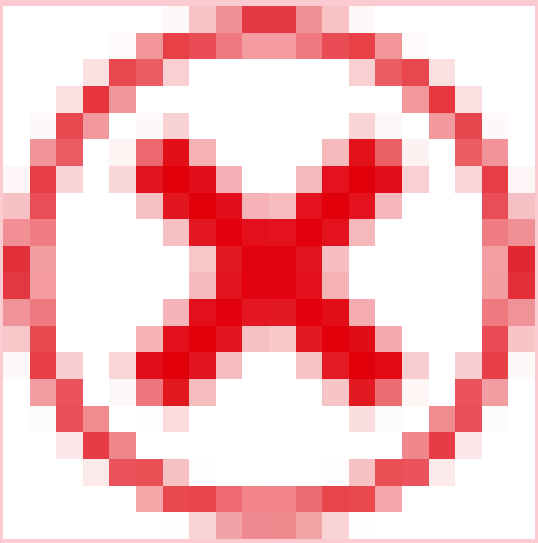
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_auto_close_stale_vi | sn_vul_container.manage_normalized_severity |
|---|---|---|
| Normalisierte Schweregradzuordnungen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

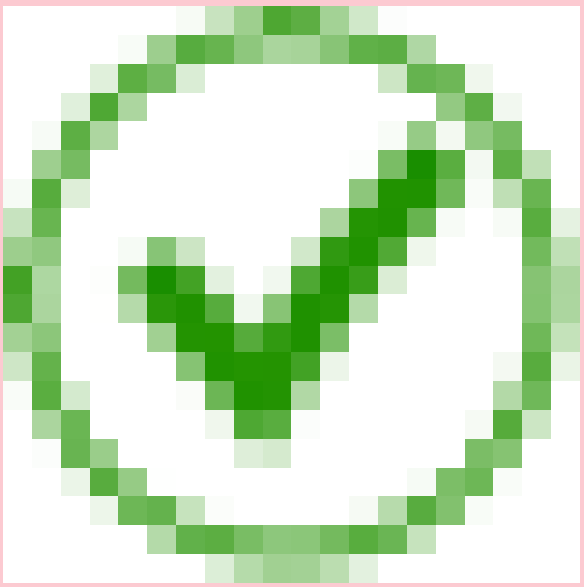
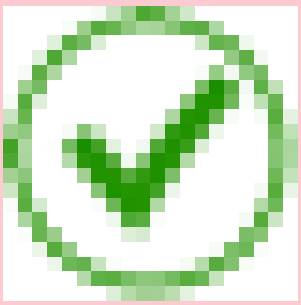
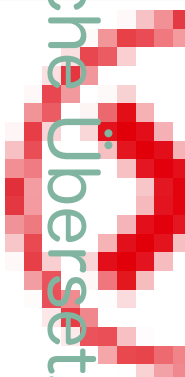
***Informationen für andere Rollen:***

*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.read_auto_exception_rule*

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| Übersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.read_auto_exception_rule*

**(Fortsetzung)**

| Modul | sn_vul_container.manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Meine Freigaben | ✗ | ✗ | ✗ |
| Angreifbare Container-Elemente | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

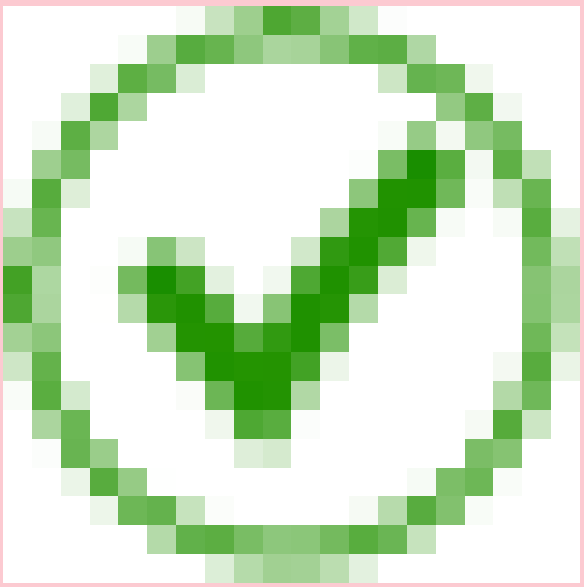
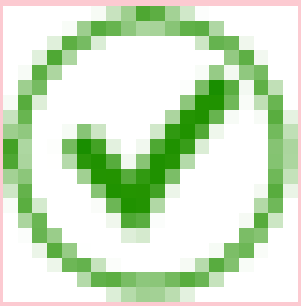
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Mir zugewiesen |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

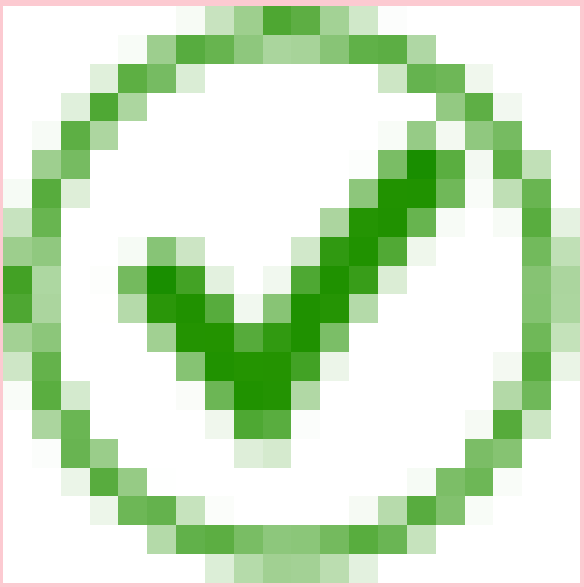
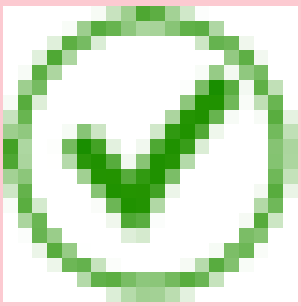
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Meinen Gruppen zugewiesen |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

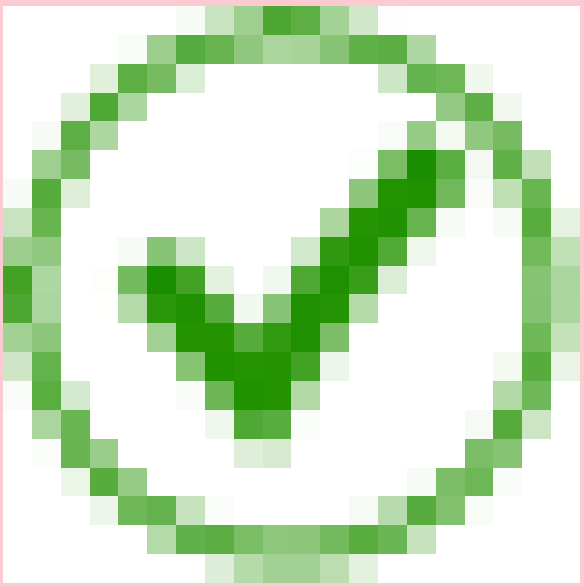
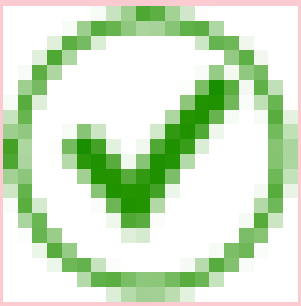
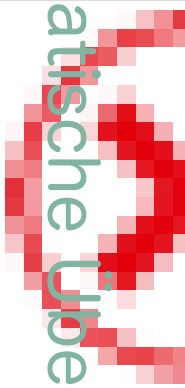
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Kritisches und hohes Risiko |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

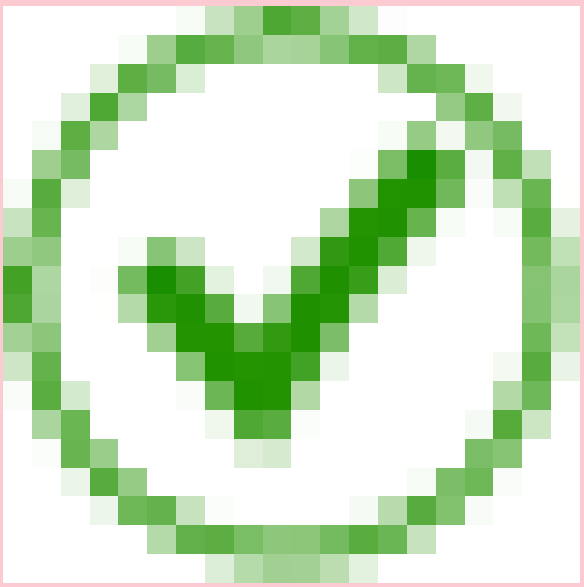
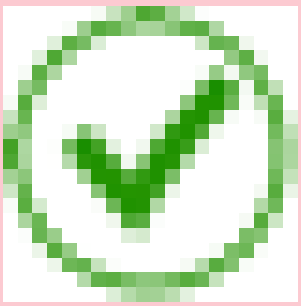
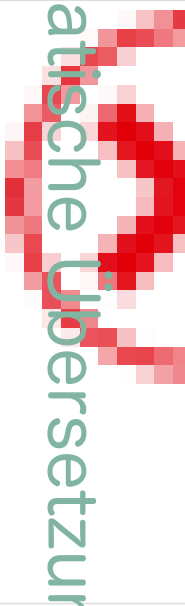
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Nutzbar |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Ziel rückt näher | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Verfehltes Ziel | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

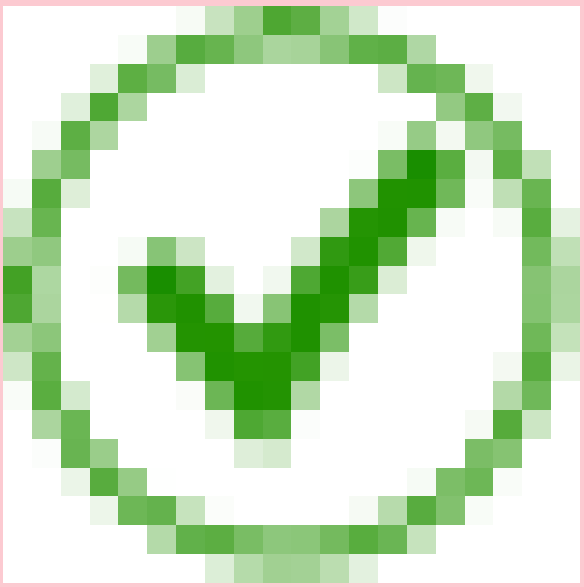
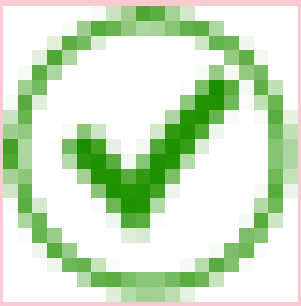
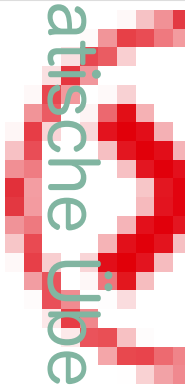
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Alle |  |  |  |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

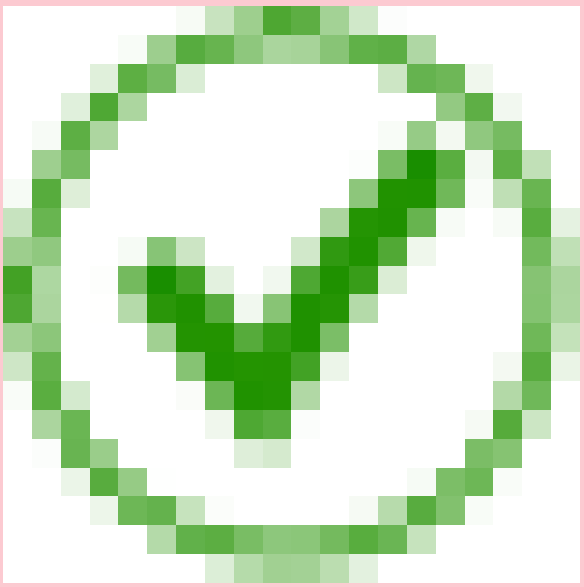
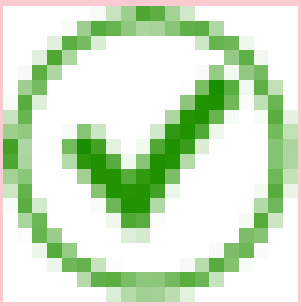
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| NVD |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

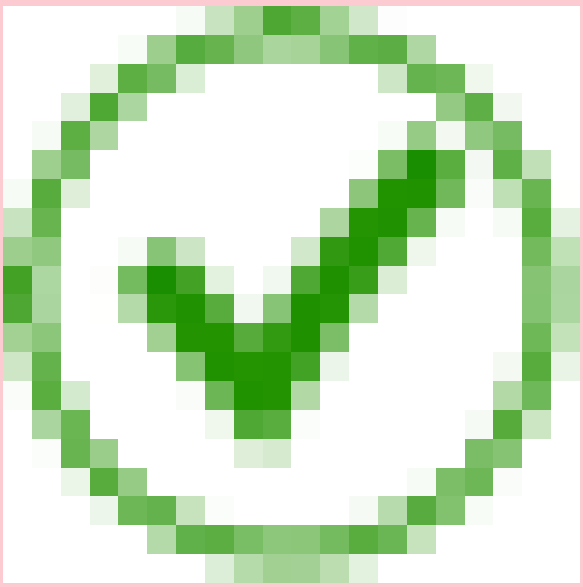
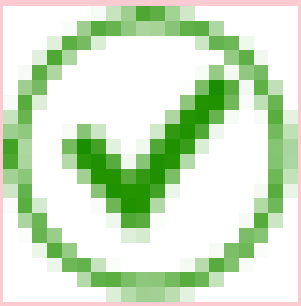
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Drittpartei |  |  | |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

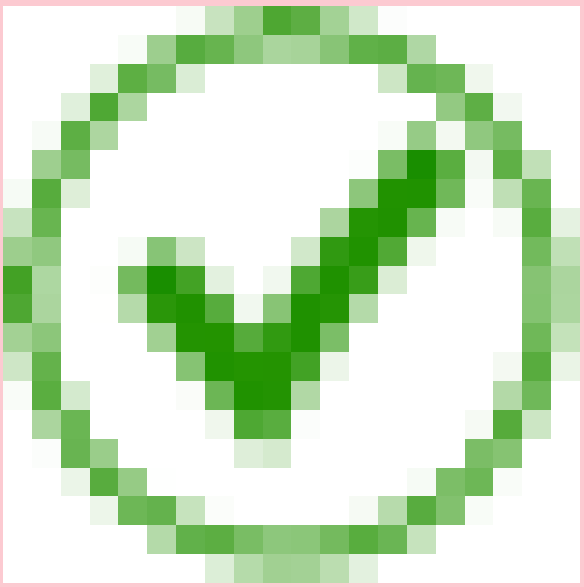
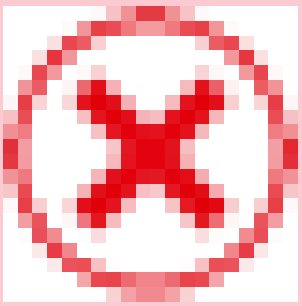
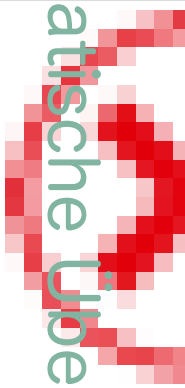
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Sicherheitsrisiko-Rechner |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

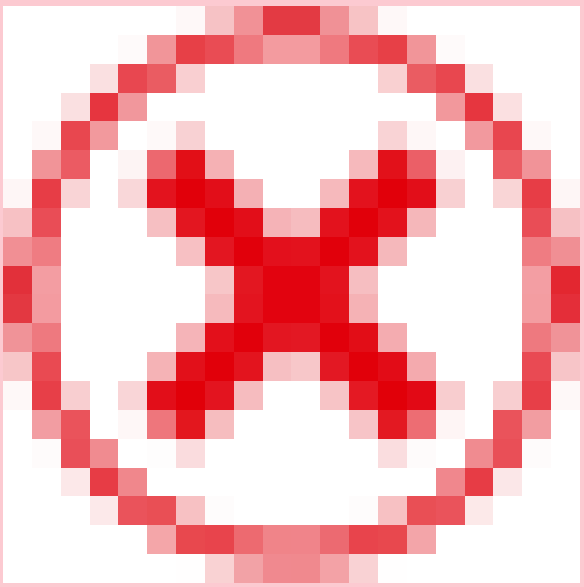
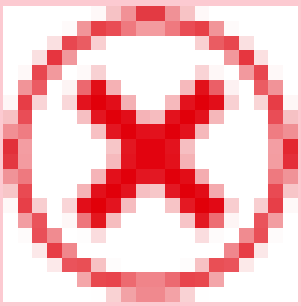
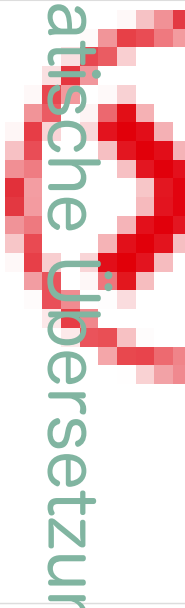
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Nachbesserungszielregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

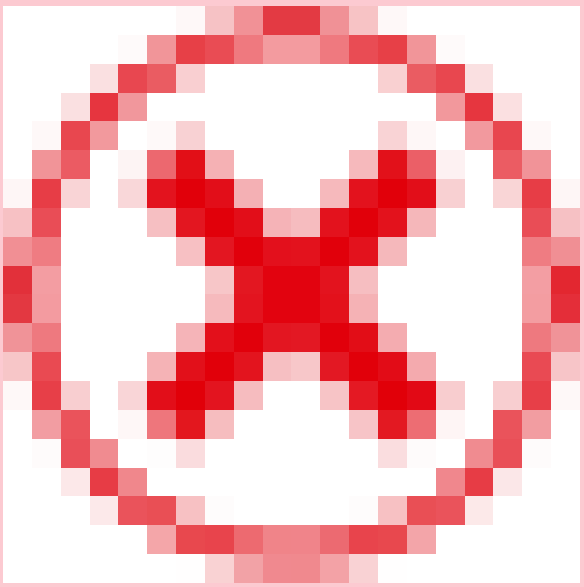
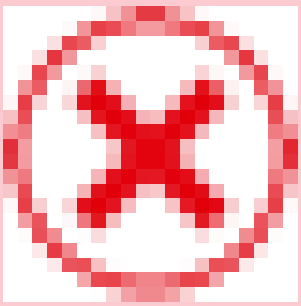
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| VI-Granularität konfigurieren |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Ausnahmeregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Genehmigungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Container-Sicherheitsintegrationen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

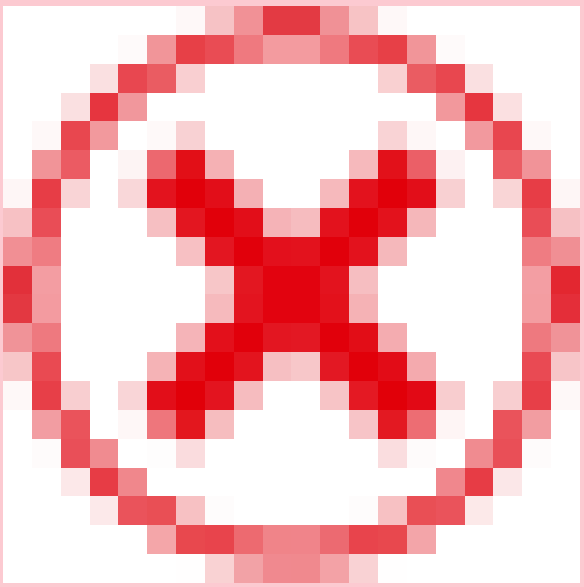
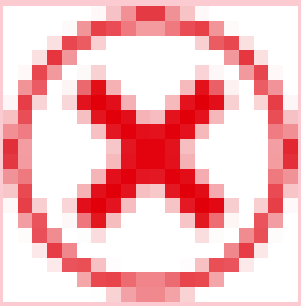
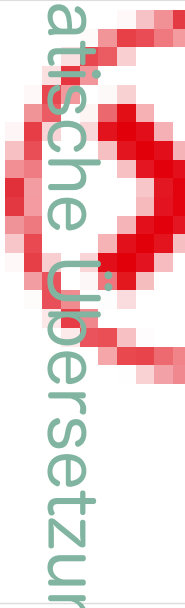
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Angreifbare Elemente automatisch schließen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned**

***Informationen für andere Rollen:***

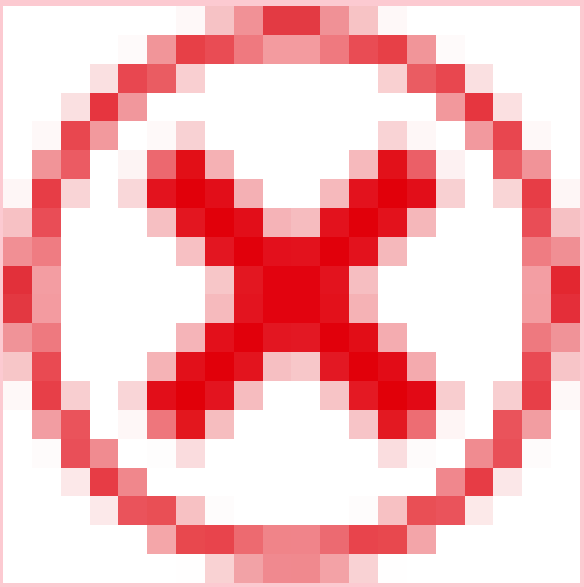
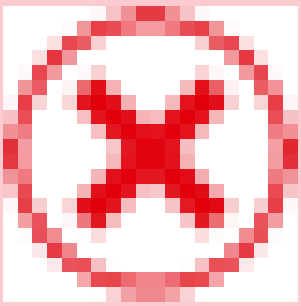
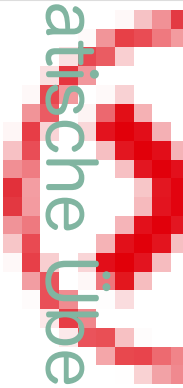
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.read_auto_exception_rule***

**(Fortsetzung)**

| Modul | sn_vul_container.<br>manage_risk_score_configuration | sn_vul_container.read_all | sn_vul_containe |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul_container.read_auto_exception_rule

### Modulzugriff für: sn_vul_container.read_auto_exception_rule

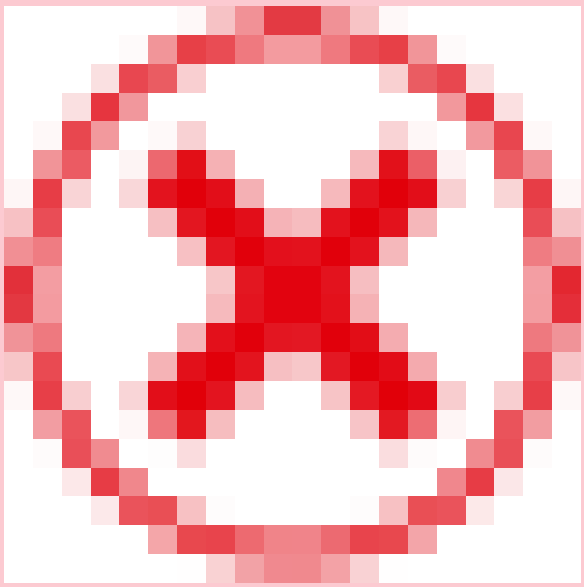
*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| (Haupt-App-Gruppe) | |
| Übersicht |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

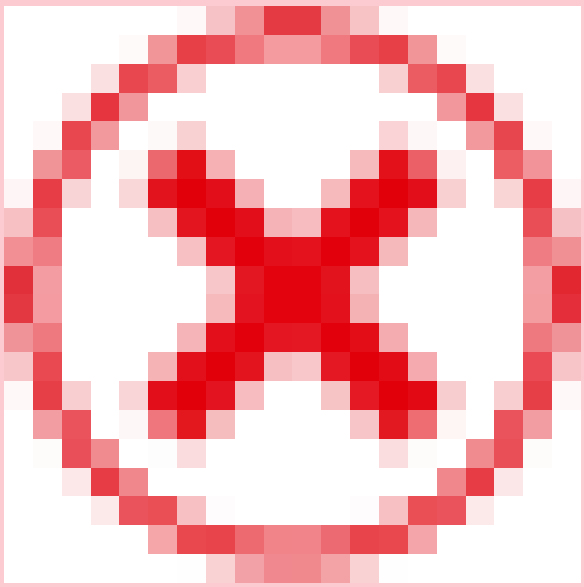
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Meine Freigaben |  |
| Angreifbare Container-Elemente | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

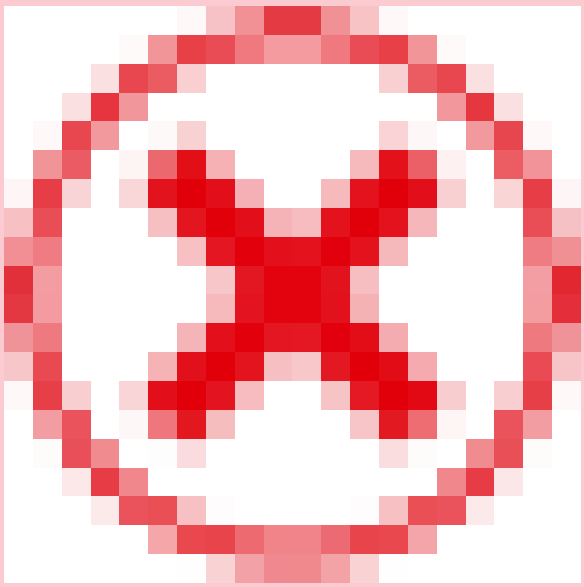
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Mir zugewiesen |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

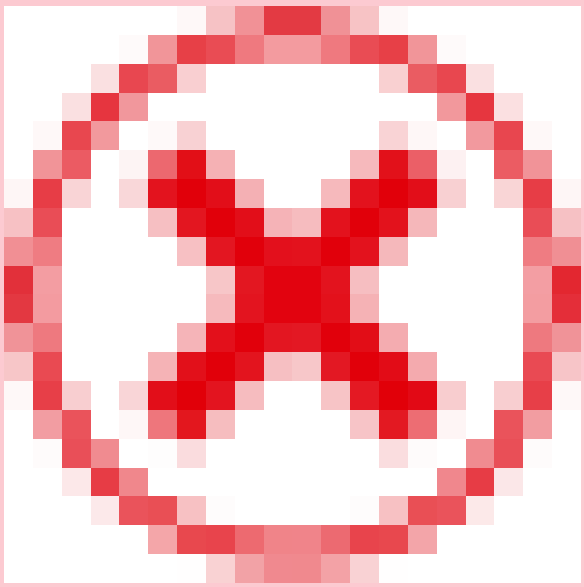
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Meinen Gruppen zugewiesen |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

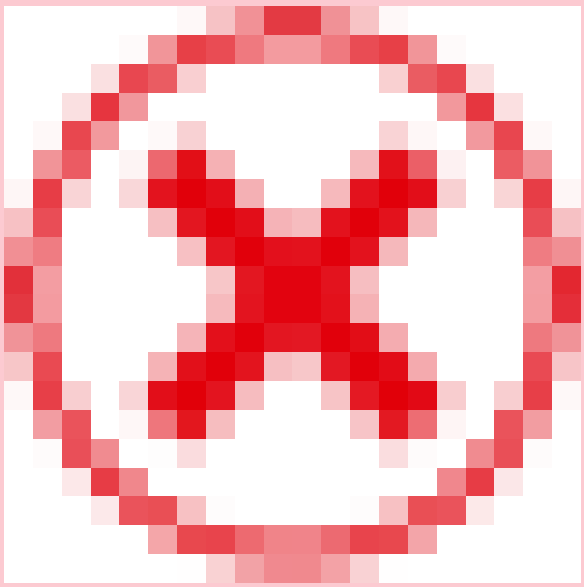
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Kritisches und hohes Risiko |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

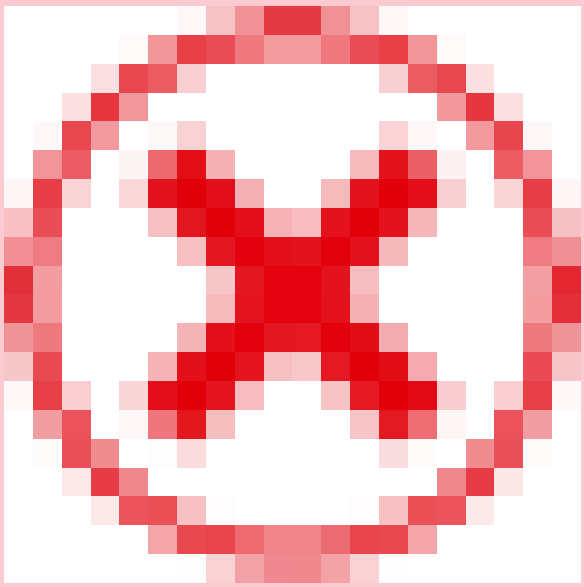
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Nutzbar |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

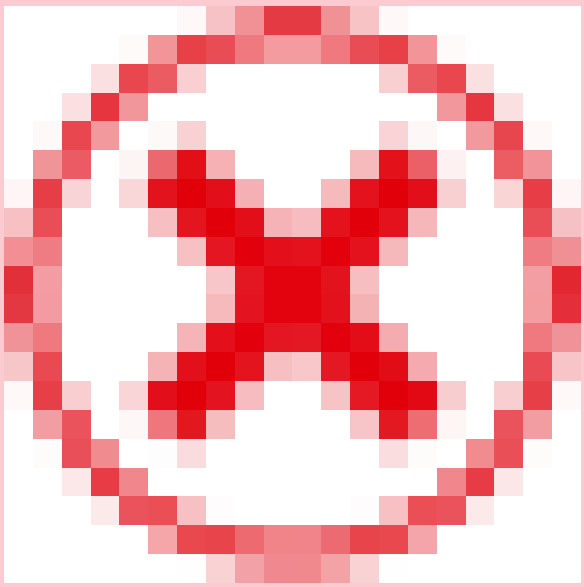
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
| --- | --- |
| Ziel rückt näher |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

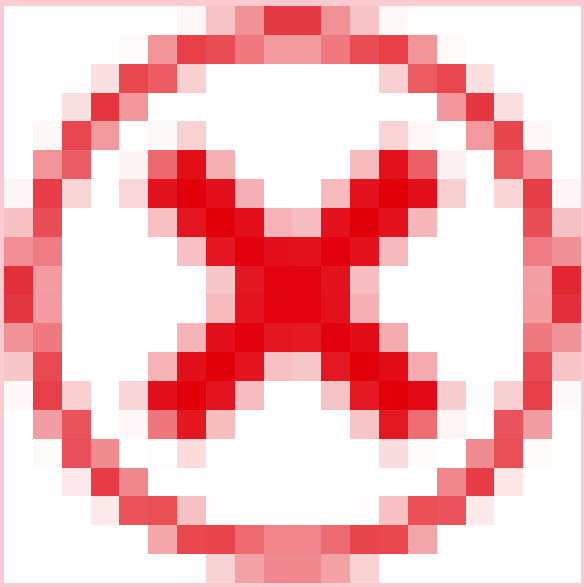
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
| --- | --- |
| Verfehltes Ziel |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

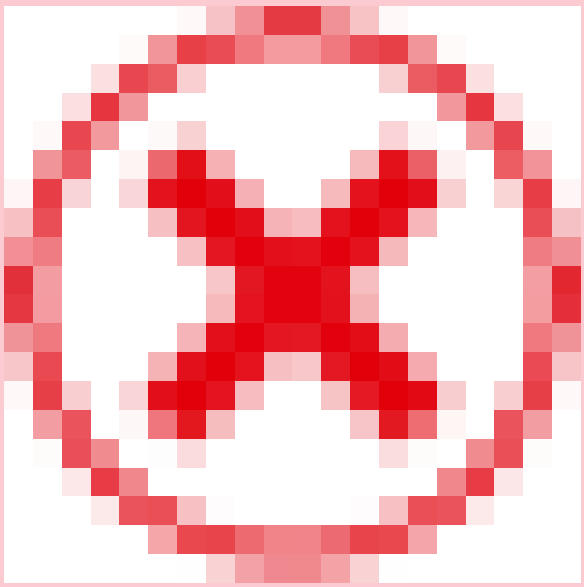
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Alle |  |
| Bibliotheken | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

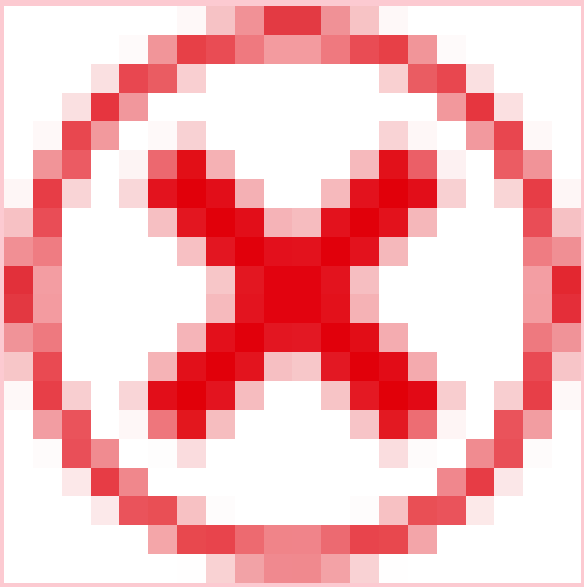
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
| --- | --- |
| NVD |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

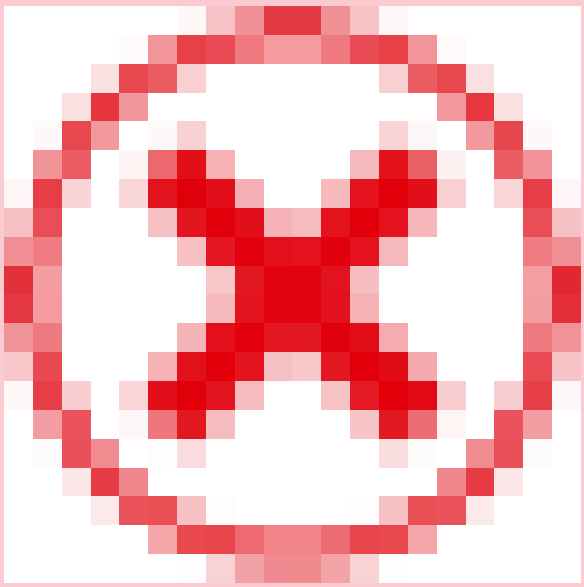
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Drittpartei |  |
| Administration | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

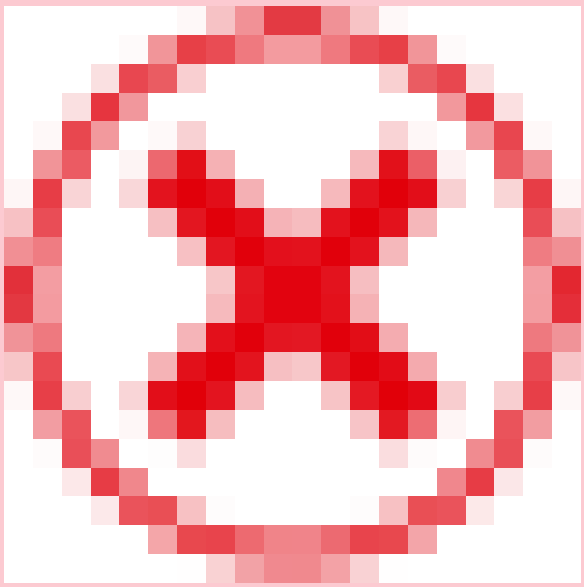
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Zuweisungsregeln |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

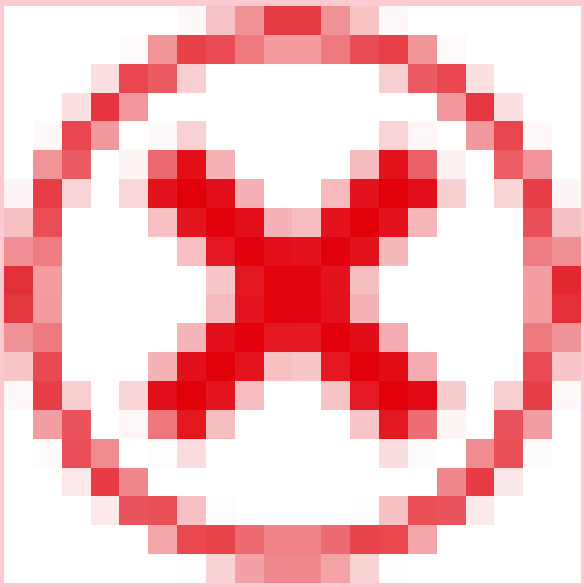
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Sicherheitsrisiko-Rechner |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

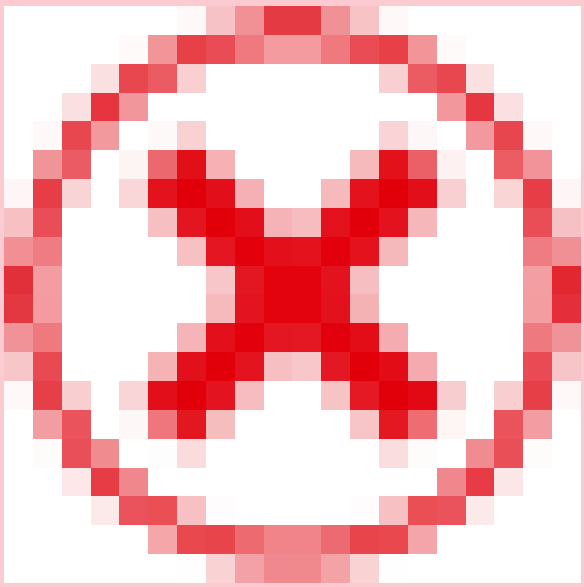
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Nachbesserungszielregeln |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

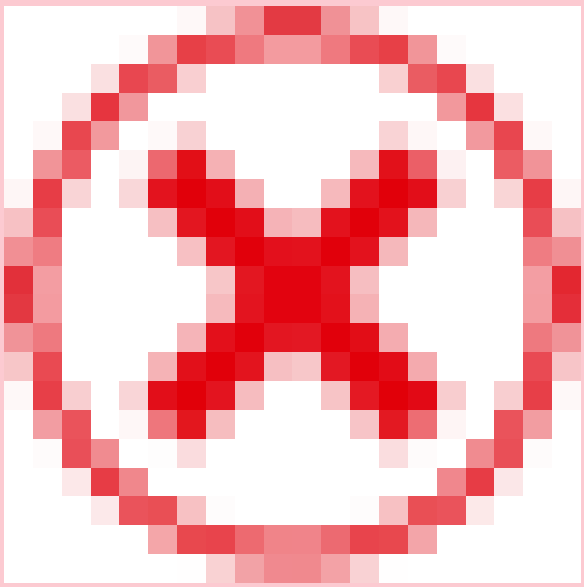
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| VI-Granularität konfigurieren |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

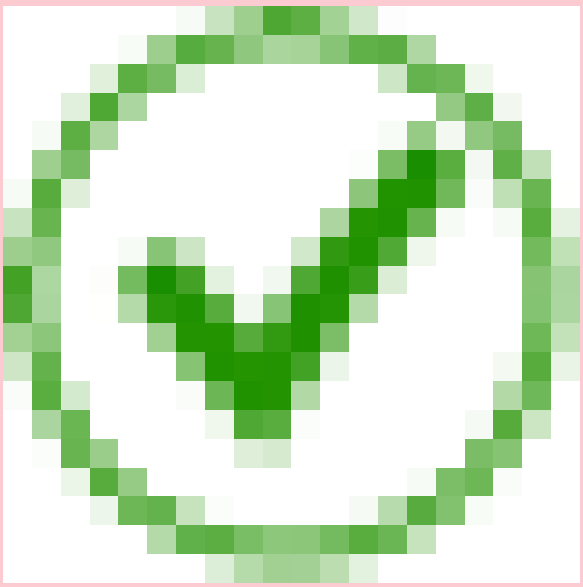
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Ausnahmeregeln |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

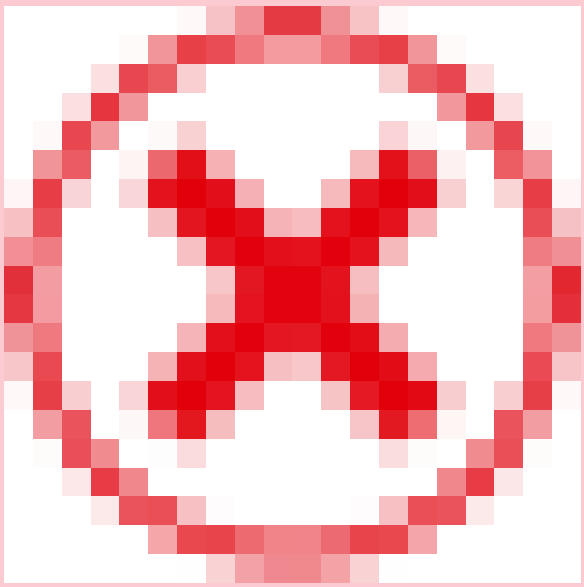
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Genehmigungsregeln |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

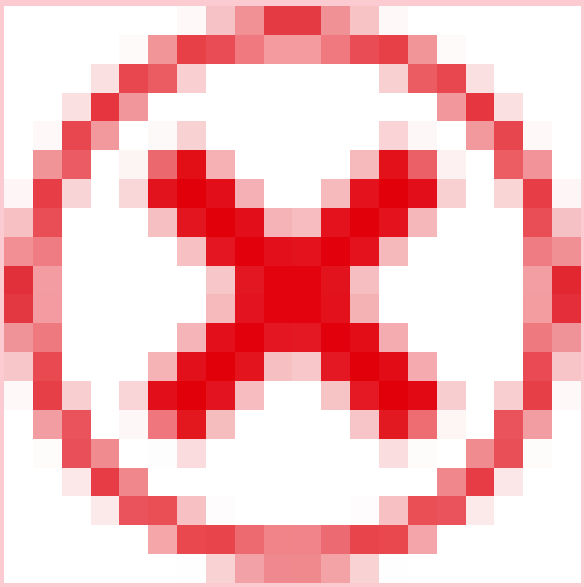
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
| --- | --- |
| Container-Sicherheitsintegrationen |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

***Informationen für andere Rollen:***

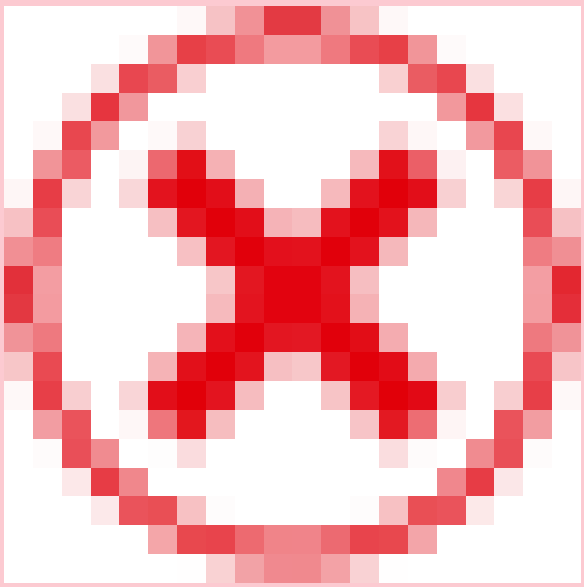
***sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity***

***sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules***

***sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules***

***sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned***

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
| --- | --- |
| Angreifbare Elemente automatisch schließen |  |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul_container.read_auto_exception_rule**

*Informationen für andere Rollen:*

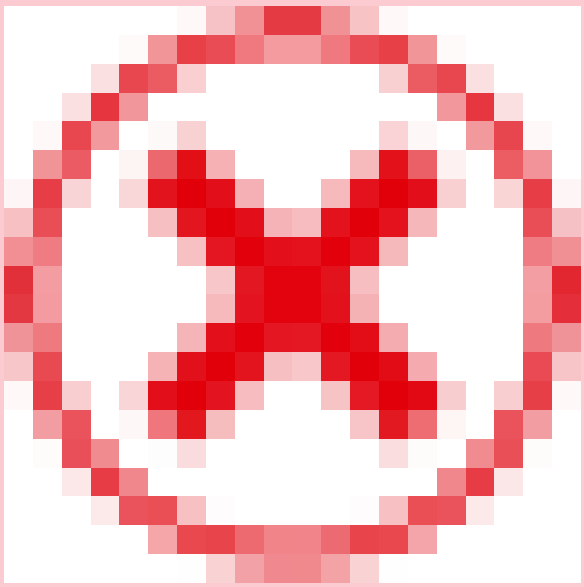
*sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity*

*sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules*

*sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules*

*sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned*

**(Fortsetzung)**

| Modul | sn_vul_container.read_auto_exception_rule |
|---|---|
| Normalisierte Schweregradzuordnungen |  |

[End]

[store-future: BEGIN review]

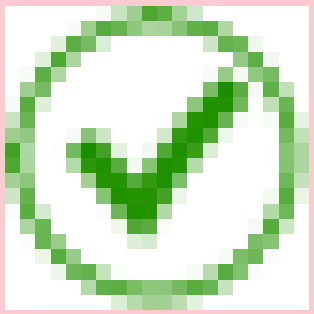
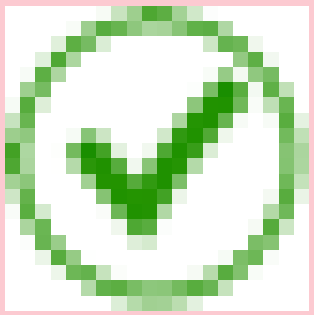
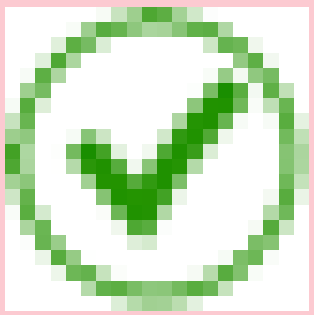
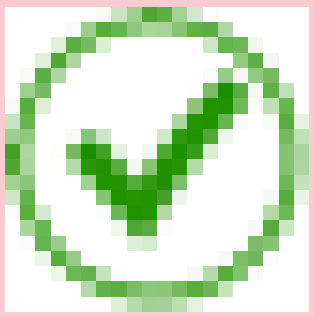
## Modulzugriff nach Rolle für DLP-Administration

Informationen zur DLP-Administration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_dlir.analyst |
|---|---|
| (Haupt-App-Gruppe) | |

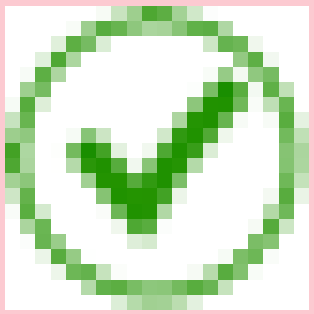
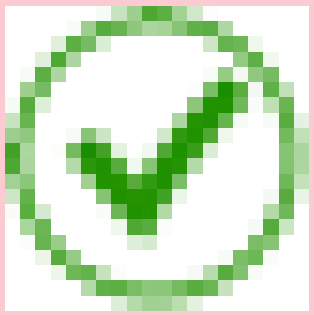
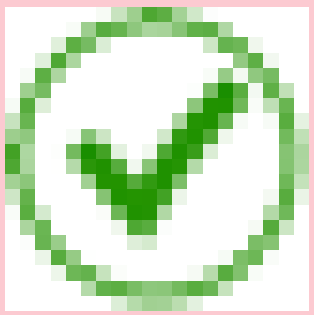
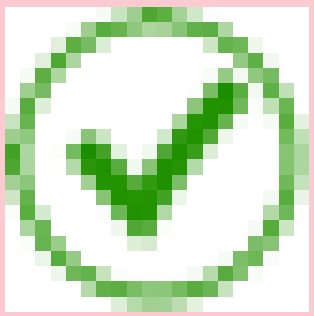


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_dlir.analyst |
| --- | --- |
| Standardkonfiguration | |
| Zuweisungsregeln |  |
| Regeln für Antwortfälligkeitsdatum |  |
| E-Mail-Vorlagen |  |
| Bewertungen |  |

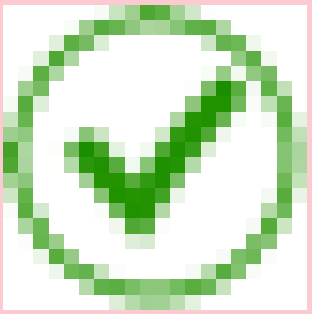
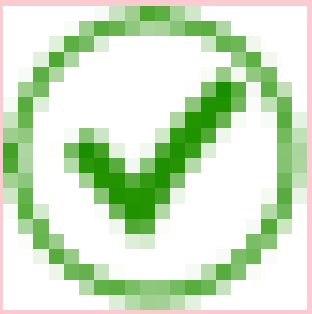
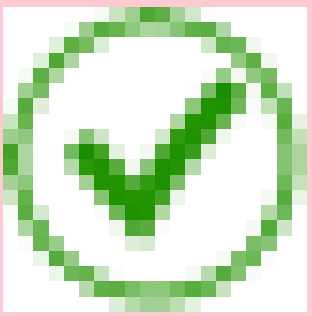
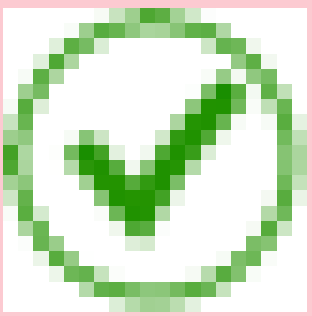
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_dlir.analyst |
| --- | --- |
| Optionen für die Reaktion auf Incidents | |
| Konfiguration des Altersdiagramms |  |
| Delegierten-Konfiguration |  |
| Benutzerdefinierte Status |  |
| Wiederholte Vergehen-Identifizierungsregeln |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_dlir.analyst |
| --- | --- |
| Benutzerdefinierte Felder |  |
| Erweiterte Einstellungen |  |
| Incident-Zugriffsbeschränkungen | |
| Einschränkungen auf Datensatzebene |  |
| Einschränkungen auf Feldebene |  |

[End]

[store-future: BEGIN review]

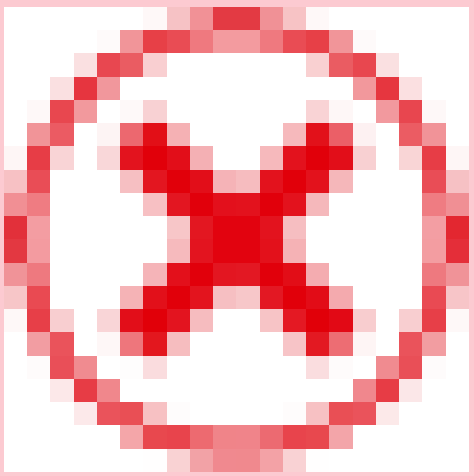
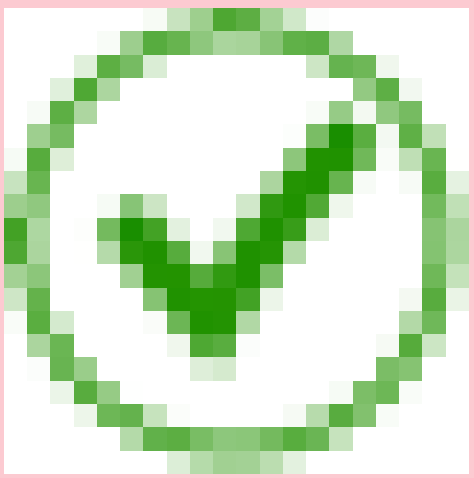
## Modulzugriff nach Rolle für DLP Incident Management

Informationen zu DLP Incident Management finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_dlir.analyst |
| --- | --- |
| (Haupt-App-Gruppe) | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_dlir.analyst |
| --- | --- |
| DLP Ops-Portal | |
| DLP-Endbenutzerportal |  |
| DLP-Dashboard |  |

[End]

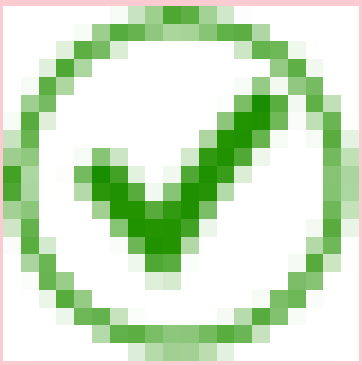
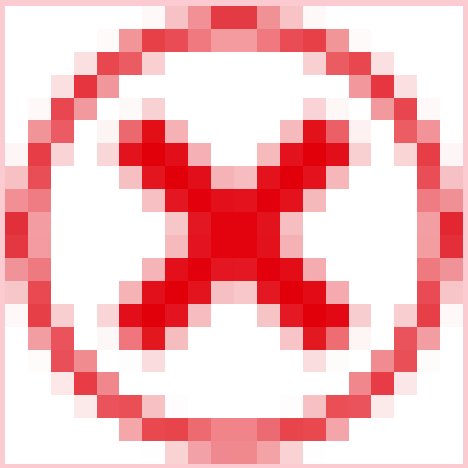
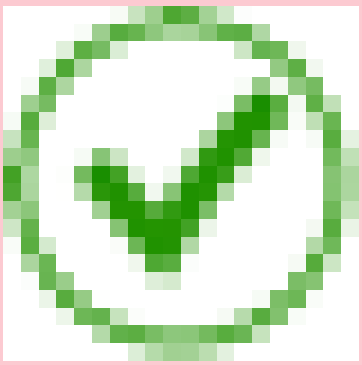
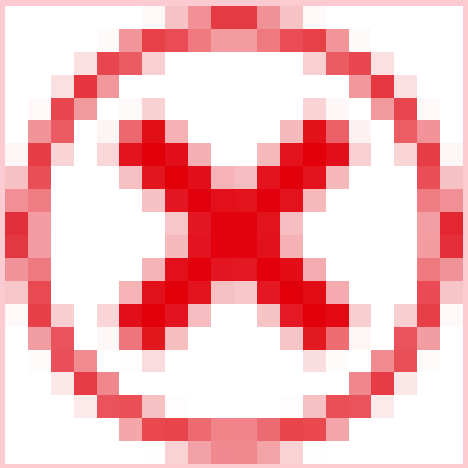
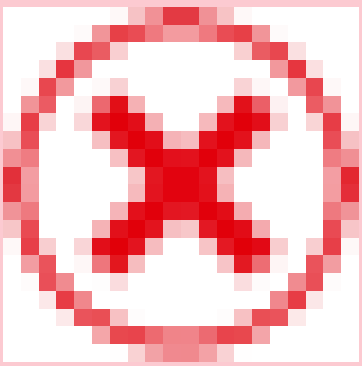
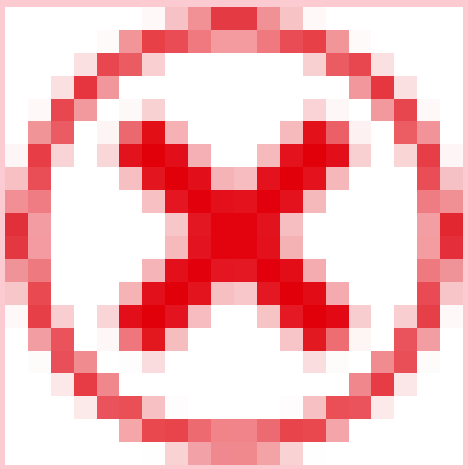
[store-future: BEGIN review]

## Modulzugriff nach Rolle für Datenzertifizierung

Informationen zur Datenzertifizierung finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

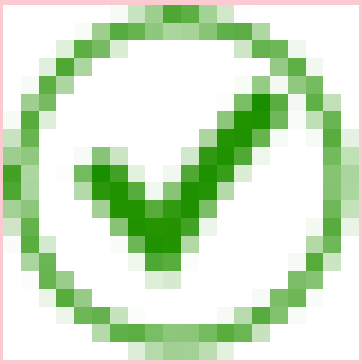
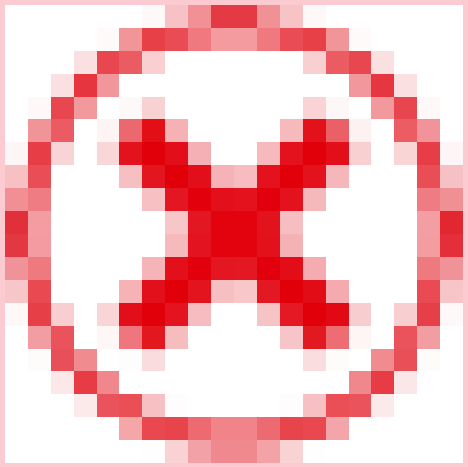
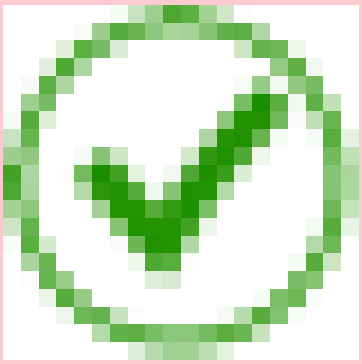
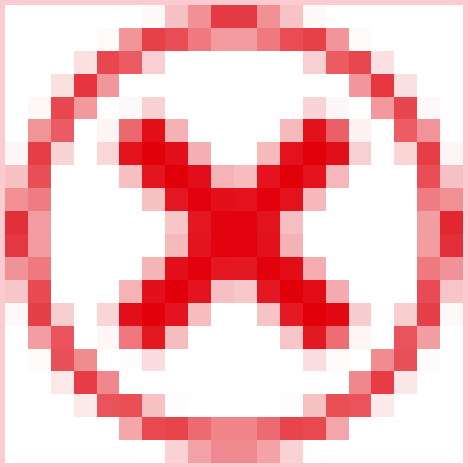
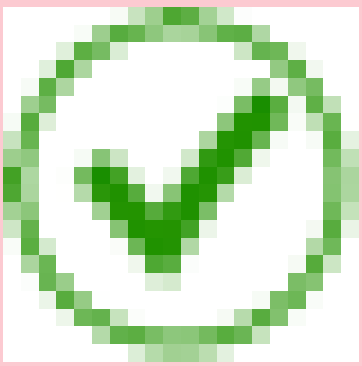
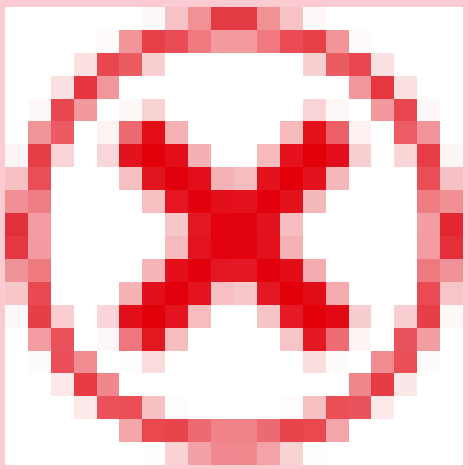
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | certification_admin | certification_filter_admin |
| --- | --- | --- |
| (Haupt-App-Gruppe) | | |
| Übersicht |  |  |
| Erste Schritte |  |  |
| Aufgaben | | |
| Meine Aufgaben |  |  |

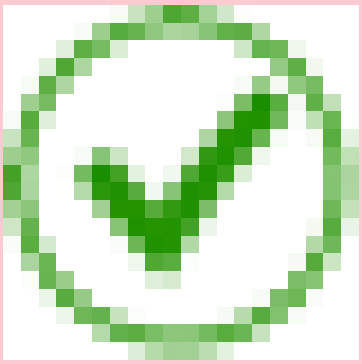
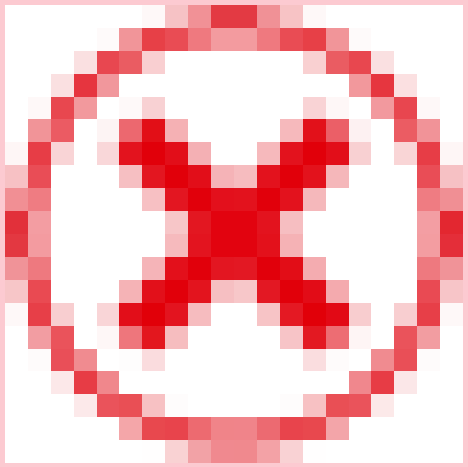
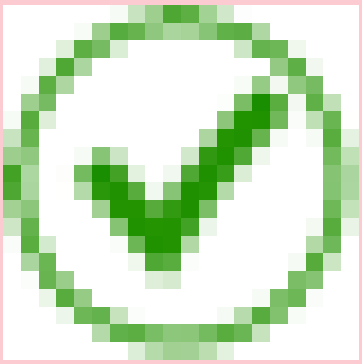
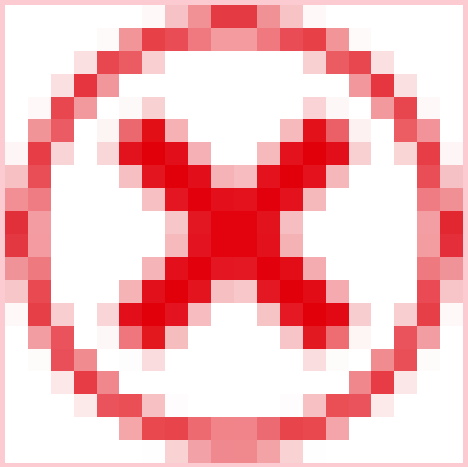
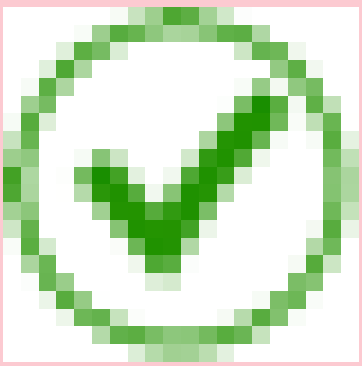
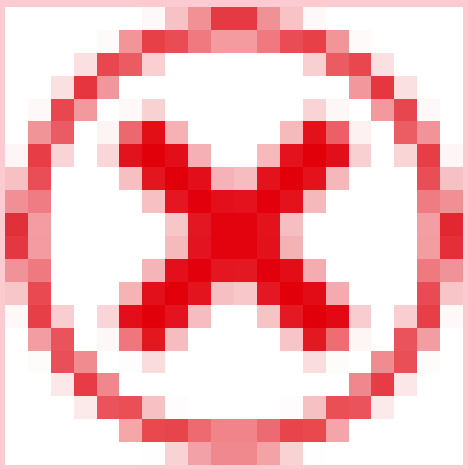
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | certification_admin | certification_filter_admin |
| --- | --- | --- |
| Offen |  |  |
| Alle Aufgaben |  |  |
| Zertifizierungen | | |
| Zertifiziert |  |  |

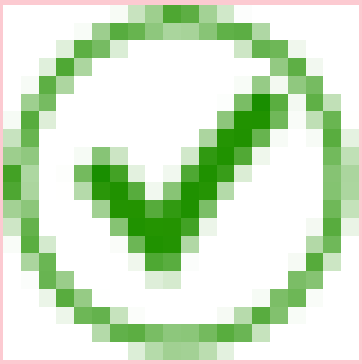
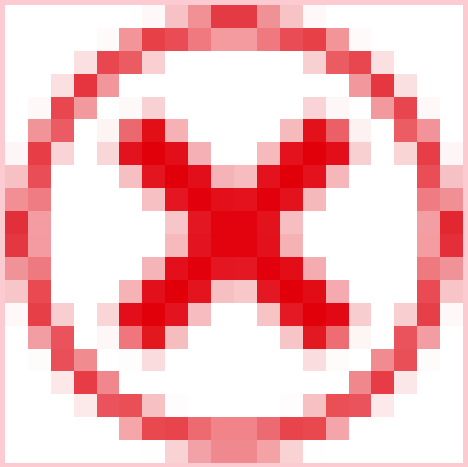
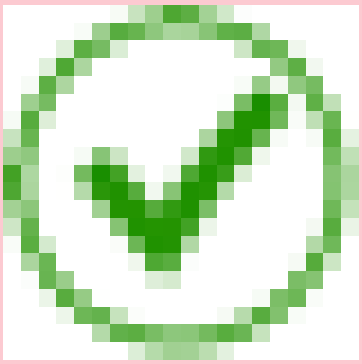
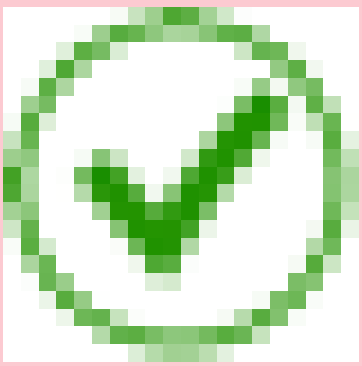
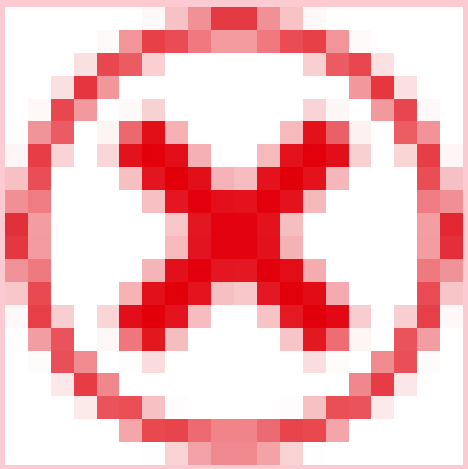
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | certification_admin | certification_filter_admin |
| --- | --- | --- |
| Ausstehend |  |  |
| Alle |  |  |
| Zeitpläne | | |
| Neu erstellen |  |  |

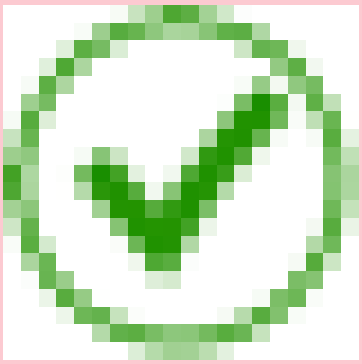
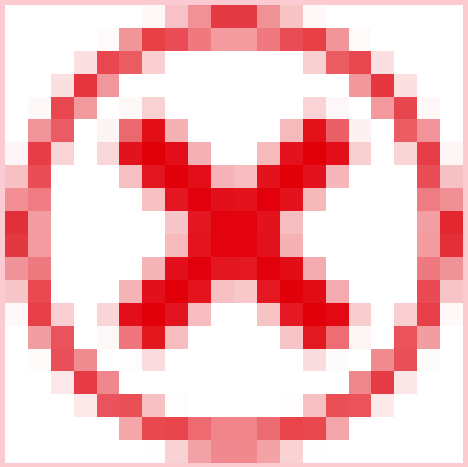
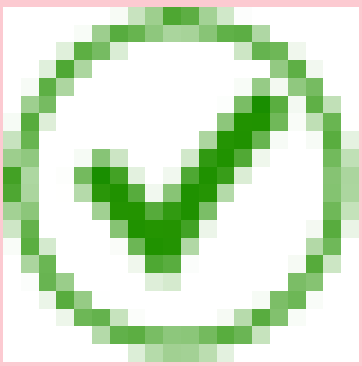
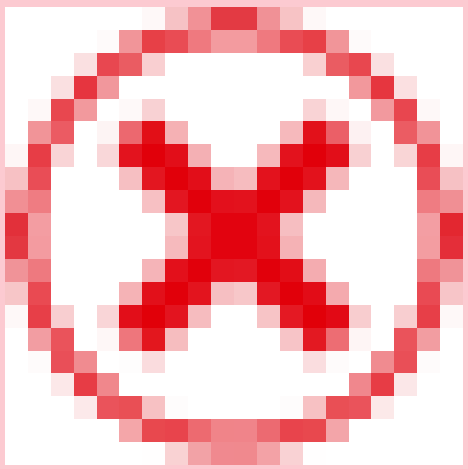
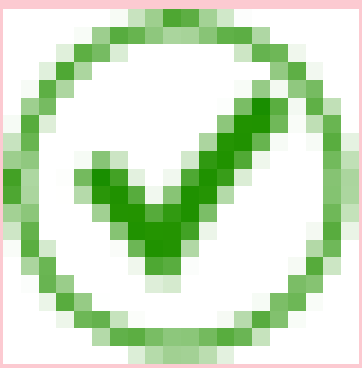
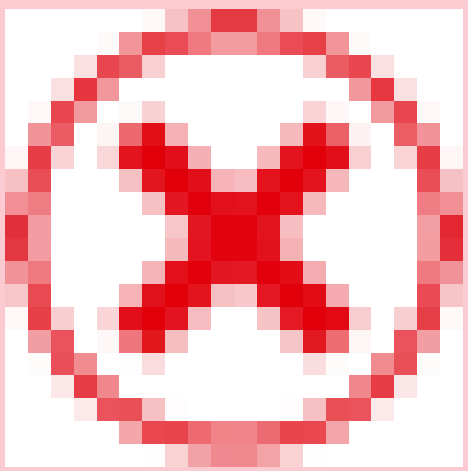
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | certification_admin | certification_filter_admin |
| --- | --- | --- |
| Plandefinitionen |  |  |
| Zertifizierungsfilter |  | |
| Instanzen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | certification_admin | certification_filter_admin |
| --- | --- | --- |
| Audit-Ergebnisse |  |  |
| Audits | | |
| Auditdefinitionen |  |  |
| Auditinstanzen |  |  |

[End]

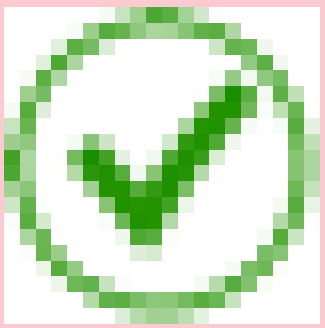
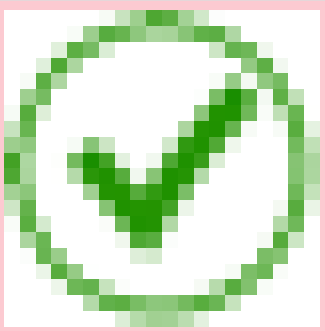
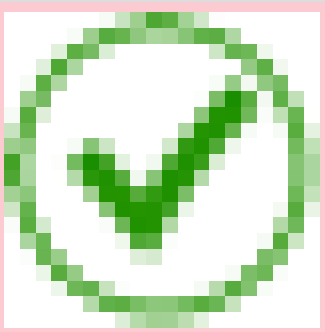
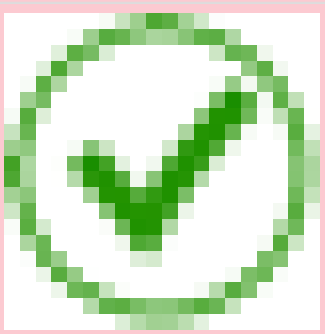
[store-future: BEGIN review]

## Modulzugriff nach Rolle für IBM QRadar-Integration

Informationen zur IBM QRadar-Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.analyst |
| --- | --- |
| (Haupt-App-Gruppe) | |
| IBM QRadar-Profil | |
| IBM QRadar-Offense-Import |  |
| IBM QRadar – Vergehen zu Aufgabe |  |
| IBM QRadar-Feldübersetzung |  |
| IBM QRadar-Integrationseinstellungen |  |

Automatische Übersetzung

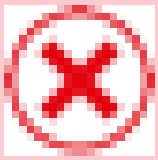
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für die MISP-Integration

Informationen zur MISP-Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_si.admin | sn_si.analyst | sn_ti.admin | sn_ti.read | sn_ti.write |
|---|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | | |
| Integrationseinstellungen | | | | | |
| Sichtungssuche: Konfiguration | |  | | | |
| Profile für die automatische Erstellung von Ereignissen | | | | | |
| Warteschlange für automatische Ereigniserstellung | | | | | |
| MISP-Ereignis-Daten | | | | | |
| Zugeordnete MISP-Ereignisse | | | | | |
| MISP-Anwenderinformationen | | | | | |

[End]

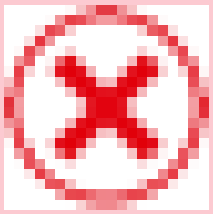
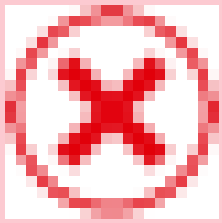
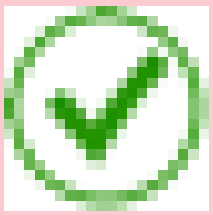
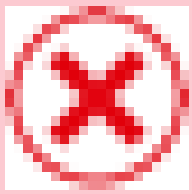
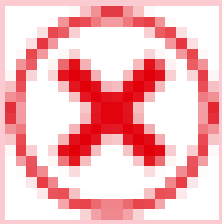
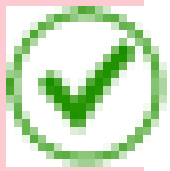
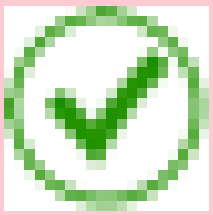
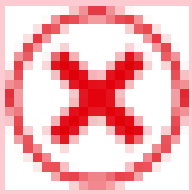
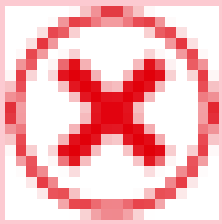
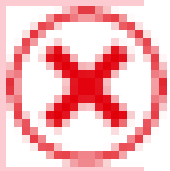
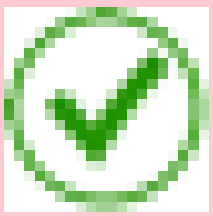
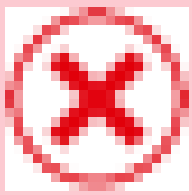
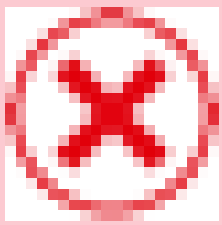
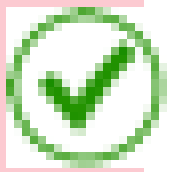
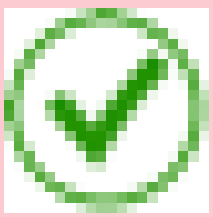
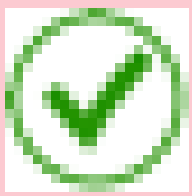
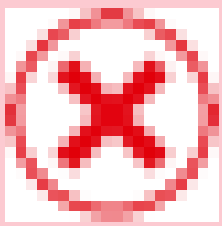
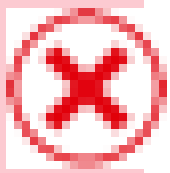
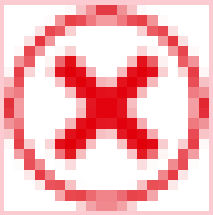
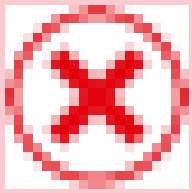
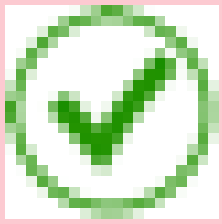
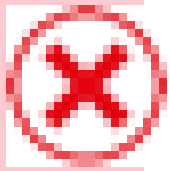
[store-future: BEGIN review]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

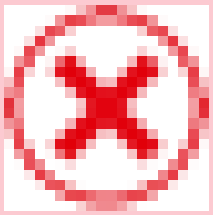
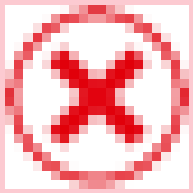
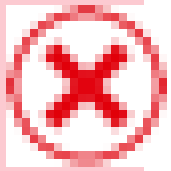
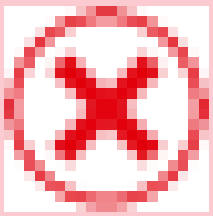
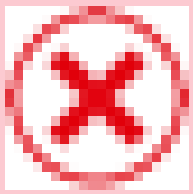
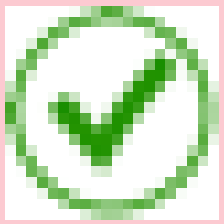
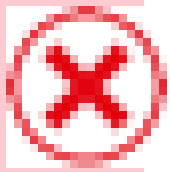
## Modulzugriff nach Rolle für Microsoft Azure Defender for IoT

Für Microsoft Azure Defender for IoT finden Sie die Menüelemente, auf die eine bestimmte Rolle zugreifen kann.

| Modul | cmdb_inst_admin | cmdb_ot_admin | connection_admin | import_admin |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |
| Setup |  | |  | |
| Datenquellen |  |  |  |  |
| IntegrationHub ETL |  |  |  |  |
| Zeitpläne importieren |  |  |  |  |
| Eigenschaften |  |  |  |  |
| Verbindungen und Anmeldeinformationen | | | | |
| Aliasse für Verbindungsanmeldeinformationen |  |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

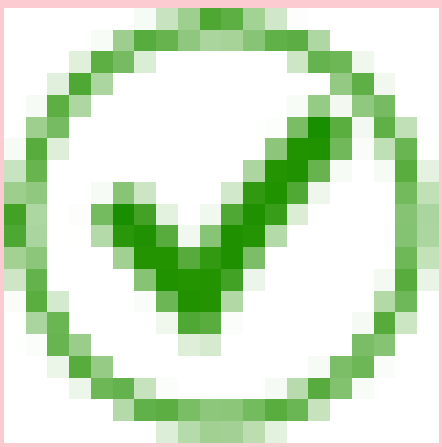
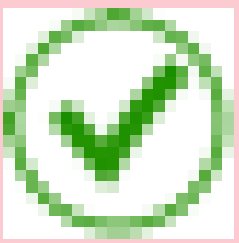
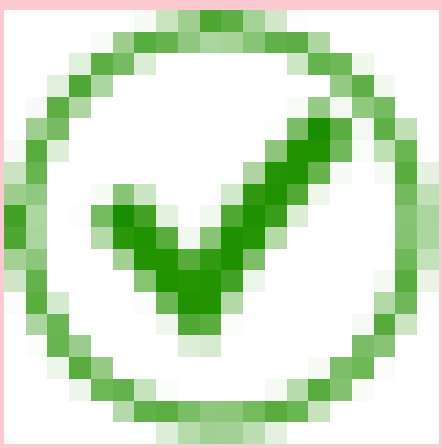
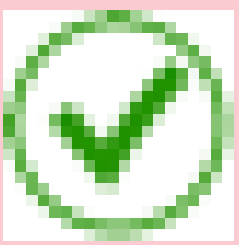
| Modul | cmdb_inst_admin | cmdb_ot_admin | connection_admin | import_admin |
|---|---|---|---|---|
| Berechtigungen |  |  | |  |
| Verbindungen |  |  |  |  |

[End]

[store-future: BEGIN review]

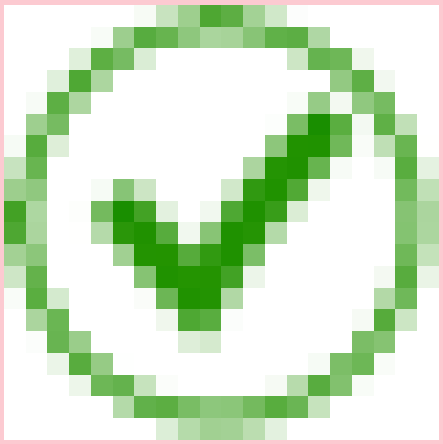
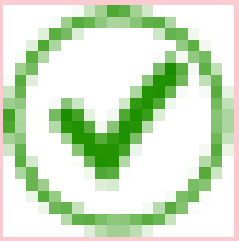
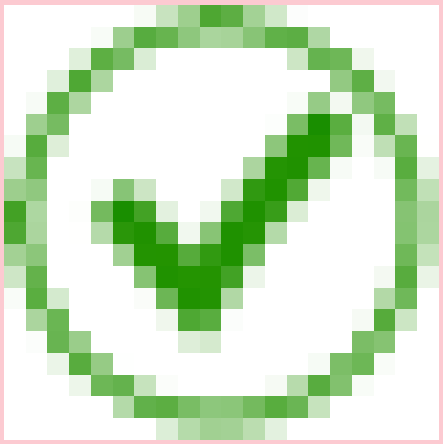
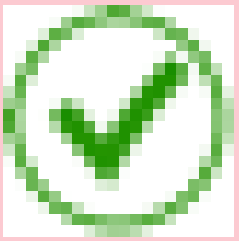
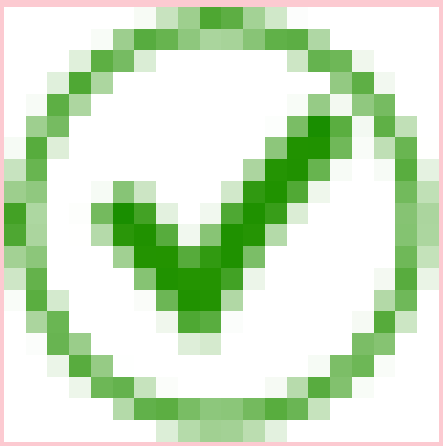
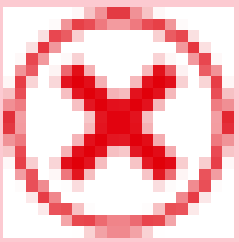
## Modulzugriff nach Rolle für Qualys Vulnerability Integration

Informationen zur Qualys Vulnerability-Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_vul.configure_qualys_integration | sn_vul_qualys.read |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| Übersicht |  |  |
| Status der Integrationsausführung |  |  |

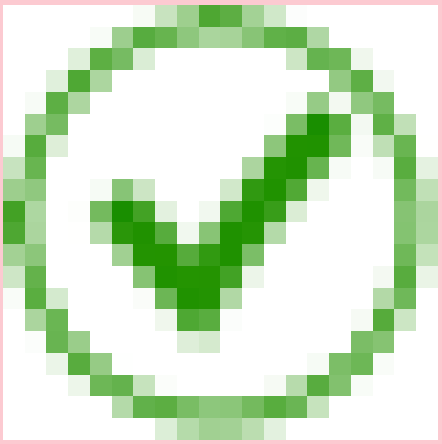
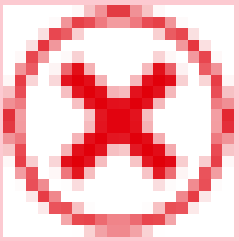
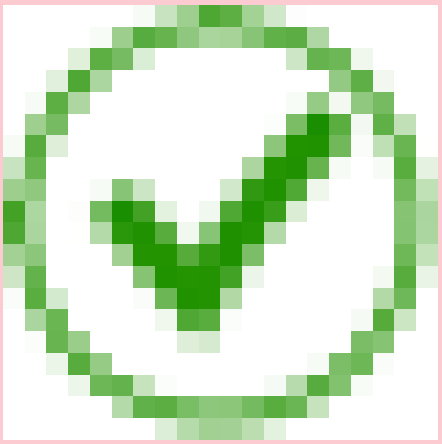
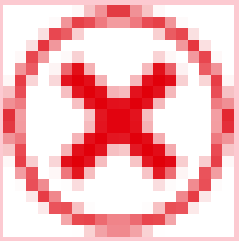
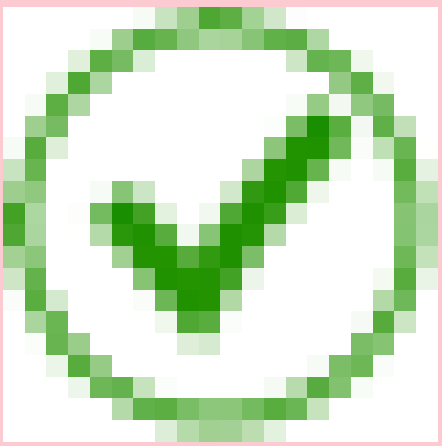
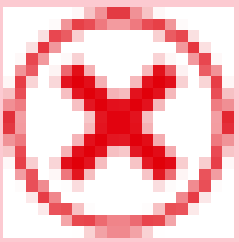
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_vul.configure_qualys_integration | sn_vul_qualys.read |
| --- | --- | --- |
| Scannergeräte |  |  |
| Suchlisten |  |  |
| Administration | | |
| Integrationsinstanzen |  |  |

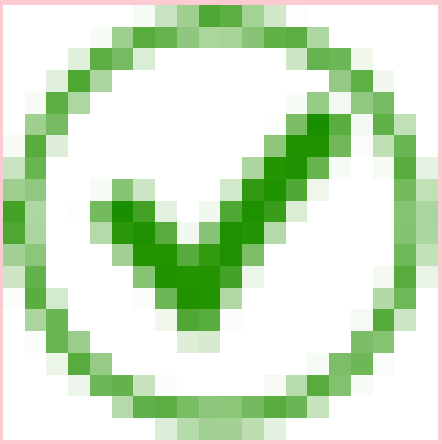
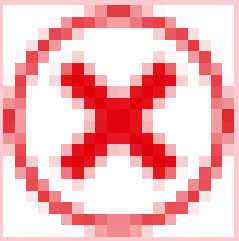
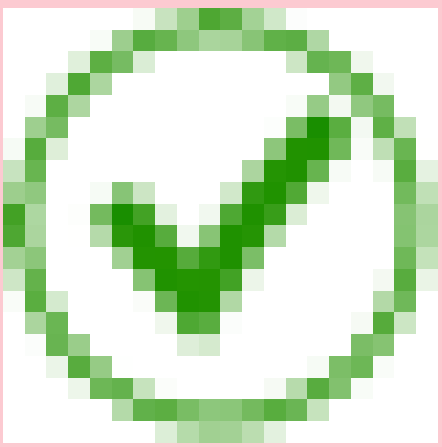
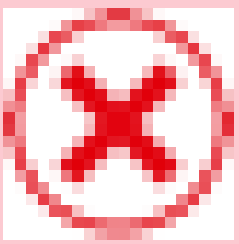
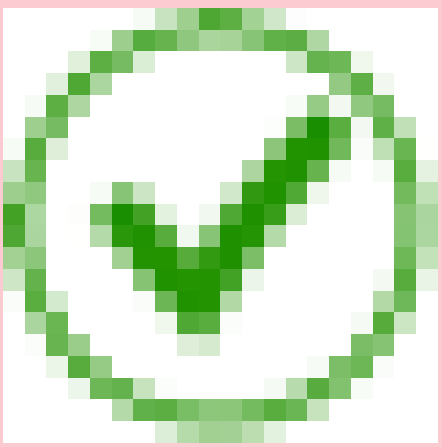
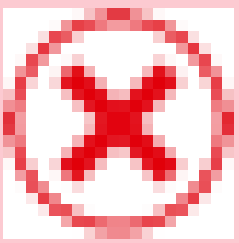
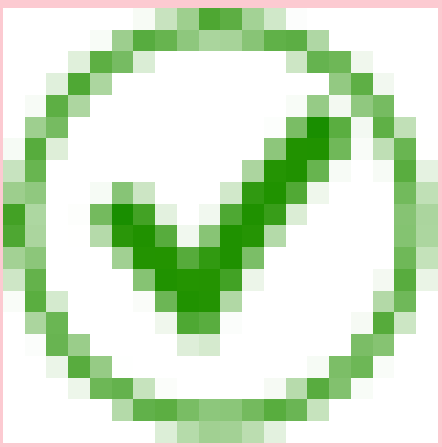
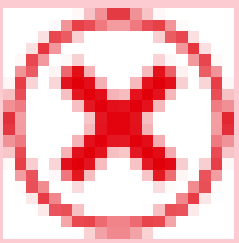
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_vul.configure_qualys_integration | sn_vul_qualys.read |
| --- | --- | --- |
| Primäre Integrationen |  |  |
| Unterstützende Integrationen |  |  |
| Importsatztabellen | | |
| Host-Import |  |  |

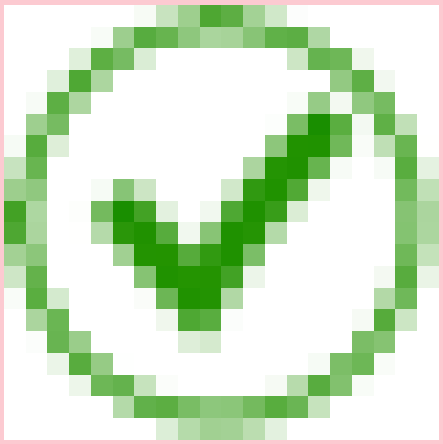
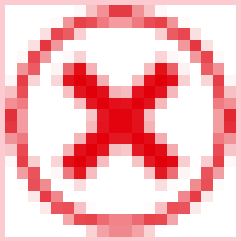
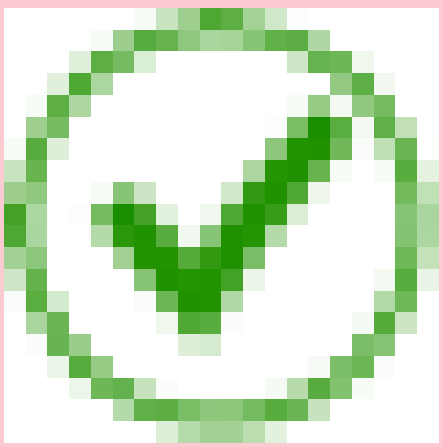
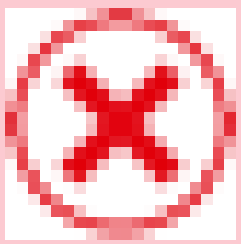
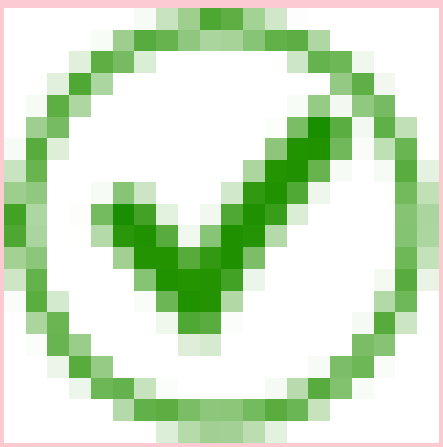
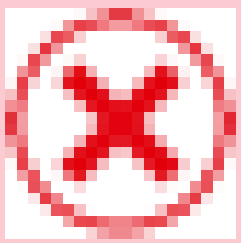
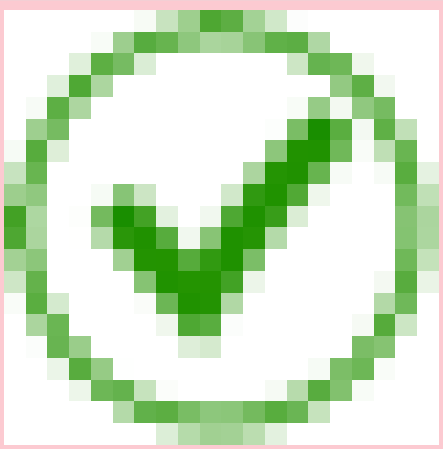
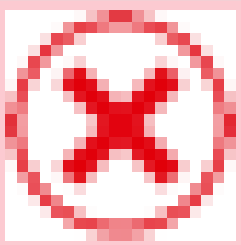
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_vul.configure_qualys_integration | sn_vul_qualys.read |
| --- | --- | --- |
| Import der Host-Erkennungsliste |  |  |
| Wissensdatenbankimport |  |  |
| Ticket-Listenimport |  |  |
| Import dynamische Suchliste |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_vul.configure_qualys_integration | sn_vul_qualys.read |
| --- | --- | --- |
| Import statische Suchliste |  |  |
| Assetgruppenimport |  |  |
| Appliance-Import |  |  |
| Import der Host-Erkennungsnummerierung |  |  |

Automatische Übersetzung

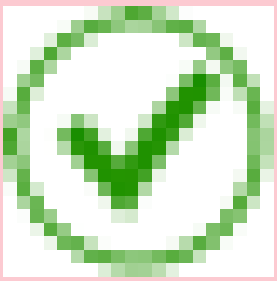
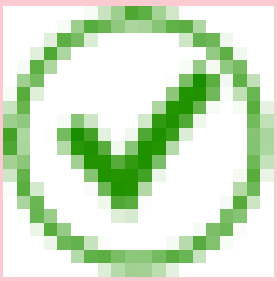
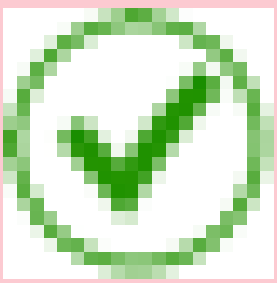
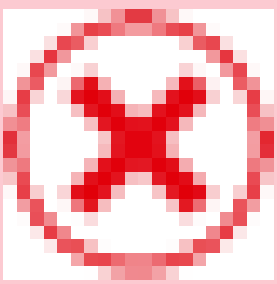
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

[store-future: BEGIN review]

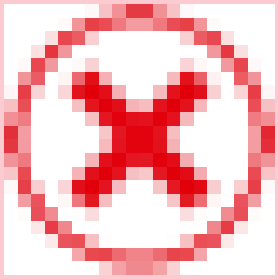
## Modulzugriff nach Rolle für Rapid7 Vulnerability Integration

Informationen zu Rapid7 Vulnerability Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_vul_r7.admin | sn_vul_r7.read |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| Status der Integrationsausführung | |  |
| Sites | |  |
| Lösungen | |  |
| Administration | | |
| Integrationen | |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_vul_r7.admin | sn_vul_r7.read |
|---|---|---|
| Konfiguration | |  |

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Security Incident

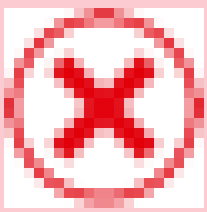
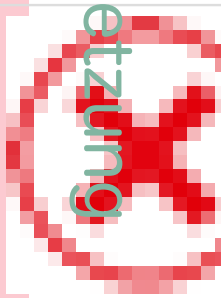
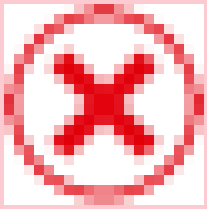
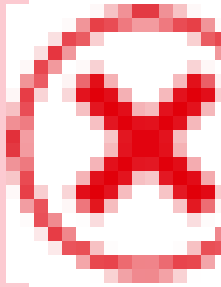
Informationen zu Security Incident finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

### Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | | | |
| Incidents Neue UI |  | | | | |  |
| Serviceeinfluss |  | | | | |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Übersicht | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Echtzeit | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Incidents | | | | | | |
| Für mich sichtbar | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Mir zugewiesen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Meine Arbeit | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Dem Team zugewiesen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Offene Incidents anzeigen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Alle Incidents anzeigen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Nicht zugewiesene Incidents | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |

Automatische Übersetzung

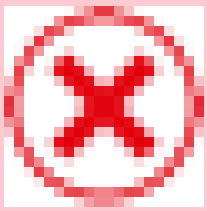
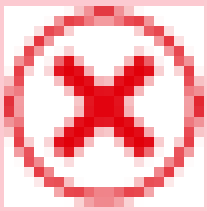
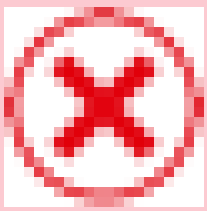
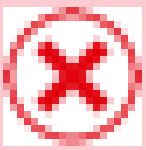
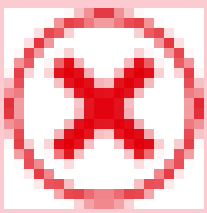
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Antwortaufgaben | | | | | | |
| Mir zugewiesen |  | | | | | |
| Dem Team zugewiesen |  | | | | | |
| Offene Aufgaben anzeigen |  | | | |  | |
| Alle Aufgaben anzeigen |  | | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Nicht zugewiesene Aufgaben | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Eingehende Anfragen | | | | | | |
| Mir zugewiesen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Dem Team zugewiesen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Meine Freigaben | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Offene Anforderungen anzeigen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Alle Anforderungen anzeigen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Nicht zugewiesene Anfragen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Meine Karte | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Warnungen und Ereignisse | | | | | | |
| Überprüfung nach Incident | | | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Meine ausstehenden Überprüfungen | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Ausstehende Teamüberprüfungen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Alle unvollständigen Überprüfungen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Setup | | | | | | |
| Security Incident-Rechnergruppen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

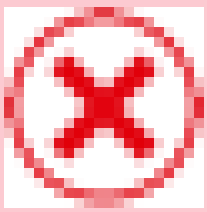
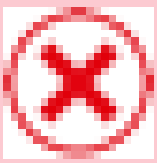
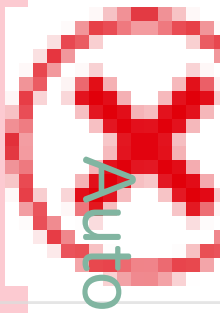
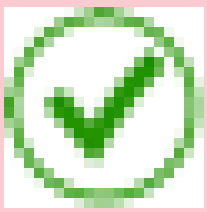
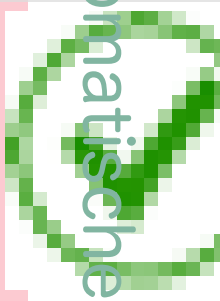
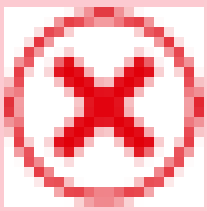
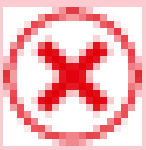
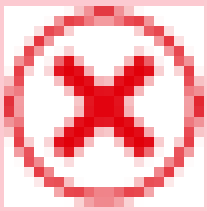
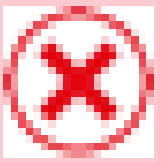
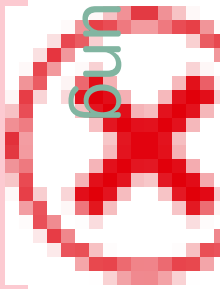
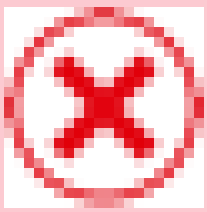
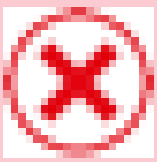
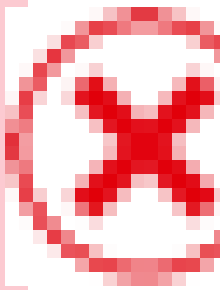
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Schweregradsrechner |  | |  | | |  |
| Risikopunktzahlkonfiguration |  | | | | |  |
| Nachrichtenfeed-Konfiguration |  | | | |  | |
| Gruppen |  | |  | | |  |
| Rollen |  | |  | | |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| SLAs | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Setup von Analyst Workspace (neue UI) | | | | | | |
| Setup-Assistent | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Konfiguration der Zielseitenfilter | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| UI-Aktionen für Formulare | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

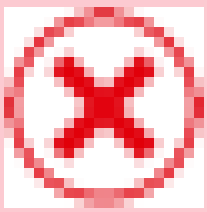
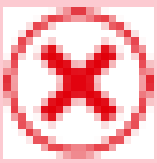
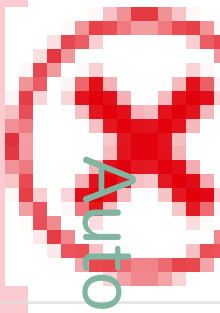
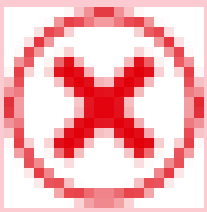
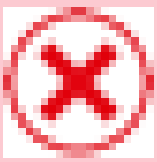
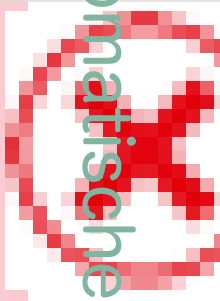
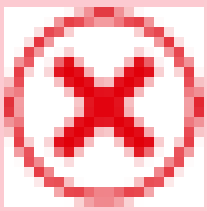
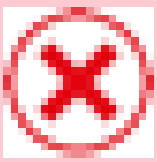
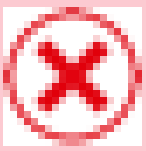
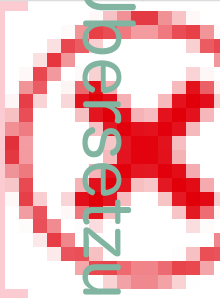
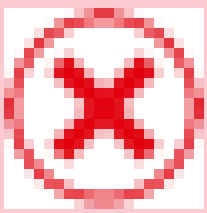
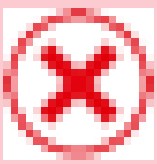
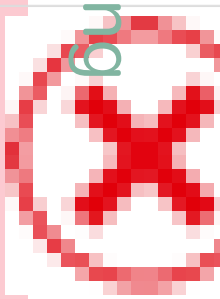
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Konfiguration zugehöriger Listen |  | |  | | |  |
| Eigenschaften des Analystenarbeitsbereichs |  | |  | | |  |
| Katalog & Wissen | | | | | | |
| Vorlagen für Security Incidents |  | |  | |  |  |
| Katalogelemente pflegen |  | |  | | |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Wissen | ✗ | ✓ | ✗ | ✗ | ✗ | |
| Manuelles Runbook | | | | | | |
| Neues Runbook erstellen | ✗ | ✓ | ✗ | ✗ | ✗ | |
| Zeigen Sie Runbook-Dokumente an | ✗ | ✓ | ✗ | ✗ | ✗ | |
| Administration | | | | | | |
| Eigenschaften | ✗ | ✓ | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Konfiguration | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Benachrichtigungen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Servicerelevanz-Berichterstellungsdefinition | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Servicerelevanzdefinition | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Serviceeinfluss-Definitionen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Setup für Bewertungen nach Incident-Überprüfung | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Setup des Berichts zur Überprüfung nach Incidents | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Echtzeitdefinition | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Prozessauswahl | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Prozessdefinitionen | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

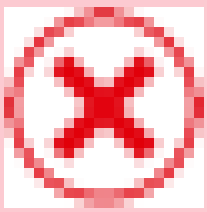
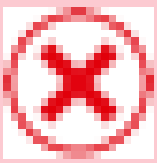
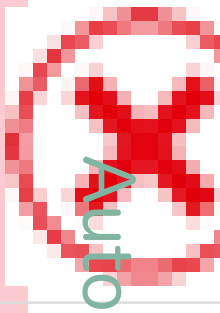
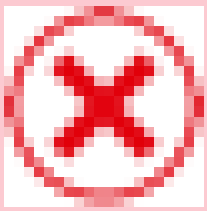
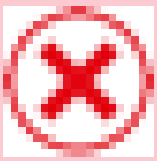
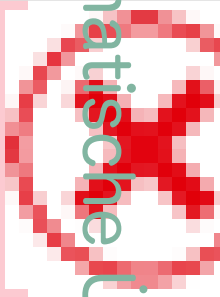
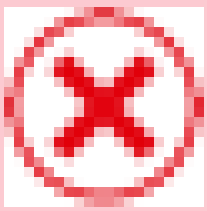
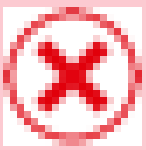
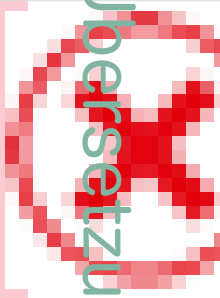
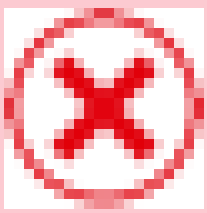
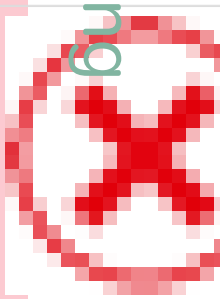
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read**

***Informationen für andere Rollen:***

***sn_si.special_access, sn_si_approver_user***

**(Fortsetzung)**

| Modul | sn_sec_cmn.read | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.extern | sn_si.knowledge_a |
|---|---|---|---|---|---|---|
| Vorlagenworkflow – Ergebnisauswertung |  | |  | | |  |
| Phishing-E-Mails | | | | | | |
| Lizenzverwaltung |  | |  | | |  |
| Phishing-E-Mail melden |  | | | |  |  |
| Alle Phishing-E-Mails anzeigen |  | | | | |  |

Automatische Übersetzung

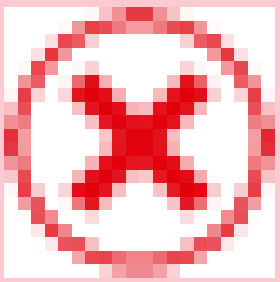
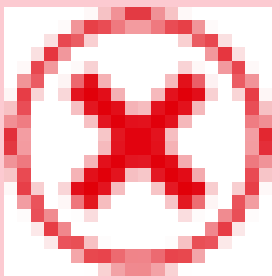
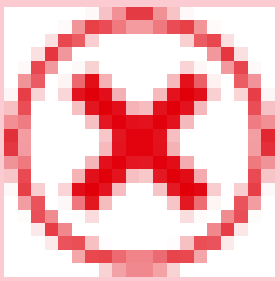
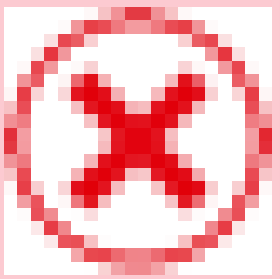
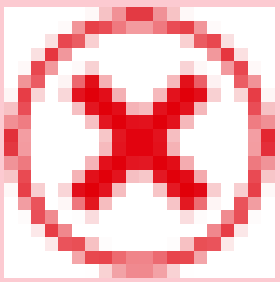
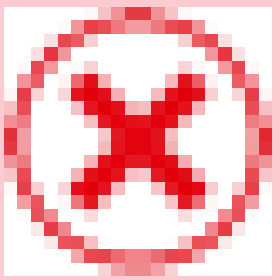
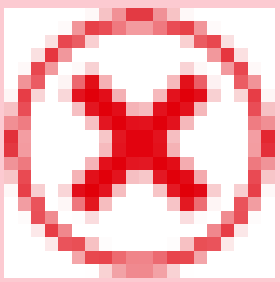
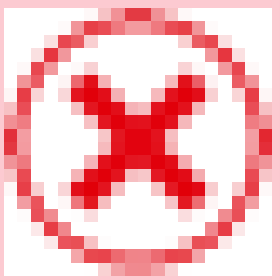
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_si.special_access, sn_si_approver_user

### Modulzugriff für: sn_si.special_access, sn_si_approver_user

*Informationen für andere Rollen:*

*sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read*

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| Incidents Neue UI |  |  |
| Serviceeinfluss |  |  |
| Übersicht |  |  |
| Echtzeit |  |  |
| Incidents | | |

Automatische Übersetzung

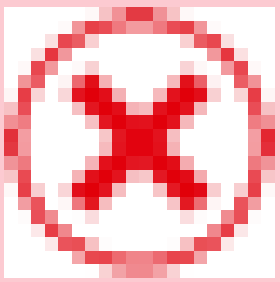
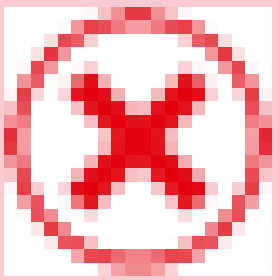
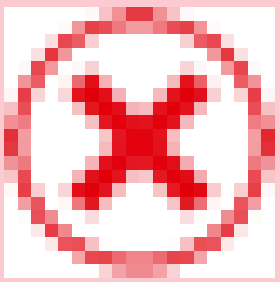
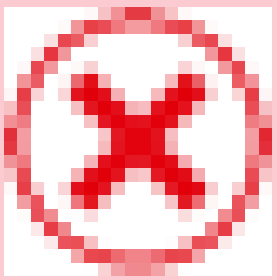
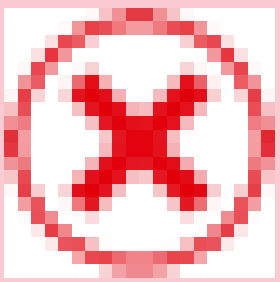
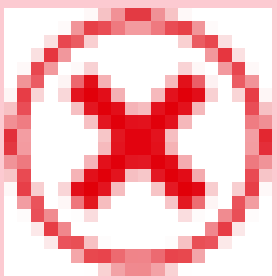
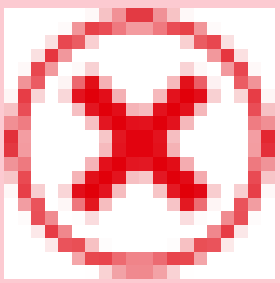
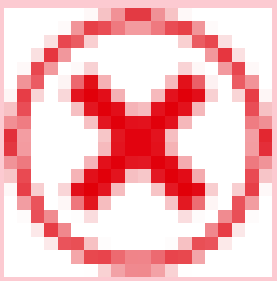
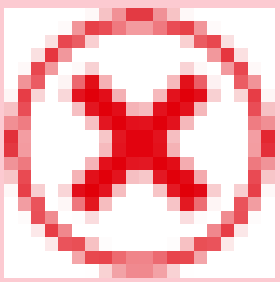
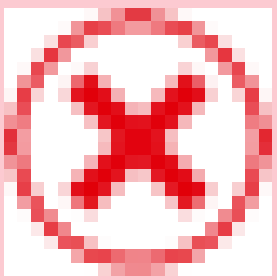
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Für mich sichtbar |  |  |
| Mir zugewiesen |  |  |
| Meine Arbeit |  |  |
| Dem Team zugewiesen |  |  |
| Offene Incidents anzeigen |  |  |

Automatische Übersetzung

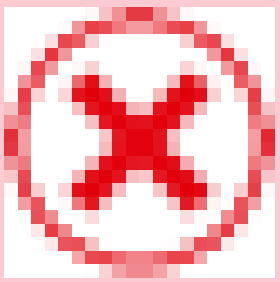
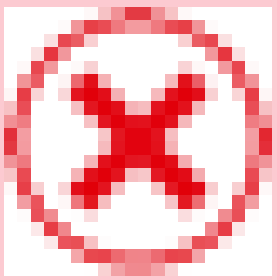
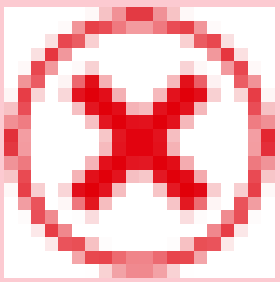
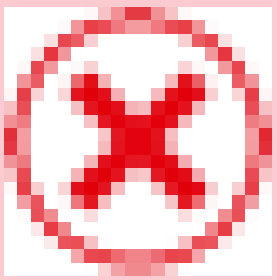
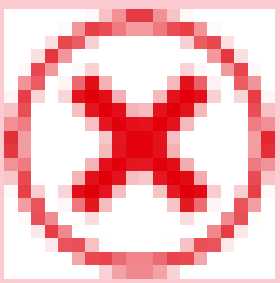
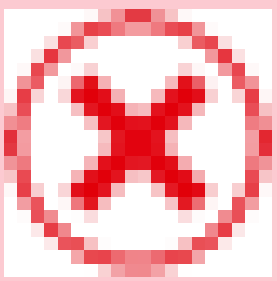
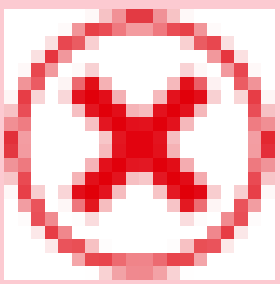
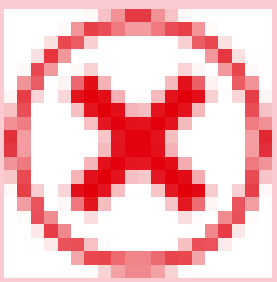
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Alle Incidents anzeigen |  |  |
| Nicht zugewiesene Incidents |  |  |
| Antwortaufgaben | | |
| Mir zugewiesen |  |  |
| Dem Team zugewiesen |  |  |

Automatische Übersetzung

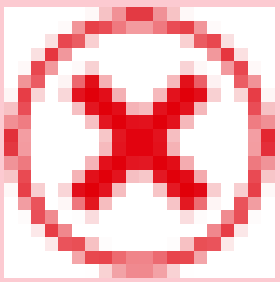
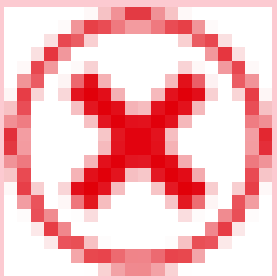
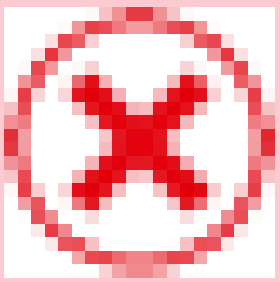
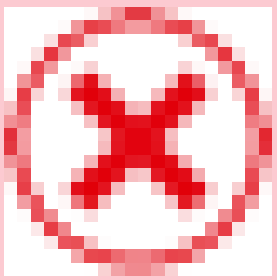
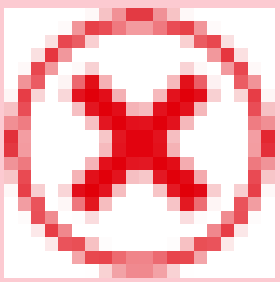
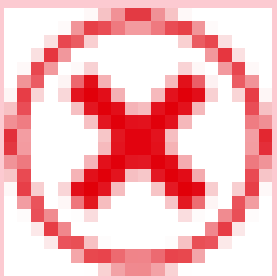
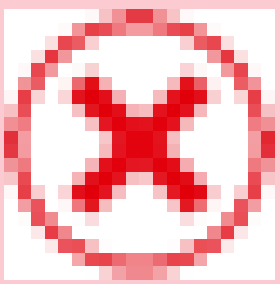
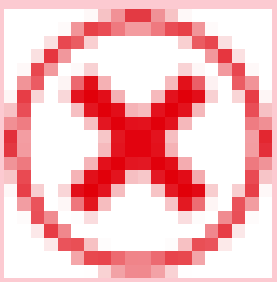
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Offene Aufgaben anzeigen |  |  |
| Alle Aufgaben anzeigen |  |  |
| Nicht zugewiesene Aufgaben |  |  |
| Eingehende Anfragen | | |
| Mir zugewiesen |  |  |

Automatische Übersetzung

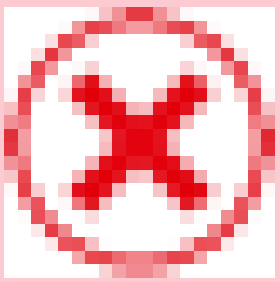
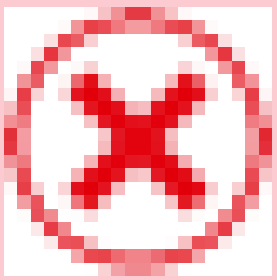
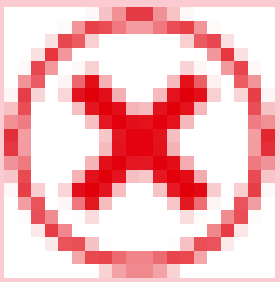
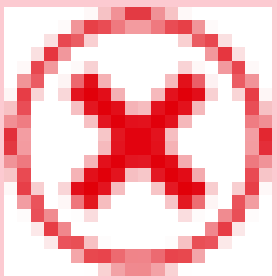
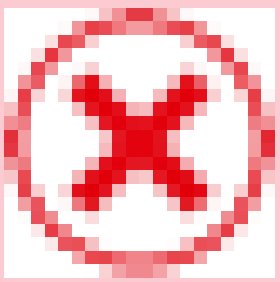
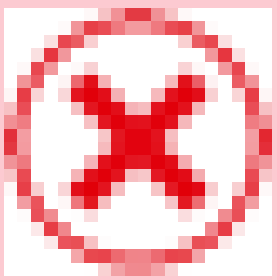
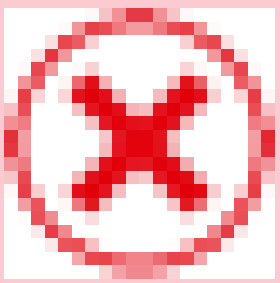
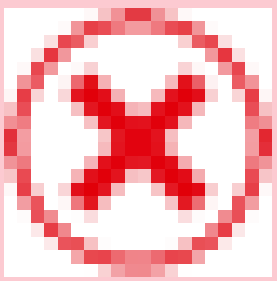
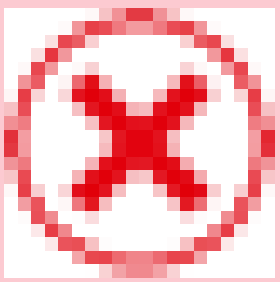
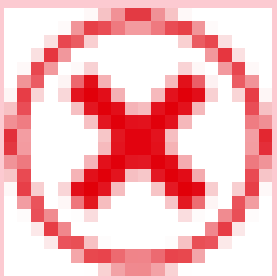
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Dem Team zugewiesen |  |  |
| Meine Freigaben |  |  |
| Offene Anforderungen anzeigen |  |  |
| Alle Anforderungen anzeigen |  |  |
| Nicht zugewiesene Anfragen |  |  |

Automatische Übersetzung

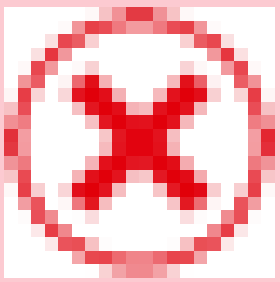
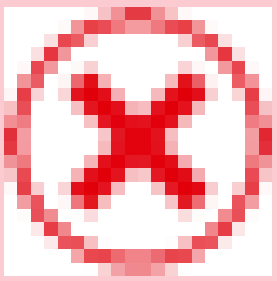
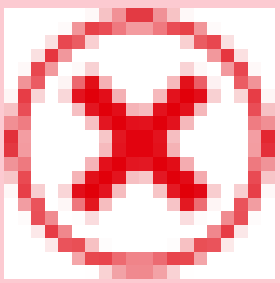
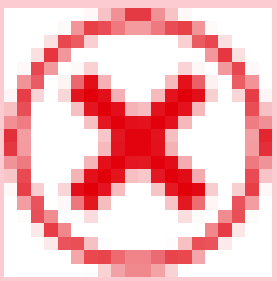
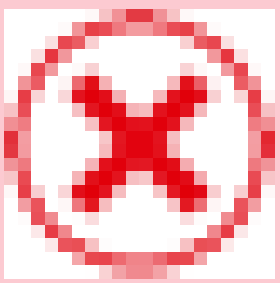
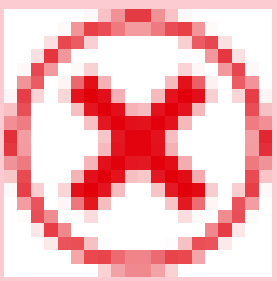
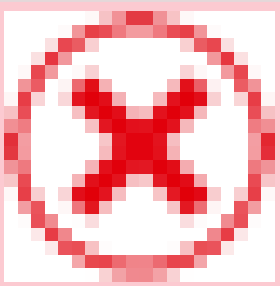
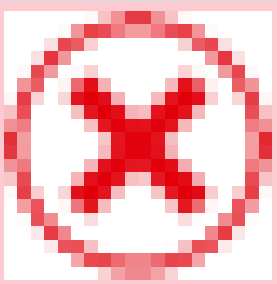
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Meine Karte |  |  |
| Warnungen und Ereignisse | | |
| Überprüfung nach Incident | | |
| Meine ausstehenden Überprüfungen |  |  |
| Ausstehende Teamüberprüfungen |  |  |
| Alle unvollständigen Überprüfungen |  |  |
| Setup | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Security Incident-Rechnergruppen | ✗ | ✗ |
| Schweregradsrechner | ✗ | ✗ |
| Risikopunktzahlkonfiguration | ✗ | ✗ |
| Nachrichtenfeed-Konfiguration | ✗ | ✗ |
| Gruppen | ✗ | ✗ |

Automatische Übersetzung

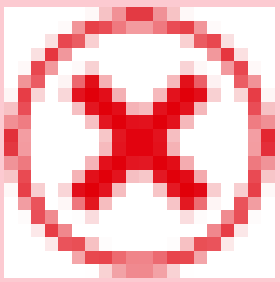
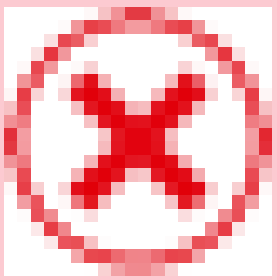
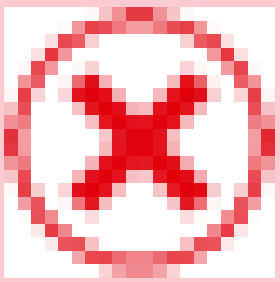
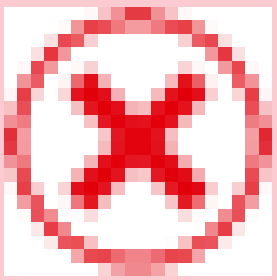
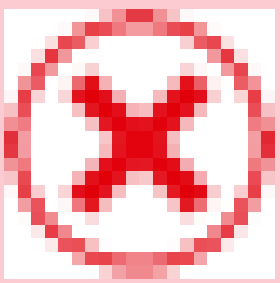
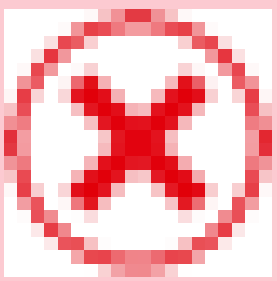
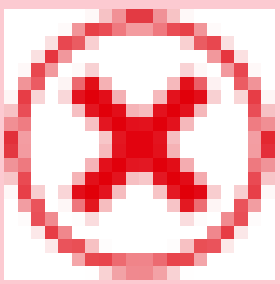
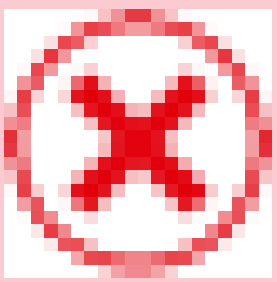
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Rollen |  |  |
| SLAs |  |  |
| Setup von Analyst Workspace (neue UI) | | |
| Setup-Assistent |  |  |
| Konfiguration der Zielseitenfilter |  |  |

Automatische Übersetzung

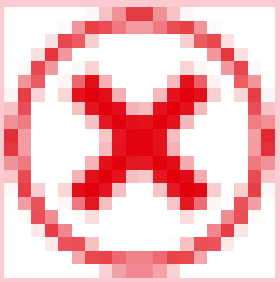
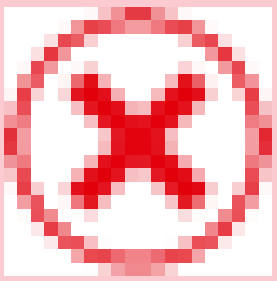
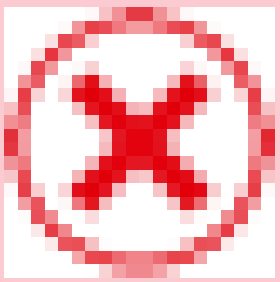
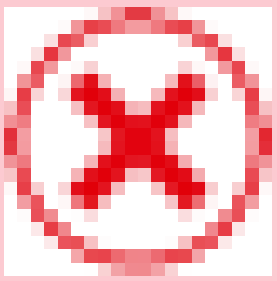
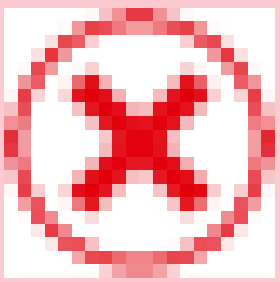
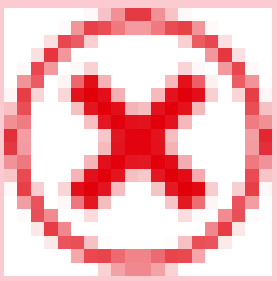
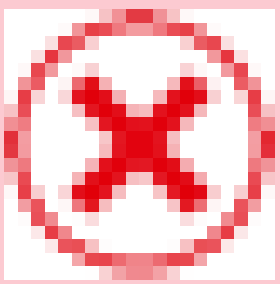
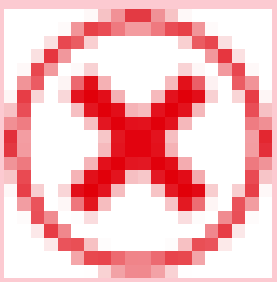
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| UI-Aktionen für Formulare |  |  |
| Konfiguration zugehöriger Listen |  |  |
| Eigenschaften des Analystenarbeitsbereichs |  |  |
| Katalog & Wissen | | |
| Vorlagen für Security Incidents |  |  |

Automatische Übersetzung

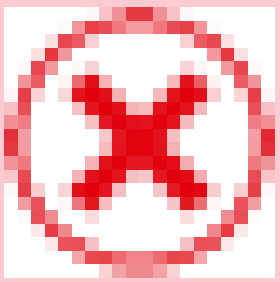
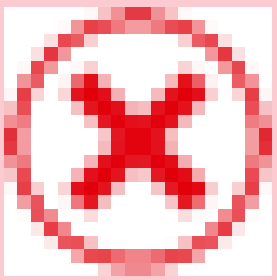
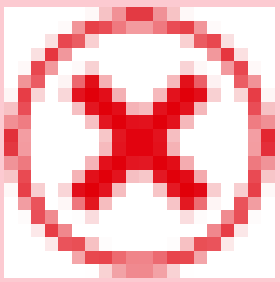
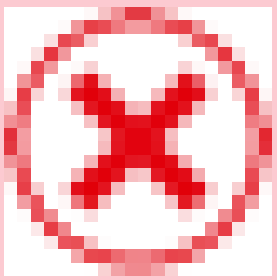
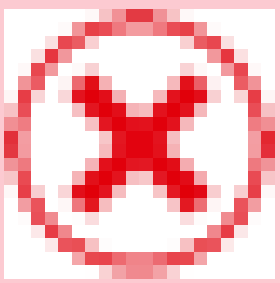
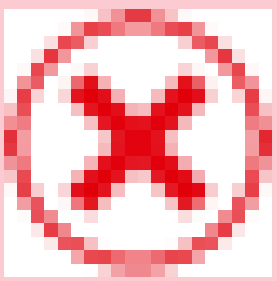
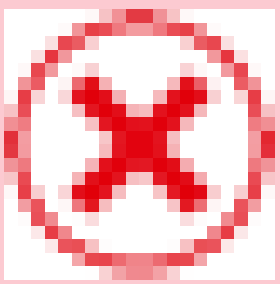
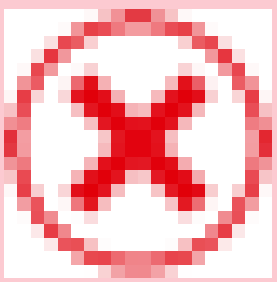
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Katalogelemente pflegen |  |  |
| Wissen |  |  |
| Manuelles Runbook | | |
| Neues Runbook erstellen |  |  |
| Zeigen Sie Runbook-Dokumente an |  |  |
| Administration | | |

Automatische Übersetzung

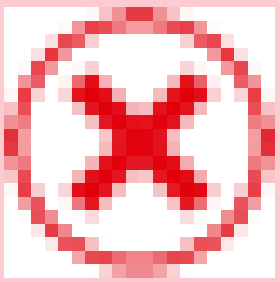
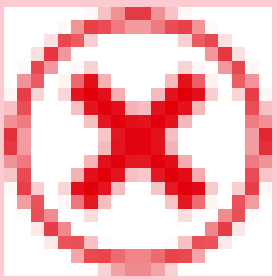
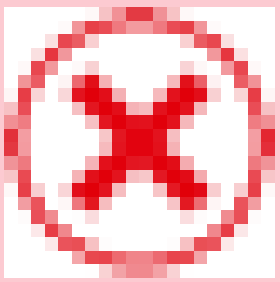
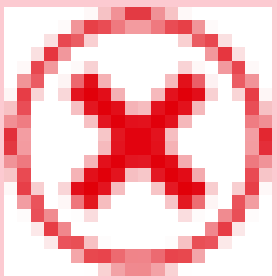
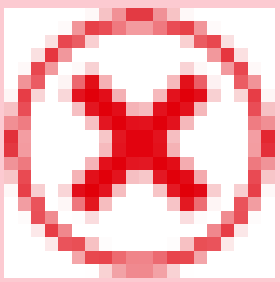
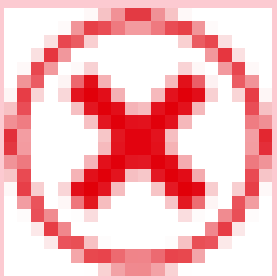
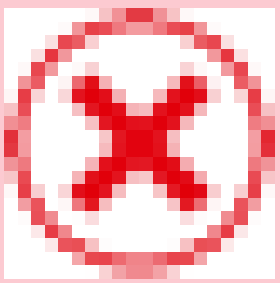
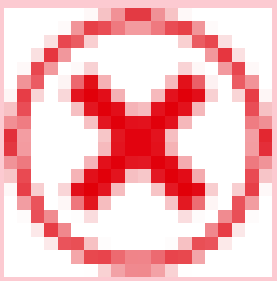
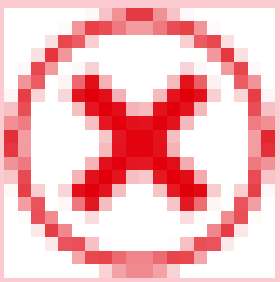
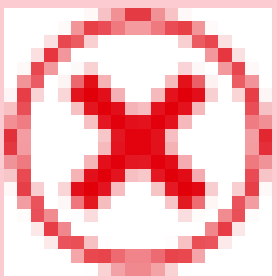
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

*Informationen für andere Rollen:*

*sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read*

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Eigenschaften |  |  |
| Konfiguration |  |  |
| Benachrichtigungen |  |  |
| Servicerelevanz-Berichterstellungsdefinition |  |  |
| Servicerelevanzdefinition |  |  |

Automatische Übersetzung

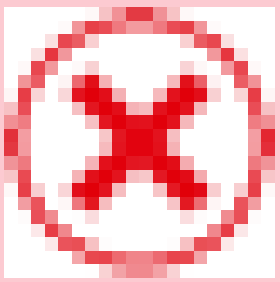
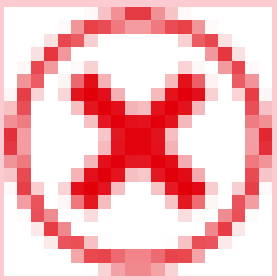
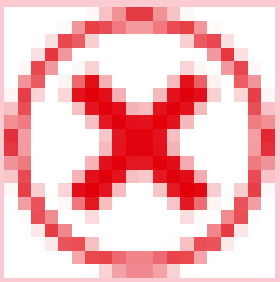
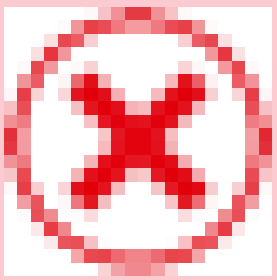
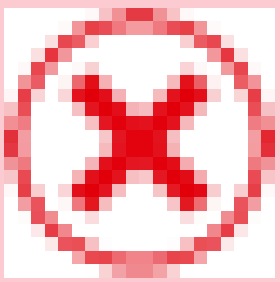
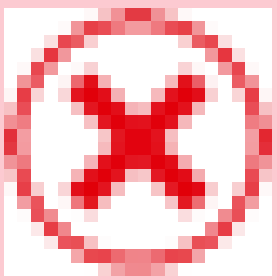
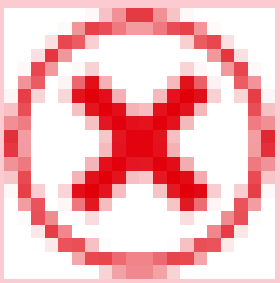
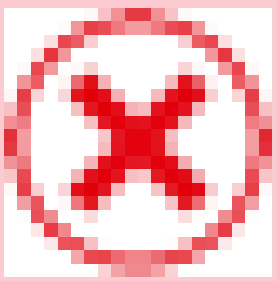
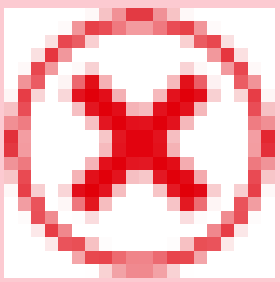
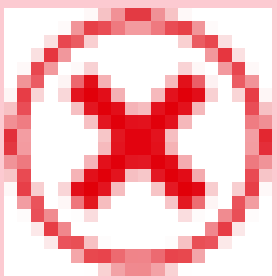
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Serviceeinfluss-Definitionen |  |  |
| Setup für Bewertungen nach Incident-Überprüfung |  |  |
| Setup des Berichts zur Überprüfung nach Incidents |  |  |
| Echtzeitdefinition |  |  |
| Prozessauswahl |  |  |

Automatische Übersetzung

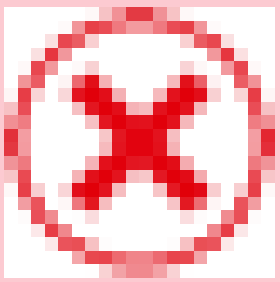
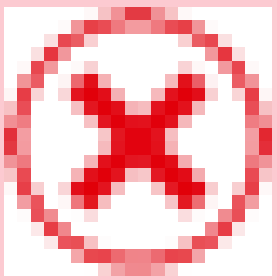
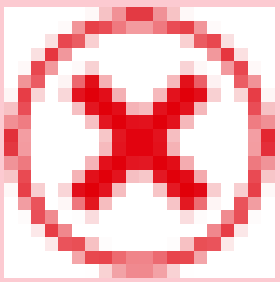
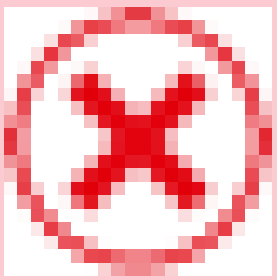
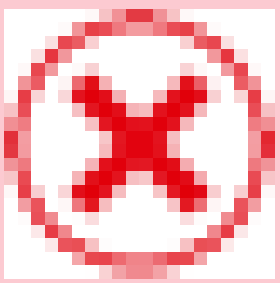
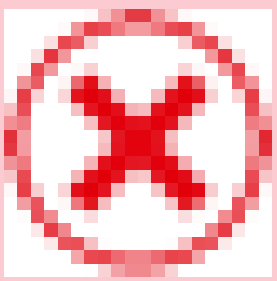
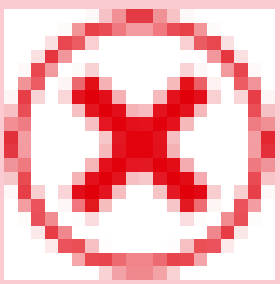
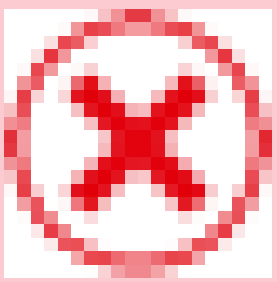
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

***Informationen für andere Rollen:***

***sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read***

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Prozessdefinitionen |  |  |
| Vorlagenworkflow – Ergebnisauswertung |  |  |
| Phishing-E-Mails | | |
| Lizenzverwaltung |  |  |
| Phishing-E-Mail melden |  |  |

Automatische Übersetzung

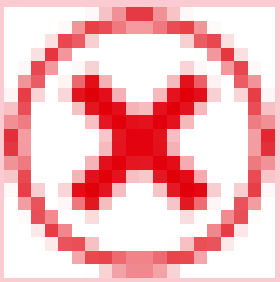
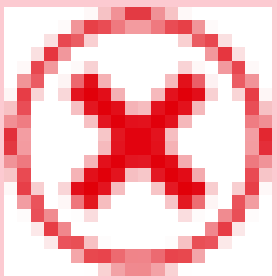
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_si.special_access, sn_si_approver_user**

*Informationen für andere Rollen:*

*sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read*

**(Fortsetzung)**

| Modul | sn_si.special_access | sn_si_approver_user |
|---|---|---|
| Alle Phishing-E-Mails anzeigen |  |  |

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Security Operations

Informationen zu Sicherheitsvorgängen finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

### Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |

Automatische Übersetzung

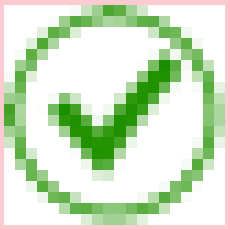
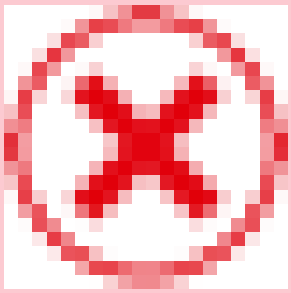
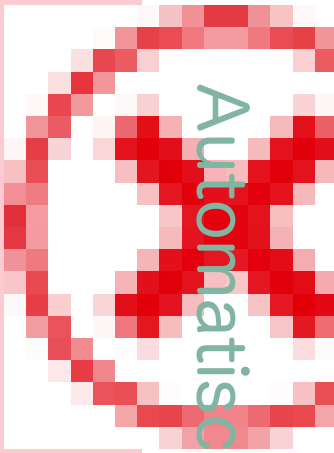
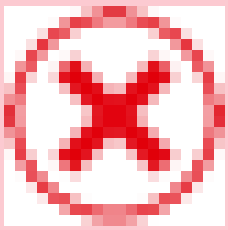
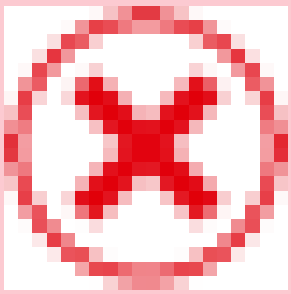
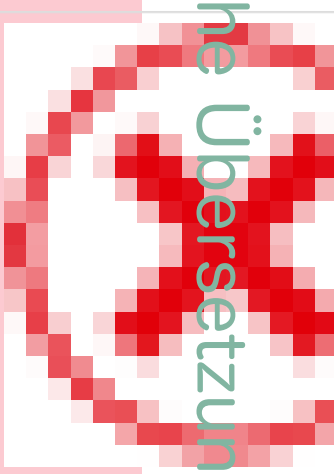
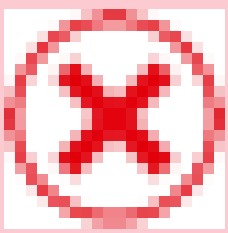
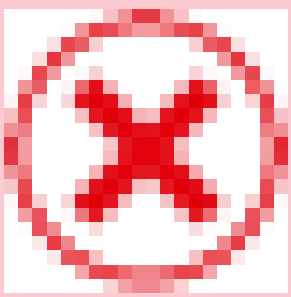
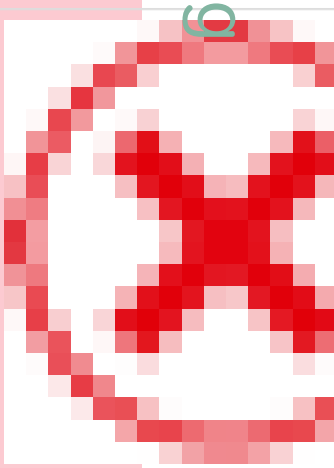
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Integrationen | |  |  |  |
| Flows für Integrationsfähigkeiten | |  |  |  |
| Fähigkeitsausführungen | |  |  |  |

Automatische Übersetzung

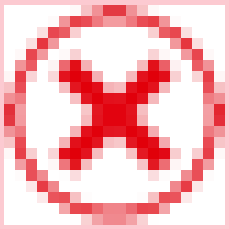
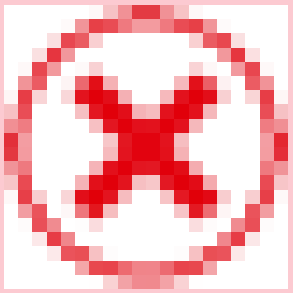
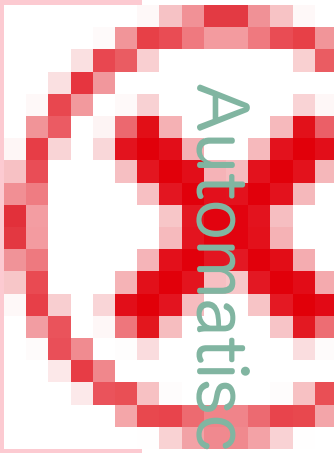
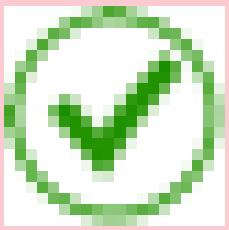
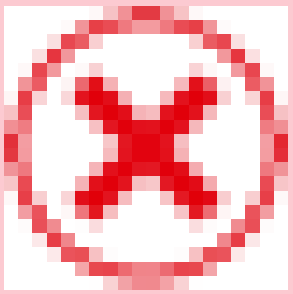
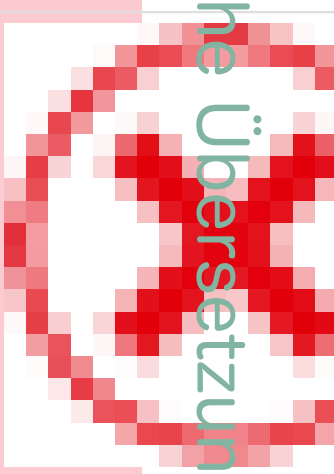
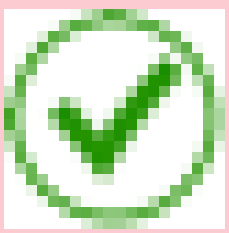
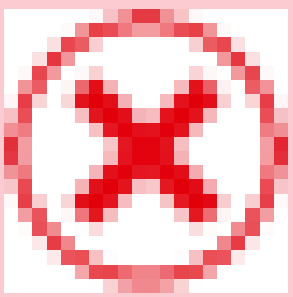
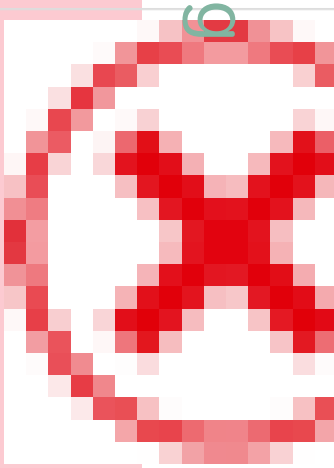
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

***Informationen für andere Rollen:***

***sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image***

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Ratenbegrenzung für Fähigkeitsimplementierungen | |  |  |  |
| Integrationskonfigurationen | |  |  |  |
| Sichtungssuche – Konfiguration | |  |  |  |

Automatische Übersetzung

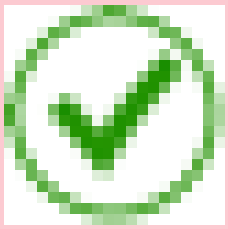
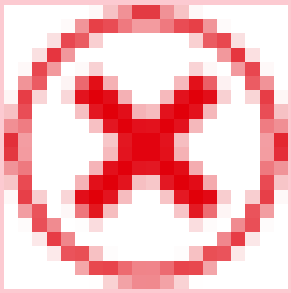
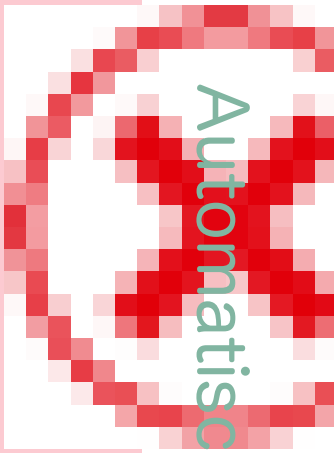
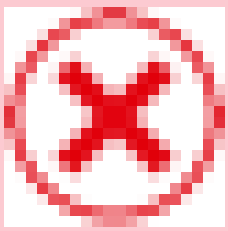
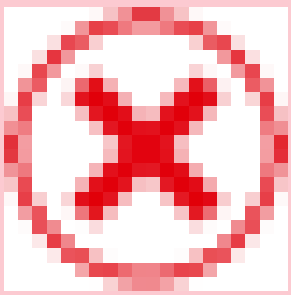
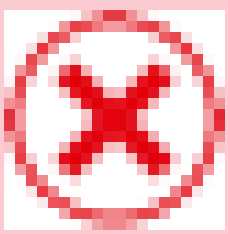
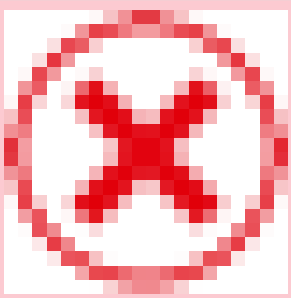
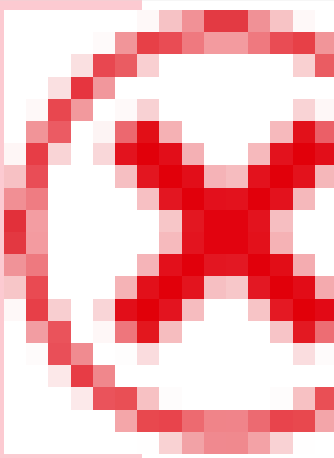
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Integrationsfunktionen | |  |  |  |
| Integrationen | | | | |
| Flows für Integrationsfähigkeiten | |  |  | |
| Fähigkeitsausführungen | |  |  |  |

Automatische Übersetzung

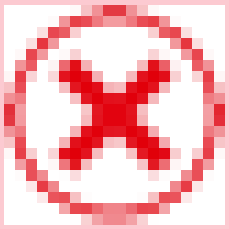
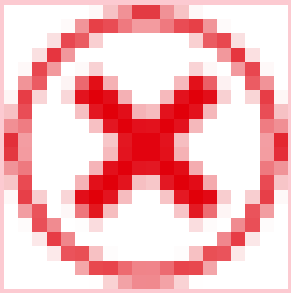
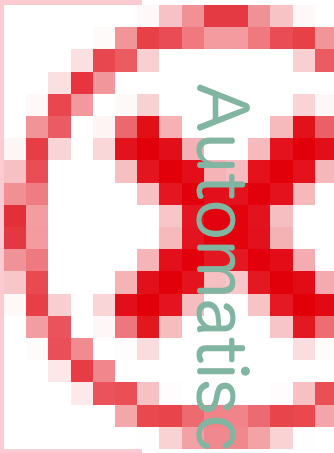
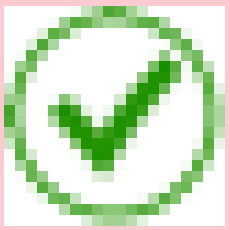
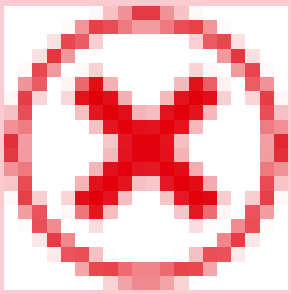
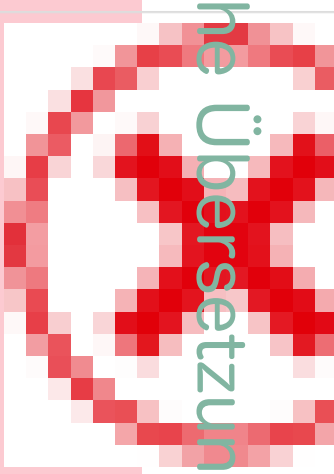
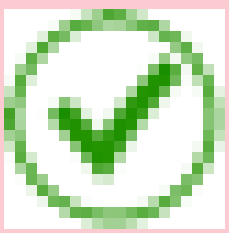
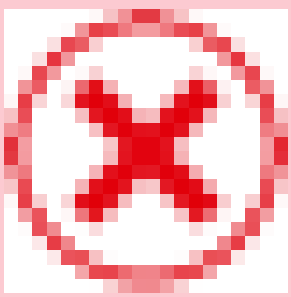
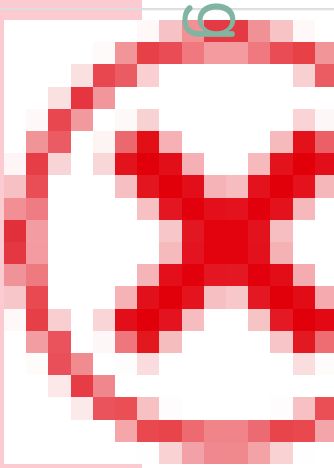
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

***Informationen für andere Rollen:***

***sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image***

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Ratenbegrenzung für Fähigkeitsimplementierungen | |  |  |  |
| Integrationskonfigurationen | |  |  |  |
| Sichtungssuche – Konfiguration | |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Integrationsfunktionen | ✓ | ✓ | ✗ | ✗ |
| E-Mail-Verarbeitung | | | | |
| E-Mail-Analyse | ✓ | ✓ | ✗ | ✗ |
| Duplizierungsregeln | ✓ | ✓ | ✗ | ✗ |

Automatische Übersetzung

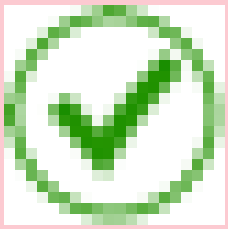
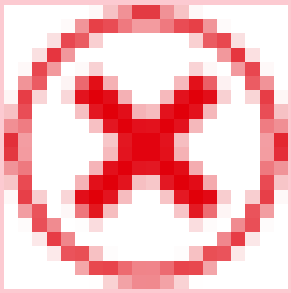
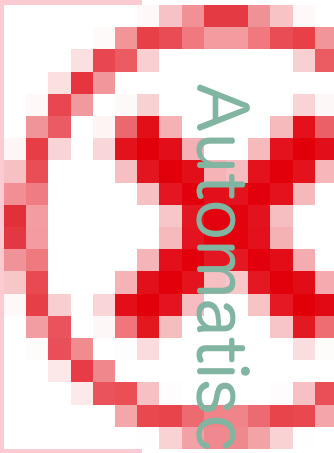
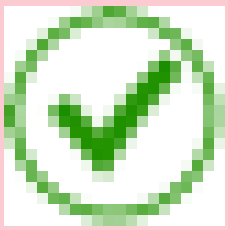
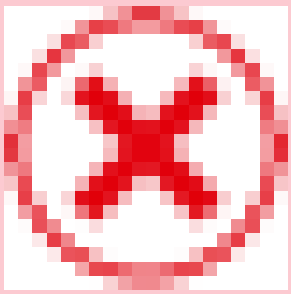
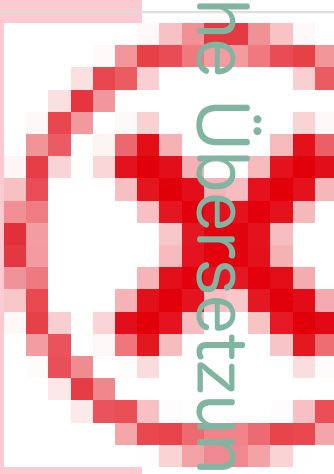
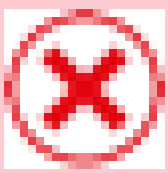
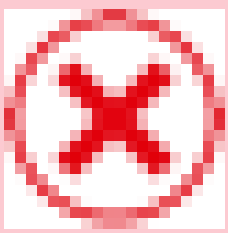
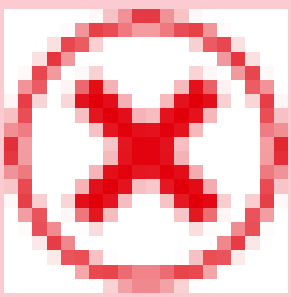
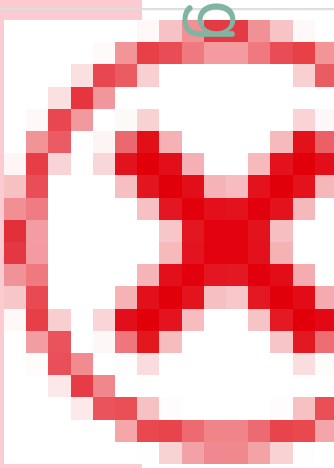
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Eigenschaften | |  |  |  |
| Nicht übereinstimmende E-Mails | |  |  |  |
| Erfassungsregeln, von Anwender gemeldetes Phishing |  |  |  |  |

Automatische Übersetzung

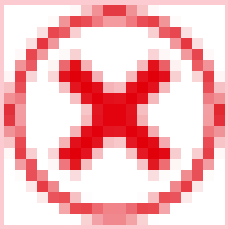
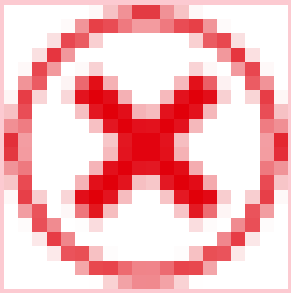
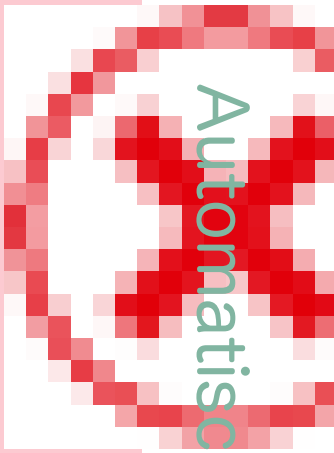
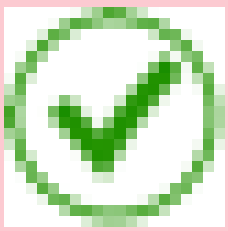
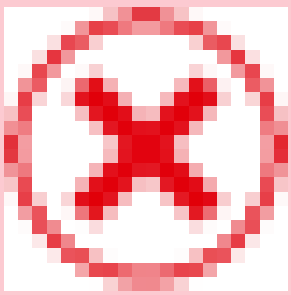
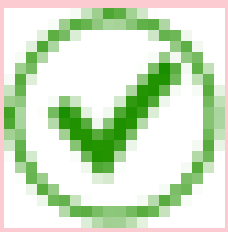
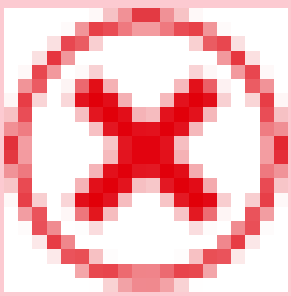
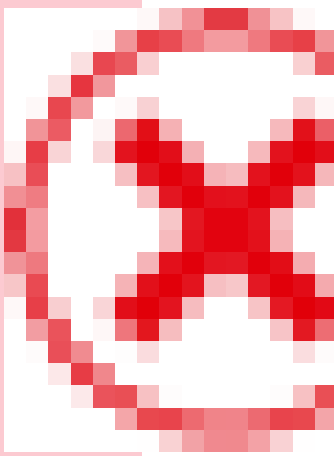
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Eigenschaften des vom Anwender gemeldeten Phishing | |  |  |  |
| Gruppen | | | | |
| Filtergruppen | |  |  | |
| Eskalationen | |  |  |  |

Automatische Übersetzung

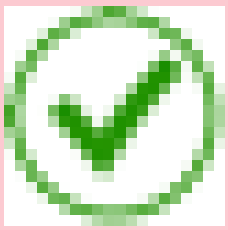
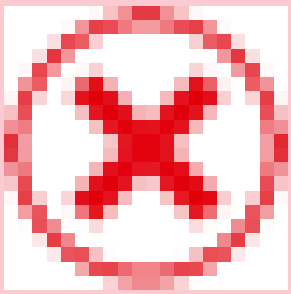
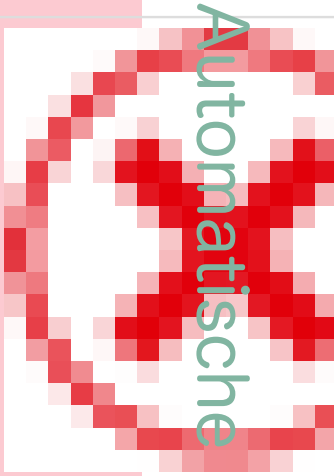
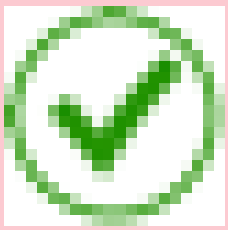
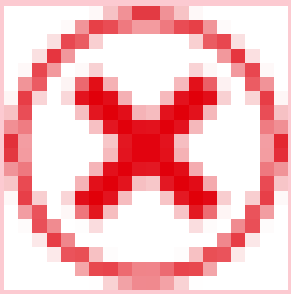
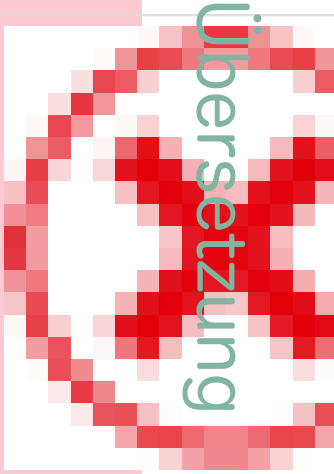
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Datenergänzungen | | | | |
| Sicherheits-Tags | | | | |
| Gruppen | |  |  |  |
| Tags | |  |  |  |
| Workflows | | | | |

Automatische Übersetzung

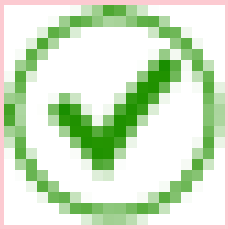
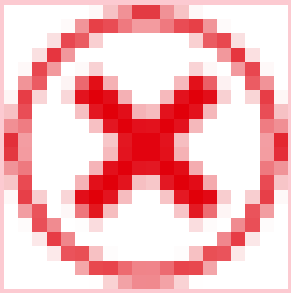
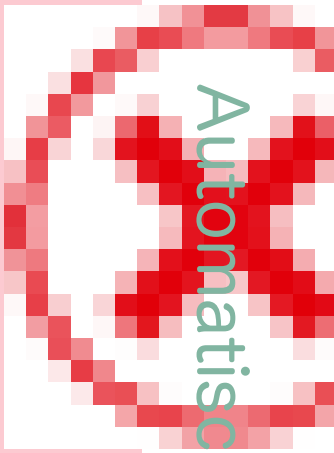
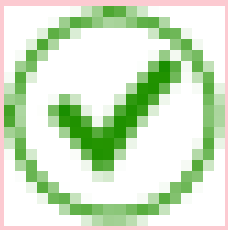
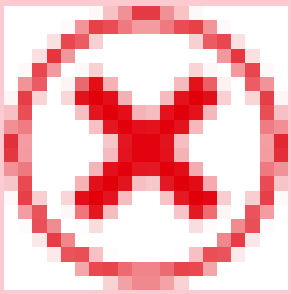
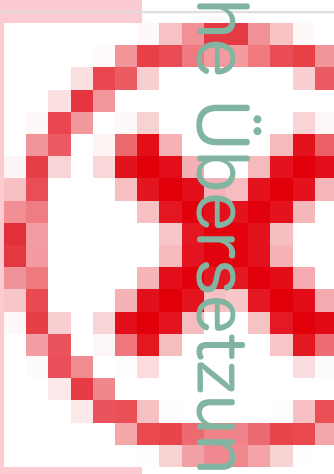
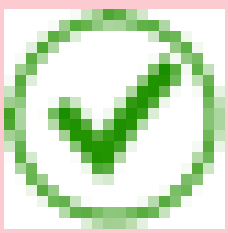
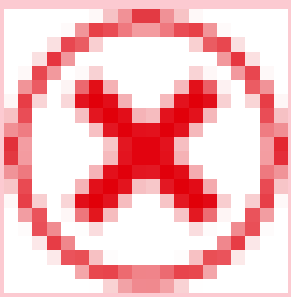
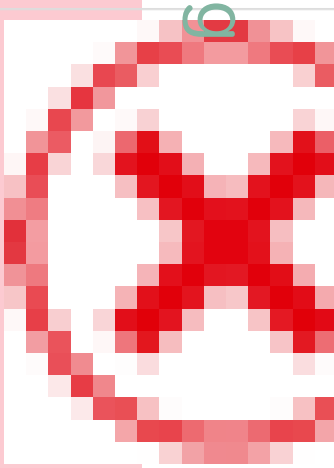
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Ausführungsverfolgung | |  |  |  |
| Sicherheitsworkflows anzeigen | |  |  |  |
| Workflow-Auslöser | |  |  |  |
| Dienstprogramme | | | | |

Automatische Übersetzung

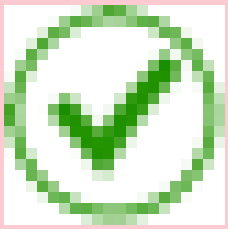
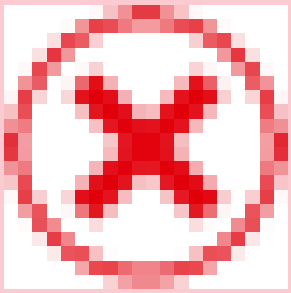
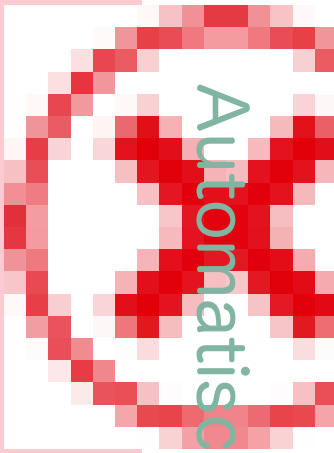
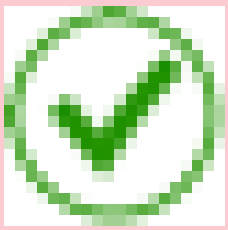
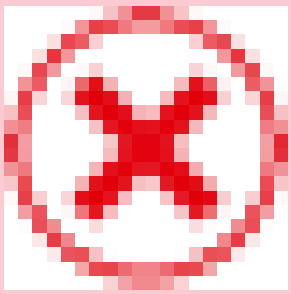
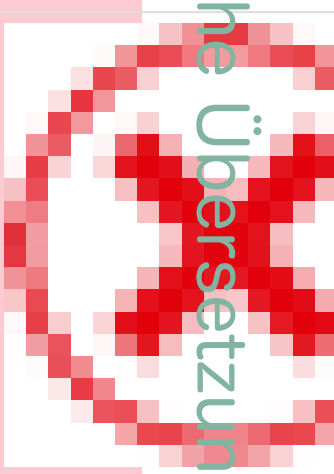
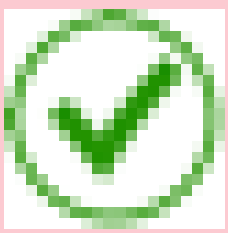
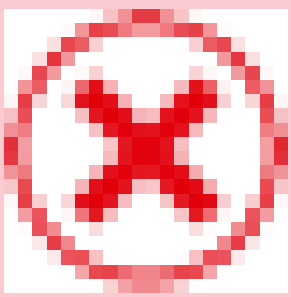
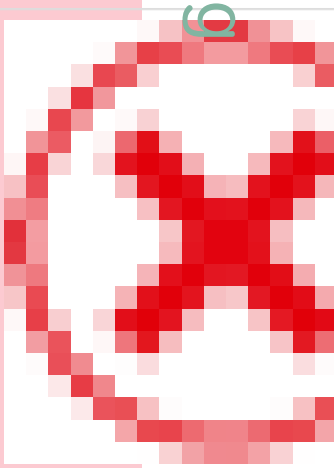
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Ergänzungsdatenzuordnung | |  |  |  |
| Feldwertumwandlungen | |  |  |  |
| Feldzuordnung | |  |  |  |

Automatische Übersetzung

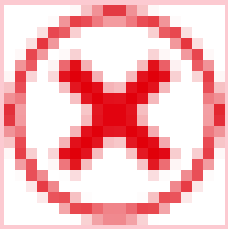
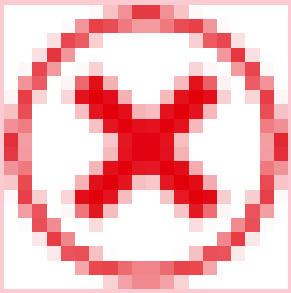
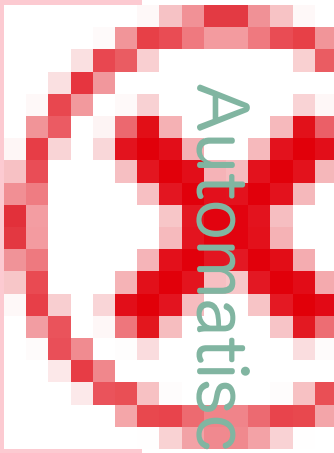
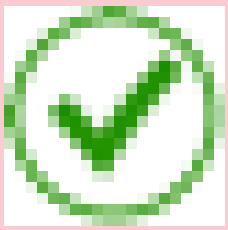
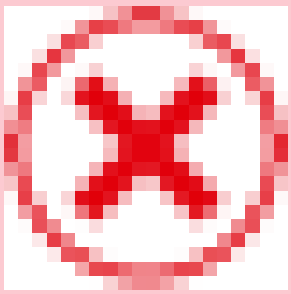
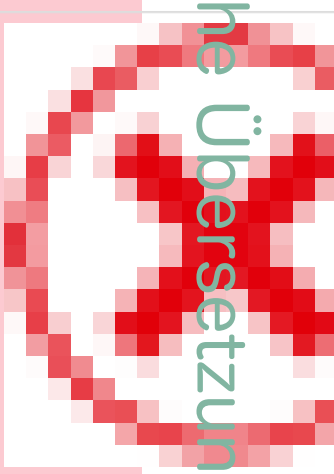
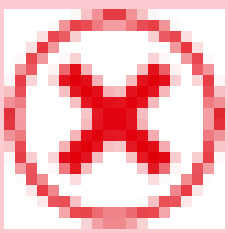
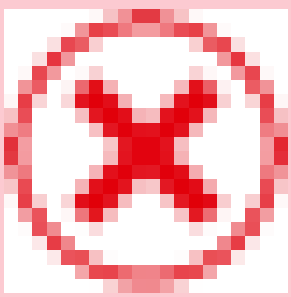
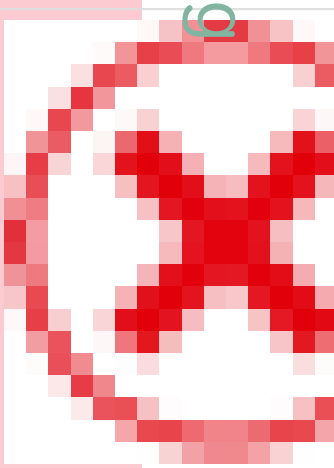
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

***Informationen für andere Rollen:***

***sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image***

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Orchestration bei Bedarf | |  |  |  |
| Betriebssystemgruppen | |  |  |  |
| SecOps-Applikationsregistrierung | |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

***Informationen für andere Rollen:***

***sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image***

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Hintergrundauftrags-Konfiguration | ✓ | ✓ | ✗ | ✓ |
| CMDB | | | | |
| CI-Suchregeln | ✓ | ✓ | ✓ | ✗ |
| Erkannte Elemente | ✓ | ✓ | ✓ | ✗ |

Automatische Übersetzung

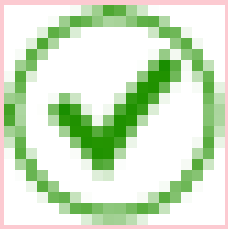
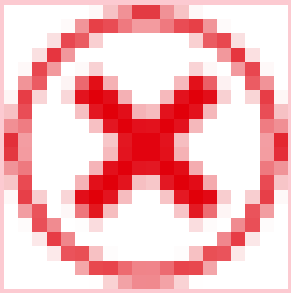
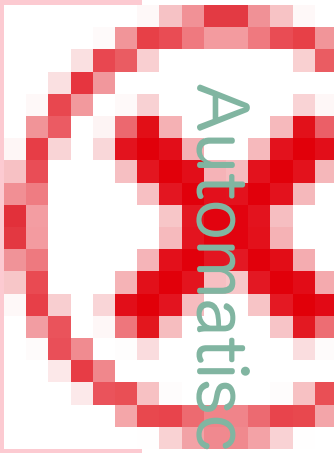
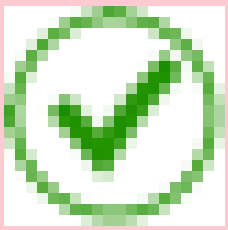
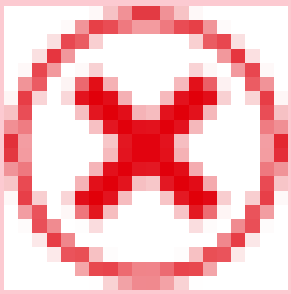
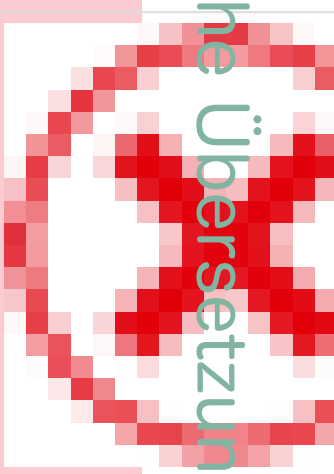
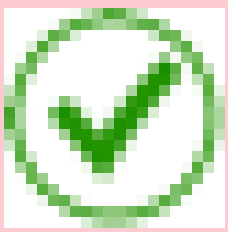
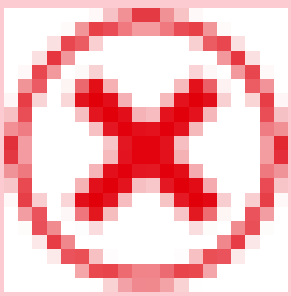
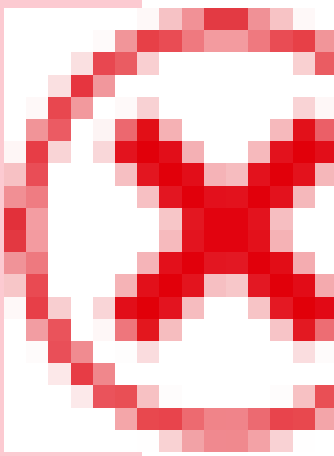
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Nicht übereinstimmende erkannte Elemente abstimmen | |  |  |  |
| Erkannte Container-Images | |  |  |  |
| WatchDog | | | | |
| Konfiguration | |  |  |  |

Automatische Übersetzung

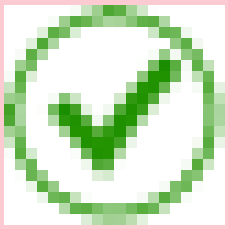
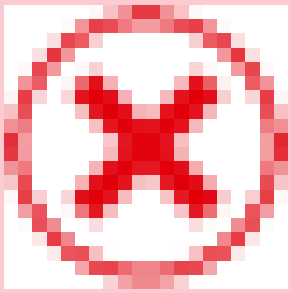
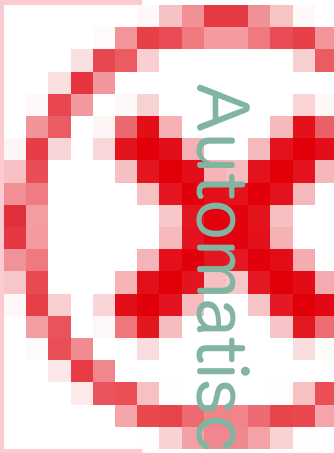
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job**

*Informationen für andere Rollen:*

*sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image*

**(Fortsetzung)**

| Modul | Administrator | sn_sec_cmn.admin | sn_sec_cmn.ci_manager | sn_sec_cmn.manage_backgr |
|---|---|---|---|---|
| Übersicht | |  |  |  |

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

*Informationen für andere Rollen:*

*admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job*

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |

Automatische Übersetzung

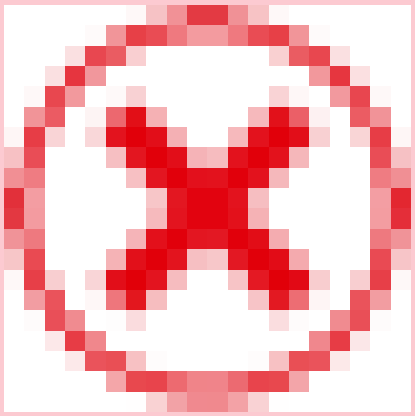
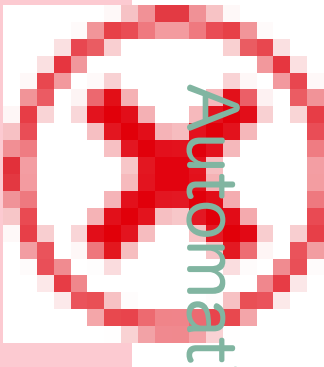
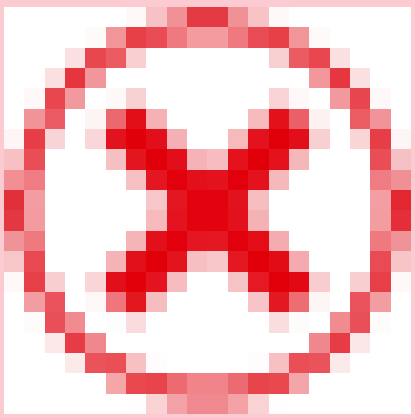
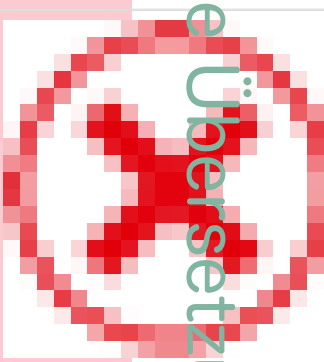
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Integrationen |  | | |  |
| Flows für Integrationsfähigkeiten |  | | |  |

Automatische Übersetzung

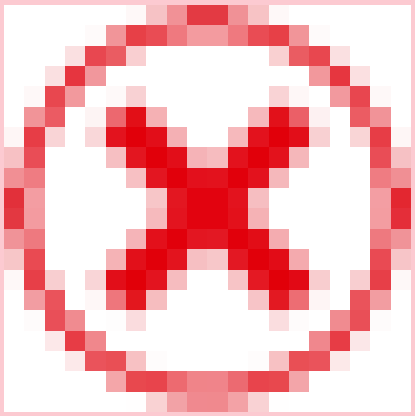
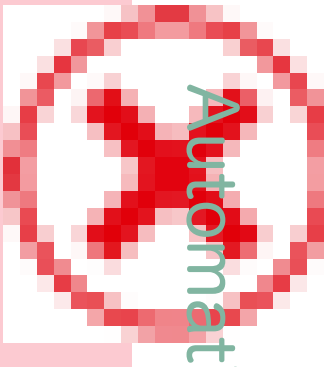
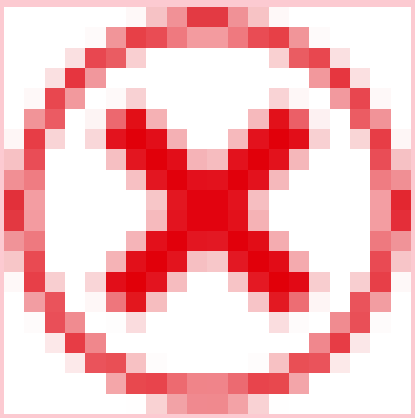
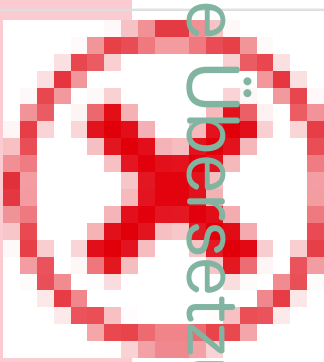
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Fähigkeitsausführungen |  | | |  |
| Ratenbegrenzung für Fähigkeitsimplementierungen |  | | |  |

Automatische Übersetzung

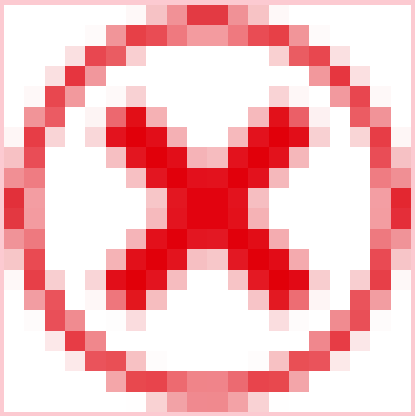
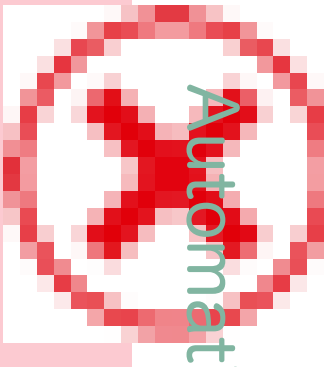
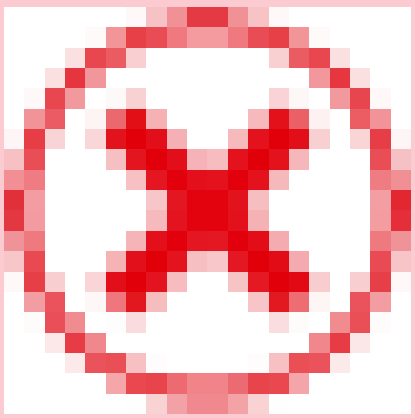
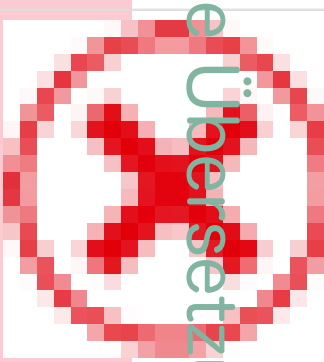
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Integrationskonfigurationen |  | | |  |
| Sichtungssuche – Konfiguration |  | | |  |

Automatische Übersetzung

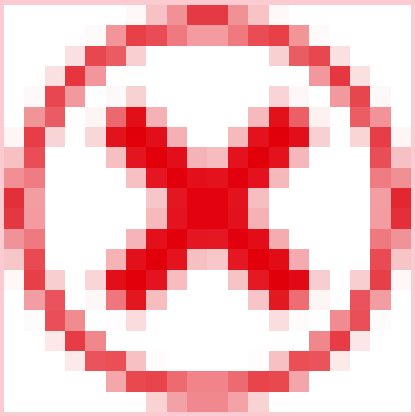
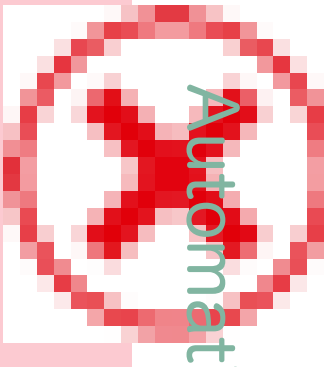
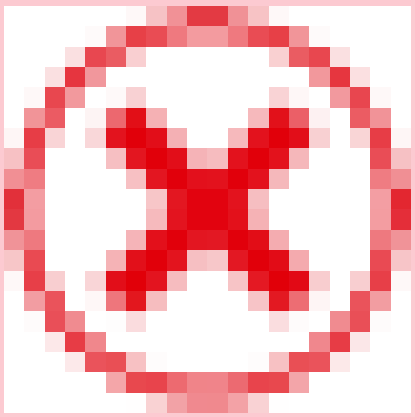
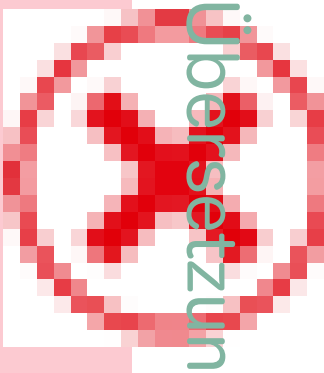
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Integrationsfunktionen |  | | |  |
| Integrationen | | | | |
| Flows für Integrationsfähigkeiten |  | | |  |

Automatische Übersetzung

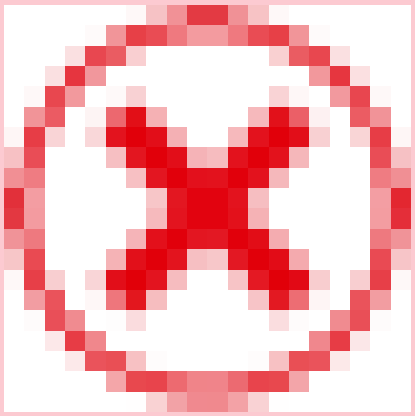
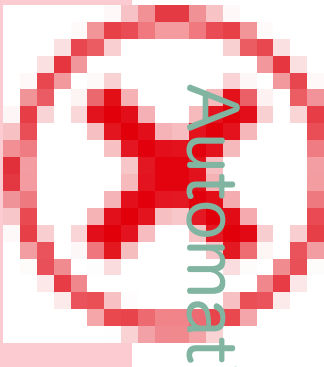
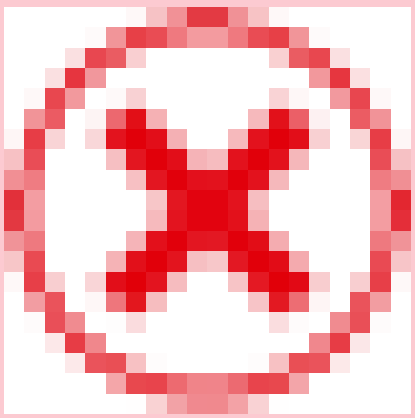
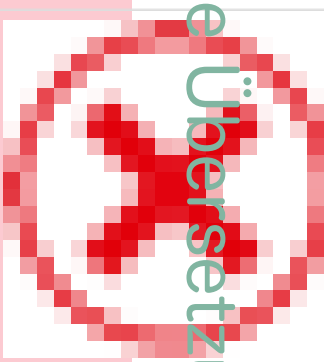
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Fähigkeitsausführungen |  | | |  |
| Ratenbegrenzung für Fähigkeitsimplementierungen |  | | |  |

Automatische Übersetzung

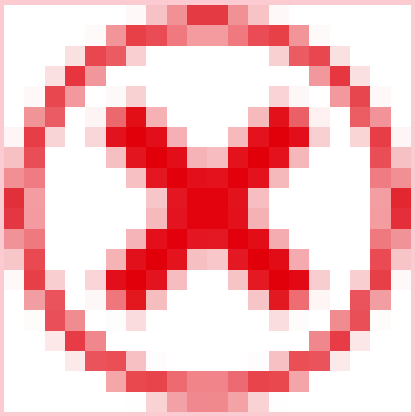
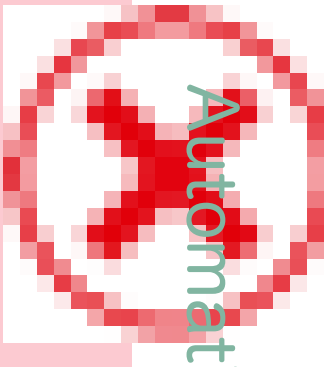
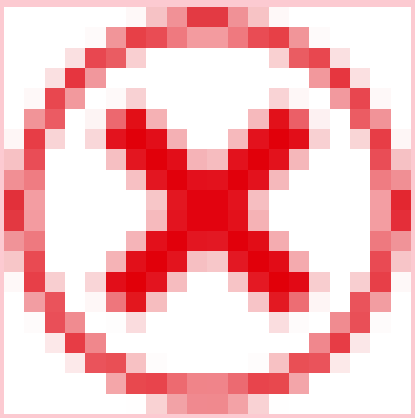
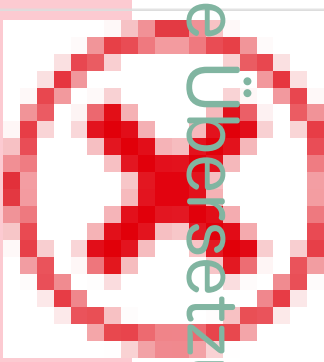
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Integrationskonfigurationen |  | | |  |
| Sichtungssuche – Konfiguration |  | | |  |

Automatische Übersetzung

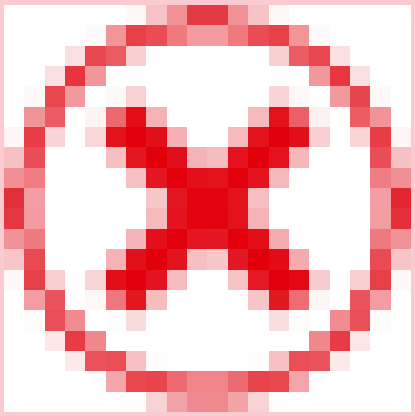
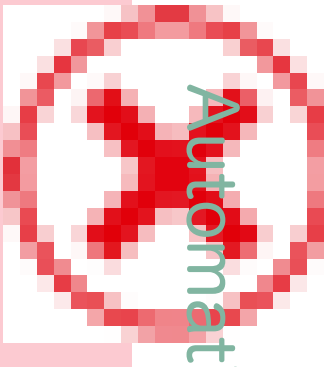
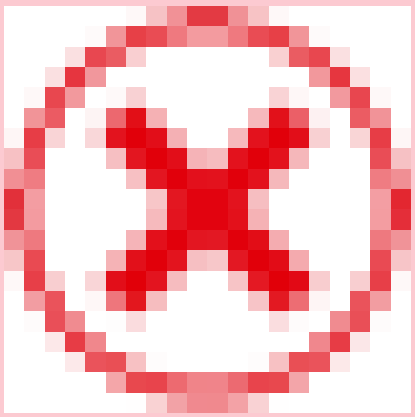
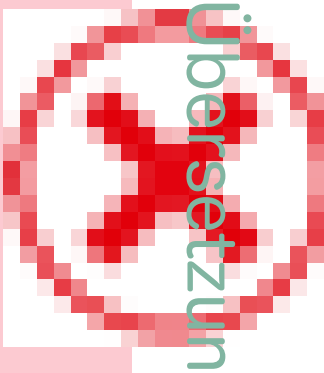
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Integrationsfunktionen |  | | |  |
| E-Mail-Verarbeitung | | | | |
| E-Mail-Analyse |  | | |  |

Automatische Übersetzung

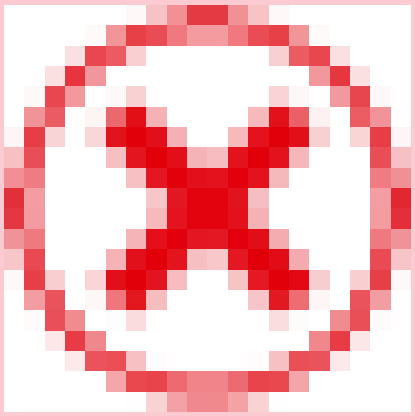
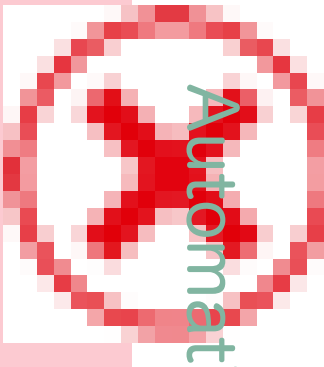
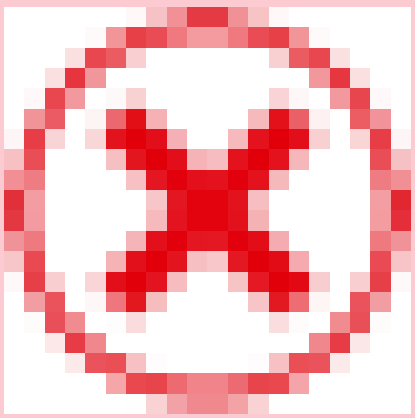
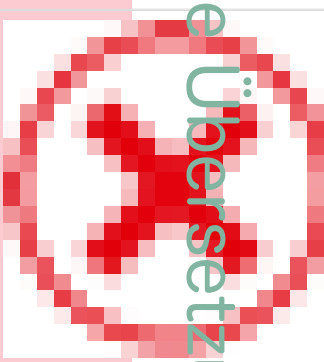
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Duplizierungsregeln |  | | |  |
| Eigenschaften |  | | |  |

Automatische Übersetzung

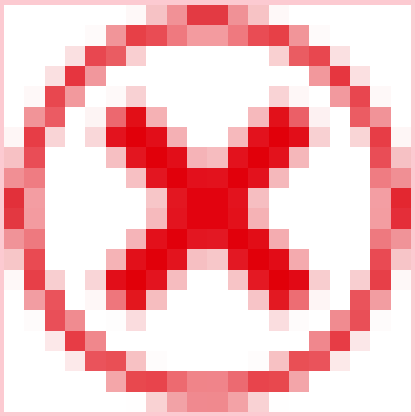
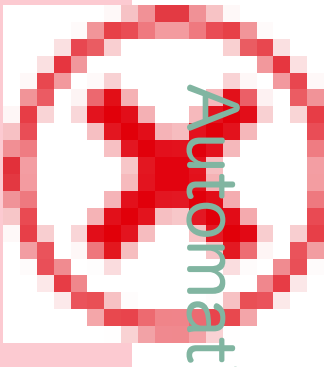
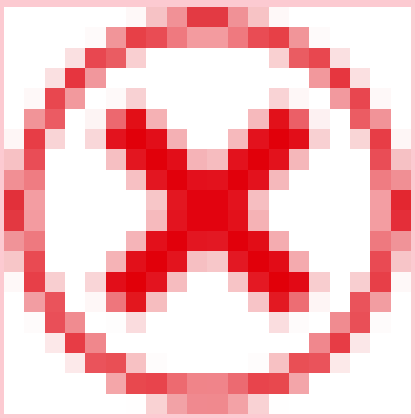
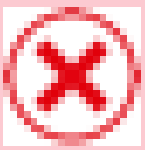
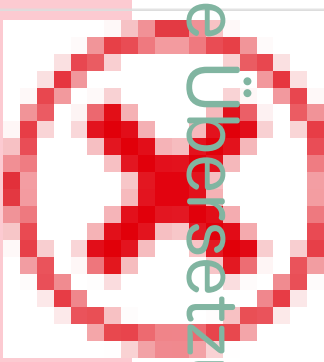
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Nicht übereinstimmende E-Mails |  | | |  |
| Erfassungsregeln, von Anwender gemeldetes Phishing |  |  | |  |

Automatische Übersetzung

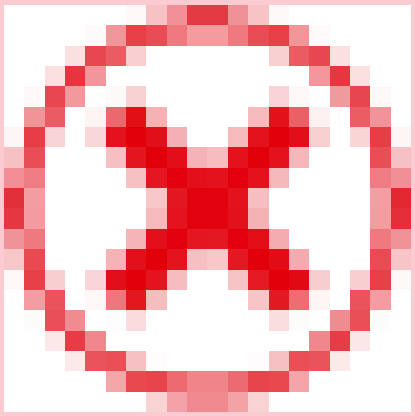
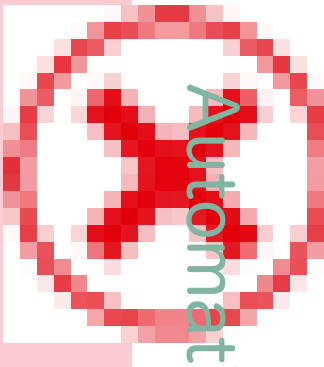
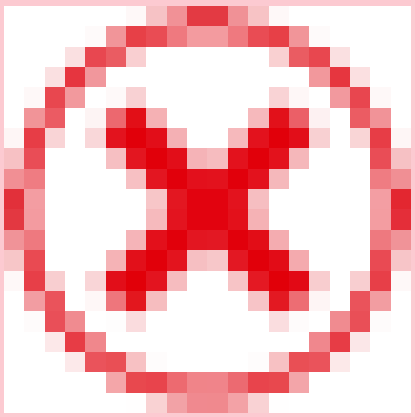
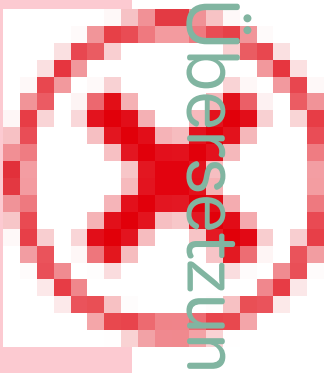
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Eigenschaften des vom Anwender gemeldeten Phishing |  | | |  |
| Gruppen | | | | |
| Filtergruppen |  | | |  |

Automatische Übersetzung

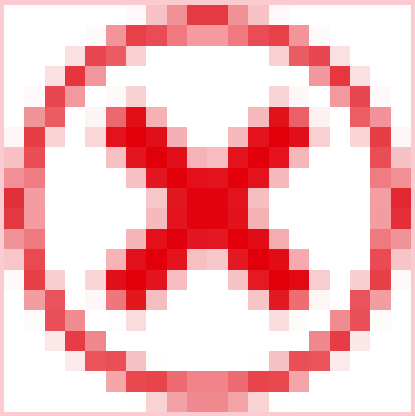
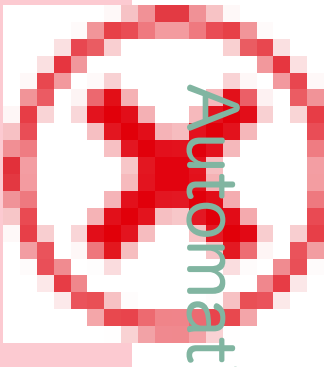
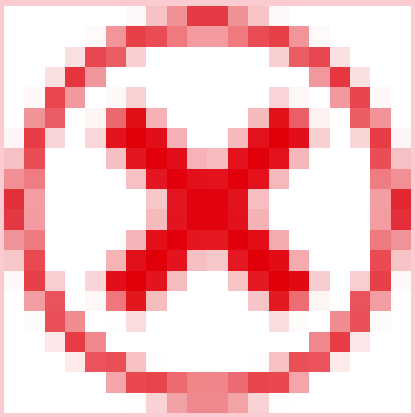
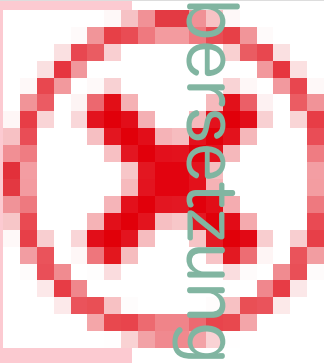
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Eskalationen |  | | |  |
| Datenergänzungen | | | | |
| Sicherheits-Tags | | | | |
| Gruppen |  | | |  |

Automatische Übersetzung

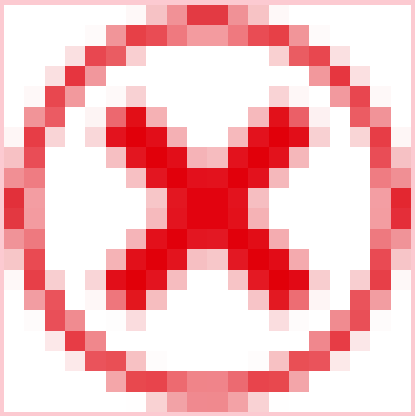
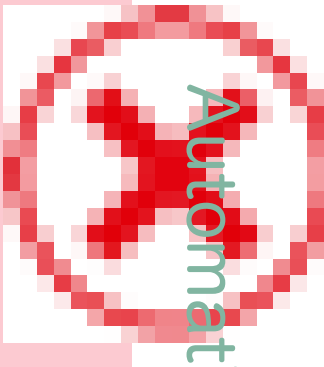
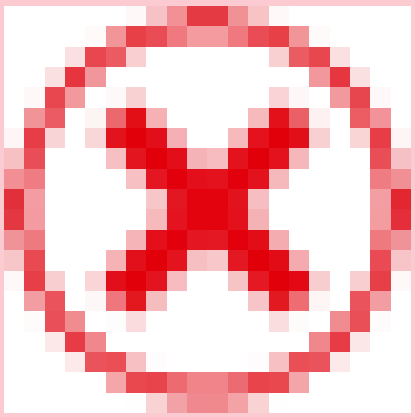
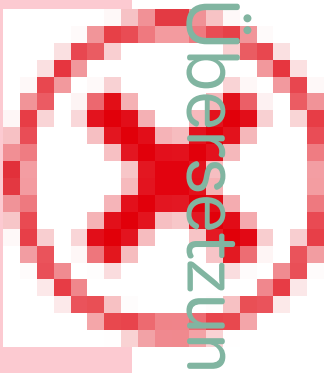
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Tags |  | | |  |
| Workflows | | | | |
| Ausführungsverfolgung |  | | |  |

Automatische Übersetzung

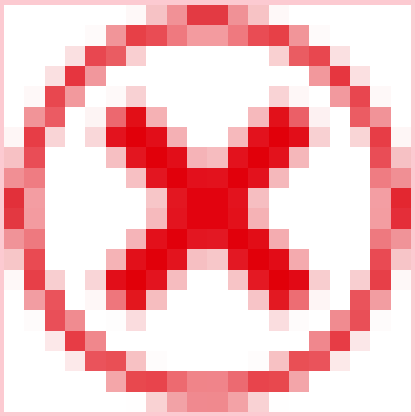
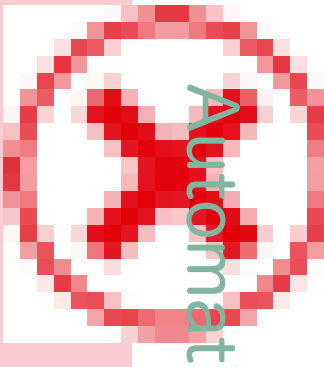
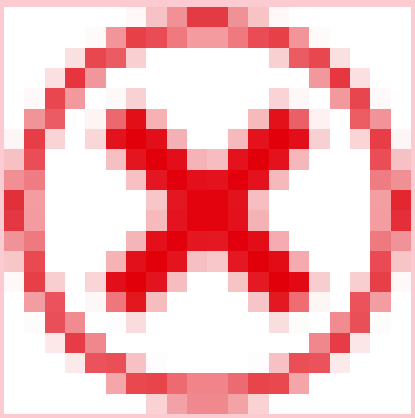
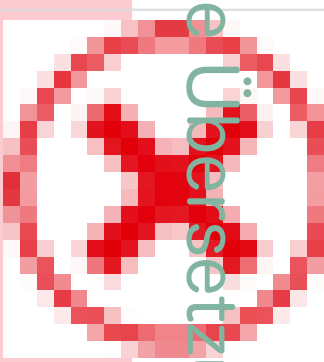
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Sicherheitsworkflows anzeigen |  | | |  |
| Workflow-Auslöser |  | | |  |
| Dienstprogramme | | | | |

Automatische Übersetzung

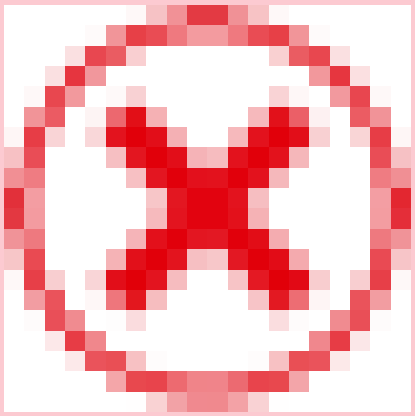
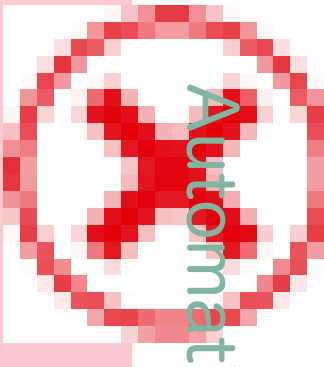
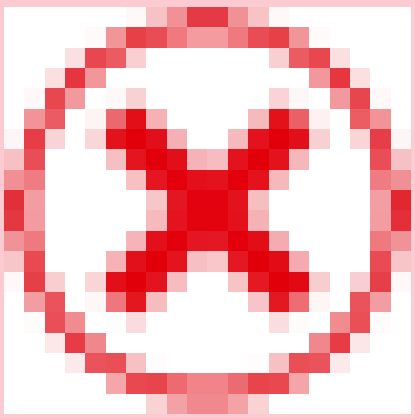
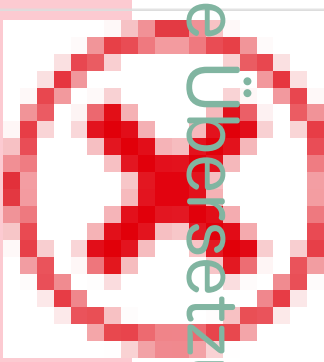
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Ergänzungsdatenzuordnung |  | | |  |
| Feldwertumwandlungen |  | | |  |

Automatische Übersetzung

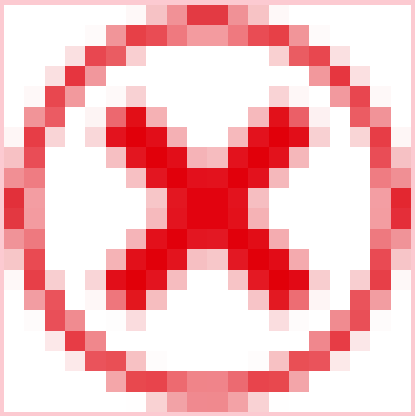
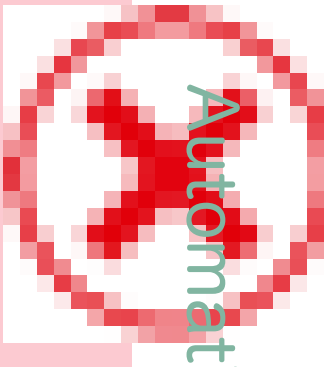
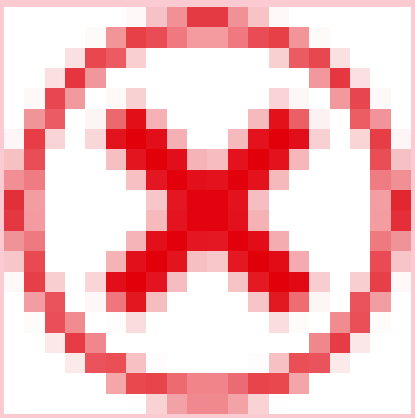
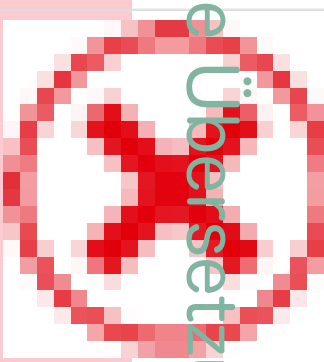
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Feldzuordnung |  | | |  |
| Orchestration bei Bedarf |  | | |  |

Automatische Übersetzung

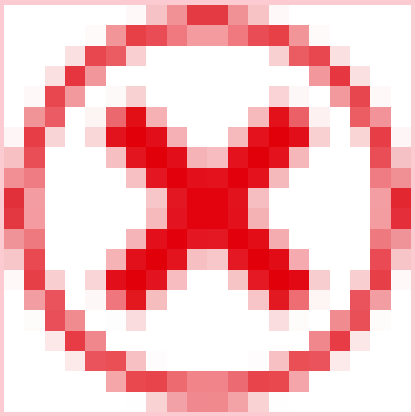
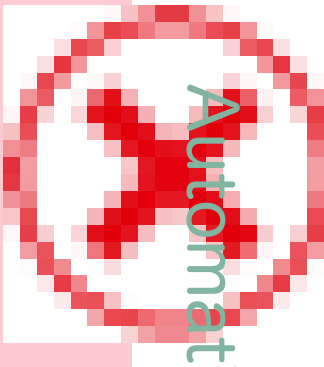
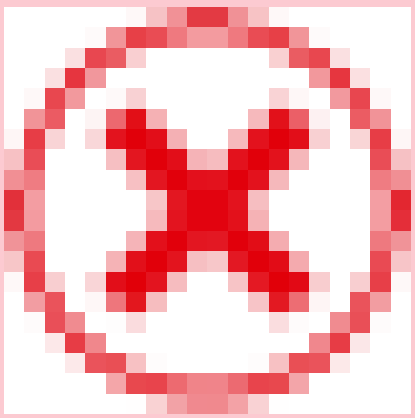
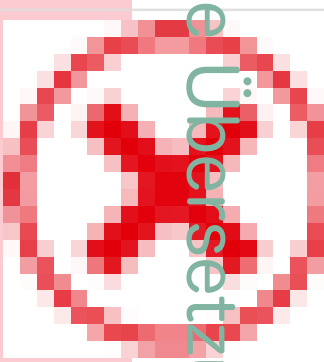
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Betriebssystemgruppen |  | | |  |
| SecOps-Applikationsregistrierung |  | | |  |

Automatische Übersetzung

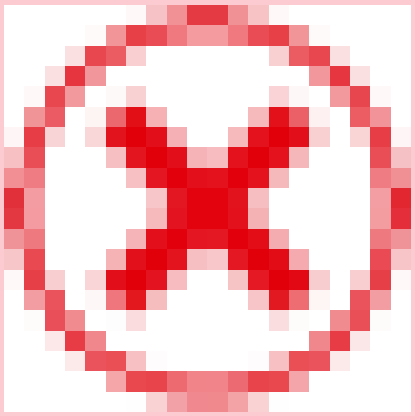
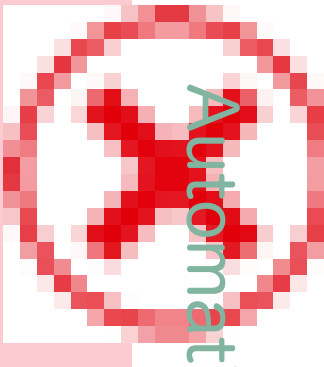
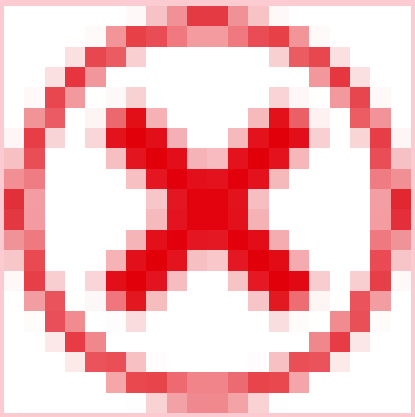
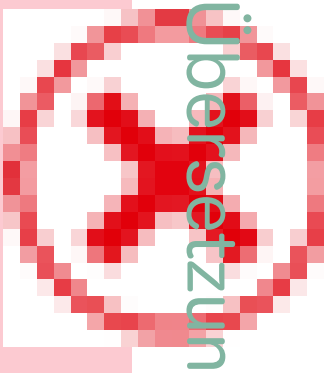
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Hintergrundauftrags-Konfiguration |  | | |  |
| CMDB | | | | |
| CI-Suchregeln |  | | |  |

Automatische Übersetzung

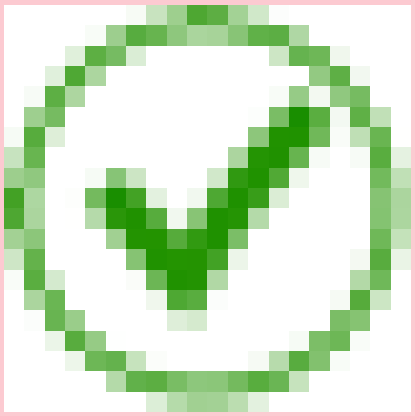
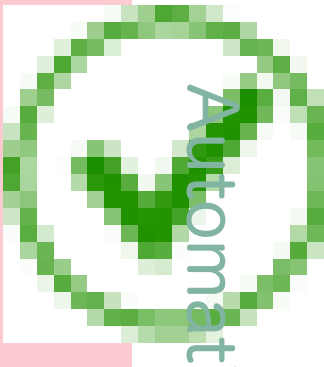
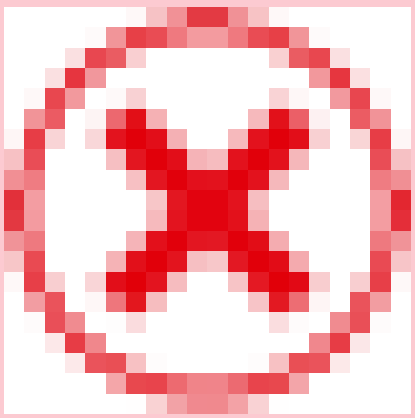
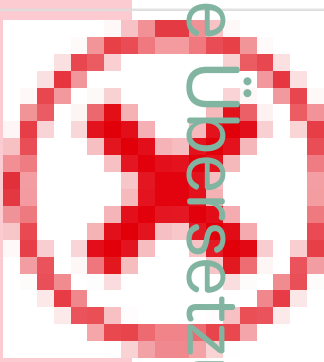
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Erkannte Elemente |  | | |  |
| Nicht übereinstimmende erkannte Elemente abstimmen |  | | |  |

Automatische Übersetzung

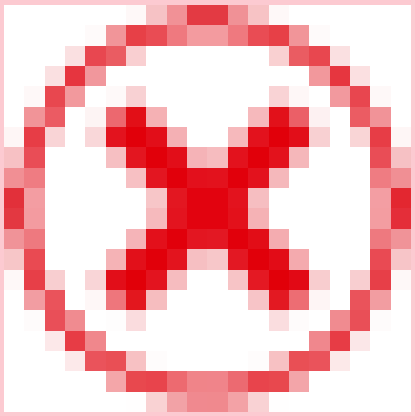
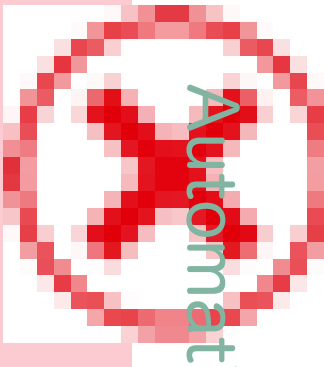
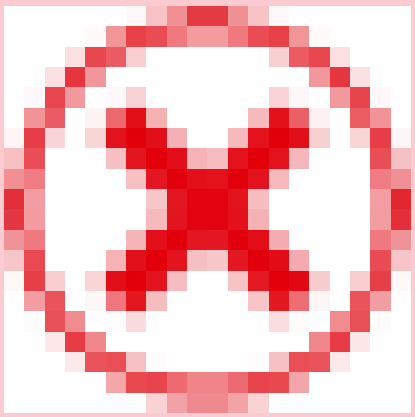
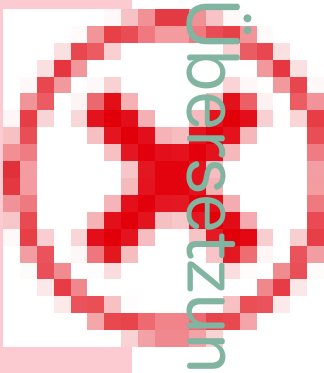
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Erkannte Container-Images |  | | |  |
| WatchDog | | | | |
| Konfiguration |  | | |  |

Automatische Übersetzung

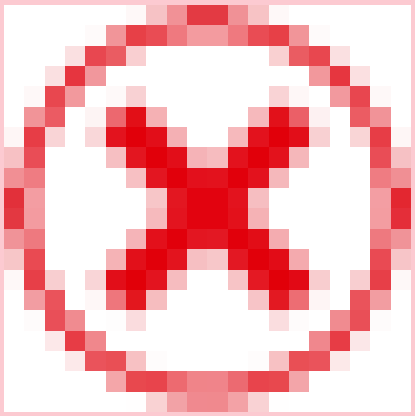
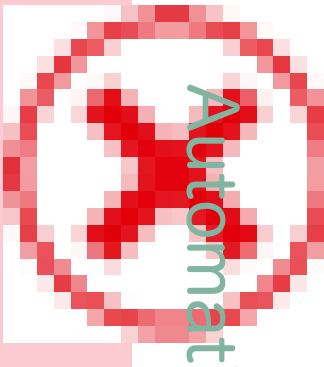
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image**

***Informationen für andere Rollen:***

***admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job***

**(Fortsetzung)**

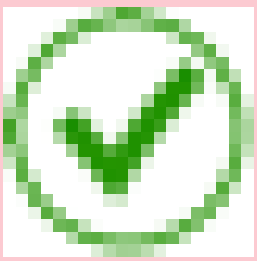
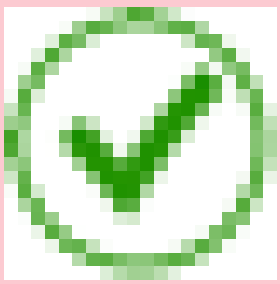
| Modul | sn_sec_cmn.reclassify_unmatch_ci | sn_si.admin | sn_si.basic | sn_vul.read_discovered_iter |
|---|---|---|---|---|
| Übersicht |  | | |  |

[End]

[store-future: BEGIN review]

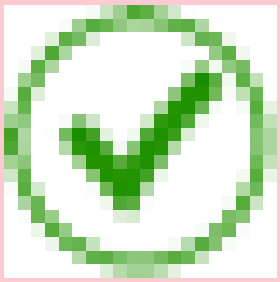
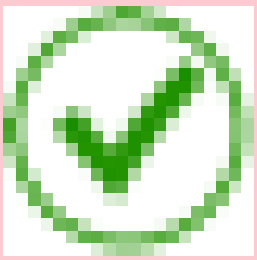
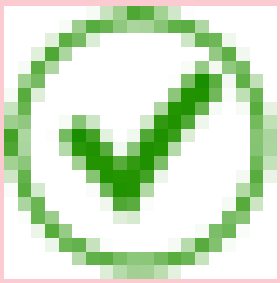
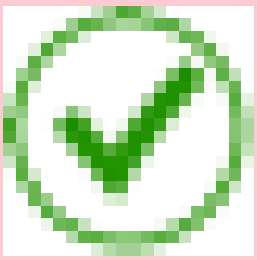
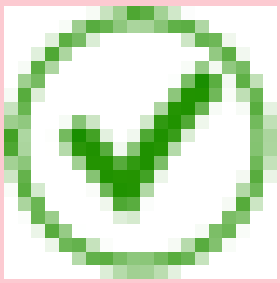
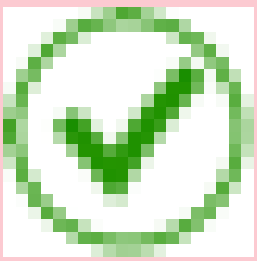
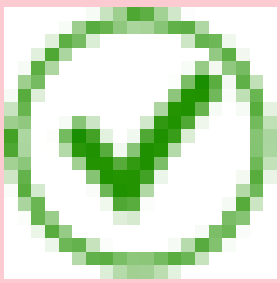
## Modulzugriff nach Rolle für Splunk-Integration

Informationen zur Splunk-Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_si.admin | sn_si.analyst |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| Splunk-Ereignisprofile |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst |
|---|---|---|
| Splunk-Feldübersetzungen | |  |
| Splunk-Event zu Aufgaben |  |  |
| Splunk-Event-Import |  |  |
| Splunk-Integrationseinstellungen |  |  |

[End]

[store-future: BEGIN review]

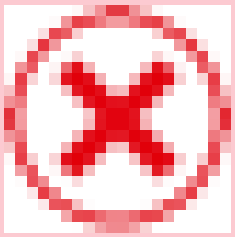
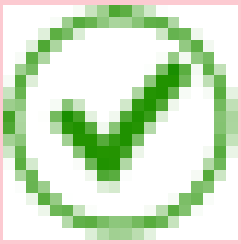
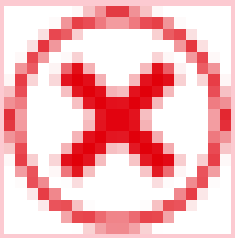
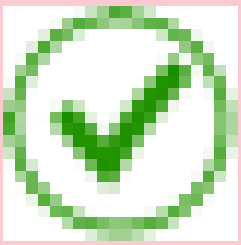
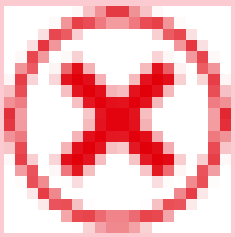
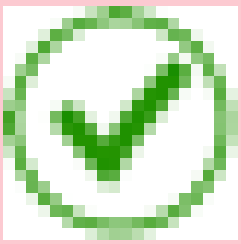
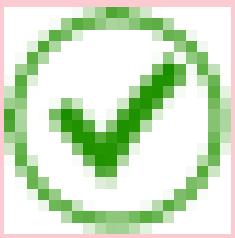
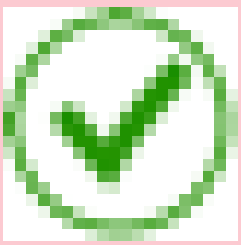
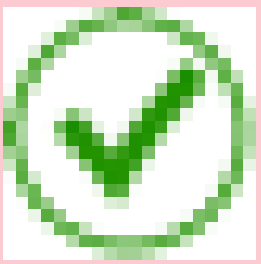
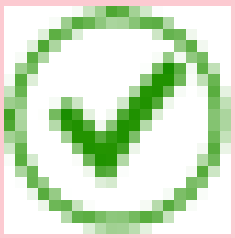
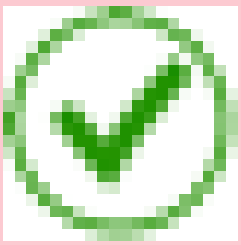
## Modulzugriff nach Rolle für Symantec DLP-Integration

Informationen zur Symantec DLP-Integration finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | agent_admin | sn_dlir.admin | sn_dlir.analyst |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | agent_admin | sn_dlir.admin | sn_dlir.analyst |
|---|---|---|---|
| Incident-Profil |  |  | |
| Incident-Statuszuordnung |  |  | |
| Einstellungen |  |  | |
| MID-Anwendung |  |  |  |
| MID-Server |  |  | |

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Threat Intelligence

Informationen zu Threat Intelligence finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | | | |

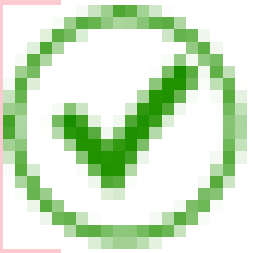
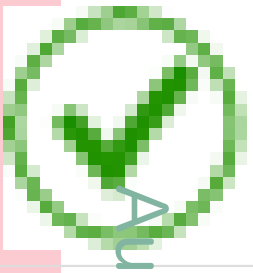
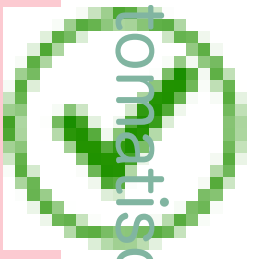
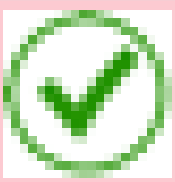
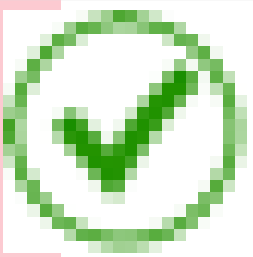
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Objekte | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Objekte | | | | | | |
| IoC-Repository | | | | | | |
| Angriffsmodusmethoden | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Indikatoren | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Erkennbare Elemente | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Angriffsmuster | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kampagnen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Vorgehensweisen | | | | | |  |
| Identitäten | | | | | |  |
| Infrastruktur | | | | | |  |
| Standorte | | | | | | |
| Malware | | | | | | |
| Angriffssatz | | | |  | |  |

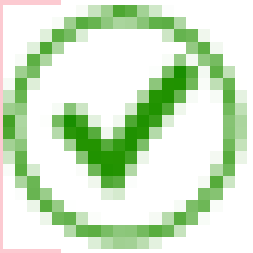
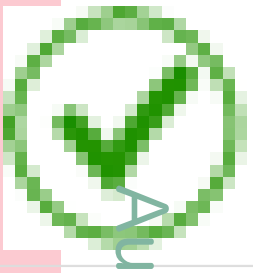
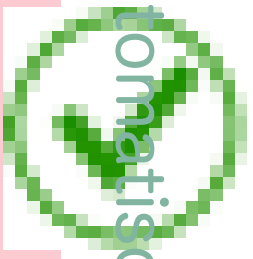
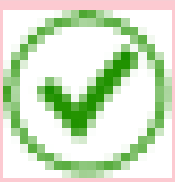
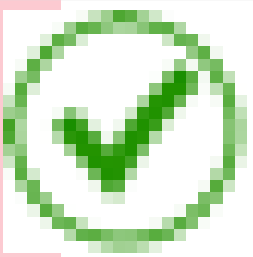
Automatisch übersetzt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Bedrohungsakteure | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Malware-Analyse | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Beobachtete Daten | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bedrohungsgruppierungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Markierungsdefinitionen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bedrohungshinweise | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Bedrohungsmeinungen | | | | | |  |
| Bedrohungsberichte | | | | | |  |
| Indikatorsichtungen | | | | | |  |
| Objektsichtungen | | | | | | |
| Schwachstellen | | | | | | |
| Tools | | | |  | |  |

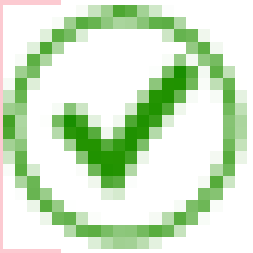
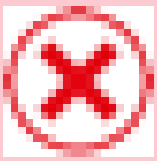
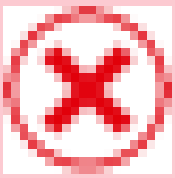
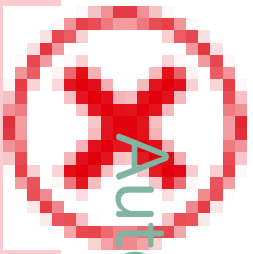
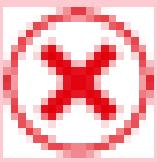
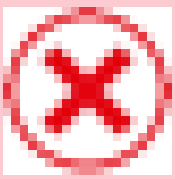
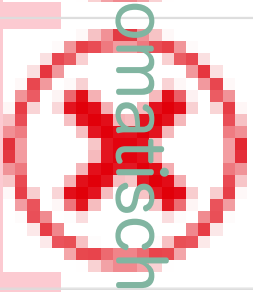
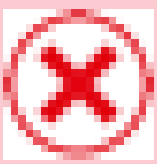
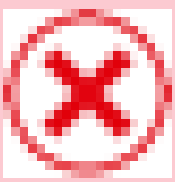
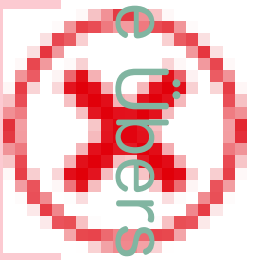
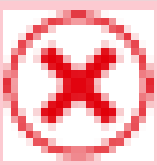
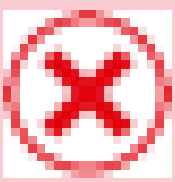
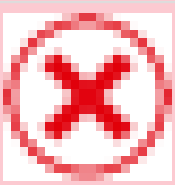
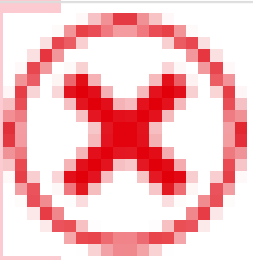
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| ObjectObject-Beziehungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ObjectIndicator-Beziehungen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Object Observable Relationships | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Quellen | | | | | | |
| Bedrohungsquellen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| TAXII-Profile | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Externe Intelligenz | | | | | | |
| Datenschutzverletzung – Bibliothek | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| WHOIS-Bibliothek | | | | | |  |
| Administration | | | | | | |
| Eigenschaften | |  | |  | |  |
| Angriffsmechanismen | |  | |  | |  |
| Angriffsmotivationen | |  | |  | |  |
| Discovery-Methoden | |  | |  | | |
| Feeds | | | |  | |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Indikatortypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Infrastrukturtypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Beabsichtigte Wirkungen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Malware-Fähigkeiten | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Schadsoftwaretypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Benachrichtigungen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Erkennbare Typen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Quotengrenzdefinitionen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Berichtstypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Bedrohungsakteurrollen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Bedrohungsakteurtypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Tooltypen | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Fallverwaltung | | | | | | |

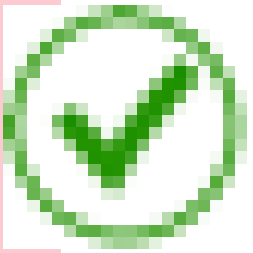
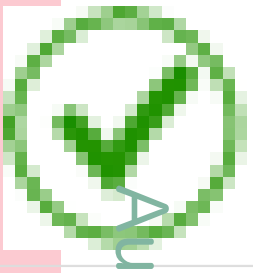
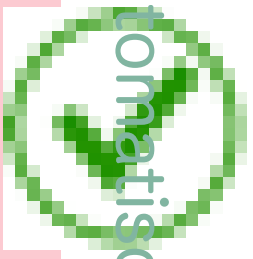
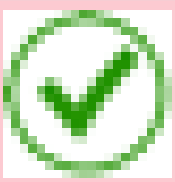
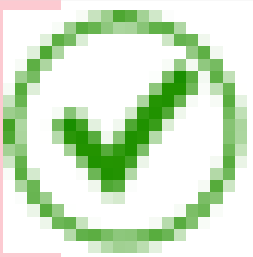
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Alle Fälle | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| Offene Fälle | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| Meine Fälle | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| MITRE ATT&CK-Repository | | | | | | |
| Übersicht | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Matrizen | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Techniken | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Mitigationen | | | | | |  |
| Gruppen | | | | | |  |
| Malware | | | | | |  |
| Tools | | | | | | |
| MITRE-Beziehungen | | | | | | |
| Heatmap und Navigator | | | |  | |  |

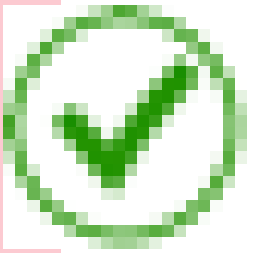
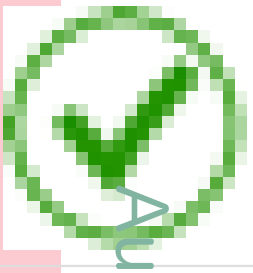
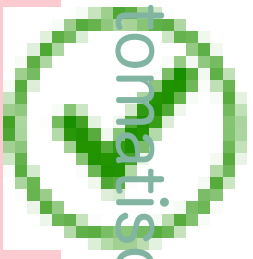
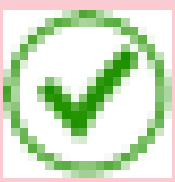
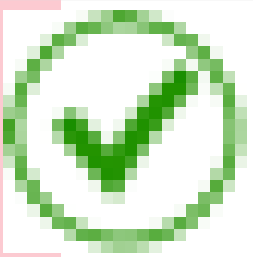
Automatisch übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| CVE-Technikzuordnung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| MITRE ATT&CK-Administration | | | | | | |
| Datenquellenzuordnung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Datenkomponentenzuordnung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Definition der Erkennungsabdeckung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Zuordnung der Abdeckung durch Erkennung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Definition der Abdeckung durch Risikominderung | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

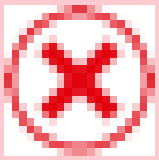
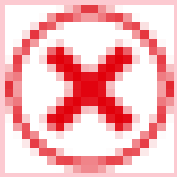
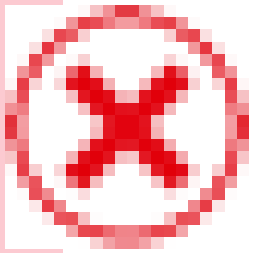
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Rechner für Abdeckung durch Risikominderung | | | | | |  |
| Zuordnung der Abdeckung durch Risikominderung | | | | | |  |
| Extraktionsregel für Technik | | | | | |  |
| Erkennungsregeln MITRE ATTCK-Zuordnung | | | | | | |
| Definition der Bedrohungsgruppentechnik-Heatmap | | | | | | |
| Bedrohungsgruppe MITRE ATTCK-Technikzuordnung | | | |  | |  |

Automatisch übersetzt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Modul | sn_si.admin | sn_si.analyst | sn_si.ciso | sn_si.manager | sn_ti.admin | sn_ti.case_user_read |
|---|---|---|---|---|---|---|
| Eigenschaften | |  | |  | |  |

[End]

[store-future: BEGIN review]

## Modulzugriff nach Rolle für Vulnerability Response

Informationen zu Vulnerability Response finden Sie unter den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

## Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| CISO-Dashboard | ✗ | ✗ | ✓ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Korrekturübersicht | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Übersicht | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Genehmiger-Übersicht | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Übersicht | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Meine Freigaben | ✗ | ✓ | ✗ | |
| Korrekturaufgaben | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Aktiv | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Mir zugewiesen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Meinen Gruppen zugewiesen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Alle | ✗ | ✓ | ✗ | |
| Angreifbare Elemente | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Kritisches Risiko | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Hohes Risiko | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

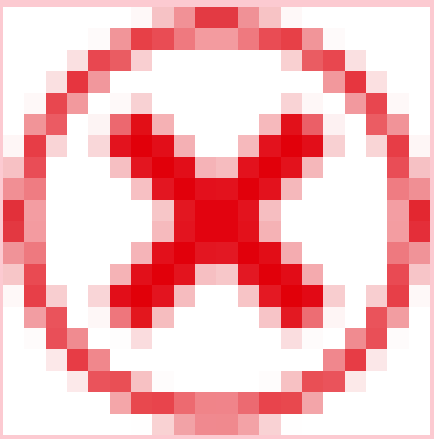
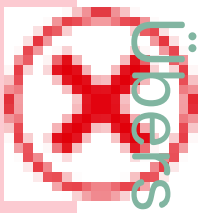
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Nutzbar |  | |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Ziel rückt näher | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Verfehltes Ziel | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Innerhalb der letzten 90 Tage | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Älter als 90 Tage | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Nicht zugewiesen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

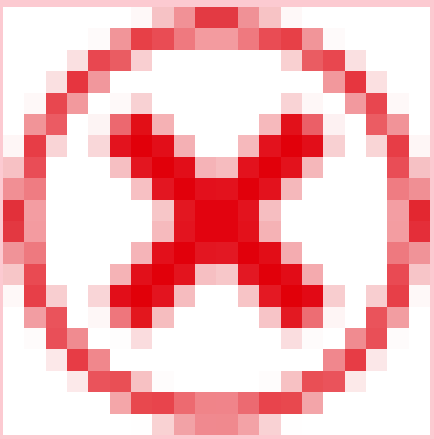
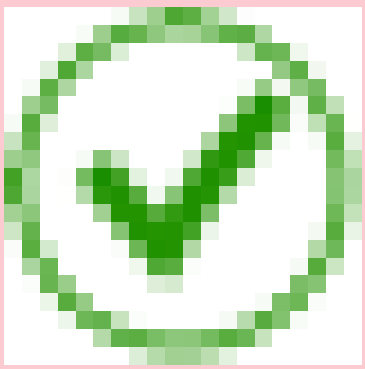
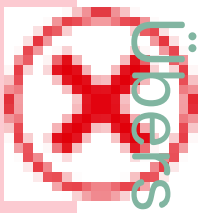
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Nicht gruppiert |  |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Außer Betrieb genommen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Mehrere Zurückstellungen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

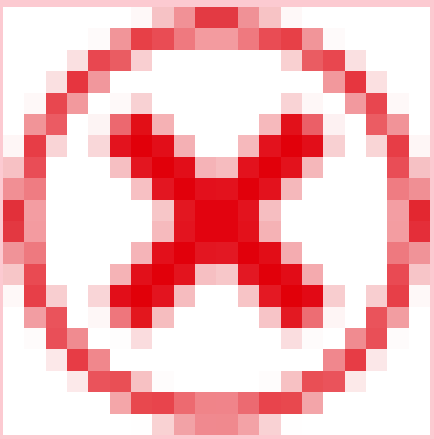
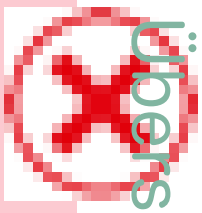
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Alle |  | |  | |
| Lösungen | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Alle | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Ersetzung mit höchster Priorität | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Mit angreifbaren Elementen | ✗ | ✓ | ✗ | |
| Bibliotheken | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| NVD | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| CWE | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Drittpartei | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Software mit Schwachstellen | ✗ | ✓ | ✗ | |
| Schwachstellenscan | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Überprüfungen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Scanner | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Scan-Warteschlange | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Quotengrenzdefinitionen | ✗ | ✓ | ✗ | |
| Administration | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Setup-Assistent | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Überwachungsthemen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Zuweisungsregeln | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Sicherheitsrisiko-Rechner | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Rechner für Schwachstellen-Rollup | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| AutoClose-Konfiguration | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Ausnahmeregeln | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Genehmigungsregeln | ✓ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Klassifizierungsregeln | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Benachrichtigungen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

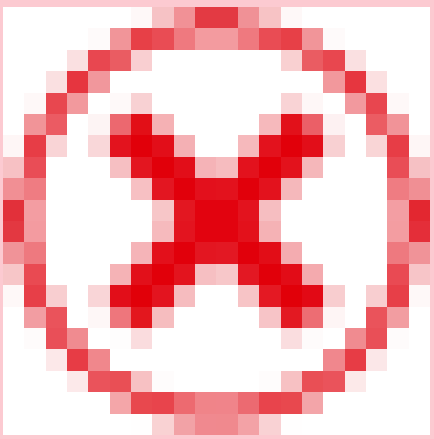
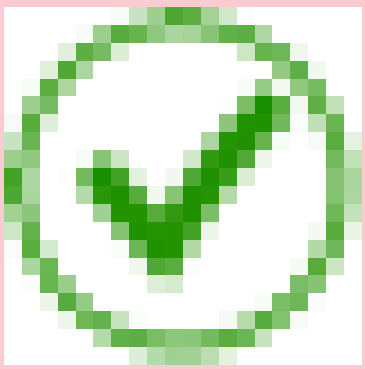
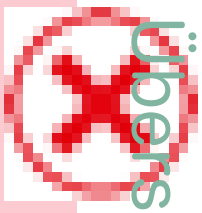
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Warteschlange importieren |  |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Integrationen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| SLA-Definitionen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| SAM-NVD konfigurieren | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Konfiguration der Scan-Abdeckung | ✗ | ✓ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Ausnahmenverwaltung | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Verwendungsbericht | ✗ | ✗ | ✗ | |
| Diagnosen | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations**

***Informationen für andere Rollen:***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_sec_cmn.manage_approval_rules | sn_vul.access_setup_assistant | sn_vul.ciso_read | sn_v |
|---|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

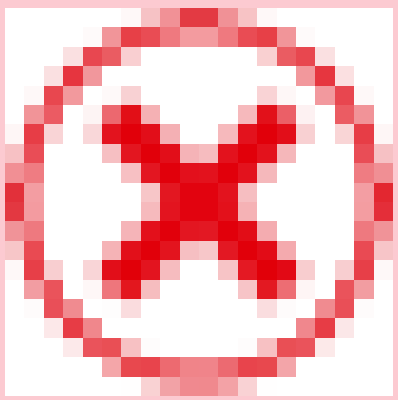
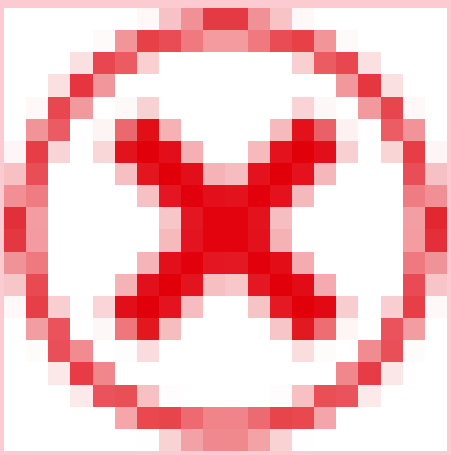
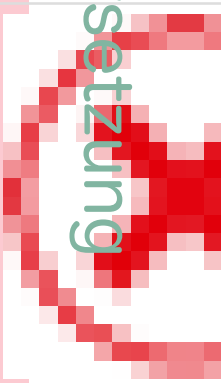
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| CISO-Dashboard |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Korrekturübersicht | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

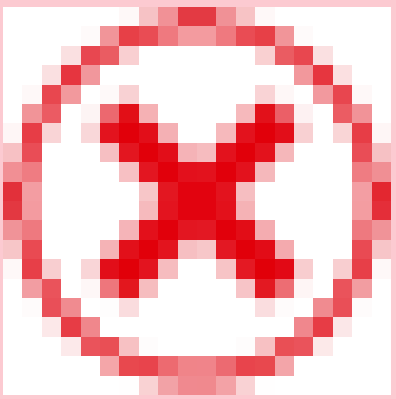
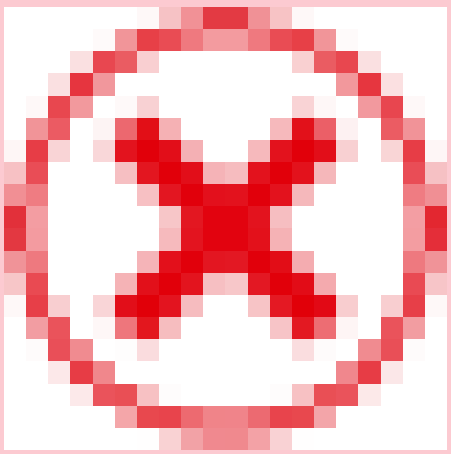
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Übersicht |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Genehmiger-Übersicht | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Übersicht | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Meine Freigaben | | | |
| Korrekturaufgaben | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Aktiv | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Mir zugewiesen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Meinen Gruppen zugewiesen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Alle | | | |

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Kritisches Risiko | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Hohes Risiko | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Nutzbar | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Ziel rückt näher | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Verfehltes Ziel | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Innerhalb der letzten 90 Tage | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Älter als 90 Tage | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Nicht zugewiesen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Nicht gruppiert | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Außer Betrieb genommen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Mehrere Zurückstellungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Alle | | | |

Lösungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Alle | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Ersetzung mit höchster Priorität | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Mit angreifbaren Elementen | | | |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| NVD | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| CWE | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Drittpartei | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Software mit Schwachstellen | ✗ | ✗ | ✗ |
| Schwachstellenscan | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Scanner | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Scan-Warteschlange | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Quotengrenzdefinitionen | | | |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Setup-Assistent | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Überwachungsthemen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Sicherheitsrisiko-Rechner | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Rechner für Schwachstellen-Rollup | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| AutoClose-Konfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Ausnahmeregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Genehmigungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Klassifizierungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Benachrichtigungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Warteschlange importieren | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Integrationen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| SLA-Definitionen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| SAM-NVD konfigurieren | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Konfiguration der Scan-Abdeckung | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Ausnahmenverwaltung | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Verwendungsbericht | | | |
| Diagnosen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.configure_nvd_integration | sn_vul.configure_scan_coverage_read | sn_vul.configure_v |
|---|---|---|---|
| Überprüfungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| CISO-Dashboard | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Korrekturübersicht | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Übersicht | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Genehmiger-Übersicht | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Übersicht | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Meine Freigaben | ✓ | ✓ | ✗ |
| Korrekturaufgaben | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Aktiv | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Mir zugewiesen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Meinen Gruppen zugewiesen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

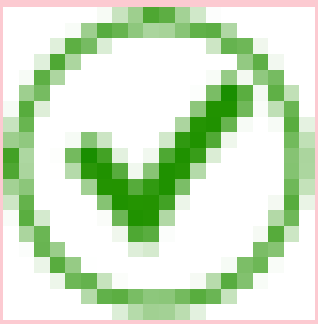
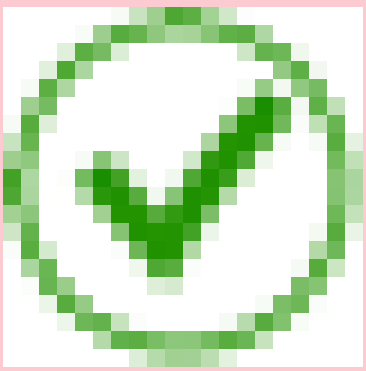
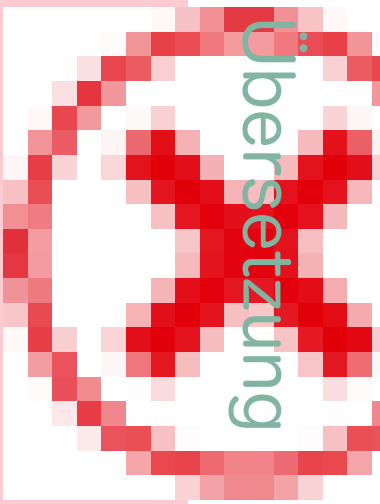
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Alle |  |  |  |

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Kritisches Risiko | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Hohes Risiko | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Nutzbar | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Ziel rückt näher | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Verfehltes Ziel | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Innerhalb der letzten 90 Tage | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Älter als 90 Tage | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Nicht zugewiesen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Nicht gruppiert | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Außer Betrieb genommen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Mehrere Zurückstellungen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

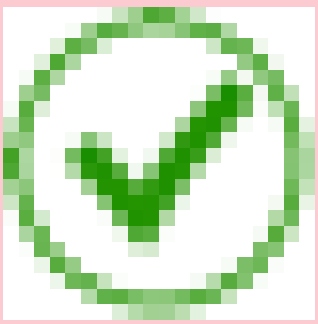
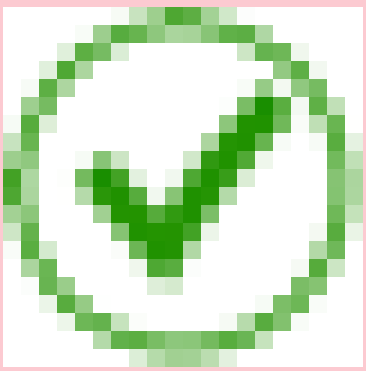
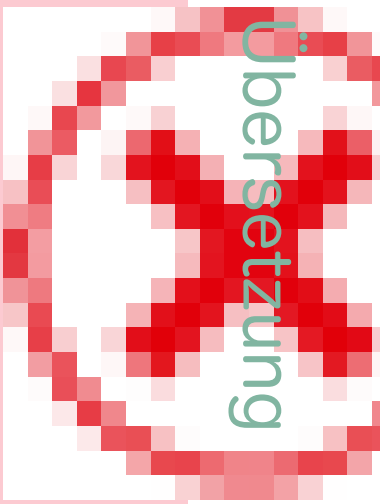
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Alle |  |  |  |
| Lösungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Alle | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Ersetzung mit höchster Priorität | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Mit angreifbaren Elementen | ✓ | ✓ | ✗ |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| NVD | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| CWE | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Drittpartei | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Software mit Schwachstellen | ✓ | ✓ | ✗ |
| Schwachstellenscan | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Überprüfungen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Scanner | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Scan-Warteschlange | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Quotengrenzdefinitionen | ✗ | ✗ | ✗ |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

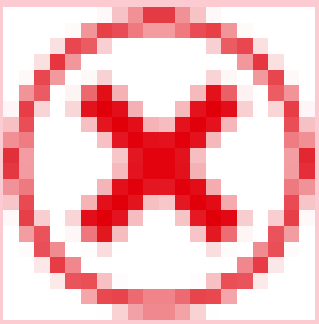
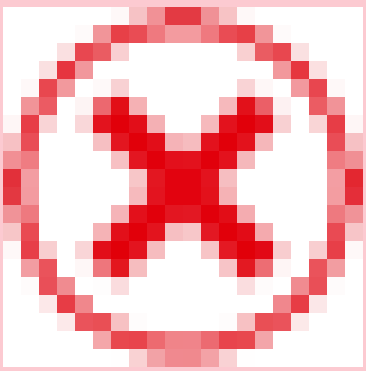
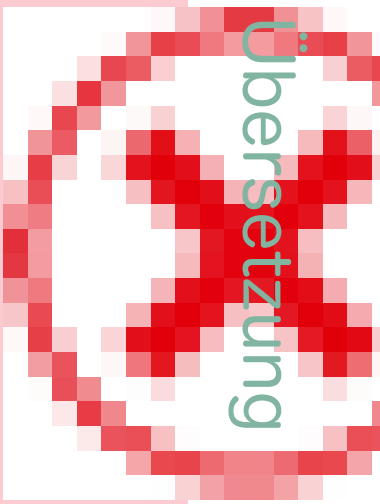
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Setup-Assistent |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Überwachungsthemen | ✓ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Sicherheitsrisiko-Rechner | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Rechner für Schwachstellen-Rollup | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| AutoClose-Konfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

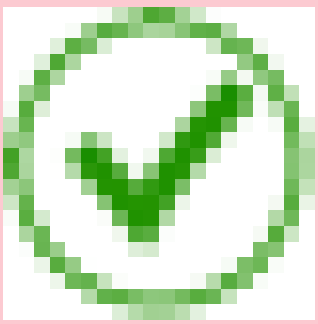
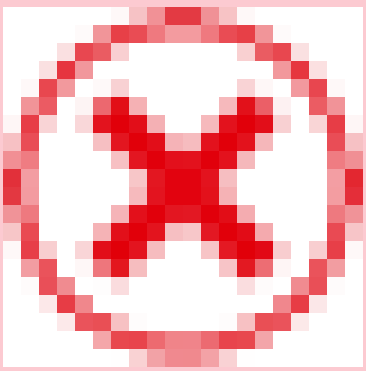
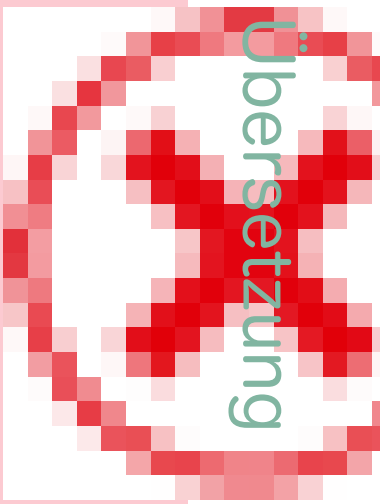
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Ausnahmeregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Genehmigungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Klassifizierungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Benachrichtigungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Warteschlange importieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Integrationen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

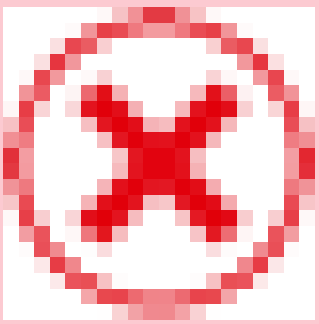
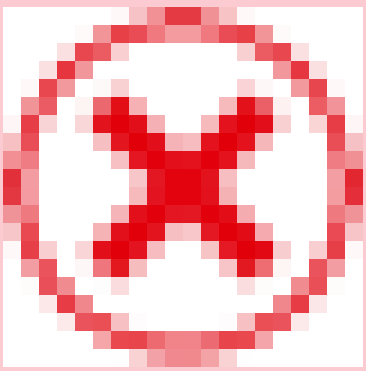
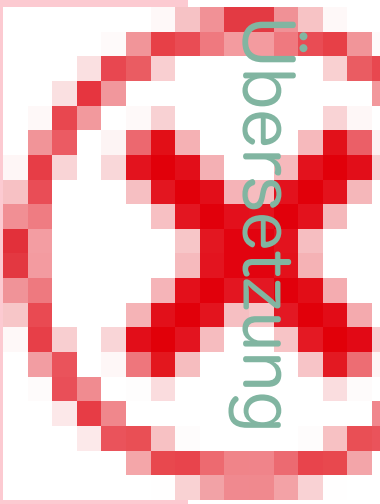
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| SLA-Definitionen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| SAM-NVD konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Konfiguration der Scan-Abdeckung | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Ausnahmenverwaltung | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Verwendungsbericht | ✗ | ✗ | ✗ |
| Diagnosen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.exception_approver | sn_vul.false_positive_approver | sn_vul.manage_assignment_reco |
|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificati |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| CISO-Dashboard | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Korrekturübersicht | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Übersicht | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Genehmiger-Übersicht | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Übersicht | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Meine Freigaben | ✗ | ✗ | ✗ |
| Korrekturaufgaben | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Aktiv | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Mir zugewiesen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Meinen Gruppen zugewiesen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Alle | ✗ | ✗ | ✓ |

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Kritisches Risiko | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Hohes Risiko | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Nutzbar | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Ziel rückt näher | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

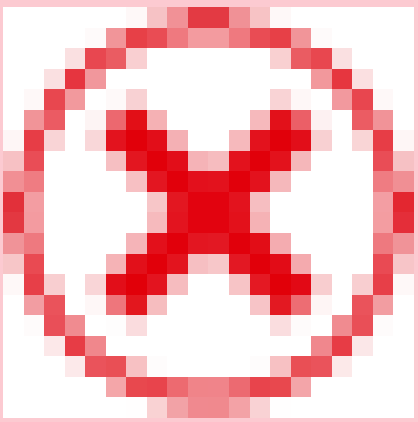
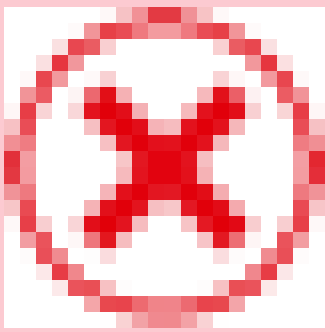
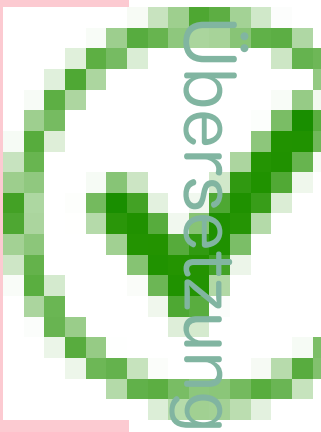
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Verfehltes Ziel |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Innerhalb der letzten 90 Tage | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Älter als 90 Tage | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Nicht zugewiesen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificati |
|---|---|---|---|
| Nicht gruppiert | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Außer Betrieb genommen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Mehrere Zurückstellungen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Alle | ✗ | ✗ | ✓ |
| Lösungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Alle | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Ersetzung mit höchster Priorität | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Mit angreifbaren Elementen | ✗ | ✗ | ✓ |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| NVD | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| CWE | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Drittpartei | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

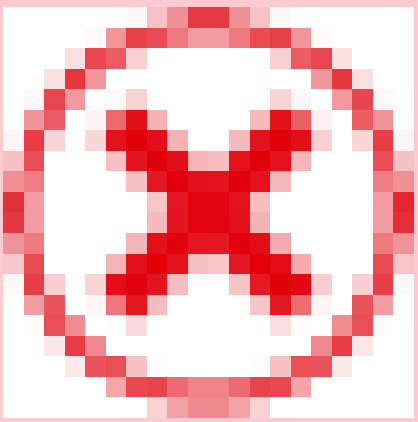
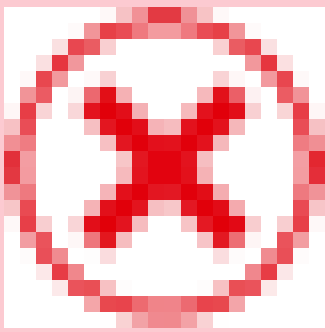
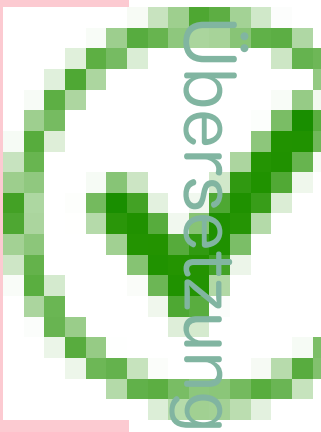
***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificati |
|---|---|---|---|
| Software mit Schwachstellen |  |  |  |
| Schwachstellenscan | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificati |
|---|---|---|---|
| Scanner | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Scan-Warteschlange | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Quotengrenzdefinitionen | ✗ | ✗ | ✗ |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Setup-Assistent | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Überwachungsthemen | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Sicherheitsrisiko-Rechner | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Rechner für Schwachstellen-Rollup | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| AutoClose-Konfiguration | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Ausnahmeregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Genehmigungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Klassifizierungsregeln | ✗ | ✗ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Benachrichtigungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Warteschlange importieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Integrationen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| SLA-Definitionen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| SAM-NVD konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Konfiguration der Scan-Abdeckung | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Ausnahmenverwaltung | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Verwendungsbericht | ✗ | ✗ | ✗ |
| Diagnosen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_auto_close_stale_vi | sn_vul.manage_auto_delete | sn_vul.manage_classificatio |
|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

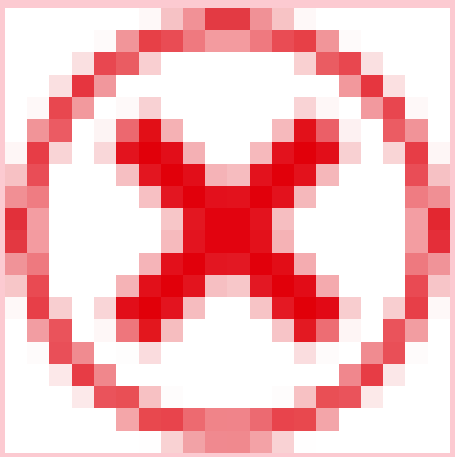
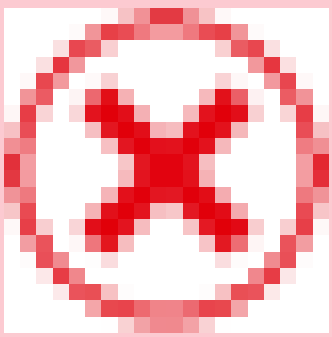
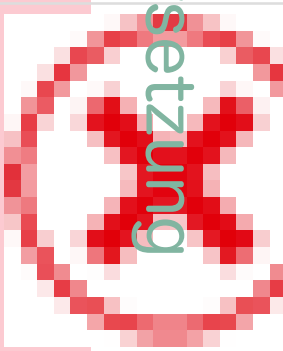
*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notificat |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| CISO-Dashboard |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

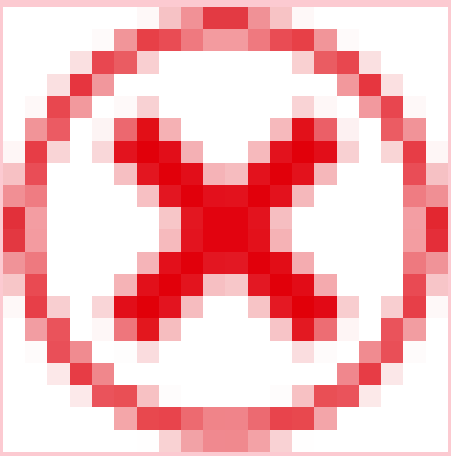
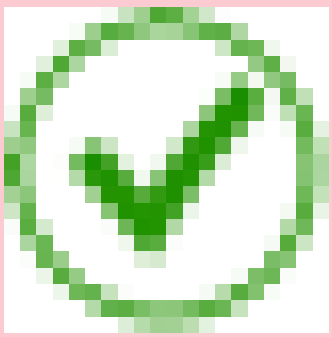
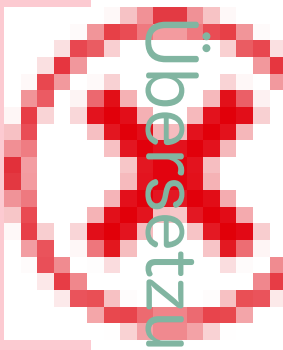
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Korrekturübersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

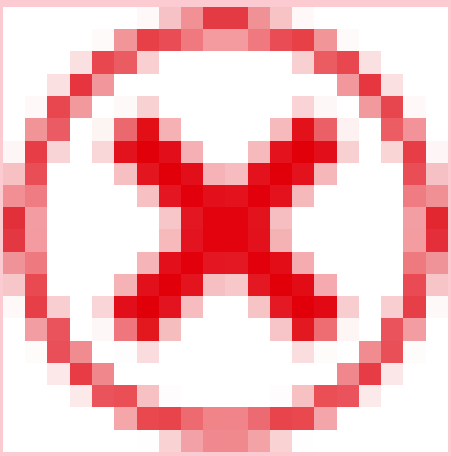
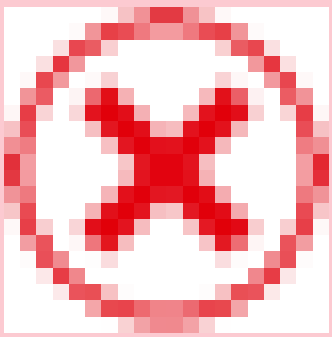
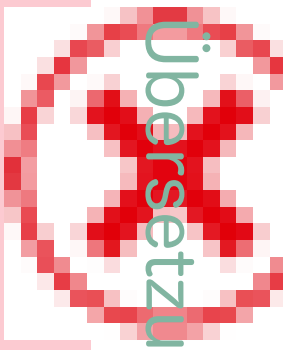
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

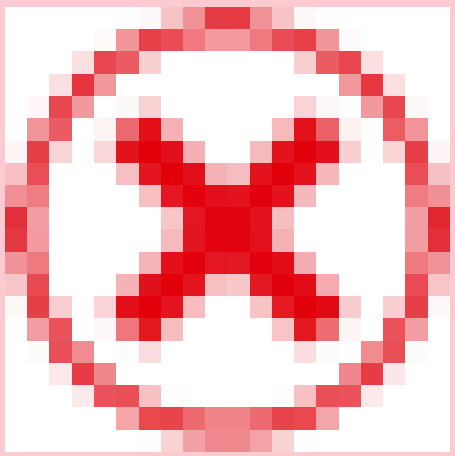
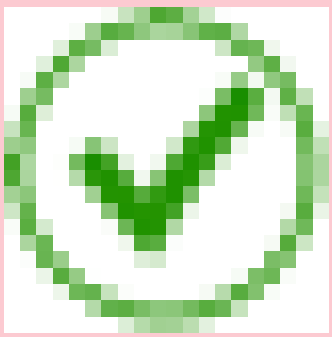
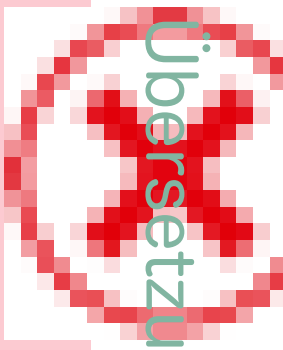
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Übersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

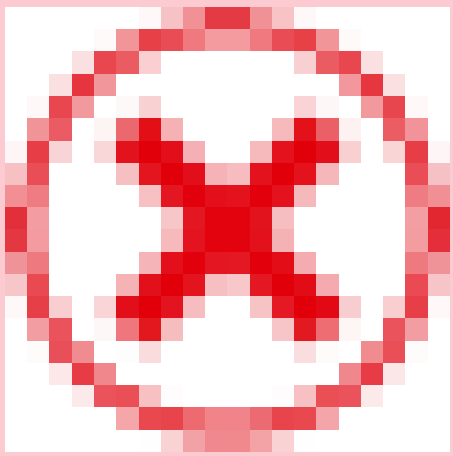
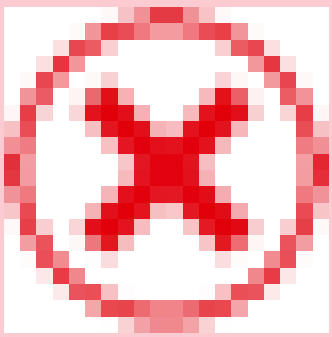
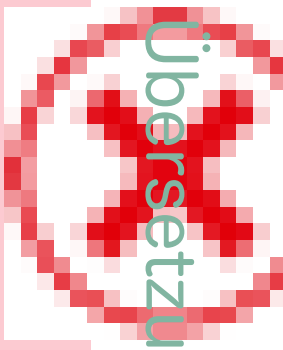
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

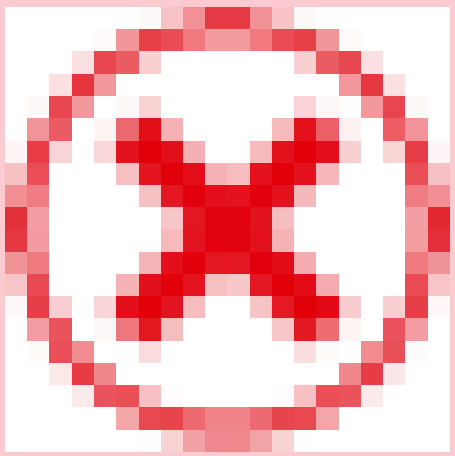
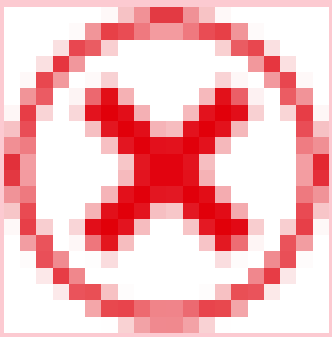
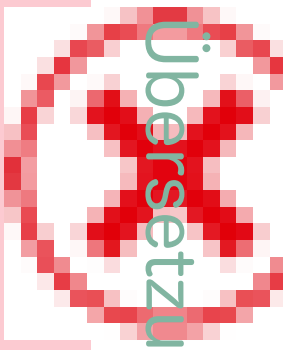
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Genehmiger-Übersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

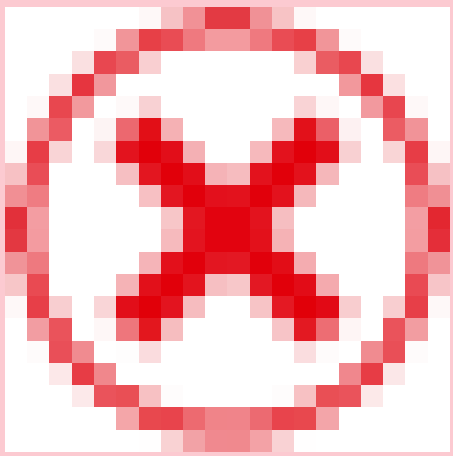
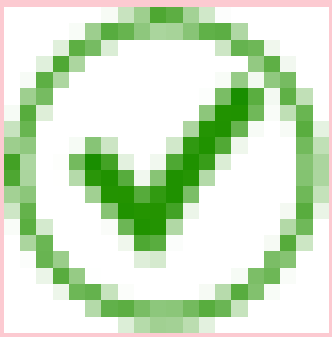
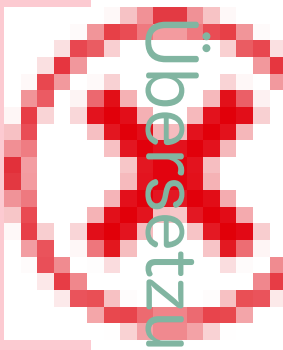
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Übersicht |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

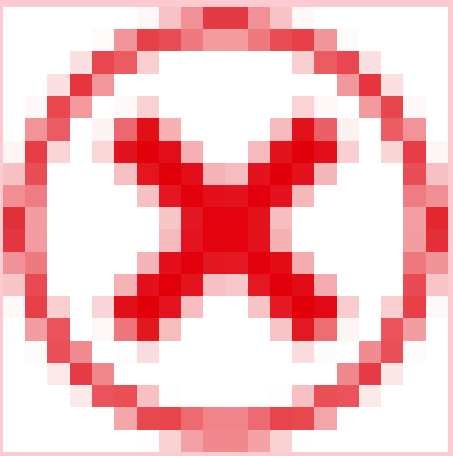
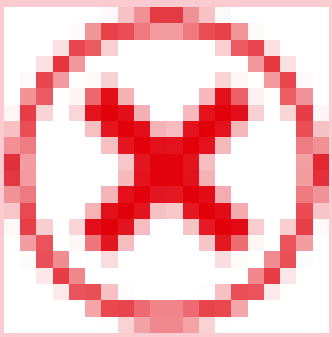
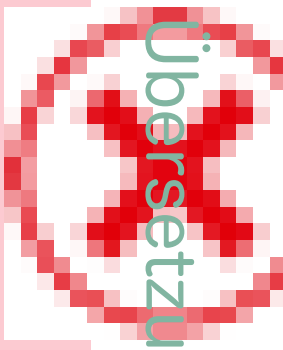
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Meine Freigaben |  |  |  |
| Korrekturaufgaben | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

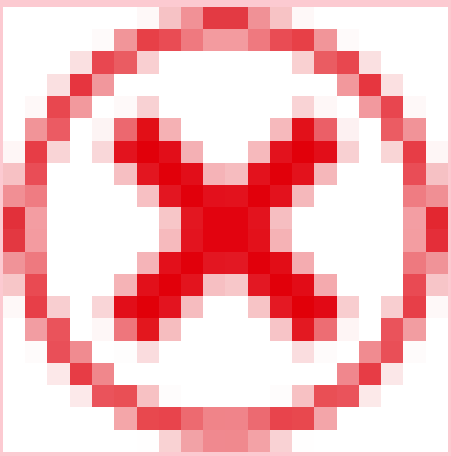
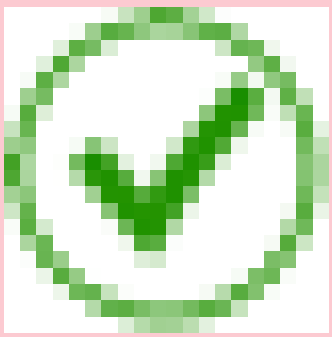
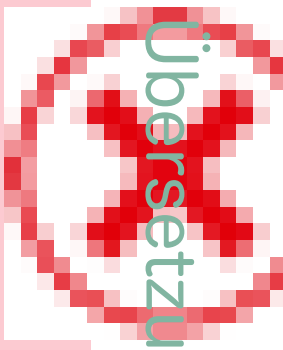
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Aktiv |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

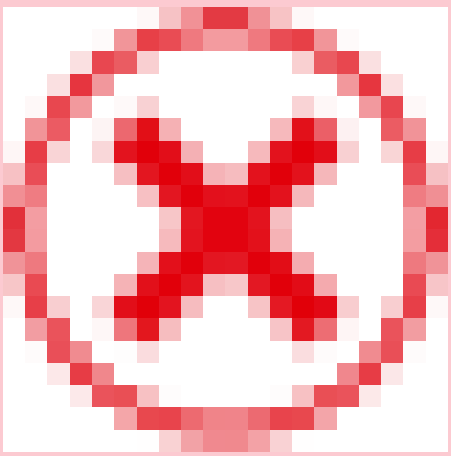
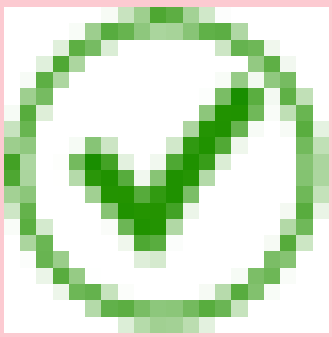
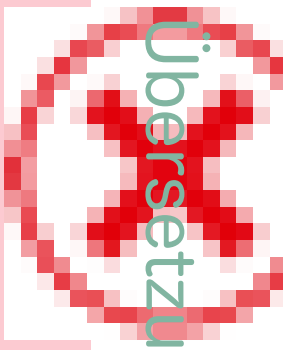
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Mir zugewiesen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

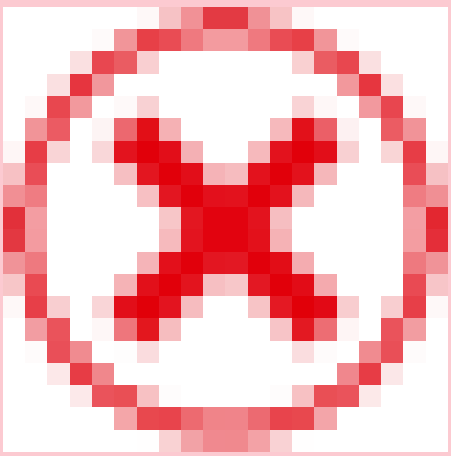
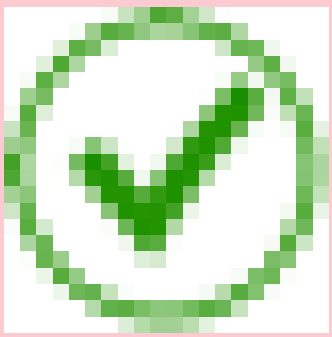
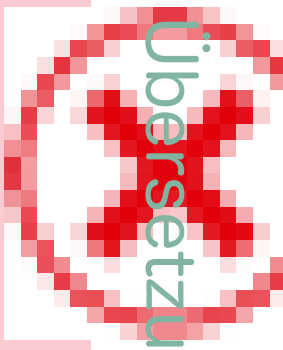
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Meinen Gruppen zugewiesen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

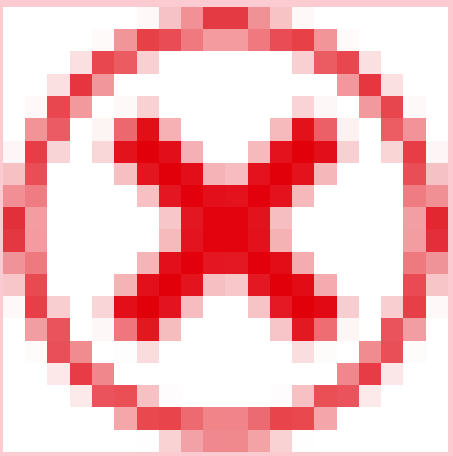
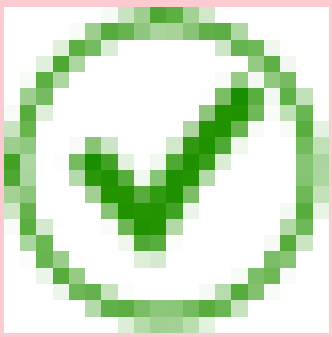
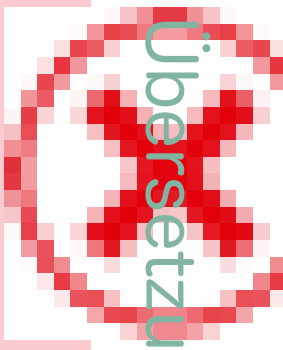
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Alle |  |  |  |
| Angreifbare Elemente | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

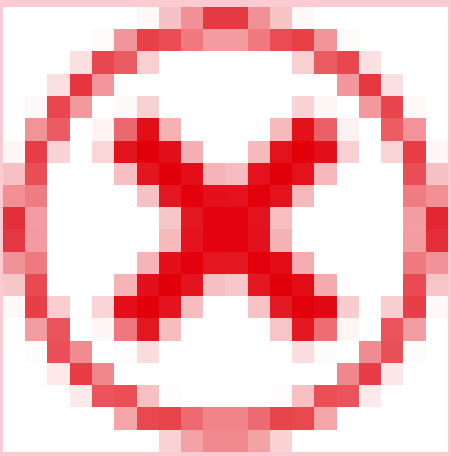
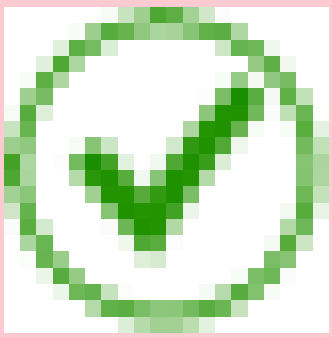
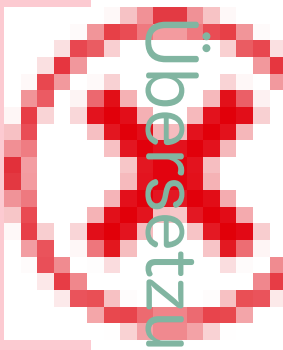
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Kritisches Risiko |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

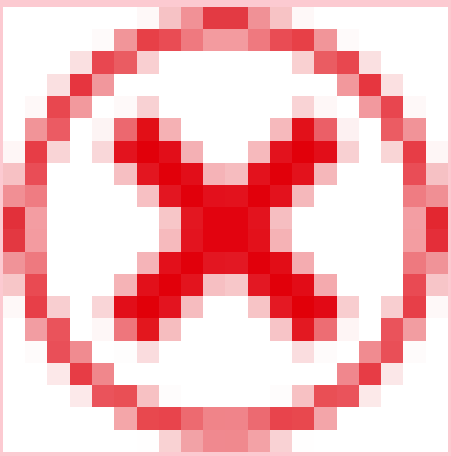
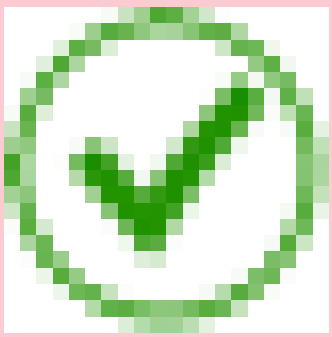
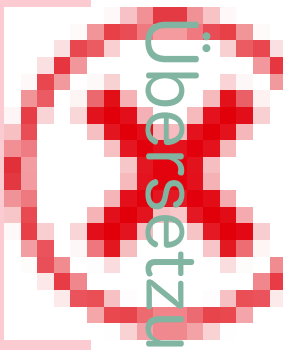
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Hohes Risiko |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

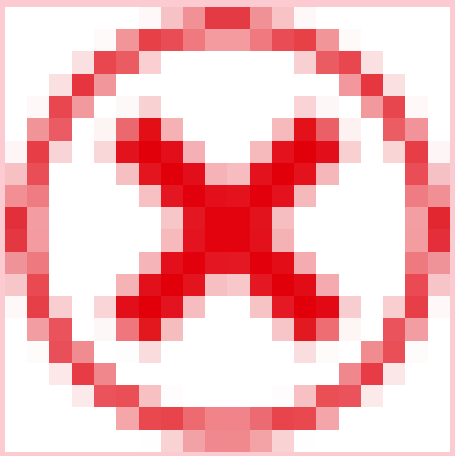
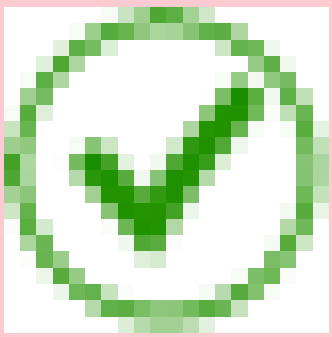
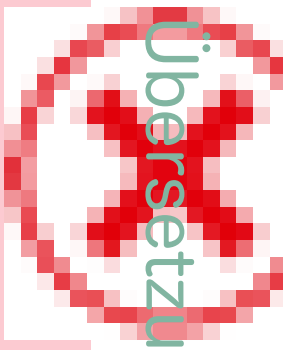
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Nutzbar |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

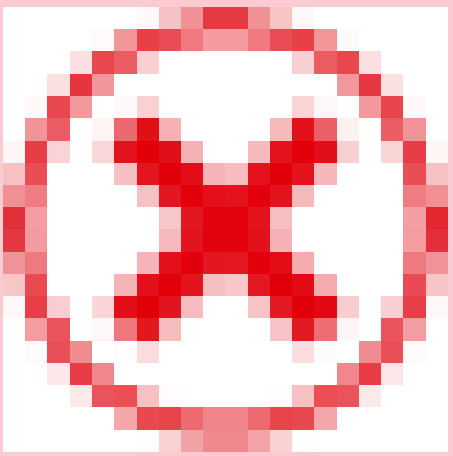
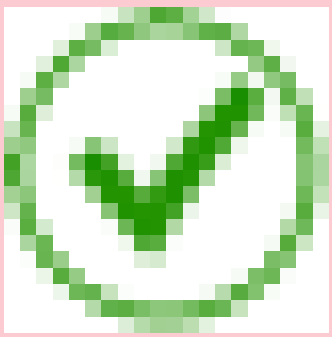
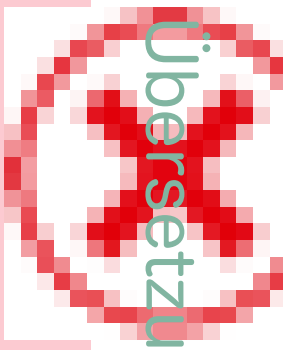
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Ziel rückt näher |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

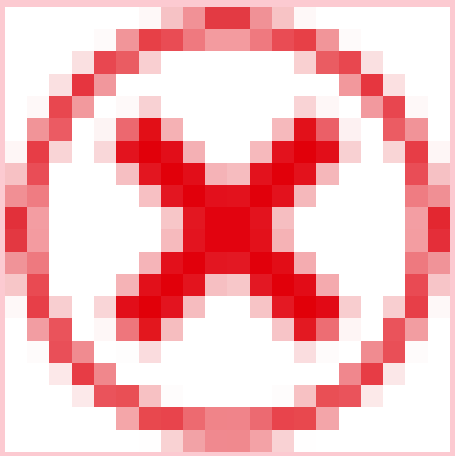
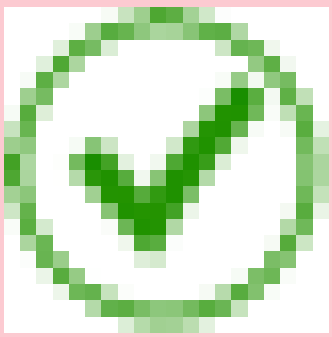
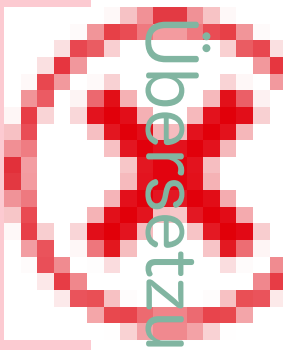
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Verfehltes Ziel |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

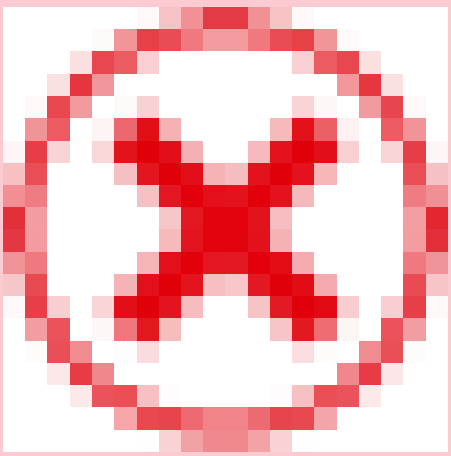
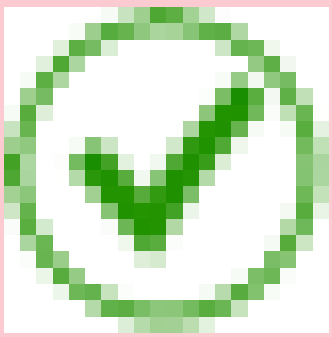
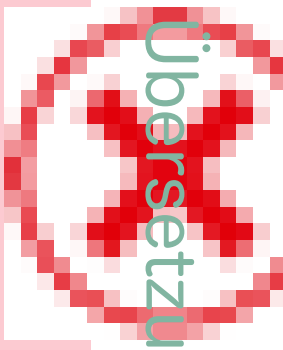
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Innerhalb der letzten 90 Tage |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

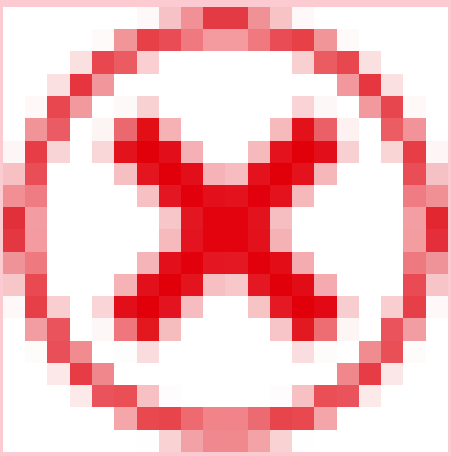
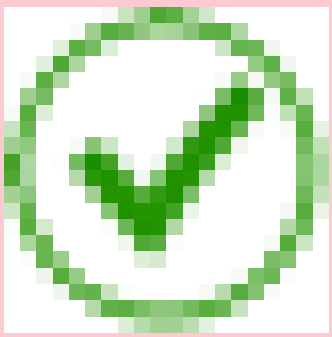
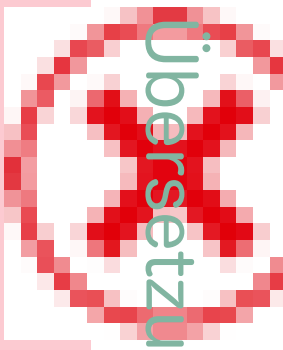
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Älter als 90 Tage |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

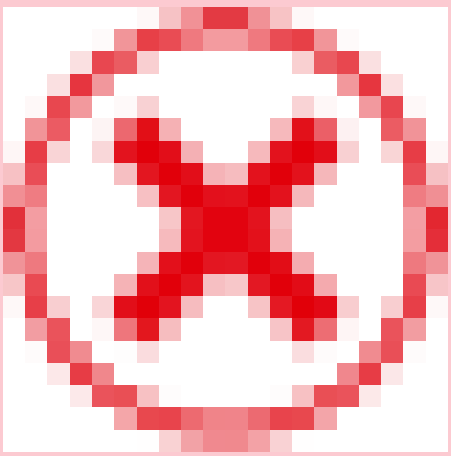
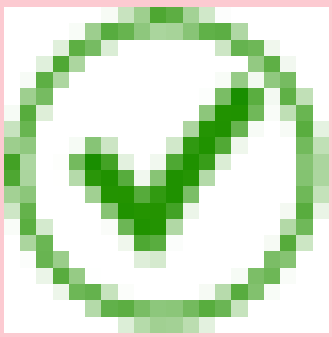
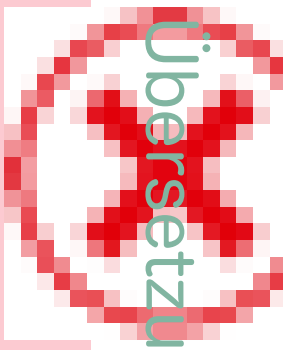
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Nicht zugewiesen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

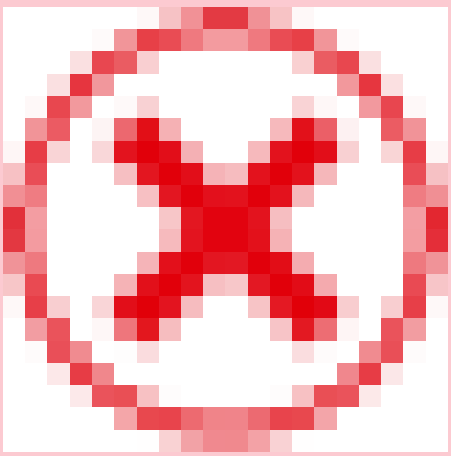
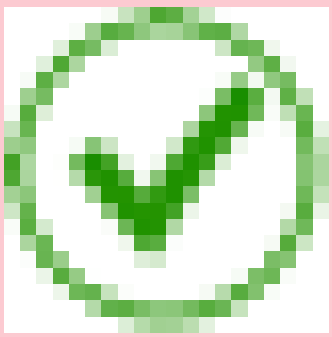
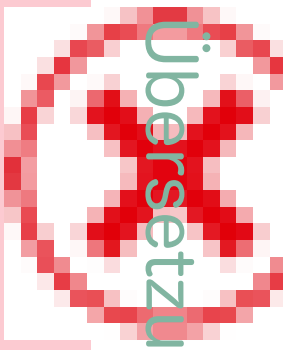
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Nicht gruppiert |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

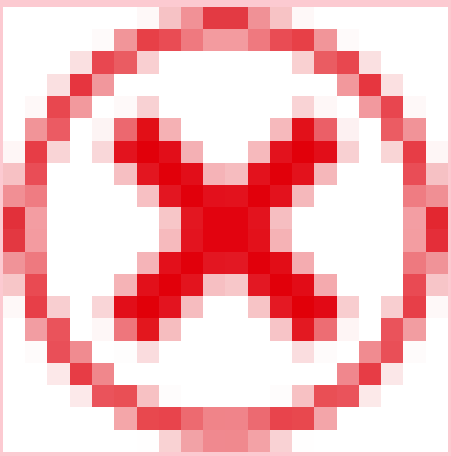
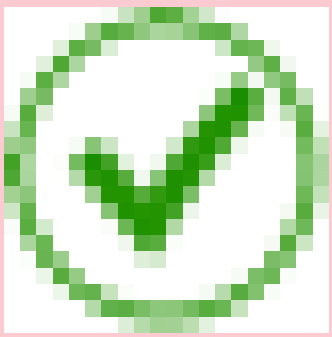
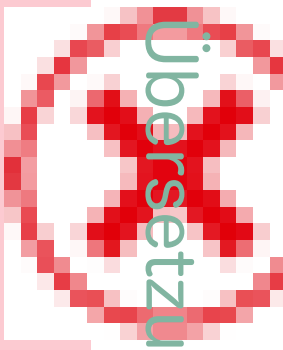
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Außer Betrieb genommen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

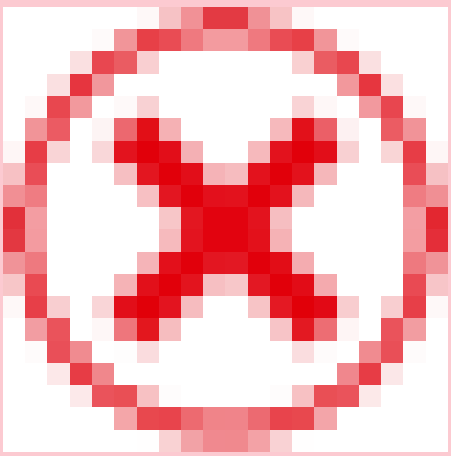
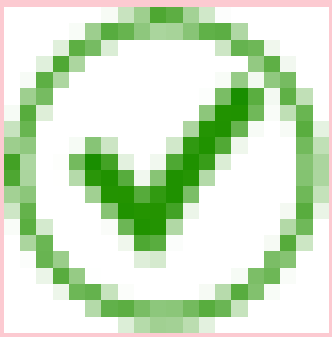
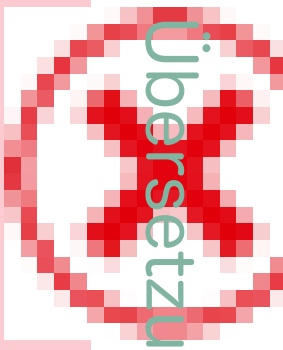
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Mehrere Zurückstellungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

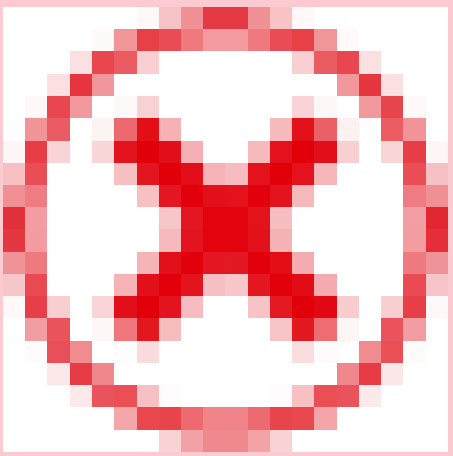
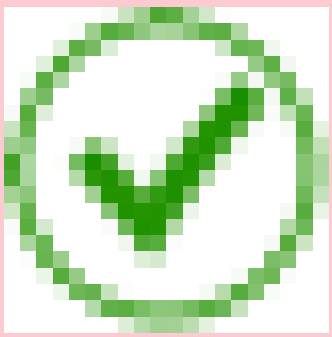
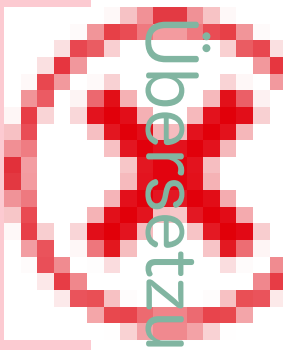
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Alle |  |  |  |
| Lösungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

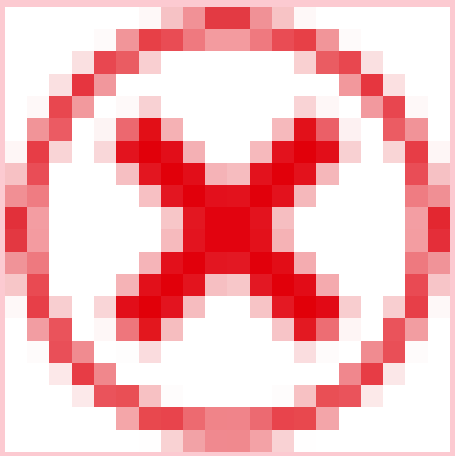
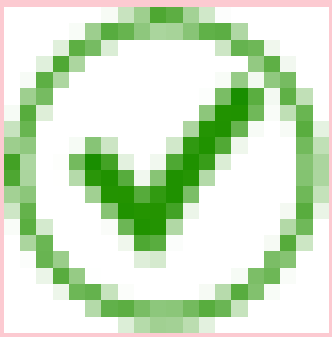
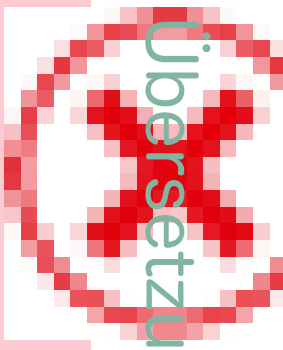
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Alle |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

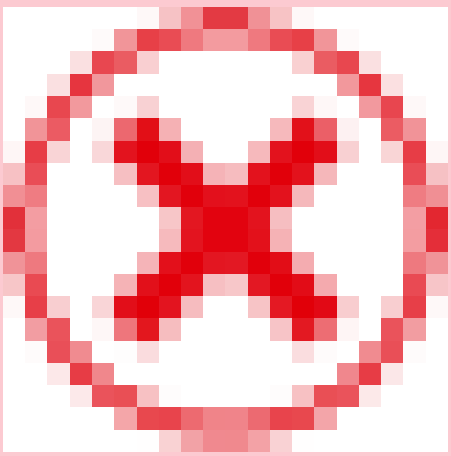
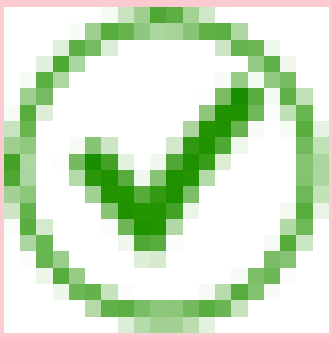
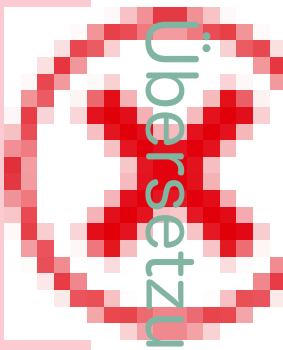
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Ersetzung mit höchster Priorität |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

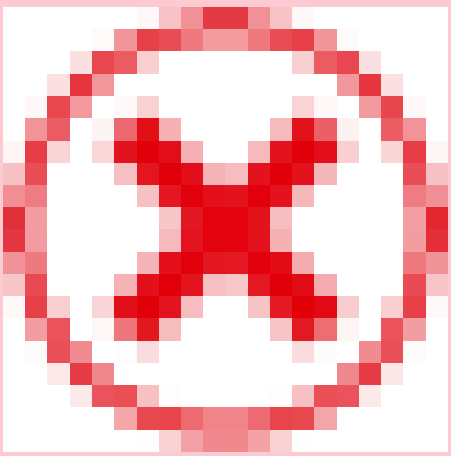
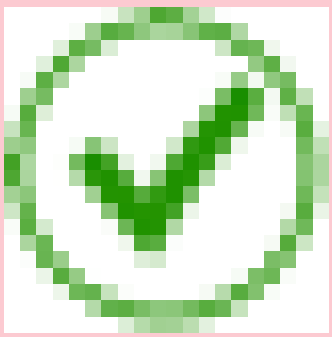
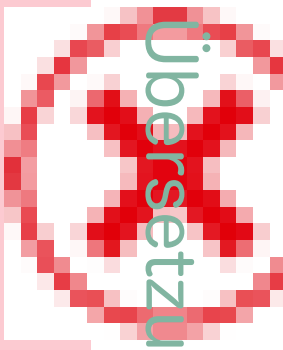
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Mit angreifbaren Elementen |  |  |  |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

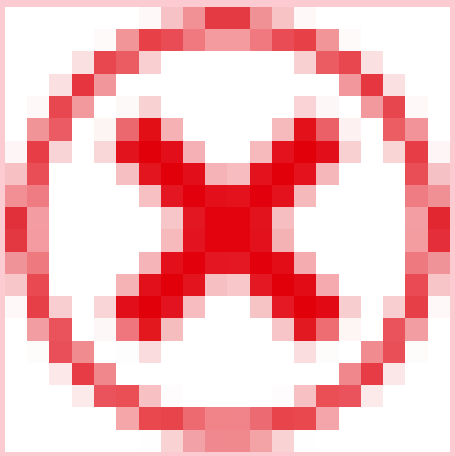
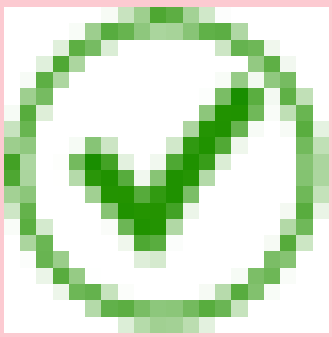
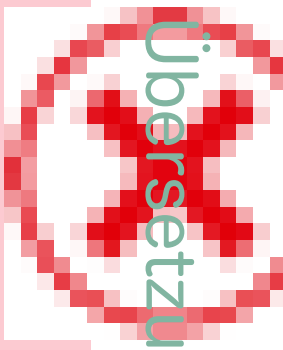
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| NVD |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

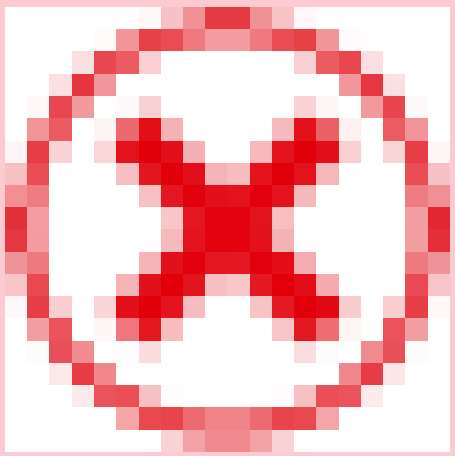
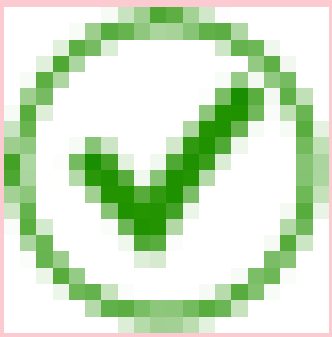
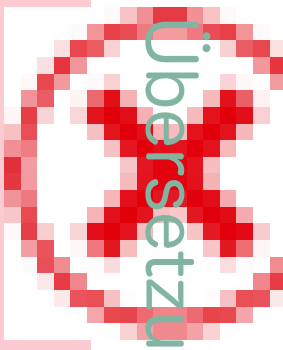
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| CWE |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

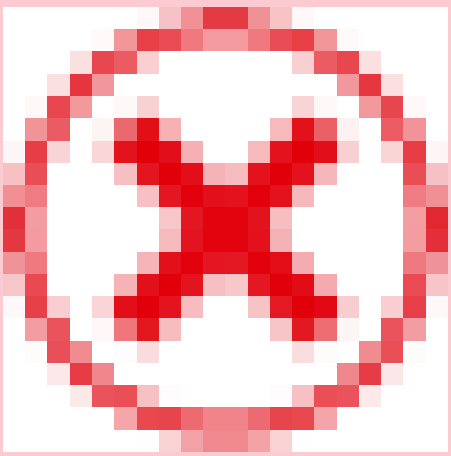
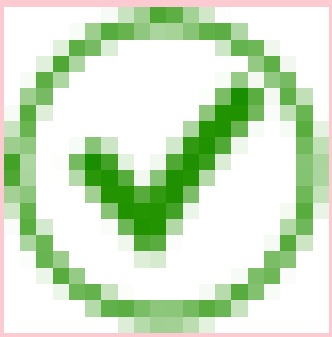
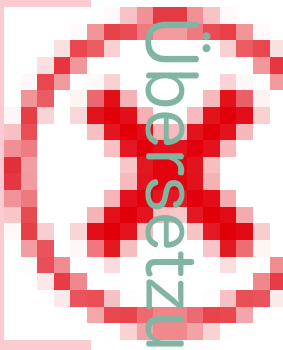
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Drittpartei |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

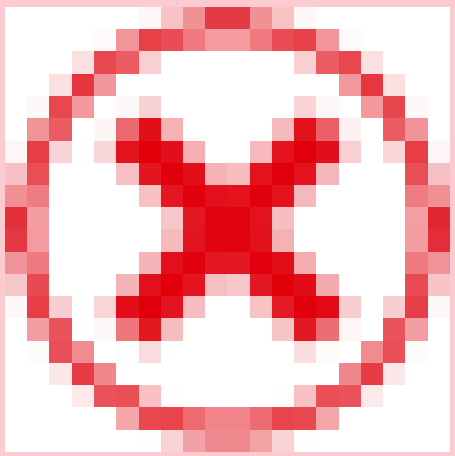
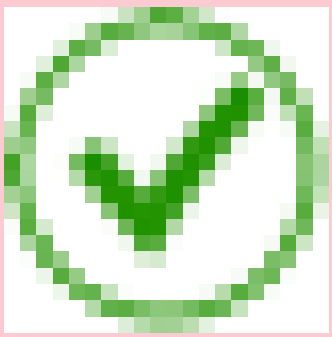
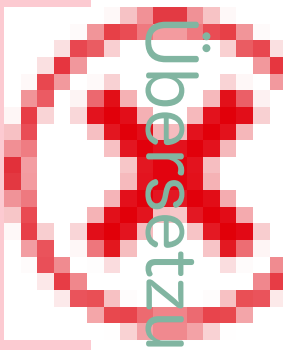
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Software mit Schwachstellen |  |  |  |
| Schwachstellenscan | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

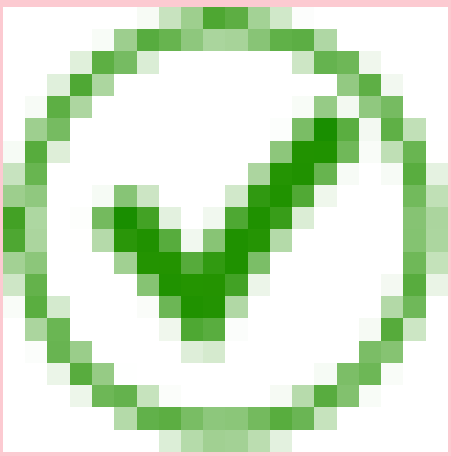
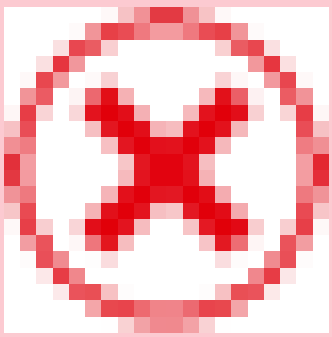
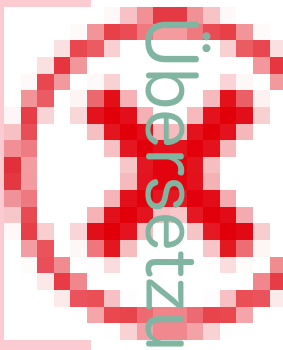
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Bewertung des Gefahrenpotenzials |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

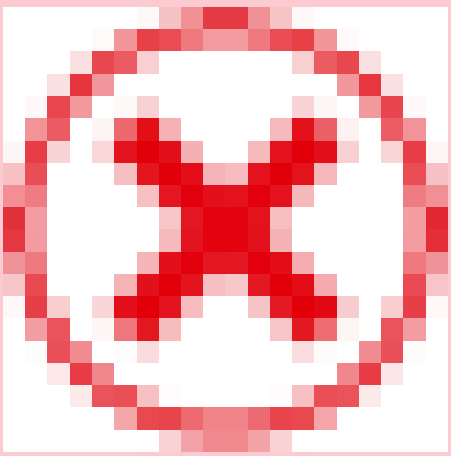
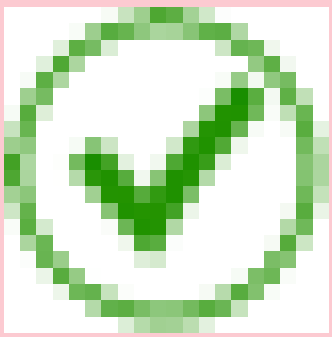
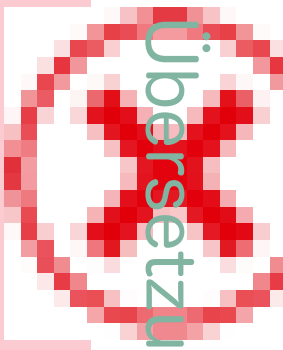
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Überprüfungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Scanner | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

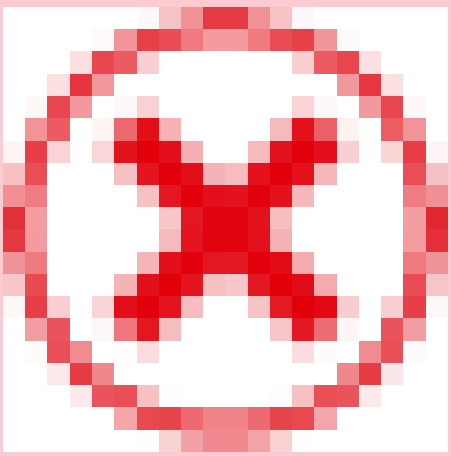
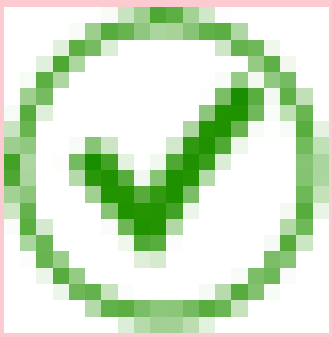
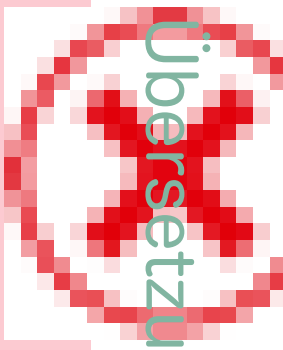
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Scan-Warteschlange |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

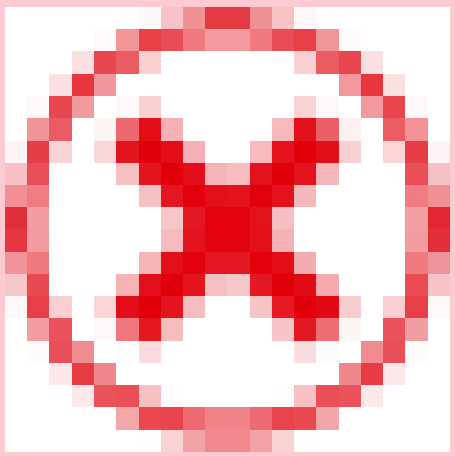
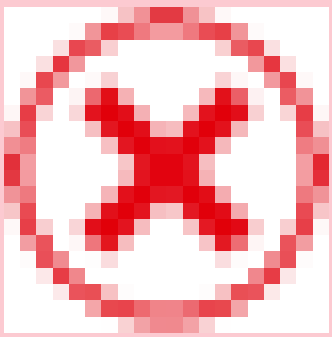
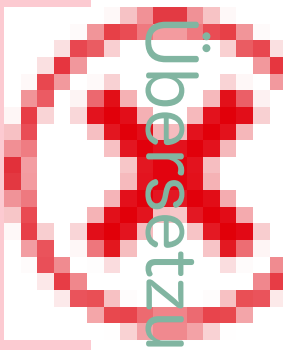
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Scannerquotengrenzen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

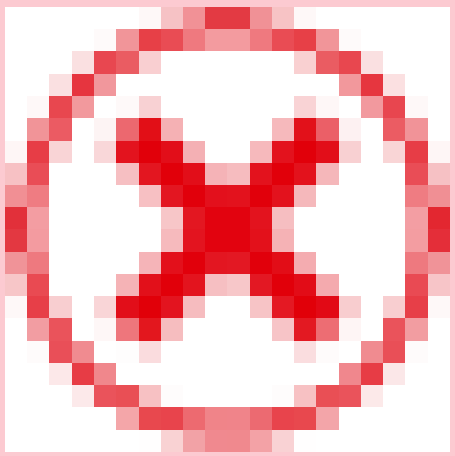
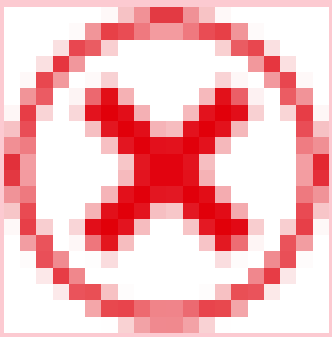
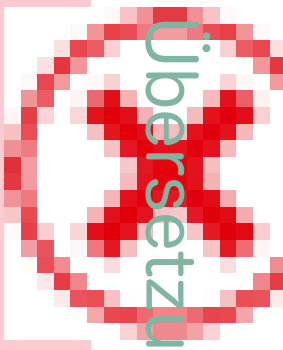
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Quotengrenzdefinitionen |  |  |  |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

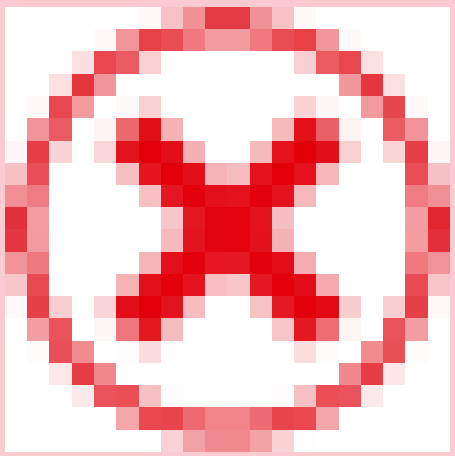
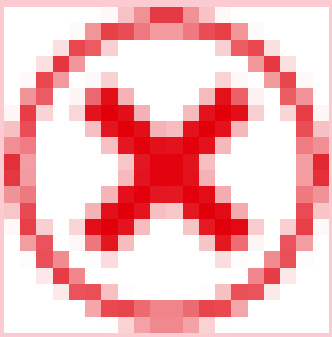
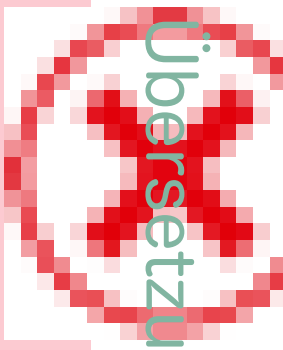
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Setup-Assistent |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

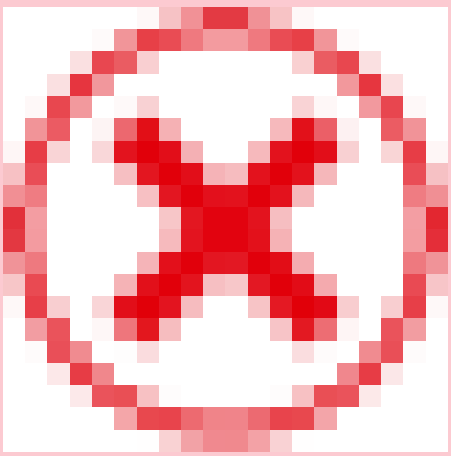
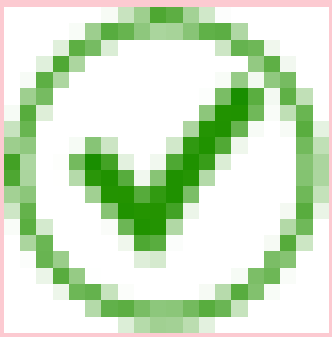
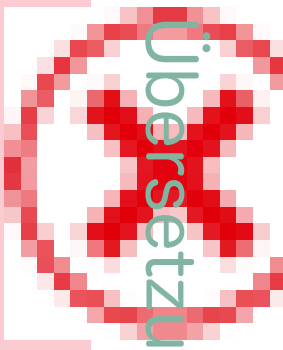
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Überwachungsthemen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

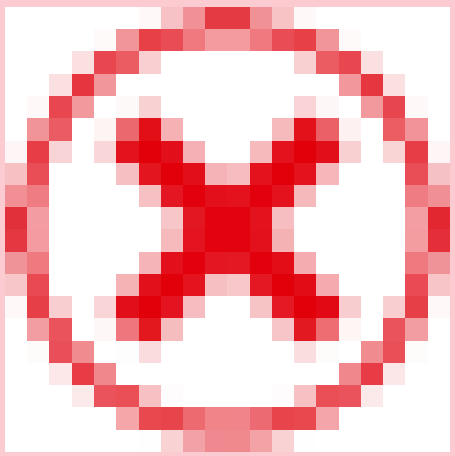
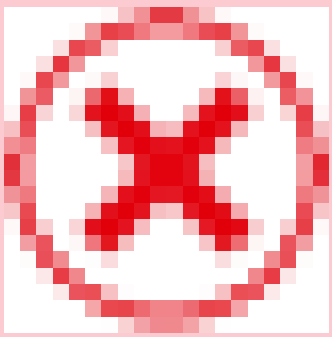
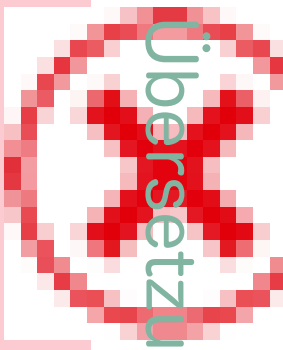
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Zuweisungsregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

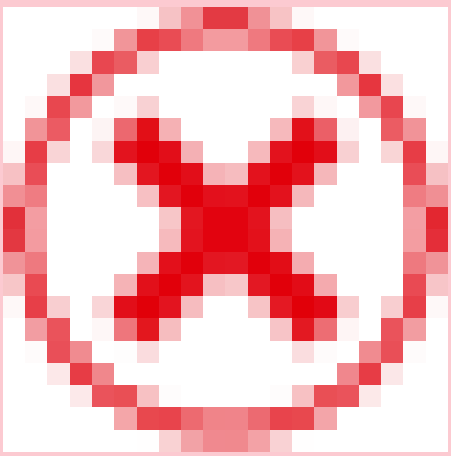
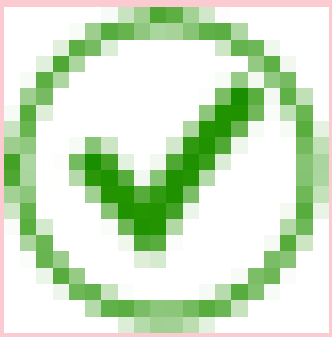
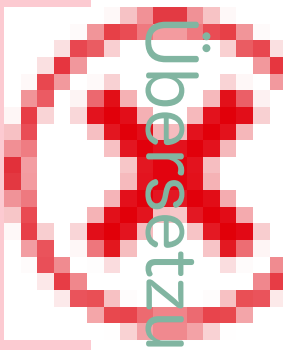
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Regeln für Korrekturaufgaben |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

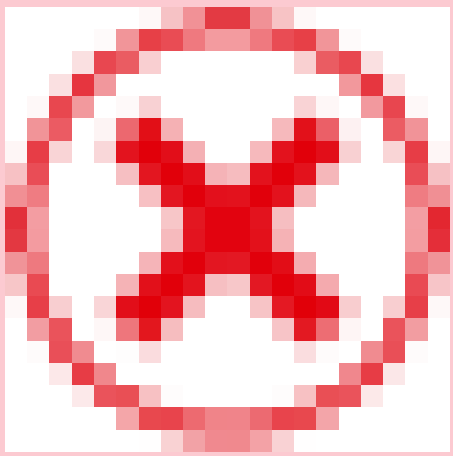
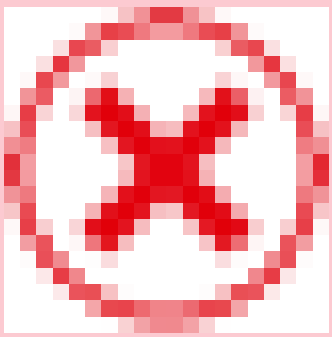
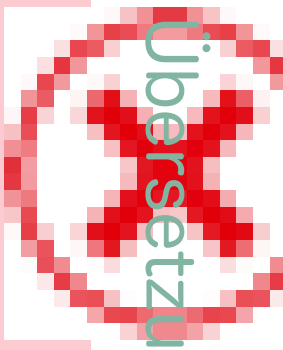
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Zuweisungsempfehlungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

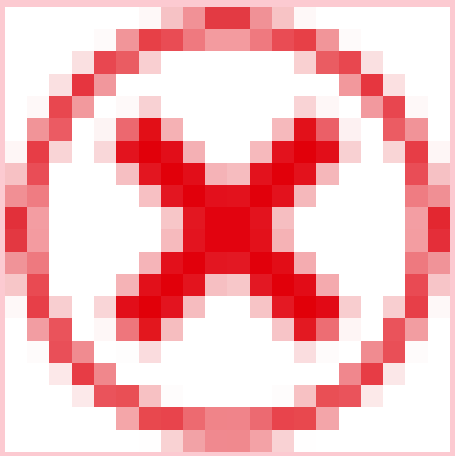
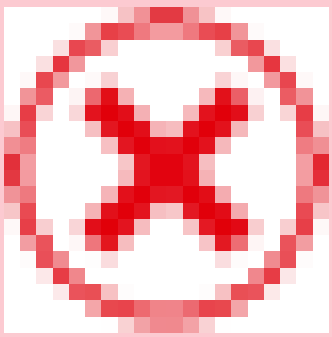
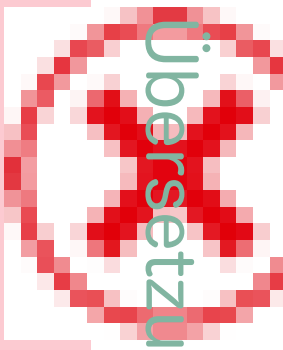
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Sicherheitsrisiko-Rechner |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

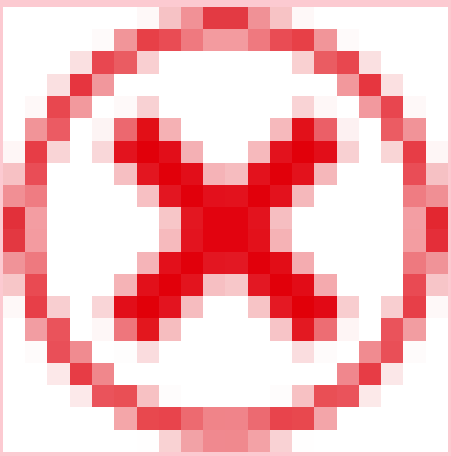
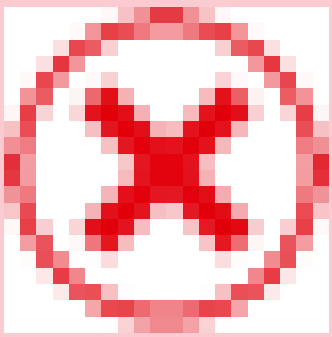
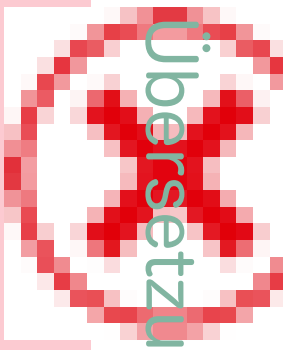
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Rechner für Schwachstellen-Rollup |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

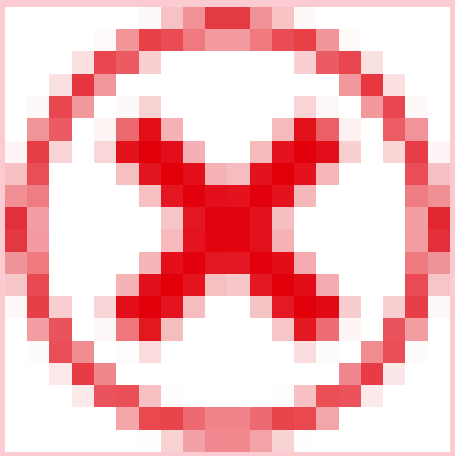
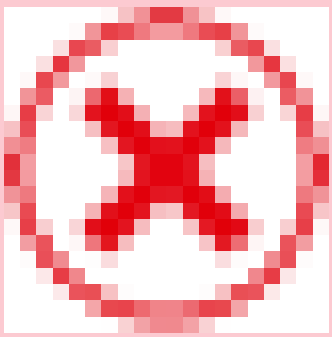
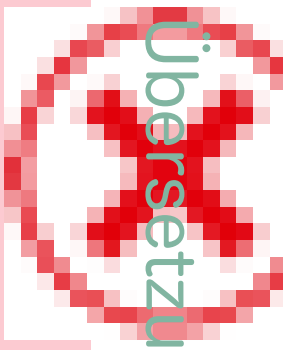
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Nachbesserungszielregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

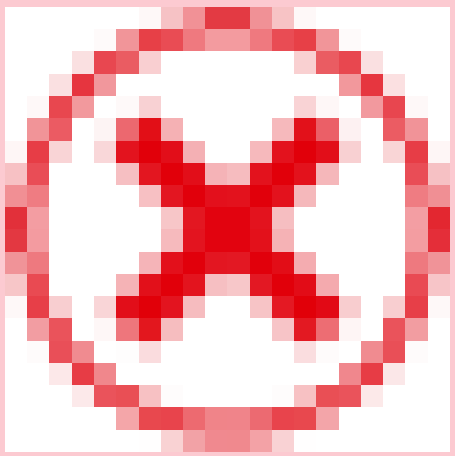
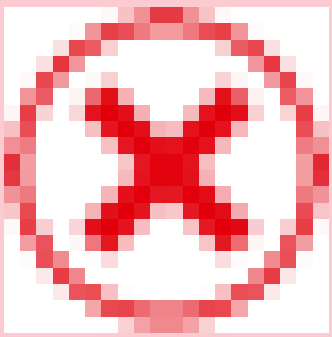
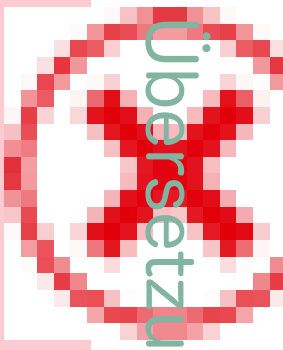
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| AutoClose-Konfiguration |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

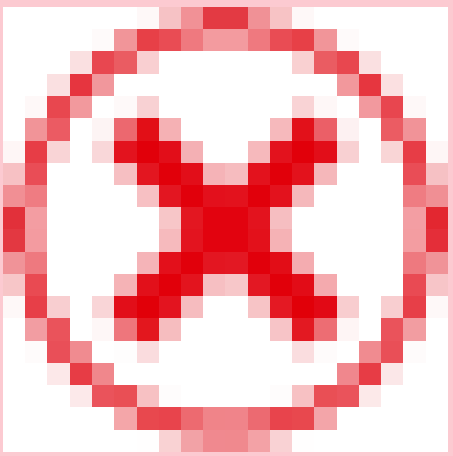
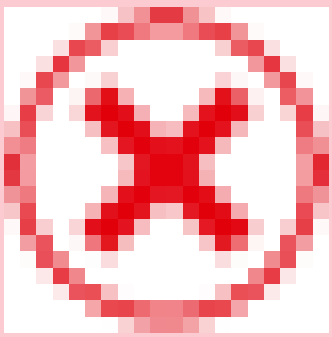
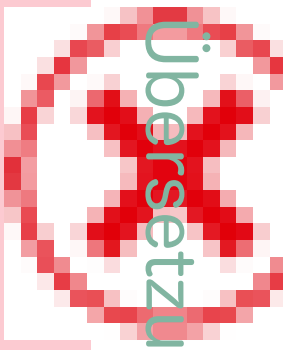
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Ausnahmeregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

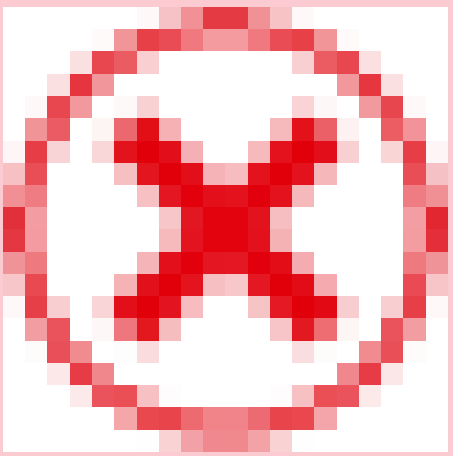
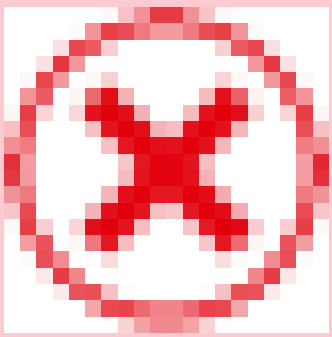
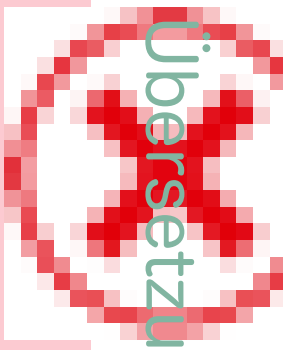
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Genehmigungsregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

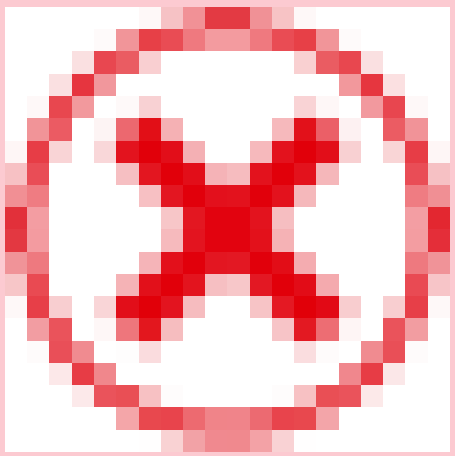
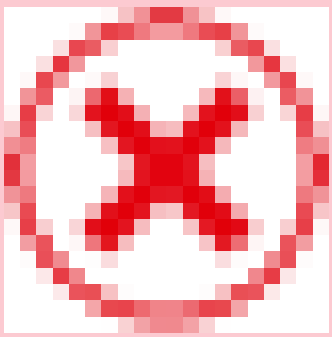
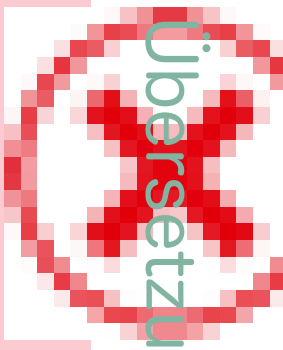
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Klassifizierungsregeln |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

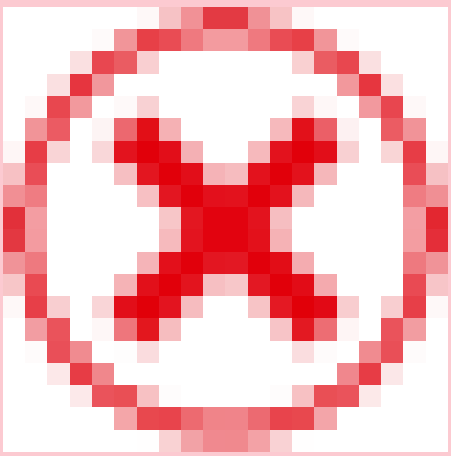
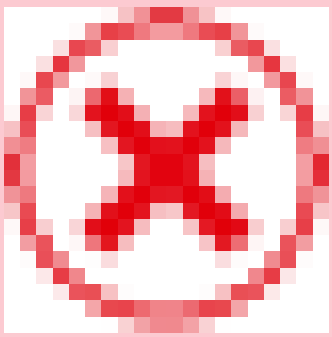
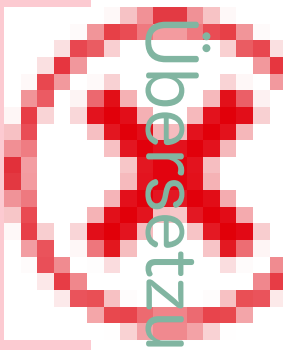
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Leistungskonfiguration |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

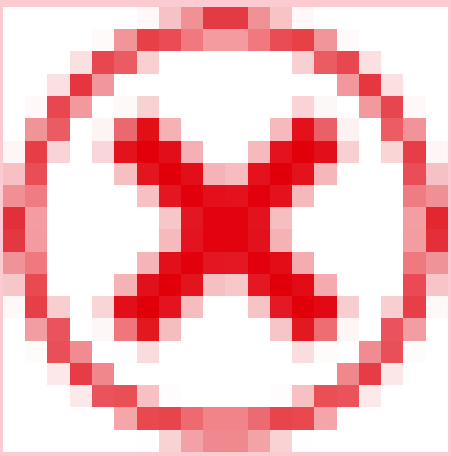
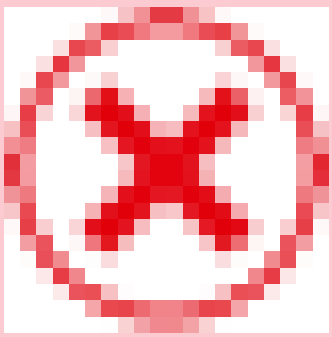
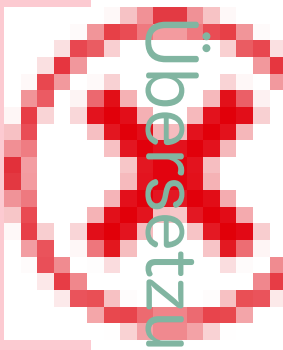
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| VI-Granularität konfigurieren |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

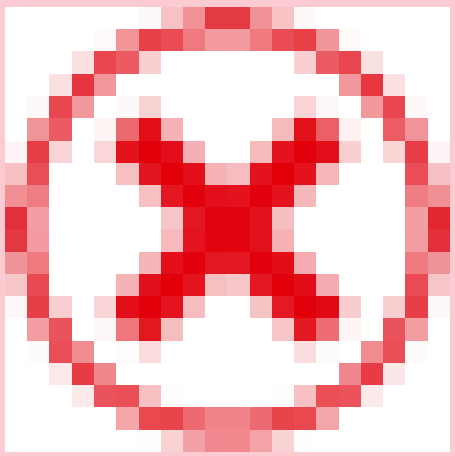
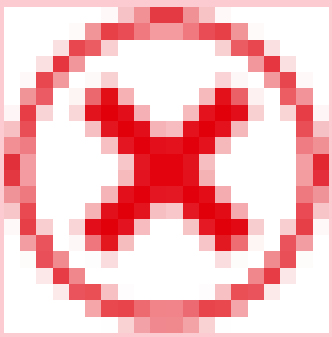
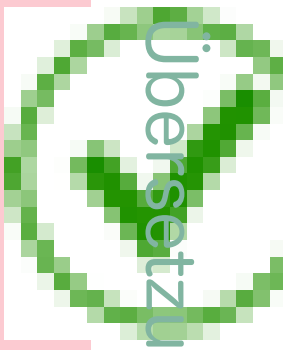
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Benachrichtigungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

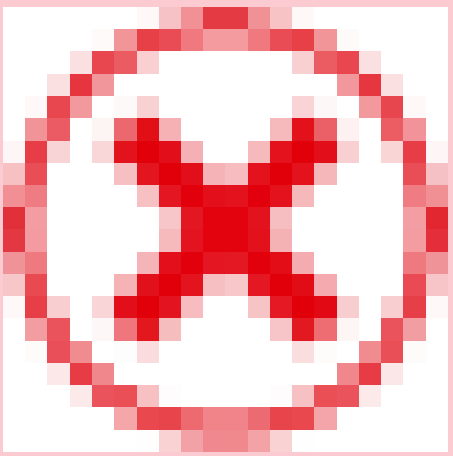
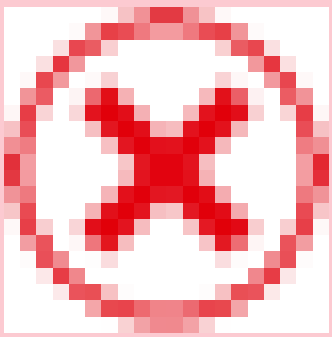
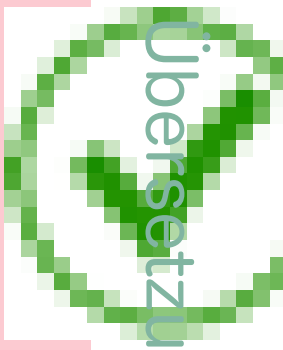
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| E-Mail-Vorlagen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

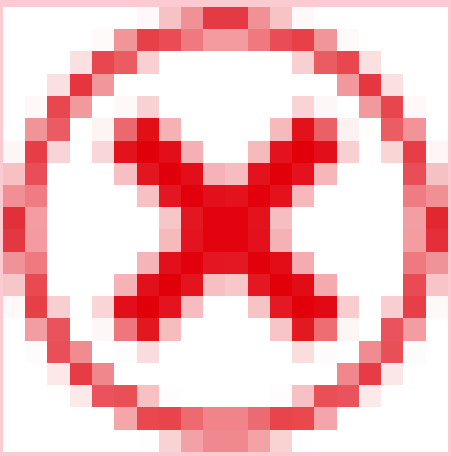
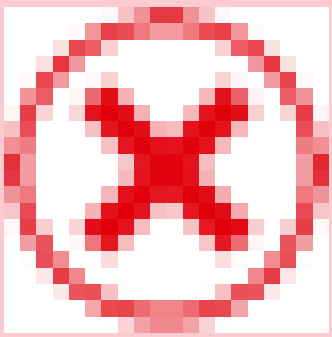
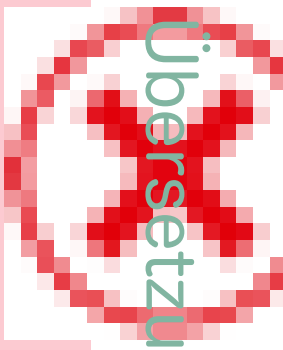
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Warteschlange importieren |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

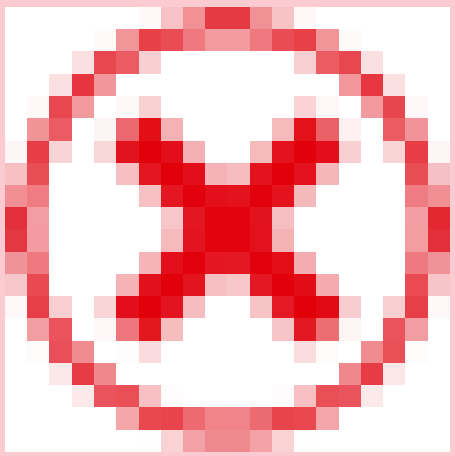
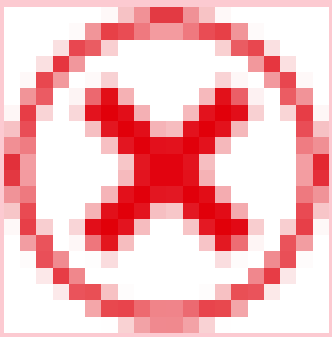
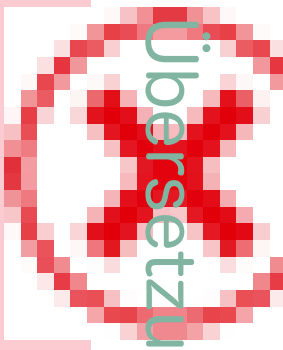
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Integrationen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| SLA-Definitionen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

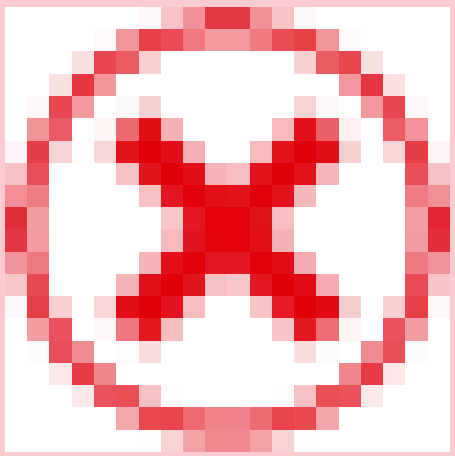
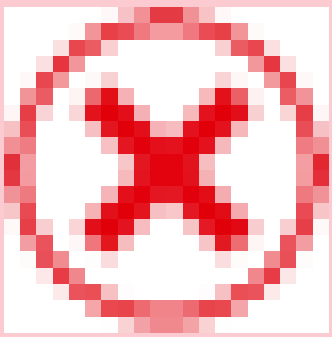
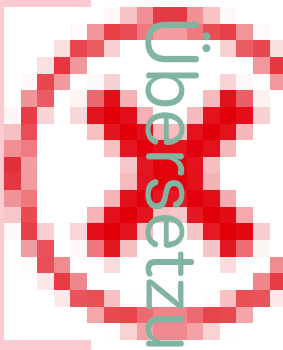
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| SAM-NVD konfigurieren |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

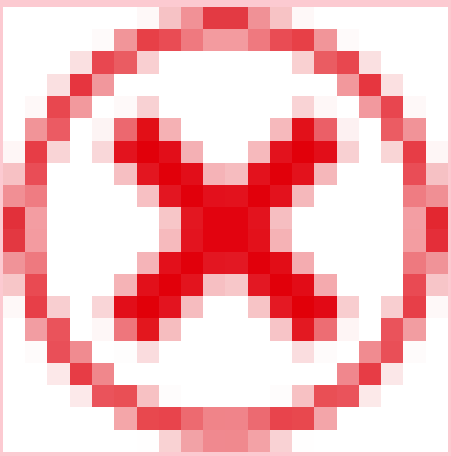
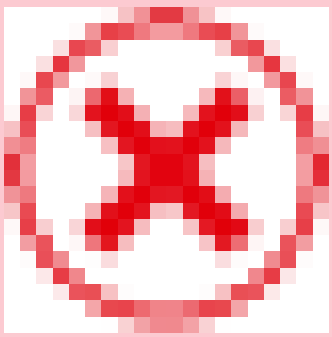
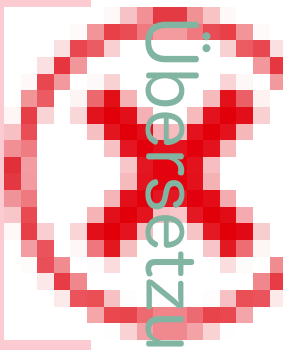
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

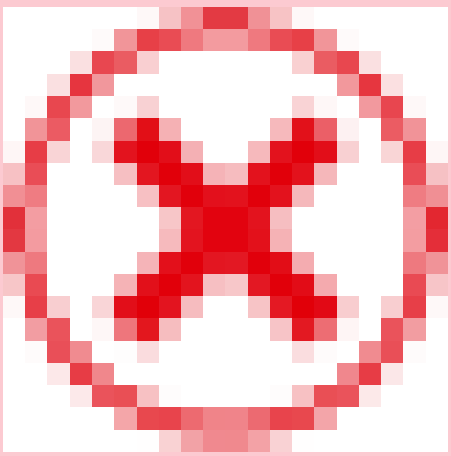
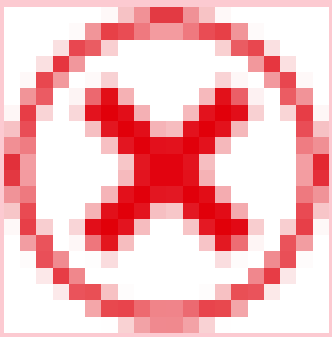
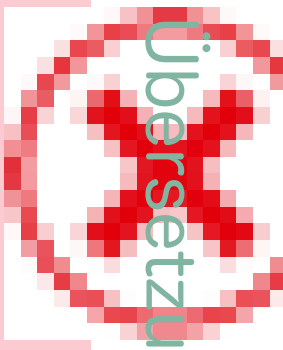
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Konfiguration der Scan-Abdeckung |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

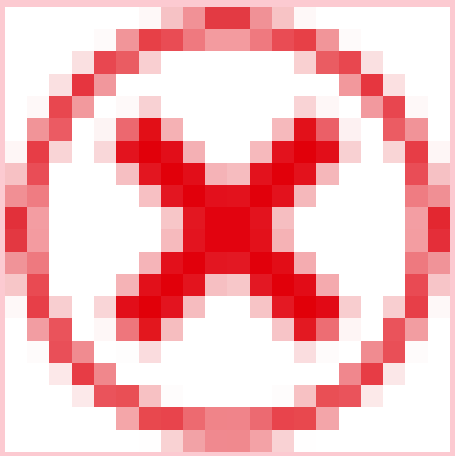
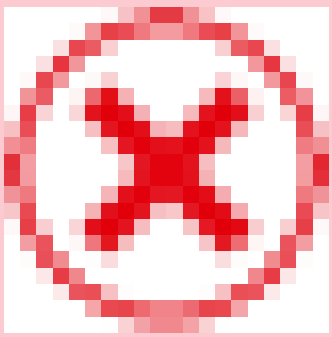
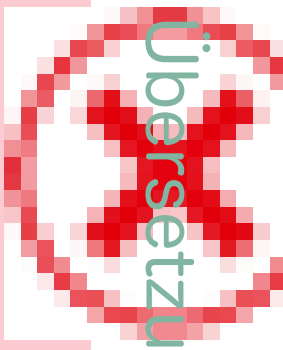
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Ausnahmenverwaltung |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

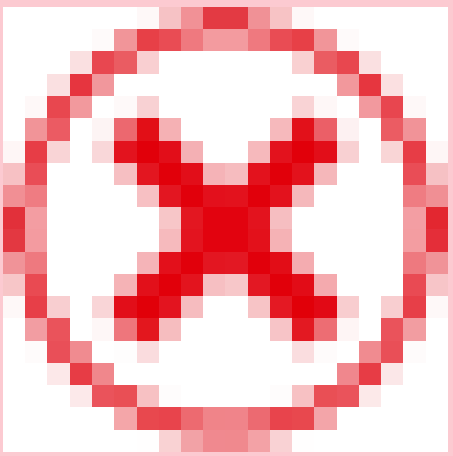
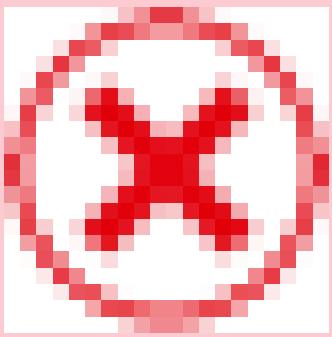
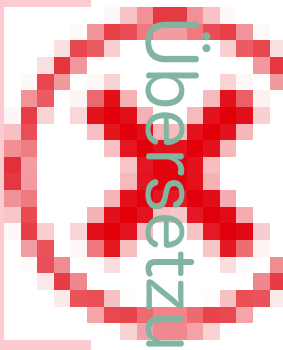
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Verwendungsbericht |  |  |  |
| Diagnosen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

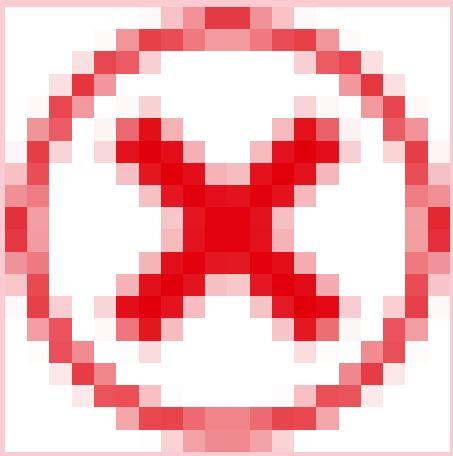
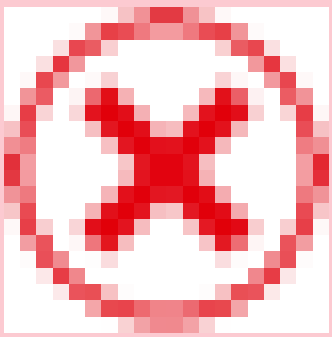
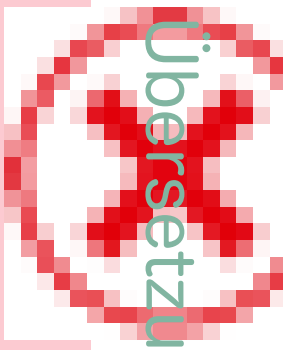
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_exposure_assessment | sn_vul.manage_group_rules | sn_vul.manage_notifica |
|---|---|---|---|
| Überprüfungen |  |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| (Haupt-App-Gruppe) | | | |
| CISO-Dashboard | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Korrekturübersicht | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

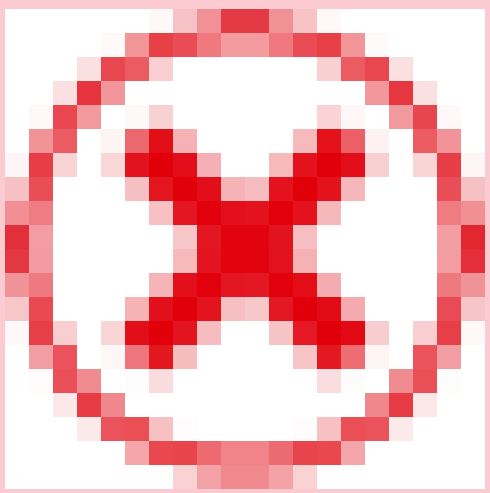
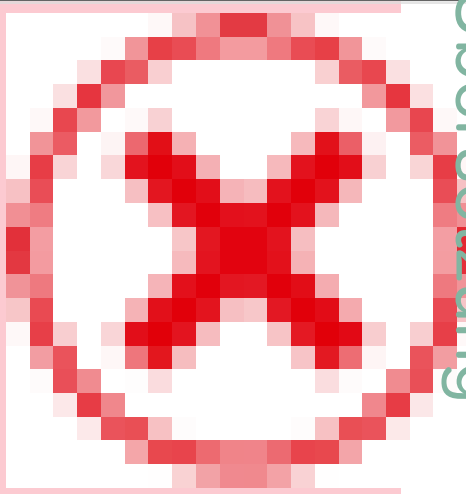
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Übersicht | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Genehmiger-Übersicht | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Übersicht | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Meine Freigaben | ✗ | ✗ | ✗ |
| Korrekturaufgaben | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Aktiv | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Mir zugewiesen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Meinen Gruppen zugewiesen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Alle | ✓ | ✓ | ✓ |
| Angreifbare Elemente | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Kritisches Risiko | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Hohes Risiko | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Nutzbar | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Ziel rückt näher | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Verfehltes Ziel | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

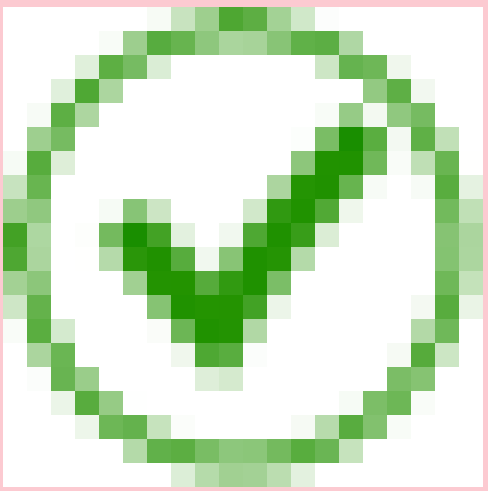
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Innerhalb der letzten 90 Tage |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Älter als 90 Tage | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Nicht zugewiesen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Nicht gruppiert | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

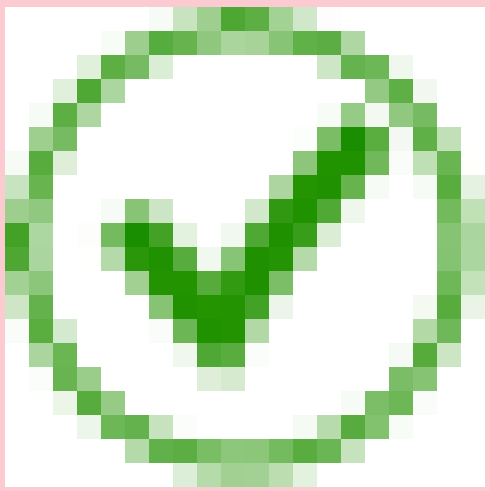
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Außer Betrieb genommen |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Mehrere Zurückstellungen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

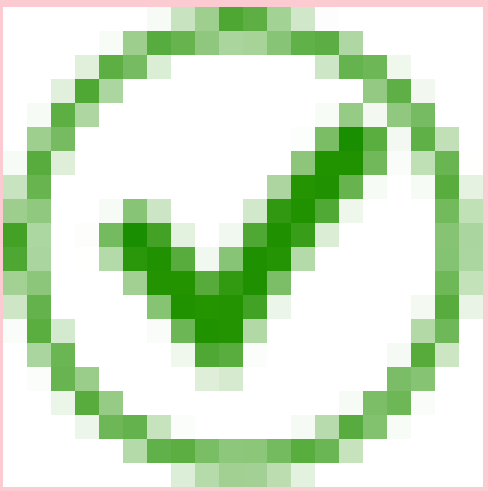
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Alle |  | | |
| Lösungen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Alle | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

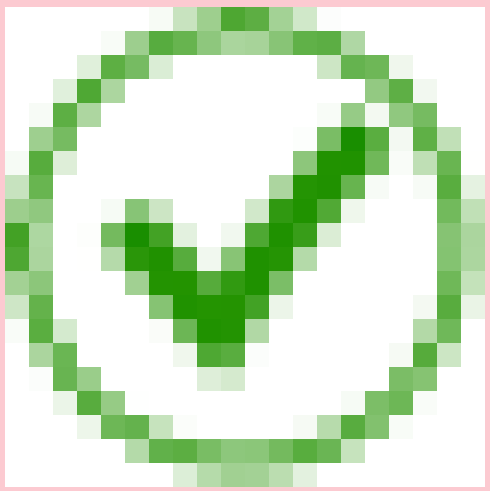
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Ersetzung mit höchster Priorität |  | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Mit angreifbaren Elementen | ✓ | ✓ | ✓ |
| Bibliotheken | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| NVD | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| CWE | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Drittpartei | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Software mit Schwachstellen | ✓ | ✓ | ✓ |
| Schwachstellenscan | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Überprüfungen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Scanner | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Scan-Warteschlange | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Quotengrenzdefinitionen | ✗ | ✗ | ✗ |
| Administration | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Setup-Assistent | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Überwachungsthemen | ✓ | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Sicherheitsrisiko-Rechner | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Rechner für Schwachstellen-Rollup | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Nachbesserungszielregeln | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| AutoClose-Konfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Ausnahmeregeln | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Genehmigungsregeln | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Klassifizierungsregeln | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Benachrichtigungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Warteschlange importieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Integrationen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| SLA-Definitionen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| SAM-NVD konfigurieren | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

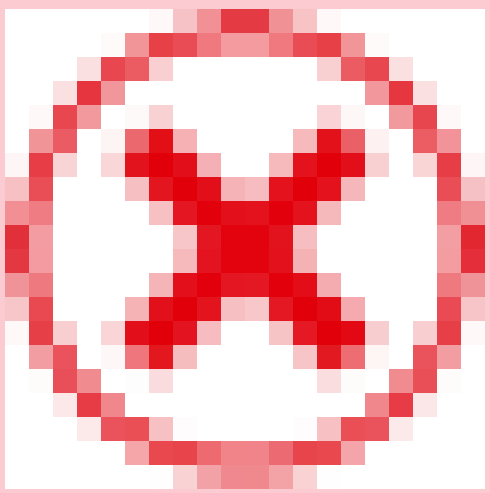
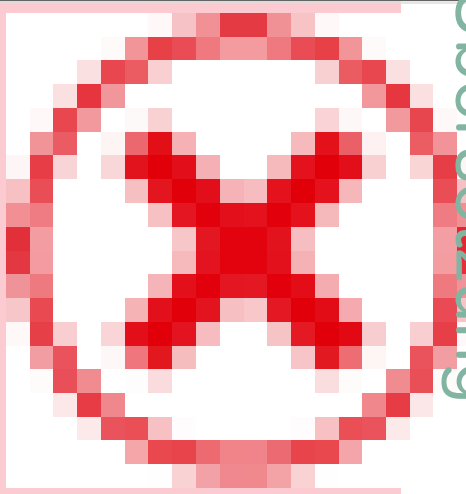
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Konfiguration der Scan-Abdeckung |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

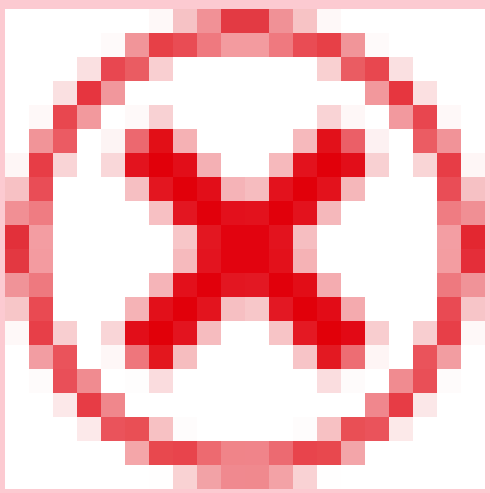
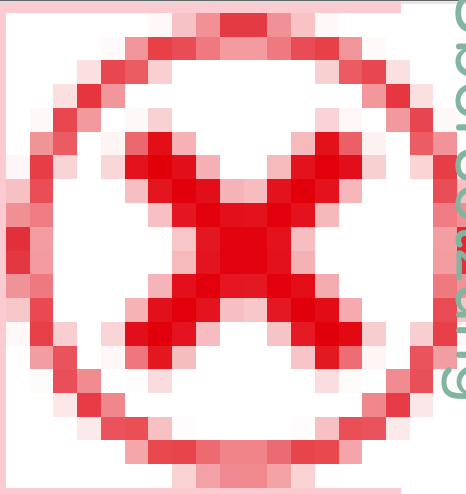
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Ausnahmenverwaltung |  |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Verwendungsbericht | | | |
| Diagnosen | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

**(Fortsetzung)**

| Modul | sn_vul.manage_remediation_target_rules | sn_vul.manage_risk_score_configuration | sn_vul.r |
|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst*

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| (Haupt-App-Gruppe) | | | | |
| CISO-Dashboard | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Korrekturübersicht | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Arbeitsbereich des Schwachstellenmanagers | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Übersicht | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Genehmiger-Übersicht | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Übersicht | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Meine Freigaben | ✗ | ✗ | ✗ | ✓ |
| Korrekturaufgaben | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Aktiv | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Mir zugewiesen | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Meinen Gruppen zugewiesen | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Alle | ✗ | ✗ | ✗ | ✗ |

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Kritisches Risiko | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Hohes Risiko | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Nutzbar | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Ziel rückt näher | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Verfehltes Ziel | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Innerhalb der letzten 90 Tage | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Älter als 90 Tage | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Nicht zugewiesen | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Nicht gruppiert | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Außer Betrieb genommen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Mehrere Zurückstellungen | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Alle | ✗ | ✗ | ✗ | ✗ |
| Lösungen | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Alle | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Ersetzung mit höchster Priorität | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Mit angreifbaren Elementen | ✗ | ✗ | ✗ | ✗ |
| Bibliotheken | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| NVD | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| CWE | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Drittpartei | ✗ | ✗ | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Software mit Schwachstellen | ✗ | ✗ | ✗ | ✗ |
| Schwachstellenscan | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Bewertung des Gefahrenpotenzials | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Scanner | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Scan-Warteschlange | ✓ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Scannerquotengrenzen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Quotengrenzdefinitionen | ✗ | ✗ | ✗ | ✗ |
| Administration | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Setup-Assistent | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Überwachungsthemen | ✗ | ✓ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Zuweisungsregeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Regeln für Korrekturaufgaben | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Sicherheitsrisiko-Rechner | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Rechner für Schwachstellen-Rollup | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Nachbesserungszielregeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| AutoClose-Konfiguration | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| AutoDelete-Regeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Ausnahmeregeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Genehmigungsregeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Klassifizierungsregeln | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Leistungskonfiguration | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| VI-Granularität konfigurieren | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Benachrichtigungen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| E-Mail-Vorlagen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Warteschlange importieren | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Integrationen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| SLA-Definitionen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| SAM-NVD konfigurieren | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Normalisierte Schweregradzuordnungen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Konfiguration der Scan-Abdeckung | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Ausnahmenverwaltung | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Verwendungsbericht | ✗ | ✗ | ✗ | ✗ |
| Diagnosen | | | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst***

**(Fortsetzung)**

| Modul | sn_vul.read_integrations | sn_vul.read_watch_topic | sn_vul.remediation_owner | sn_vul.unass |
|---|---|---|---|---|
| Überprüfungen | ✗ | ✗ | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

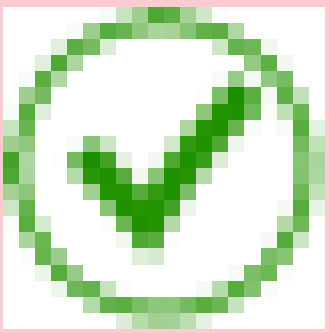
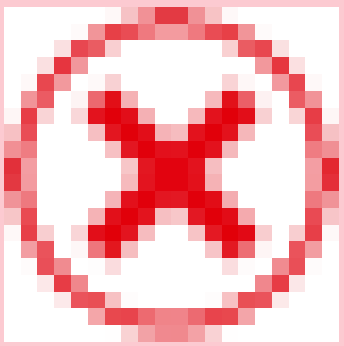
*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| (Haupt-App-Gruppe) | | |
| CISO-Dashboard |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Korrekturübersicht | ✓ | ✓ |
| Arbeitsbereich des Schwachstellenmanagers | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Übersicht | ✓ | ✓ |
| Arbeitsbereich für IT-Korrekturen | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

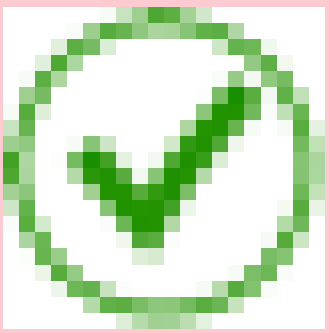
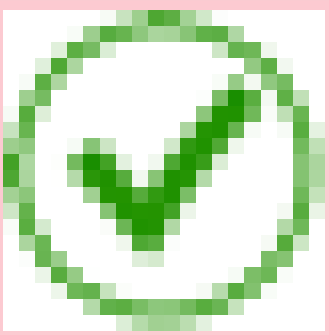
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Genehmiger-Übersicht |  | |
| Übersicht |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

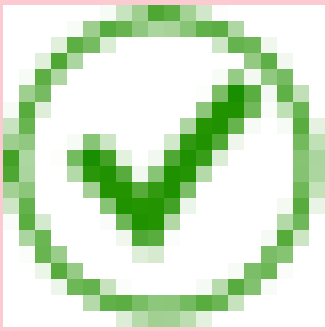
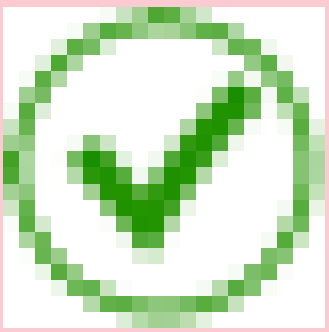
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Meine Freigaben |  | |
| Korrekturaufgaben | | |
| Aktiv |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

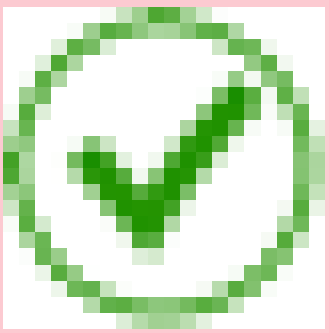
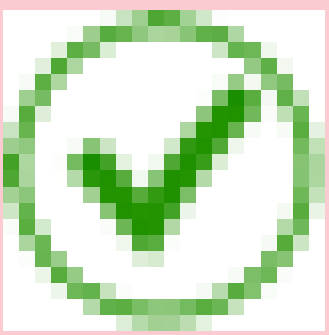
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Mir zugewiesen |  | |
| Meinen Gruppen zugewiesen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

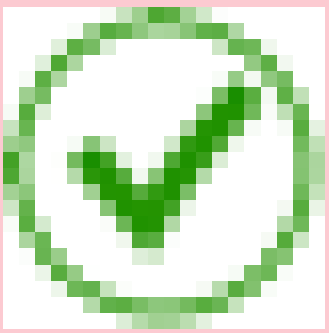
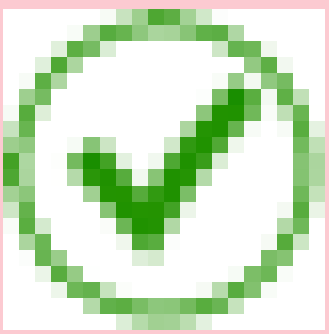
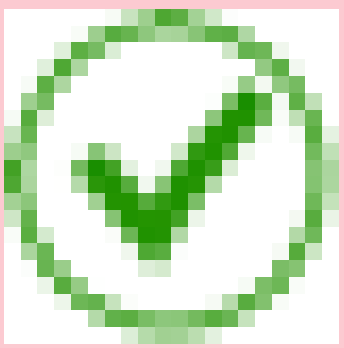
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Alle |  | |
| Angreifbare Elemente | | |
| Kritisches Risiko |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Hohes Risiko | ✓ | ✓ |
| Nutzbar | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Ziel rückt näher | ✓ | ✓ |
| Verfehltes Ziel | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

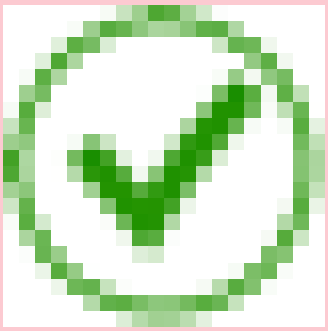
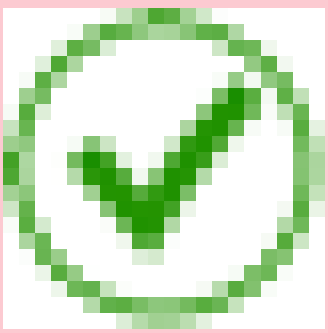
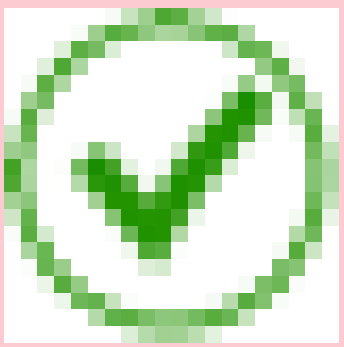
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Innerhalb der letzten 90 Tage |  | |
| Älter als 90 Tage |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Nicht zugewiesen | ✓ | ✓ |
| Nicht gruppiert | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

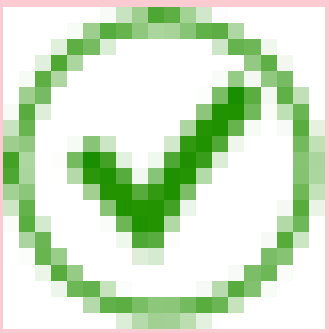
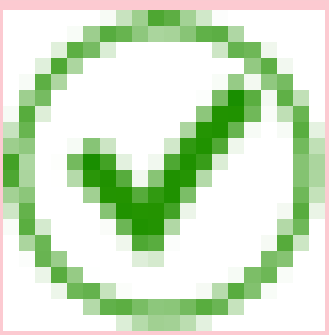
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Außer Betrieb genommen |  | |
| Mehrere Zurückstellungen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Alle | ✓ | ✓ |
| Lösungen | | |
| Alle | ✓ | ✓ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

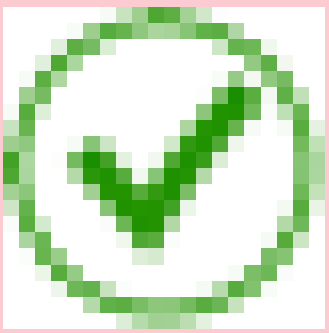
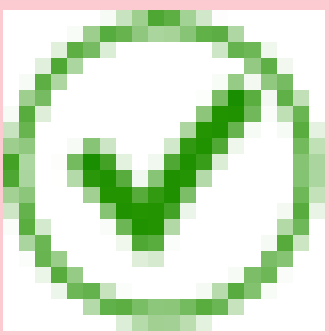
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Ersetzung mit höchster Priorität |  | |
| Mit angreifbaren Elementen |  | |
| Bibliotheken | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

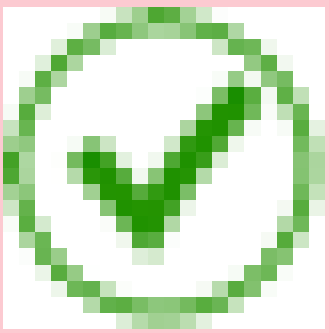
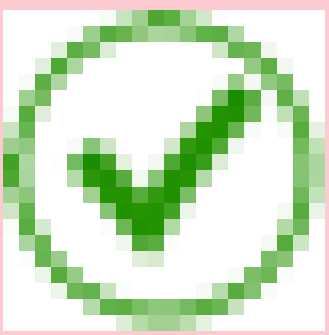
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| NVD |  | |
| CWE |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Drittpartei | ✓ | ✓ |
| Software mit Schwachstellen | ✓ | ✓ |
| Schwachstellenscan | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

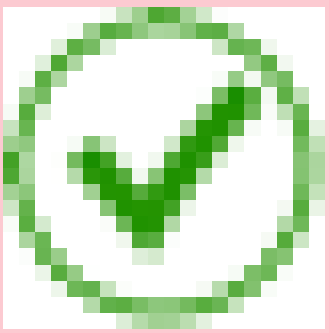
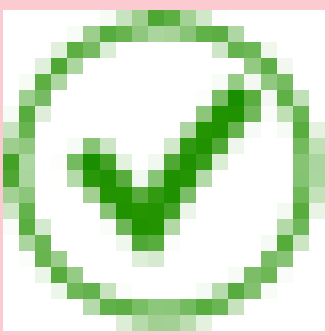
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Bewertung des Gefahrenpotenzials |  | |
| Überprüfungen |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

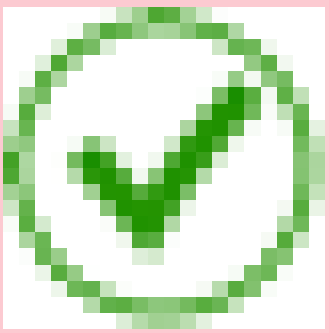
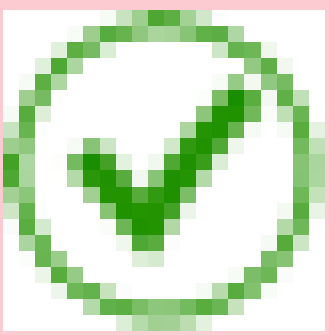
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Scanner |  | |
| Scan-Warteschlange |  | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

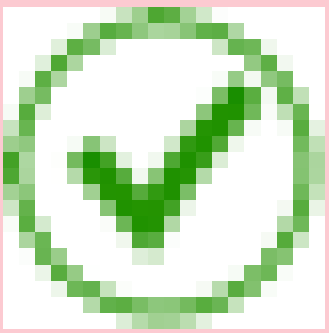
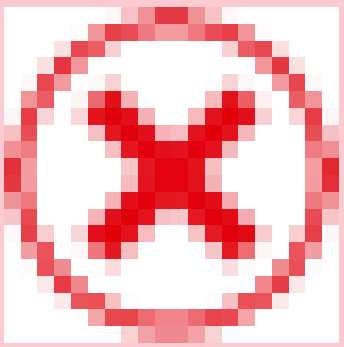
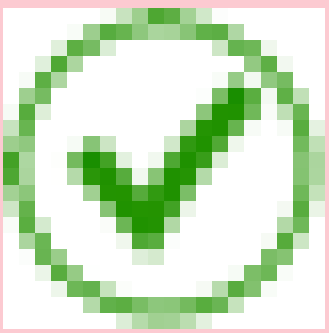
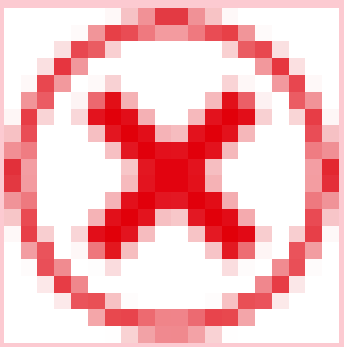
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Scannerquotengrenzen |  |  |
| Quotengrenzdefinitionen |  |  |
| Administration | | |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

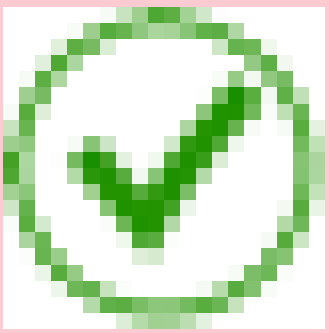
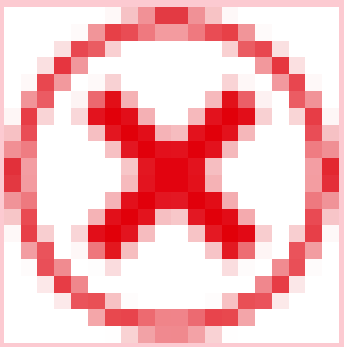
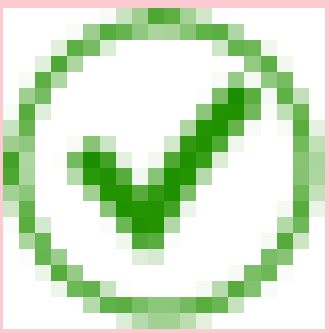
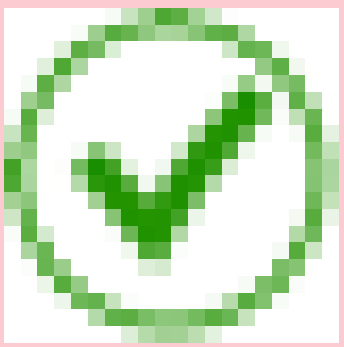
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Setup-Assistent |  |  |
| Überwachungsthemen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

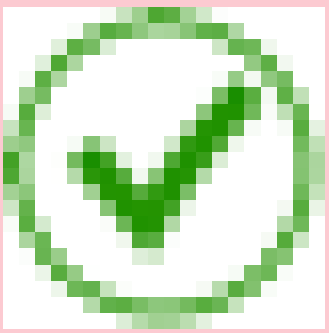
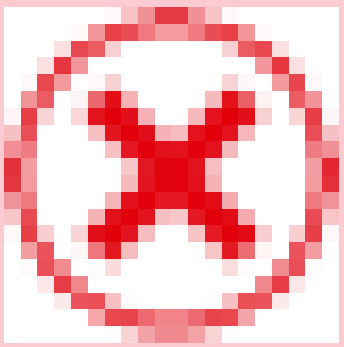
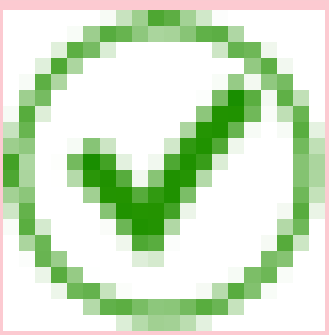
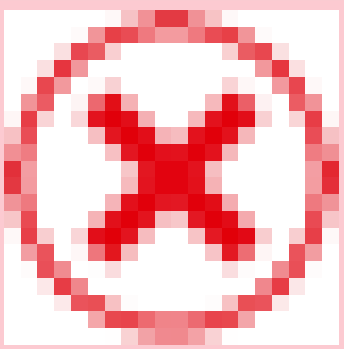
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Zuweisungsregeln |  |  |
| Regeln für Korrekturaufgaben |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Zuweisungsempfehlungen | ✗ | ✗ |
| Sicherheitsrisiko-Rechner | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

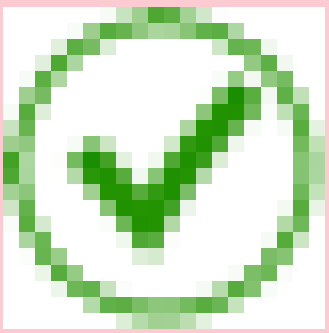
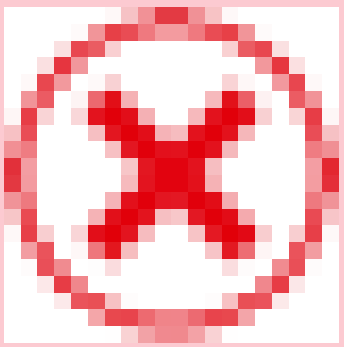
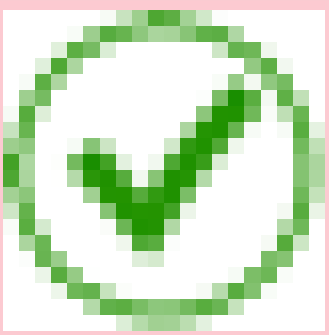
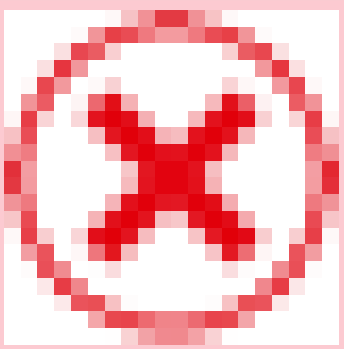
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Rechner für Schwachstellen-Rollup |  |  |
| Nachbesserungszielregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

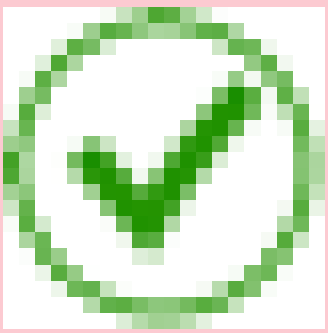
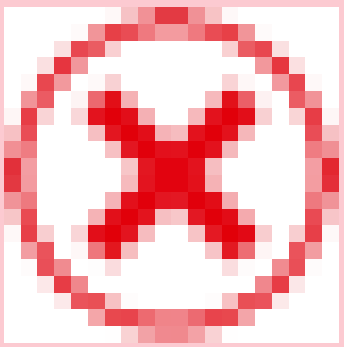
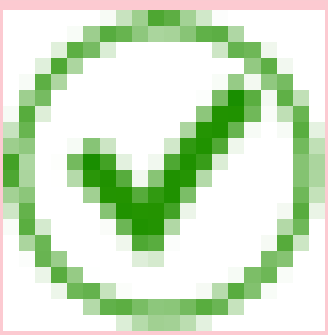
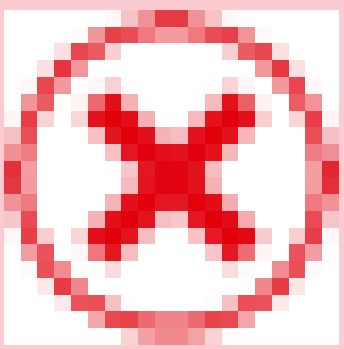
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| AutoClose-Konfiguration |  |  |
| AutoDelete-Regeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

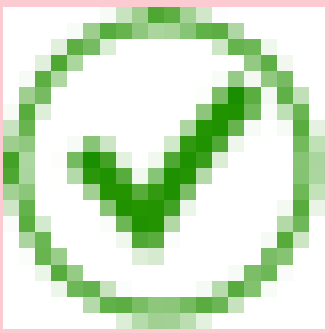
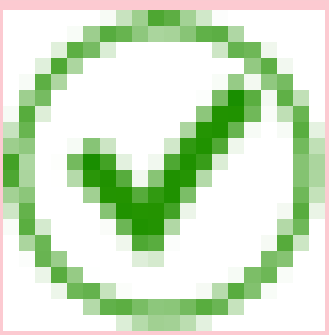
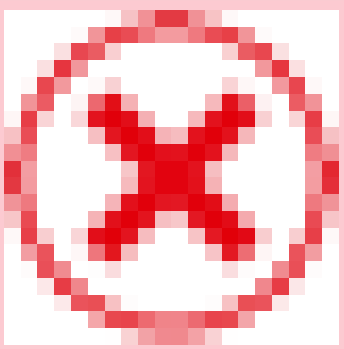
*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Ausnahmeregeln |  | |
| Genehmigungsregeln |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

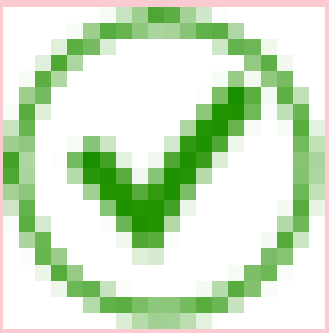
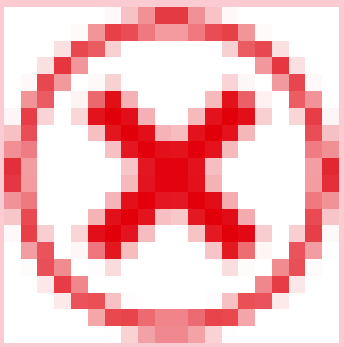
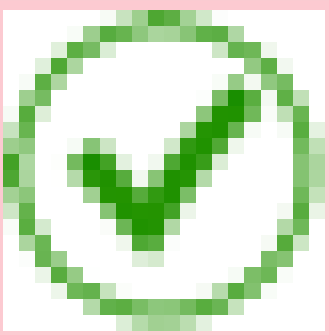
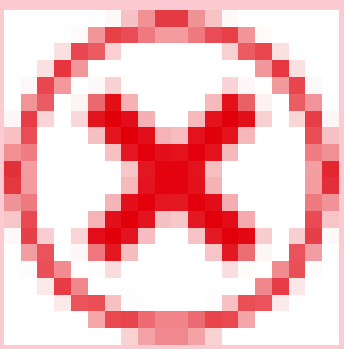
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Klassifizierungsregeln |  |  |
| Leistungskonfiguration |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

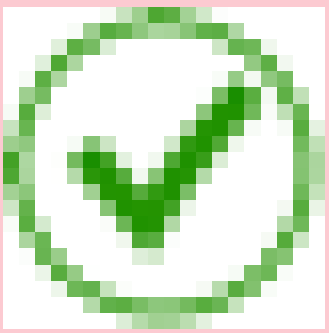
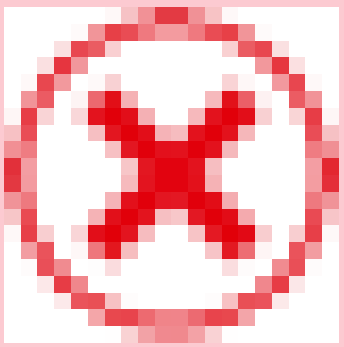
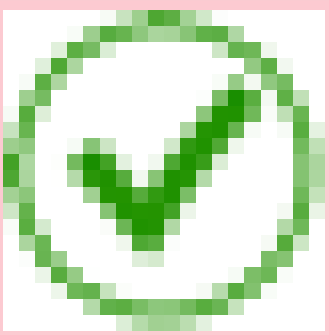
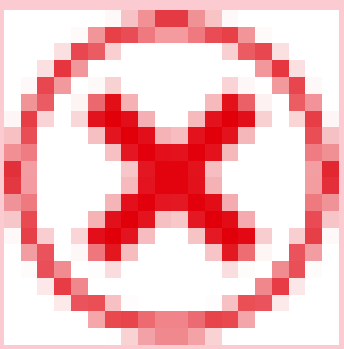
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| VI-Granularität konfigurieren |  |  |
| Benachrichtigungen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

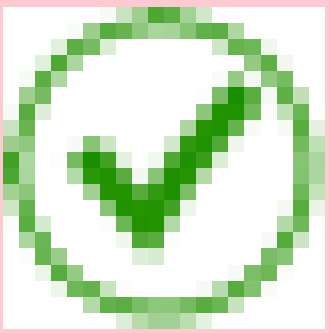
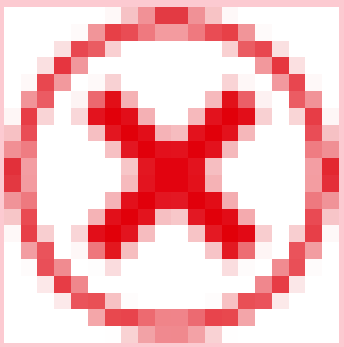
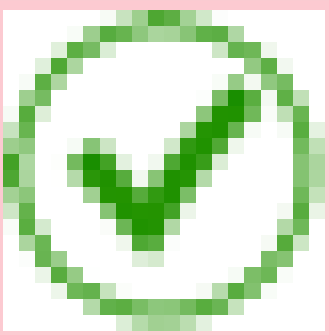
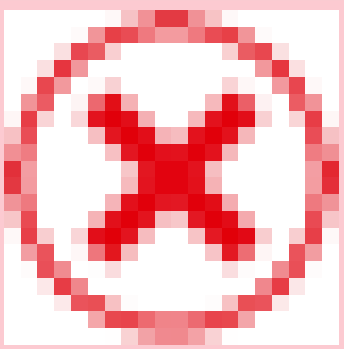
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| E-Mail-Vorlagen |  |  |
| Warteschlange importieren |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

*Informationen für andere Rollen:*

*sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations*

*sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance*

*sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules*

*sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration*

*sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions*

*sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule*

*sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats*

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Integrationen | ✓ | ✗ |
| SLA-Definitionen | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

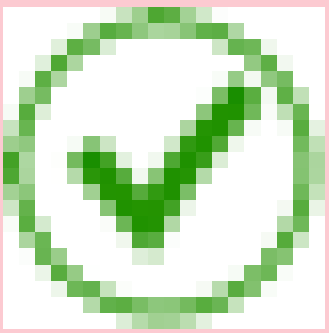
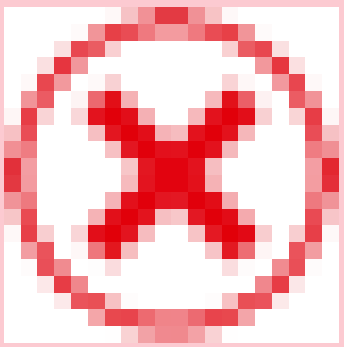
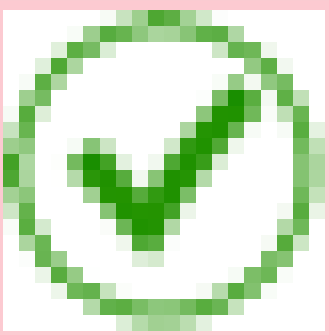
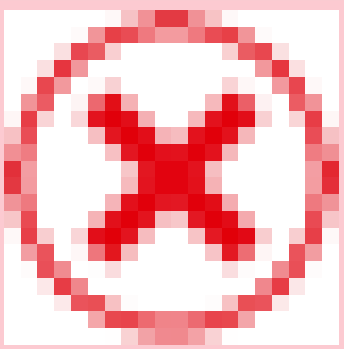
***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| SAM-NVD konfigurieren |  |  |
| Normalisierte Schweregradzuordnungen |  |  |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Konfiguration der Scan-Abdeckung | ✓ | ✓ |
| Ausnahmenverwaltung | ✓ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Modulzugriff für: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst**

***Informationen für andere Rollen:***

***sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations***

***sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance***

***sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules***

***sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration***

***sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions***

***sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule***

***sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_width_stats***

**(Fortsetzung)**

| Modul | sn_vul.vulnerability_admin | sn_vul.vulnerability_analyst |
|---|---|---|
| Verwendungsbericht | ✓ | ✗ |
| Diagnosen | | |
| Überprüfungen | ✗ | ✗ |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

## Suche Security Operations

Sie können Informationen in jeder Anwendung von Security Operations schnell finden, indem Sie das Suchsymbol im Header des Bildschirms verwenden. Zing ist die Textindizierungs- und Suchmaschine, die alle Textsuchen in Ihrer Instanz durchführt.

### Vorbereitungen

Erforderliche Rolle: sn_si.read oder höher

### Prozedur

1. Klicken Sie oben rechts auf dem Bildschirm auf das Suchsymbol ( ).
2. Geben Sie die Kriterien ein, nach denen Sie suchen möchten, und drücken Sie die **Eingabetaste**.
   Wenn Sie das Plugin Security Incident Response aktiviert haben, zeigen die von Ihnen eingegebenen Suchkriterien übereinstimmende Kurzbeschreibungen, CIs, IP-Adressen oder URLs in Ihren Security Incidents, Security Incident Response Aufgaben oder Sicherheitsanforderungen an. Wenn Sie die Plugins Vulnerability Response oder Threat Intelligence aktiviert haben, enthalten die Suchergebnisse Schwachstellen, angreifbare Elemente, angreifbare Einträge, erkennbare Elemente, IoCs und Angriffsmodus/-methoden.

#### Zugehörige Informationen

Einführung in die Suche

Zing-Textsuche

## Referenzen zur Integration mit Security Operations

Entwickler und ServiceNow-Partner können die Informationen in diesem Abschnitt verwenden, um sich mit der Funktionalität von Drittanbieterintegrationen vertraut zu machen, einschließlich Entwicklungsrichtlinien, Integrationsfunktionen und Workflows.

### ServiceNow Security Operations Entwicklungsrichtlinien für -Integrationen

Die ServiceNow -Plattform bietet mehrere Mechanismen für die Entwicklung von Integrationen mit externen Systemen. Die Produktsuite ServiceNow Security Operations fügt Integrationsfunktionen hinzu, die den Prozess der Integration mit sicherheitsorientierten externen Systemen optimieren sollen.

Die meisten Konzepte in diesem Leitfaden setzen eine gewisse Vertrautheit mit der Standardfunktionalität von ServiceNow voraus. Für die Integration mit der Suite Security Operations sind mindestens Kenntnisse der folgenden Konzepte von ServiceNow erforderlich:

- Skripteinbindungen
- Eingehende/ausgehende Webservices
- Datenquellen
- Importsätze
- Transformationszuordnungen

#### Technologiepartnerprogramm

Alle Anforderungen für die Anwendungszertifizierung oder Richtlinien, die in der Dokumentation zum Technologiepartnerprogramm angegeben sind, ersetzen die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen in diesem Leitfaden. Dieser Leitfaden ersetzt nicht die Dokumentation zum Technologiepartnerprogramm und dient nur als Ergänzung zur vorhandenen Dokumentation.

Weitere Informationen finden Sie im Blog-Beitrag zum Schulungskurs des Technologiepartnerprogramms .

#### Typen der bereitgestellten ServiceNow -Integrationen

Die Anwendungen [ Security Operations (Security Incident Response, Threat Intelligenceund Vulnerability Response) können nahtlos in andere Anwendungen von ServiceNow integriert werden, um deren Funktionalität zu verbessern.

Die folgenden Integrationen werden im Basissystem von Security Operations bereitgestellt.

### Security Incident Response – Event Management-Integration

Die Fähigkeiten der Anwendung Ereignismanagement wurden erweitert, um Security Incident Responsezu unterstützen. Das Support-Plugin Security Incident Response Ereignismanagement analysiert automatisch den Inhalt von Events in Ereignismanagement, um Felder in Security Incidents auszufüllen.

Abgedeckter Anwendungsfall:

Erstellung von Sicherheits-Events im System Ereignismanagement aus Sicherheitsinformationen und den Tools von Ereignismanagement (SIEM).

Nützliche Funktionen bereitgestellt:

- Event Management-Funktionalität – Event-Korrelation, Event-Regeln und Warnungsregeln
- Automatische Zuordnung von Additional_information-Werten zum resultierenden Security Incident

Ressourcen:

Support-Dokumentation für Security Incident Event Management

Event Management-Dokumentation

### Security Incident Response – Integration der Import Set-API

Zusätzlich zur Verwendung von Ereignismanagement zum Übertragen von sicherheitsbezogenen Events bietet die Anwendung Security Incident Response eine Import Set-API, die die direkte Erstellung von Security Incidents ermöglicht. Der REST-Endpunkt für das Security Incident-Import Set ist http://localhost:8080/api/now/import/sn_si_incident_import.

Diese Integrationstechnik ist nützlich, wenn a) Ereignismanagement nicht installiert ist oder b) Security Incidents einfach erstellt werden sollen, ohne den Event > Warnung > Security Incident-Flow zu durchlaufen, der bei Verwendung von Ereignismanagementerforderlich ist.

Abgedeckter Anwendungsfall:

Erstellung von Security Incidents direkt aus SIEM-Tools.

Nützliche Funktionen bereitgestellt:

Automatische CI-Übereinstimmung bei der Erstellung von Security Incidents basierend auf IP, NetBIOS oder vollständig qualifiziertem Domänenname.

Ressourcen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation zur Platform Import Set API

Dokumentation zu Security Incident Web Service Import Set

## Threat Intelligence – Integration der Suchquelle

Suchquellen bieten die Möglichkeit, Daten an externe Suchquellen zu senden, um festzustellen, ob diese Daten schädlich sind. Im Allgemeinen handelt es sich bei diesen Daten um eine IP-Adresse, eine URL, eine Datei oder einen Datei-Hash.

Abgedeckter Anwendungsfall:

Suchen Sie mit einem externen Suchservice nach einer IP-Adresse, einer URL, einer Datei oder einem Hash.

Nützliche Funktionen bereitgestellt:

- Konsistente Methode zum Anfordern von Suchvorgängen aus Katalogelementen und Security Incidents.
- Ratenbegrenzungs- und Drosselfunktionen mit wenig/keiner Codierung bereitgestellt.
- Automatische Erstellung von IoC-Einträgen (Indicators of Compromise) für alle Probleme, die von Suchquellen gefunden wurden.

## Threat Intelligence – Integration der Bedrohungsquelle

Bedrohungsquellen bieten die Möglichkeit, Daten aus externen Threat Intelligence-Repositorys abzurufen. Diese Daten werden dann in die verschiedenen Tabellen für Kompromittierungsindikatoren importiert, die im System vorhanden sind. TAXII-Sammlungen und einfache Sperrlisten werden nativ unterstützt. Um neue TAXII-Sammlungen (oder Profile basierend auf einem Discovery- oder Sammlungsverwaltungsservice) hinzuzufügen, müssen Sie nur einen Eintrag hinzufügen. In ähnlicher Weise müssen Sie beim Hinzufügen einer neuen einfachen Sperrliste mit einer Spalte einen neuen Datensatz eingeben und die URL der Sperrliste angeben. Für kompliziertere Datensätze kann eine benutzerdefinierte Integration bereitgestellt werden, um eine URL aufzurufen und die Antwort zu analysieren.

Abgedeckter Anwendungsfall:

Rufen Sie Daten aus einer Threat Intelligence-Quelle ab, um sie in IoC-Tabellen zu laden.

Nützliche Funktionen bereitgestellt:

- Unterstützung für einfache Sperrlisten und TAXII-Sammlungen ohne Codierung.
- Einfacher Mechanismus zum Ausführen von REST-Nachrichten zum Abrufen von Daten.
- Entkoppelter Datenabruf/-verarbeitung für die Wiederverwendbarkeit von Integrationskomponenten.
- Native Unterstützung für die Verarbeitung von Übergabedaten, die an Datenquellen zurückgegeben werden (und Importsätze/Transformationszuordnungen).
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Aufrufe) mit der Möglichkeit, den Kontext an nachfolgende Aufrufe zu übergeben

Ressourcen:

Definieren Sie eine Bedrohungsquelle



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Vulnerability Response – Integration des Scanner-Aufrufs

Der Aufruf von Vulnerability Scanner ist ein einfacher Einstiegspunkt für die Integration, der den Aufruf von Schwachstellenprüfungen über die Instanz unterstützt. Ein Schwachstellenscanner einer Drittpartei wird asynchron aufgerufen, um einen Scan für Konfigurationselemente oder IP-Adressen zu planen.

Abgedeckter Anwendungsfall:

Senden Sie eine Anforderung an einen Drittanbieter-Scanner, um ein CI (mithilfe der vom CI abgeleiteten Hostinformationen) oder eine IP-Adresse/IP-Adressen zu scannen.

Nützliche Funktionen bereitgestellt:

- Einfaches Framework zum Definieren von Scanner-Implementierungen.
- Einheitliche Methode zum Anfordern von Scans von Katalogelementen, Security Incidents und angreifbaren Elementen.
- Automatische Aktualisierung von Aufgaben mit Ergebnis des Scan-Aufrufs.

## Vulnerability Response – Datenintegration

Schwachstellendaten-Integrationen zielen darauf ab, Schwachstellendaten aus Schwachstellensystemen von Drittanbietern abzurufen. Die erwarteten Ausgaben dieser Integrationen sind Schwachstelleneinträge und angreifbare Elemente. Diese Integration ermöglicht es Schwachstellenscannern von Drittanbietern, unabhängig zu funktionieren, mit der Erwartung, dass Schwachstellen innerhalb der Instanz bearbeitet und nachverfolgt werden können.

Abgedeckte Anwendungsfälle:

- Rufen Sie Schwachstellenbibliotheken ab
- Rufen Sie Schwachstellen-/CI-Paarungen ab
- CIs mit dem Schwachstellenmanagementsystem synchronisieren

Nützliche Funktionen bereitgestellt:

- Entkoppelter Datenabruf/-verarbeitung für die Wiederverwendbarkeit von Integrationskomponenten.
- Native Unterstützung für die Verarbeitung von Übergabedaten, die an Datenquellen zurückgegeben werden (und Importsätze/Transformationszuordnungen).
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Aufrufe) mit der Möglichkeit, den Kontext an nachfolgende Aufrufe zu übergeben.

Ressourcen:

Dokumentation zur Integration von Schwachstellendaten

### Security Operations Integrationskonfigurationen

Viele der im Basissystem enthaltenen Integrationen erfordern wenig oder gar kein Setup und funktionieren auf die gleiche Weise. Bestimmte Integrationen, z. B. Qualys Cloud Platform, erfordern jedoch separate Schritte zum Einrichten der Integration. Andere unterstützen unterschiedliche Sätze von Scan- und Suchtypen und unterschiedliche Quotengrenzen.

In diesem Abschnitt werden die Unterschiede zwischen den unterstützten Integrationen beschrieben und bei Bedarf auf weitere Dokumentation verwiesen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Integration mit Carbon Black: Ermöglicht die Untersuchung und Reaktion auf Security Incidents mithilfe der Carbon Black-APIs, um Endpunkte abzufragen und mit ihnen zu interagieren, die mit Security Incidents verknüpft sind.
- Integration mit Check Point Anti-Bot - Email Parser: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von Check Point Anti-Bot verwendet, um Security Incidents zu erstellen.
- Elasticsearch Incident Enrichment-Integration: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integration „Have I Been Pwned?“: Ermöglicht die schnelle Suche in der Liste der Accounts mit Verstößen (E-Mail-Adressen und Benutzernamen) über einen RESTful-Service.
- Integration von HPE Security ArcSight ESM – Email Parser: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von HPE ArcSight ESM verwendet, um Security Incidents zu erstellen.
- HPE ArcSight Logger -Integration der Incident-Ergänzung: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- IBM QRadar – Integration der Incident-Ergänzung: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- McAfee ESM – E-Mail-Analyse-Integration: verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von McAfee ESM verwendet, um Security Incidents zu erstellen.
- McAfee ESM – Integration der Incident-Ergänzung: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integrationsüberblick OPSWAT Metadefender: Ermöglicht das Herunterladen von Bedrohungsdaten, die vom Drittanbieter-Scanner Metadefender erkannt wurden, in die Anwendung Threat Intelligence zur Nachverfolgung, Priorisierung und Lösung.
- Integration „Palo Alto Networks – AutoFocus“: Palo Alto Networks AutoFocus, ein Cloud-Service für Bedrohungsinformationen, ermöglicht die Suche nach Sitzungsinformationen im Zusammenhang mit erkennbaren Security Incident-Elementen.
- Integration „Palo Alto Networks – Firewall“: Mit der Palo Alto Networks-Firewall können Sie Firewalls einrichten und verwalten, um bekannte und unbekannte Bedrohungen im gesamten Netzwerk, in der Cloud und an den Endpunkten abzuwehren.
- Integration „Palo Alto Networks – WildFire“: Mit der Wildfire-Integration können Sie Analyseaufträge in Wildfire programmgesteuert abfragen und Verlaufsergebnisse über eine einfache XML-API-Schnittstelle abrufen.
- Qualys Vulnerability Integration verstehen: Qualys Cloud Platform wird in Vulnerability Responseverwendet.
- Integration mit Splunk - Incident Enrichment: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integration „Tanium-Endpunktplattform“: Security Operations Tanium-Integration verwendet einen Workflow und Workflow-Aktivitäten, um laufende Prozesse für betroffene CIs zurückzugeben.
- Integration mit VirusTotal: verwendet in Threat Intelligence. Um diese Suchquelle zu verwenden, müssen Sie das Plugin „VirusTotal Integration“ aktivieren.
- WhoisXML-API-Integrationssetup: Stellt konsistente, gut strukturierte Daten aus einer Whois-Suche bereit. Hält genaue Whois-Daten rund um die Uhr zugänglich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivieren und konfigurieren Sie Integrationen von Drittparteien

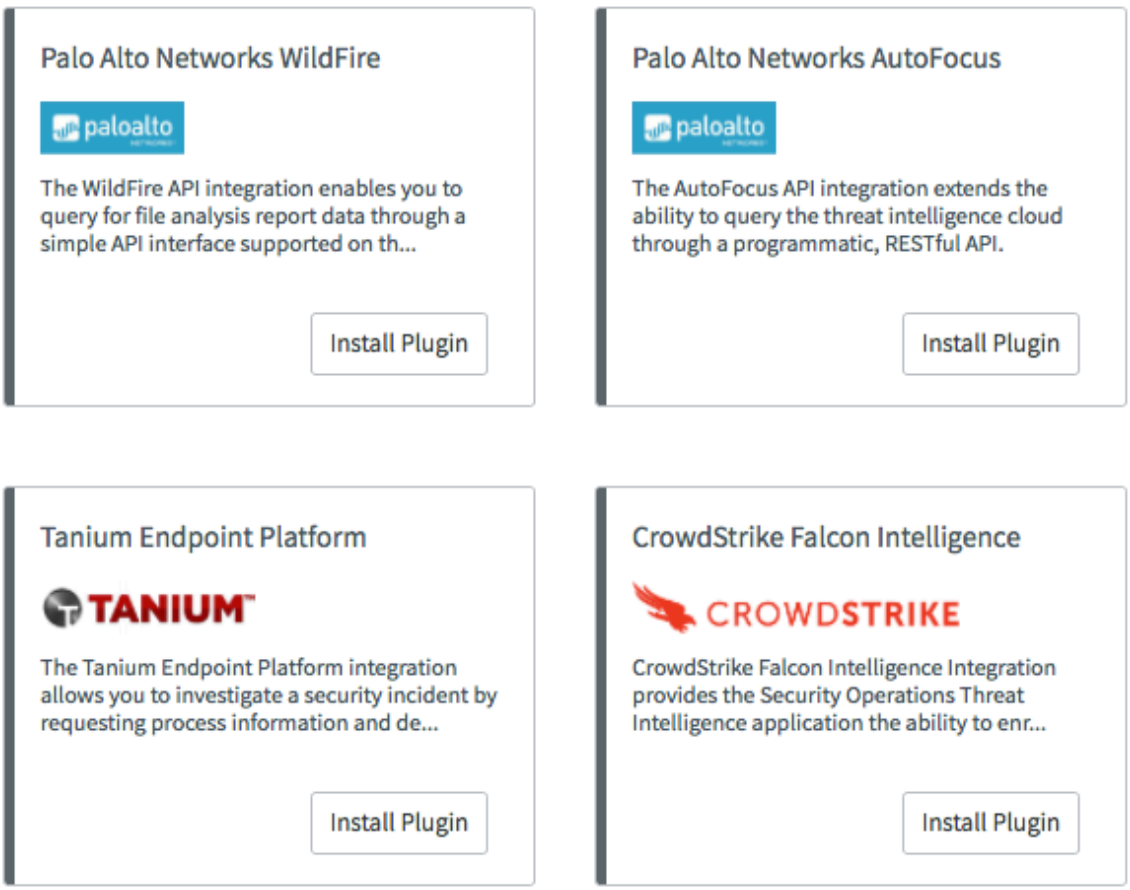
Sie können die Plugins für Integrationen von Drittanbietern aktivieren und sie für die Verwendung über denselben Bildschirm konfigurieren.

## Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationskonfiguration**.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt, ähnlich der folgenden Kartengruppe. Sie können auf eine beliebige Karte zeigen, um eine Beschreibung der Integration zu erhalten.




2. Um das Plugin für eine bestimmte Integration zu installieren, klicken Sie auf **Plugin installieren**.

   a. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie auf den zugehörigen Link **Aktivieren/Aktualisieren**.

   b. Klicken Sie auf **Aktivieren**.
   Nach Abschluss der Aktivierung wird der Bildschirm „Sicherheitsintegration“ erneut geöffnet, und die Schaltfläche für die von Ihnen aktivierte Integration wird mit **Konfigurieren**bezeichnet.

3. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Wenn Sie Qualys Vulnerability Integrationkonfigurieren, finden Sie weitere Informationen unter Installation von Vulnerability Response und unterstützten Anwendungen.

4. Geben Sie den **API-Schlüssel ein**.
5. Klicken Sie auf **Absenden**.

### Erstellen Sie eine Integration

Sie können eine Integration erstellen und die zugehörige Integrationskarte dem Bildschirm „Sicherheitsintegrationen“ hinzufügen. Dieses Verfahren ist für Partner gedacht, die Drittanbieterintegrationen erstellen.

#### Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

**Zielgruppe:**Partner, die Drittanbieterintegrationen erstellen.

#### Prozedur

1. Geben Sie im Navigationsfilter sn_sec_core_integration_item.list ein, und drücken Sie die **Eingabetaste**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

| Feld | Beschreibung |
|---|---|
| Name | Der Name der Integration. |
| Plugin-ID | Das Plugin, das zur Verwendung der Integration aktiviert werden muss. |
| Bestellung | Gibt die Reihenfolge an, in der diese Integrationskarte angezeigt wird. |
| Bannertext | Klicken Sie auf den Link, wählen Sie ein Bild oder Logo aus, das auf der Integrationskarte angezeigt werden soll, und klicken Sie auf **OK**. |
| Installiert | Schreibgeschütztes Feld, das angibt, ob das Plugin bereits installiert wurde. |
| Konfigurierbar | Gibt an, ob Sie die Integration konfigurieren können. |
| Kategorien | Wird zum Filtern der Integrationskarten verwendet. |
| Kurzbeschreibung | Eine Beschreibung der Integration, die im Tooltip-Hinweis für die Karte angezeigt wird. |
| Beschreibung | Eine längere Beschreibung der Integration. |

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die zugehörige Liste „ **Integration und Konfigurationen** “ wird angezeigt. Sie können diese zugehörige Liste verwenden, um Konfigurationsoptionen für die Integration zu definieren. Diese Optionen werden angezeigt, wenn Sie auf der zugehörigen Integrationskarte auf die Schaltfläche **Konfiguration** klicken.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Bezeichnung | Der Name des Integrationselements. |
| Name | Das Plugin, das zur Verwendung der Integration aktiviert werden muss. |
| Integration | Zeigt die Integration an, für die Sie Integrationselemente definieren |
| Bestellung | Gibt die Reihenfolge an, in der dieses Integrationselement angezeigt wird. |
| Typ | Wählen Sie in der Liste den Feldtyp aus:<br>○ Zeichenfolge<br>○ Ganzzahl<br>○ Dezimalzahl<br>○ Datum<br>○ Boolean<br>○ Passwort<br>○ IPv4<br>○ IPv6<br>○ URL |
| Wert | Geben Sie den Wert ein, der dem ausgewählten **Typ** zugeordnet ist. Wenn ein Wert eingegeben wird, der für den ausgewählten **Typ** ungültig ist, werden beim Ausführen der Integration keine Datensätze abgerufen. Wenn Sie beispielsweise den URL-Typ auswählen und den Wert 12.32.23.10 eingeben, werden keine Datensätze abgerufen. |

**7.** Klicken Sie auf **Absenden**.

### Tipps zum Schreiben von Integrationen

Vermeiden Sie einige der Gefahren, die beim Schreiben Ihrer eigenen Integrationen auftreten können, indem Sie die folgenden Richtlinien befolgen.

## Verwenden Sie nach Möglichkeit die Funktionalität der ServiceNow-Plattform

Meistens zielen die in Security Operations -Anwendungen (Security Incident Response, Threat Intelligenceund Vulnerability Response) integrierten Integrationsfunktionen darauf ab, die vorhandene Plattformintegrationsfunktionalität von ServiceNow zu verbessern oder zu optimieren. Stellen Sie beim Schreiben von Integrationen immer sicher, dass Sie die Plattformfunktionalität verwenden, sofern vorhanden. Im Folgenden sind einige allgemeine ServiceNow -Funktionalitäten aufgeführt, die anstelle des „Rollen Ihrer eigenen“ verwendet werden können.

- Ausgehende Webservices – Bei den meisten Interaktionen mit Systemen von Drittanbietern erfolgt die Kommunikation über Webservices. Verwenden Sie in diesen Fällen ausgehende Webservices der -Plattform (REST und SOAP werden unterstützt).
- Eine Datenquellen-/Importsatz-/Transformationszuordnung – Für die Verarbeitung von Daten und das Einfügen in ServiceNow -Tabellen besteht der bevorzugte Mechanismus in der Verwendung von Datenquellen und zugehörigen Komponenten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Verwenden Sie nach Möglichkeit Security Operations-Integrations-Frameworks

Da Security Operations Integrationsmechanismen viele häufige Probleme gelöst haben, ist es nicht erforderlich, grundlegende Funktionalitäten für jede Integration neu zu implementieren. Beispielsweise unterstützen die Frameworks für Schwachstellendaten und Bedrohungsquellen die Verarbeitung mehrerer Seiten und die Übergabe dieser Daten an Datenquellen/Transformationen/Importsätze. Ebenso bietet das Scan- oder Suchquellen-Framework eine konfigurierbare Ratenbegrenzungsfunktion. Überprüfen Sie bei der Implementierung einer Funktion oder einer Reihe von Funktionen in der Regel, ob das vorhandene Security Operations Integration Framework Ihren Anwendungsfall abdeckt. Wenn dies der Fall ist, verwenden Sie dieses Framework.

## Erweitern Sie die vorhandenen Security Operations-Integrations-Frameworks nach Bedarf

Die meisten Tabellen und Skripts, die von Security Operations Integration Frameworks verwendet werden, sollten so erweitert werden, dass sie zukünftigen Anforderungen entsprechen. Wenn beim Schreiben einer Integration ein Anwendungsfall auftritt, erweitern Sie eine Integrationstabelle oder ein Skript, um diesen Anwendungsfall besser anzupassen.

## Geben Sie ServiceNow Feedback zu Problemen, die während der Integration aufgetreten sind

Da eine Integration entwickelt oder getestet wird, stellen Sie sicher, dass Sie Feedback geben, wenn Probleme auftreten. Selbst wenn eine Problemumgehung erforderlich ist, können die Mitarbeiter von Kundenservice und Support in zukünftigen Releases eine Verbesserung bereitstellen, die das Problem für zukünftige Integrationen verringern könnte.

## Test unter angemessener Last

Ein häufiges Problem bei -Integrationen besteht darin, dass sie nicht für die Verarbeitung realistischer Lasten geeignet sind. Da jede Integration eine bereichsbezogene Anwendung ist, werden von der Plattform weitere Einschränkungen auferlegt, um die Systemstabilität sicherzustellen. Diese Einschränkungen können dazu führen, dass Aufträge mit langer Ausführungszeit oder API-Aufrufe beendet werden. Sie können sicherstellen, dass Prozesse mit langer Ausführungszeit oder Prozesse, die viele Daten verarbeiten, ordnungsgemäß verarbeitet werden, indem Sie die Zeit für jeden Aufruf oder Prozess reduzieren (normalerweise durch Bereitstellung einer Möglichkeit, API-Anforderungen zu paginieren oder große Datensätze in Blöcke aufzuteilen).

### Fehlerbehebung bei der Integration

Diese Vorschläge zur Fehlerbehebung können Ihnen helfen, häufige Probleme zu beheben, die beim Einrichten oder Ausführen von Integrationen auftreten können.

#### Ersetzen Sie ein nicht vertrauenswürdiges oder abgelaufenes SSL-Zertifikat einer Drittpartei

Wenn in einer Integration eine SSL-Verbindung erforderlich ist, kann es vorkommen, dass das vom Drittanbieter bereitgestellte Zertifikat in ServiceNow noch nicht vertrauenswürdig ist oder abgelaufen ist. Sie können es ersetzen oder ein neues Zertifikat hinzufügen.

**Vorbereitungen**
Erforderliche Rolle: sn_ti.write



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise wie folgt ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/`.

   b. Klicken Sie in der Adresszeile auf das Sperrsymbol.

   c. Klicken Sie auf **Weitere Informationen**, und klicken Sie auf die Registerkarte **Sicherheit**.

   d. Klicken Sie auf **Zertifikat anzeigen**, und klicken Sie auf die Registerkarte **Detail**.

   e. Klicken Sie auf **Exportieren**, um die PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.
   Er muss mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----`enden.

2. Navigieren zu **Systemdefinition** > **Zertifikate**.
3. Klicken Sie auf **Neu** und einen neuen Datensatz für die Integration erstellen.
4. Fügen Sie in **PEM-Zertifikat**das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

## Integrations Capabilities Framework 2.0

Das neue Integration Capabilities Framework 2.0 wurde neu gestaltet, um die Implementierung von Integrationen auf einfache und konsistente Weise zu ermöglichen. Dadurch wird eine konsistente Experience für ähnliche Arten von Integrationen sichergestellt (z. B. Suche nach erkennbaren Reputationen).

Das neue Framework verfügt über Fähigkeiten, die mithilfe von Flows implementiert werden.

Zu den Vorteilen der erweiterten Framework-Implementierung gehören:

- Die Fähigkeits-Flows, die nur Komponenten auf Geschäftsebene ohne implementierte spezifische Logik enthalten.
- Die Fähigkeits-Flows akzeptieren jetzt eine Vielzahl von Eingaben und Formaten für maximale Flexibilität (z. B. Referenzen erkennbarer Elemente, CI-Referenzen, Aufgaben, beliebige Tabellen oder sys_id-Kombinationen).
- Ratenbegrenzung oder Drosselung bei Integrationsausführungen ist jetzt einfach zu konfigurieren (wodurch die Notwendigkeit der Verwendung von benutzerdefiniertem Code oder Änderungen an Implementierungs-Workflows entfällt).
- Verbesserte Funktionen für Audits und Ausführungsverfolgung ermöglichen jetzt eine bessere Berichterstellung und eine einfachere Fehlerbehebung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Robuste Fehlerbehandlungsfunktionen sind in die Fähigkeits-Flows integriert, um doppelte Implementierungsroutinen zu vermeiden.
- Möglichkeit, die bedingte Auslösung der Fähigkeiten oder Integrationen zu konfigurieren. Dies bietet die Flexibilität, Automatisierungen basierend auf der Incident-Kategorie automatisch zu starten.
- Für alle -Fähigkeiten wurde eine Standardfilterbedingung eingeführt, um erkennbare Elemente auf der Allow-Liste zu filtern, bevor Eingaben für die Integrationen bereitgestellt werden.

**Hinweis:**
Dieses neue Fähigkeits-Framework aktualisiert nicht das aktuelle Fähigkeits-Framework. Beide Frameworks können parallel arbeiten. Anweisungen zur Nutzung des neuen Fähigkeits-Frameworks finden Sie unter Verwenden des neuen Capability Framework mit einer installierten Integration und Verwenden des neuen Capability Framework mit einem Flow.

### Unterstützte Integrationen und Komponenten

Das Plugin „Security Incident Response“ enthält alle in Integration Capabilities Framework 2.0 aufgeführten Fähigkeits-Flows sowie allgemeine Standardfilter, die Sie je nach Anforderung aktivieren oder deaktivieren können.

**Hinweis:**
Wenn Sie das neue Capability Integration Framework mit dem New York-Release verwenden möchten, müssen Sie das Plugin „ServiceNow IntegrationHub Starter Pack Installer“ installieren. Wenden Sie sich an den Kundensupport, um Unterstützung bei der Installation zu erhalten.

## Unterstützte Anwendungsversionen

Ab Security Incident Response 10.0 werden die folgenden Integrationen unterstützt:

| Anwendung | Mindestversion erforderlich |
|---|---|
| Security Operations Hybrid Analysis Integration | 10.0.0 |
| Security Operations PhishTank-Integration | 10.0.0 |
| Security Operations ThreatCrowd-Integration | 10.0.0 |
| Security Operations CrowdStrike Intelligence-Integration | 10.0.0 |
| Security Operations „Have I been pwned?“ -Integration | 10.0.0 |
| Security Operations Metadefender-Integration | 10.0.0 |
| Aufgezeichnete zukünftige Integration von Security Operations | 10.0.0 |
| Security Operations VirusTotal-Integration | 10.0.0 |
| Security Operations WhoIs-Integration umkehren | 10.0.0 |

Ab Security Incident Response 10.4 werden die folgenden Integrationen unterstützt:

| Anwendung | Mindestversion erforderlich |
|---|---|
| Security Operations RiskIQ-Integration | 10.0.0 |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendung | Mindestversion erforderlich |
|---|---|
| Security Operations Shodan-Integration | 10.0.0 |
| Security Operations WhoIs-Integration | 10.0.0 |
| Security Operations Carbon Black-Integration | 10.3.1 |
| Security Operations Splunk Search-Integration | 10.3.0 |
| Security Operations ArcSight Logger-Integration | 10.3.0 |
| Security Operations McAfee ESM-Integration | 10.3.0 |
| Security Operations Elasticsearch-Integration | 10.3.0 |
| Security Operations IBM QRadar-Integration | 10.3.1 |
| Security Operations CrowdStrike Falcon-Host | 10.3.0 |

## Enthaltene Komponenten

Das neue Capability Integration Framework enthält die folgenden Komponenten:

- **Fähigkeiten**: Alle der folgenden Fähigkeiten, die heute im Produkt als Workflows vorhanden sind, wurden mithilfe von Flows neu gestaltet:
  - **Anforderung**blockieren: Bietet eine Möglichkeit, erkennbare Elemente zu blockieren, die einem Security Incident auf einer Firewall, einem Web-Proxy oder einem anderen Kontrollpunkt zugeordnet sind. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **E-Mails suchen und**löschen: Bietet eine Möglichkeit, während einer Sicherheitsuntersuchung einen E-Mail-Server zu durchsuchen und bei Bedarf E-Mails vom Server zu löschen.
  - **Konfigurationselement**anreichern: Bietet eine allgemeine Möglichkeit, Konfigurationselemente mit zusätzlichen Informationen aus verschiedenen Quellen anzureichern. Diese Funktion wird bei Untersuchungen der Reaktion auf Incidents verwendet, um die mit einem Security Incident verknüpften Daten anzureichern.
  - **Erkennbares Element**anreichern: Bietet eine allgemeine Möglichkeit, erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen Quellen anzureichern. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **Event-Erfassung**: Bietet eine allgemeine Möglichkeit, einen Security Incident zu erstellen, indem Events aus einer Integrationsquelle einem Security Incident zugeordnet werden.
  - **Netzwerkstatistiken abrufen**: Ruft eine Liste der aktiven Netzwerkverbindungen von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen für die Ergänzung von Incidents verwendet.
  - **Laufende Prozesse abrufen**: Ruft eine Liste der laufenden Prozesse von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen für die Ergänzung von Incidents verwendet.
  - **Host**isolieren: Bietet eine Möglichkeit, einen Endpunkt oder einen Host zu isolieren, der einem Security Incident zugeordnet ist. „Host isolieren“ wird für ein Konfigurationselement (CI) ausgeführt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **In Beobachtungsliste veröffentlichen**: Bietet eine Möglichkeit, erkennbare Elemente, die einem Security Incident zugeordnet sind, einer Beobachtungsliste hinzuzufügen, die Sicherheits-Ereignisse überwacht und Warnungen generiert. Diese Funktion wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.
- **Sichtungssuche**: Durchsucht verschiedene SIEMs oder andere Protokollspeicher nach Instanzen von erkennbaren Elementen. Diese Funktion wird verwendet, um das Vorhandensein schädlicher IoCs in Ihrer Umgebung zu bestimmen.
- **Bedrohungssuche**: Führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein bestimmtes erkennbares Element einer bekannten Sicherheitsbedrohung zugeordnet ist. Diese Funktion wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

- **Neue Tabellen**:
  - sn_sec_cmn_capability: Fähigkeit und Flow, der die Fähigkeit implementiert.
  - sn_sec_cmn_capability_implementation: Der tatsächliche Implementierungs-Flow, der die Services der Fähigkeit bereitstellt.
  - sn_sec_cmn_capability_execution: Der Ausführungsdatensatz für eine Fähigkeit zur Laufzeit.
  - sn_sec_cmn_capability_implementation_execution: Der Ausführungsdatensatz für eine Fähigkeitsimplementierung zur Laufzeit.
  - sn_sec_cmn_filter_condition: Die Filterbedingungen, die zur Laufzeit auf die Fähigkeit oder eine Fähigkeitsimplementierung angewendet werden können.
- **Skript einschließen**: CapabilityProcessor: Behandelt den gesamten Verarbeitungscode für das Framework.
- **Quotengrenze**: Max. gleichzeitige Anforderung pro Zeitraum: Definiert, wie viele Integrationen parallel ausgeführt werden können.
- **Implementierung der Fähigkeit „Geplante Aufgabenverarbeitung“**: Wird alle 15 Sekunden ausgeführt und kann auf der Seite „Sicherheitsverwaltungseigenschaften“ deaktiviert werden (**Security Incident** > **Administration** > **Eigenschaften**.
  - Aktiviert oder deaktiviert die geplante Aufgabe „Implementierungen von Fähigkeiten verarbeiten“: Diese Aufgabe plant und verwaltet automatisch Ausführungs-Flows für die Fähigkeitsimplementierung.
  - Aktiviert oder deaktiviert automatisierte Suchen oder Ergänzungen: Einstellung, mit der die geplante Aufgabe aktiviert oder deaktiviert wird, die eine automatisierte Bedrohungssuche oder Ergänzung von erkennbaren Elementen durchführt, wenn erkennbare Elemente zu Security Incidents im aktuellen Fähigkeits-Framework hinzugefügt werden.
  - Aktiviert oder deaktiviert die geplante Aufgabe „Erkennbare Elemente für Security Incident suchen“: Diese Aufgabe plant automatisch eine Aufgabe für die Bedrohungssuche oder das Anreichern von erkennbaren Elementen, wenn einem Security Incident erkennbare Elemente hinzugefügt werden.

### Konfigurationen im neuen Capability Framework

In diesem Abschnitt werden die im neuen Framework verfügbaren Konfigurationen beschrieben.

## Vorbereitungen

Erforderliche Rolle: sn_si.admin, flow_designer, action_designer



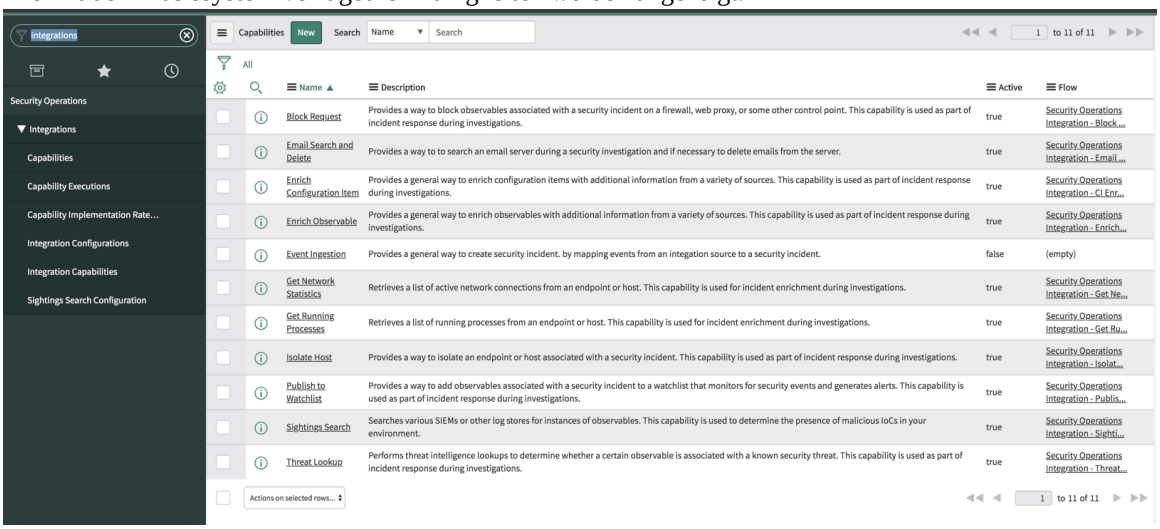
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Fähigkeiten**.

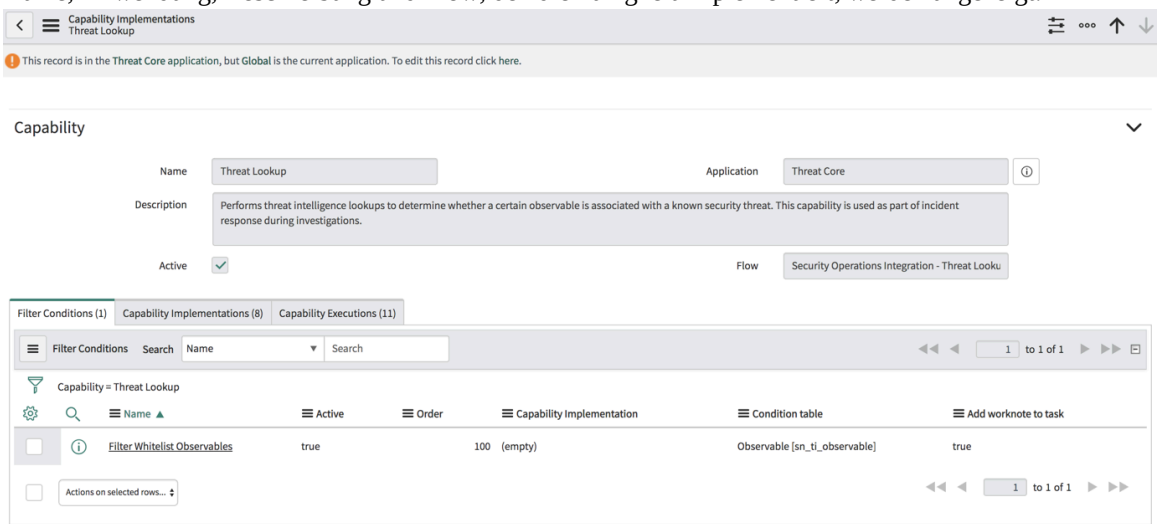
> **Hinweis:**
> Version 10.4: Ab Security Incident Response 10.4 wurde der Menüname **Fähigkeiten** in **Integration Capabilities (Flows)**geändert.

2. Die mit dem Basissystem verfügbaren Fähigkeiten werden angezeigt.




> **Hinweis:**
>
> Dies sind die mit dem Basissystem bereitgestellten Funktionen. Sie können die -Fähigkeiten von verwenden oder sie nach Bedarf anpassen. Die folgenden Schritte beschreiben die Konfiguration einer Fähigkeit und die für die Fähigkeit implementierten Integrationen.

3. Klicken Sie auf den Link in der Spalte Name, um eine Fähigkeit zu konfigurieren.
Name, Anwendung, Beschreibung und Flow, den die Fähigkeit implementiert, werden angezeigt.



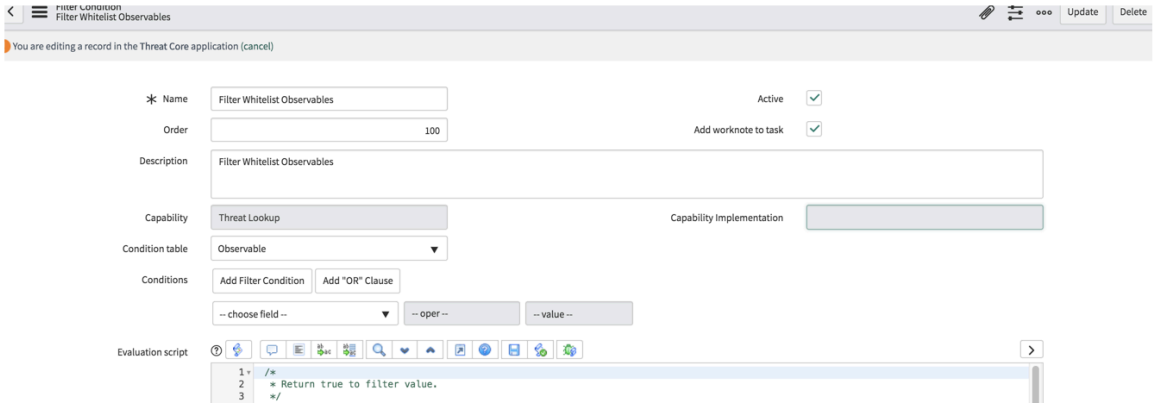

4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Fähigkeit zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Filterbedingungen auf Fähigkeitsebene**: Wenn eine Integrationsfähigkeit einen Flow implementiert, werden die dem Flow zugeordneten Filterbedingungen ausgeführt, bevor der Fähigkeits-Flow gestartet wird. Zum Beispiel enthält die Fähigkeit „Bedrohungssuche“ die Bedingung „Erkennbare Elemente auf Allow-Liste filtern“, wie oben gezeigt. Klicken Sie auf den Link Name, um die Filterbedingung zu bearbeiten.

  **Hinweis:**
  Aktivieren Sie das Kontrollkästchen **Arbeitsnotiz zu Aufgabe** hinzufügen, um Arbeitsnotizen hinzuzufügen, die Informationen zu den verwendeten Filterbedingungen enthalten.




  Sie können entweder Filterbedingungen oder ein Skript oder eine Kombination aus beidem definieren. Im obigen Beispiel wird ein Skript verwendet, um die Filterbedingungen zu definieren. Wenn der Fähigkeits-Flow ausgeführt wird, sucht das Skript nach erkennbaren Elementen auf der Allow-Liste und entfernt sie aus der Tabelle.

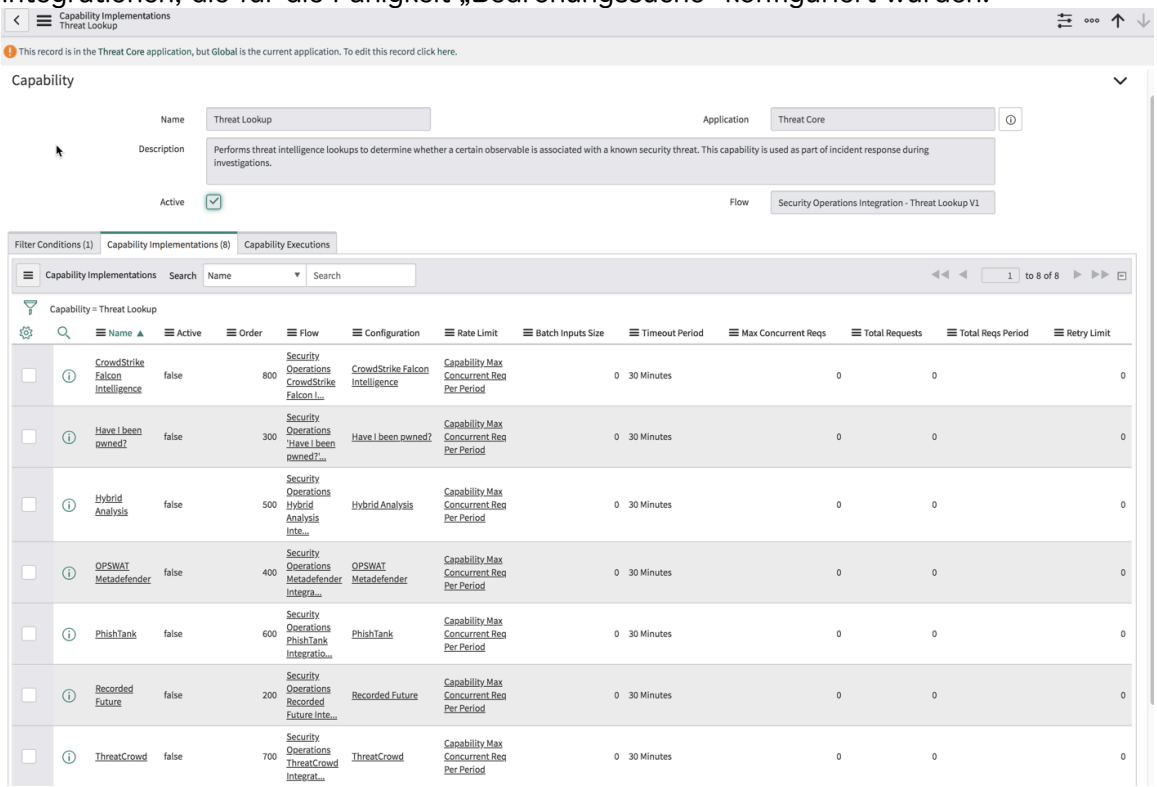
  **Hinweis:**
  Die hier festgelegten Filterbedingungen gelten für alle aktiven Integrationen, die auf der Registerkarte **„Fähigkeitsimplementierungen** “ definiert sind.

- **Fähigkeitsimplementierungen**: Klicken Sie auf die Registerkarte **Fähigkeitsimplementierungen**. Die Implementierungen (Integrationen), die für die

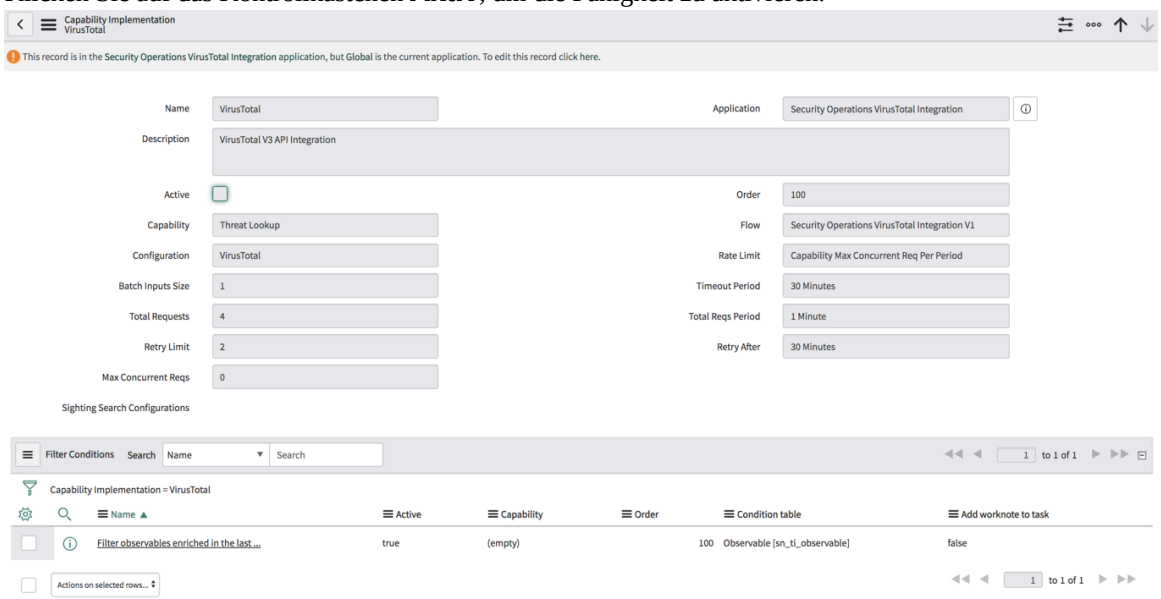


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fähigkeit konfiguriert wurden, werden angezeigt. Das folgende Beispiel zeigt die Integrationen, die für die Fähigkeit „Bedrohungssuche“ konfiguriert wurden:




5. Klicken Sie auf den Link Name, um die Fähigkeitsimplementierung anzuzeigen.
   Name, Anwendung, Beschreibung und Flow, den die Fähigkeit implementiert, werden angezeigt.
6. Klicken Sie auf das Kontrollkästchen **Aktiv**, um die Fähigkeit zu aktivieren.



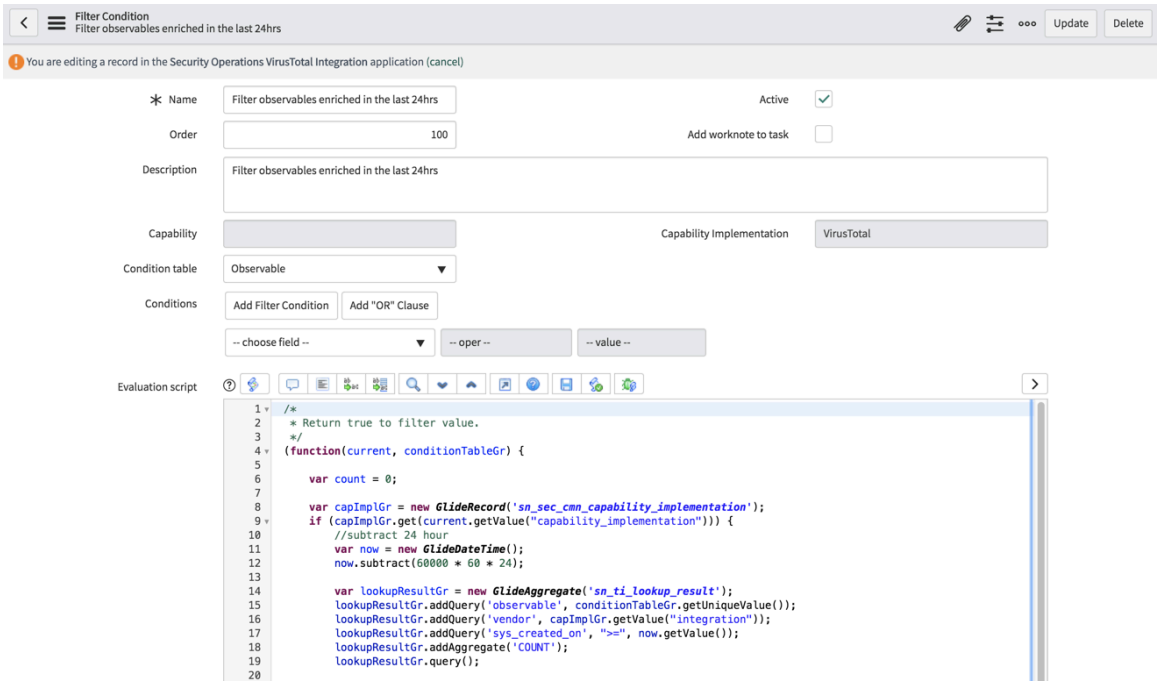

Sie können die folgenden Details angeben:

Klicken Sie im Abschnitt „Filterbedingungen“ auf den Link Name, um die für die Implementierung definierten Bedingungen zu konfigurieren. Fügen Sie Filterbedingungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

hinzu oder löschen Sie sie, ändern Sie das Skript bei Bedarf, und aktualisieren Sie den Datensatz.




### Verwenden des neuen Capability Framework mit einer installierten Integration

In diesem Abschnitt wird beschrieben, wie Sie das neue Framework für eine vorhandene Integration verwenden.

Führen Sie die folgenden Schritte aus, um eine bereits installierte und konfigurierte Integration zu aktivieren (siehe Liste der unterstützten Integrationen in Unterstützte Integrationen und Komponenten), um das neue Fähigkeits-Framework zu verwenden.

**Hinweis:**
Integration Capability Framework 2.0, verfügbar mit Security Incident Response **10.0.2**, unterstützt Implementierungen für die Fähigkeiten „ **Bedrohungssuche“** und „Erkennbares Element anreichern“. Implementierungen für andere Fähigkeiten werden in einem zukünftigen Release verfügbar gemacht.

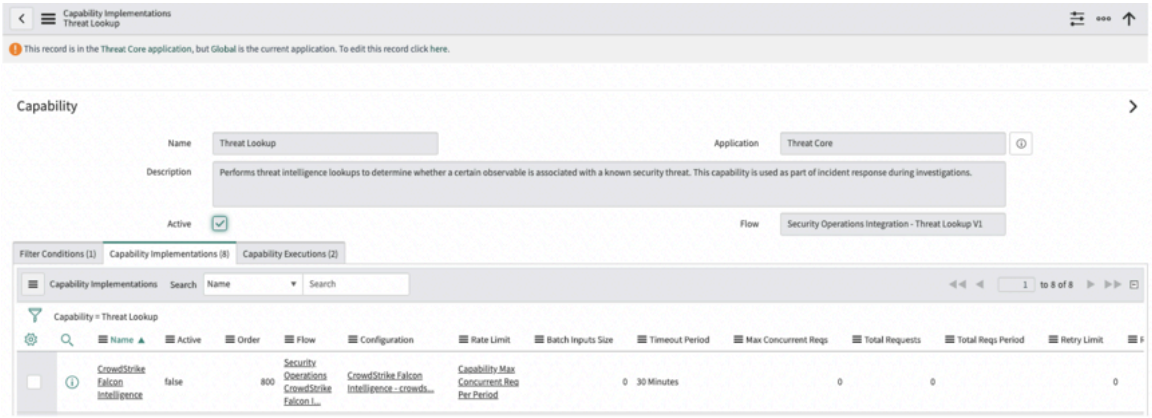
#### Bevor Sie beginnen

- Erforderliche Rolle: sn_si.admin
- Security Incident Response 10.0.2

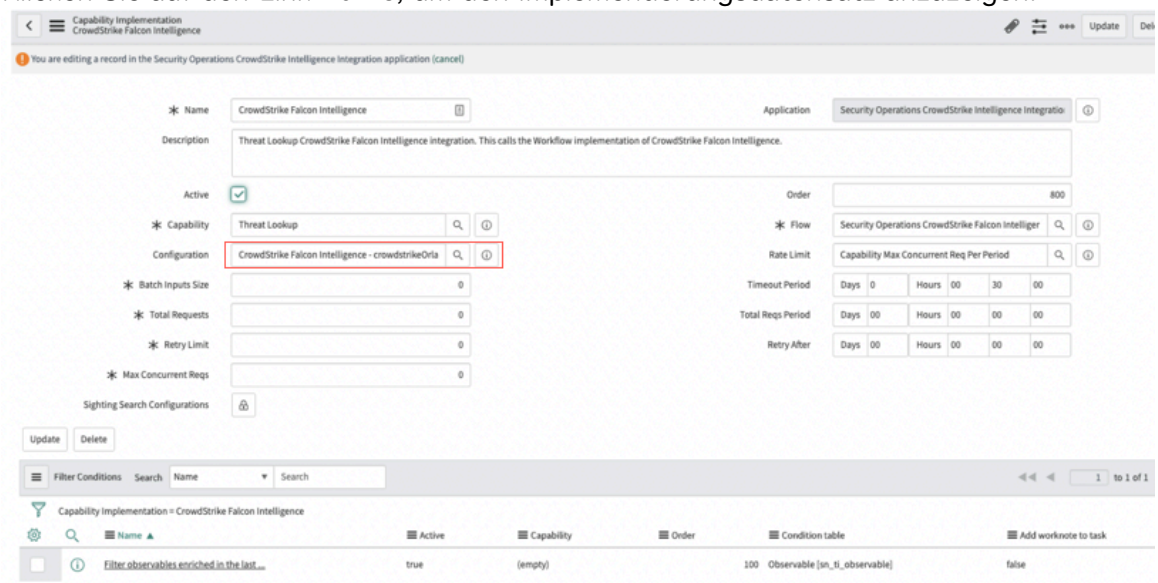
1. Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeiten**.
2. Klicken Sie auf die Fähigkeit **„Bedrohungssuche“**.
3. Klicken Sie auf die Registerkarte Fähigkeiten – Implementierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



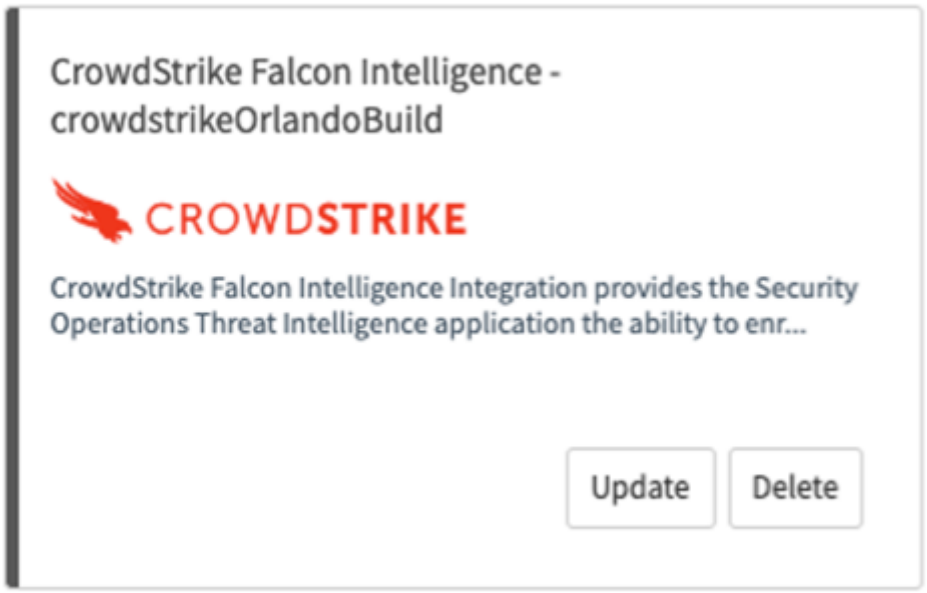

4. 4. Zeigen Sie den Fähigkeitsimplementierungsdatensatz für die gewünschte Integration an (Beispiel: Crowdstrike Falcon Intelligence). Die Spalte **Aktiv** muss den Wert **False**haben.
5. Klicken Sie auf den Link **Name**, um den Implementierungsdatensatz anzuzeigen.




6. Aktivieren Sie die Checkbox **Aktiv**.
7. Stellen Sie sicher, dass der Implementierungsdatensatz auf den richtigen Konfigurationsdatensatz verweist (den Kachelnamen für die Integration in). **Integrationskonfigurationen** > **Konfigurationen anzeigen (Ja)**) an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




8. Die Implementierung von ist für die Verwendung mit dem neuen Framework aktiviert.

**Hinweis:**
Alle unterstützten Integrationen, wenn sie mit Security Incident Response 10.0.2 installiert werden, werden automatisch unter dem neuen Integration Capability Framework aktiviert.

### Verwenden des neuen Capability Framework mit einem Flow

Führen Sie die folgenden Schritte aus, um einen Flow zu erstellen und den vom neuen Fähigkeits-Framework bereitgestellten Subflow aufzurufen.

### Vorbereitungen

- Erforderliche Rolle: sn_si.admin, flow_designer, action_designer
- Installieren Sie eine der unterstützten Integrationen (siehe Unterstützte Integrationen und Komponenten).

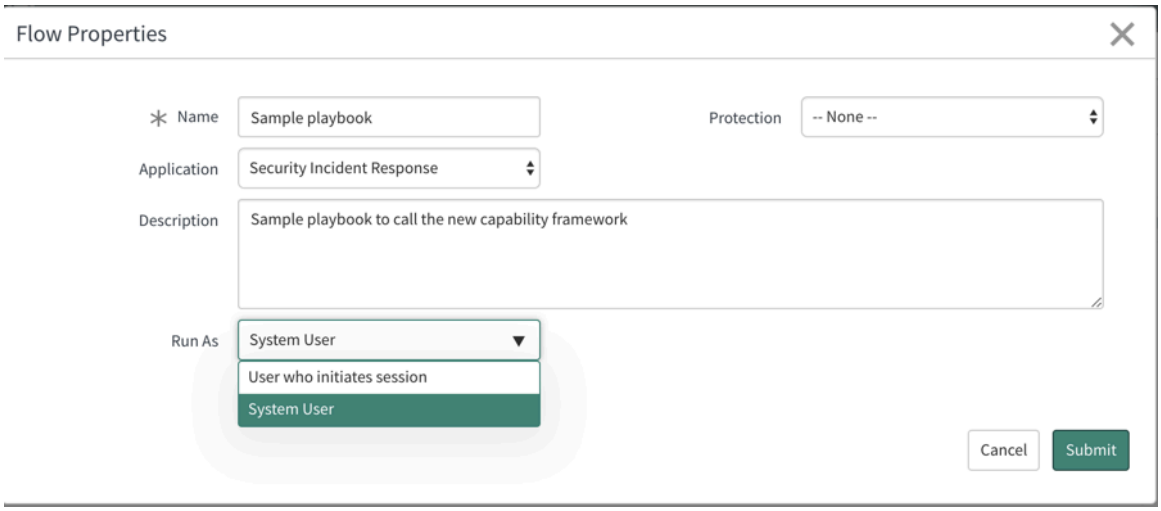
Die folgenden Schritte beschreiben, wie Sie einen Beispiel-Flow erstellen und einen der mit dem neuen Fähigkeits-Framework bereitgestellten Subflows aufrufen.

### Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer**.
2. Klicken Sie auf **Neu**, um einen neuen Flow zu erstellen und die erforderlichen Informationen für die Eigenschaften anzugeben.



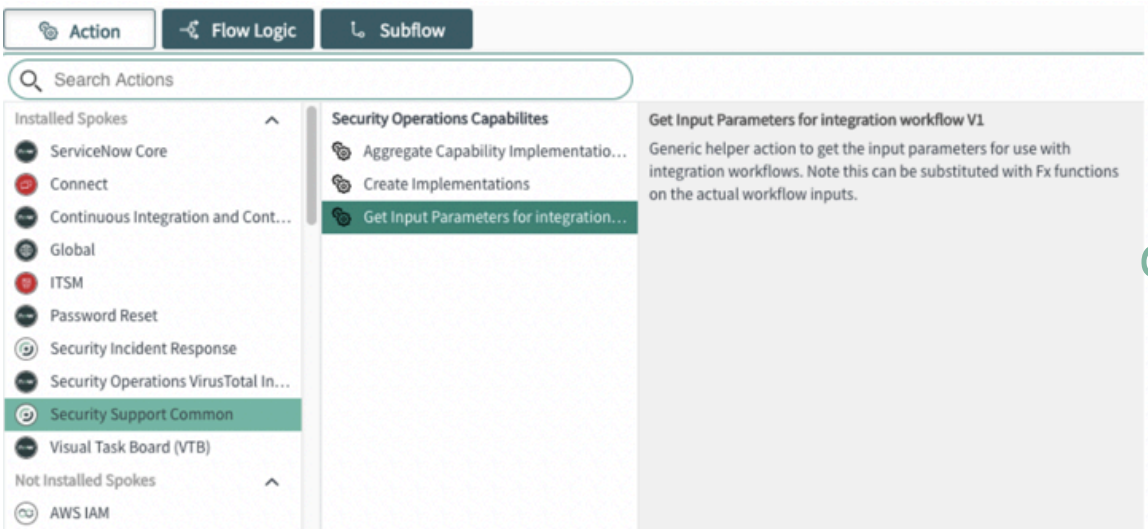
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Hinweis:**
Wählen Sie **Systembenutzer** in der Auswahlliste Ausführen als aus, wie in der obigen Abbildung gezeigt.

3. Wählen Sie eine Auslöserbedingung für den Flow aus (ein häufiger Auslöser ist die Erstellung eines Security Incident-Datensatzes für eine bestimmte Incident-Kategorie).

4. Wählen Sie in Schritt 1 des Flows eine Aktion aus, um Eingaben aus dem Security Incident zu erhalten (z. B. erkennbare Elemente).
Sie können eine Aktion aus den mit dem Basissystem bereitgestellten Aktionen mit der allgemeinen Sicherheitssupport-Spoke auswählen.

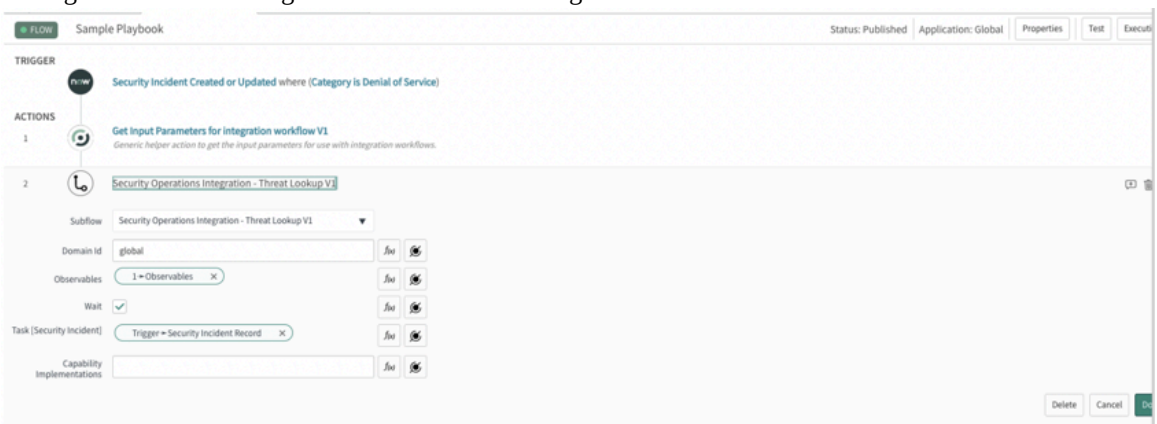



5. Wählen Sie in Schritt 2 einen Subflow aus (z. B. Bedrohungssuche).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**6.** Konfigurieren Sie den ausgewählten Subflow wie folgt:




**7.** Speichern und veröffentlichen Sie den Flow.

### Problembehandlung bei Integration Capability-Flows

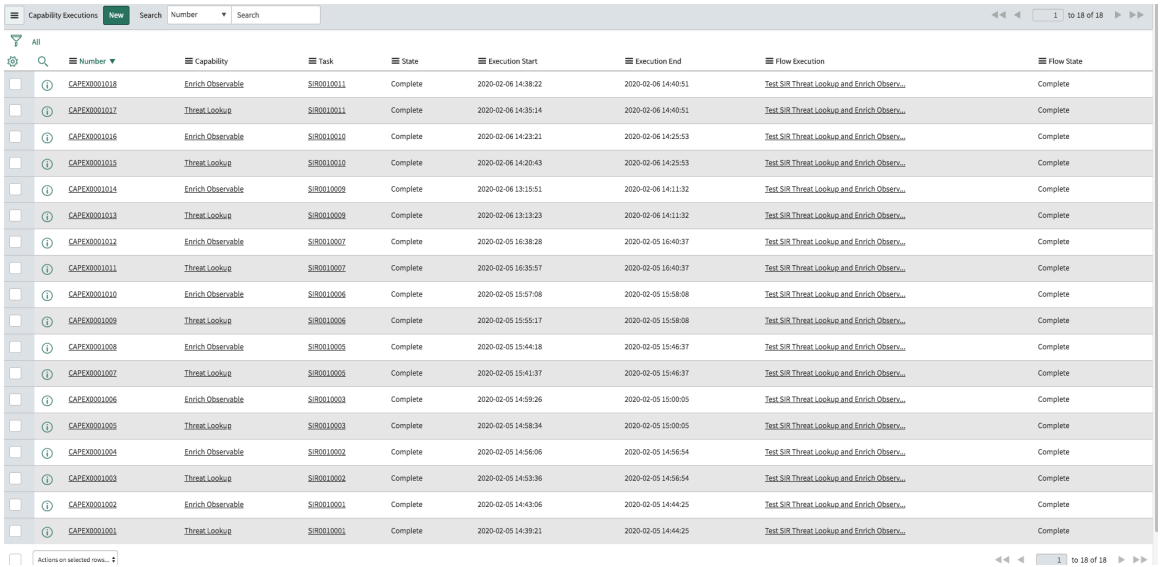
Die Option Fähigkeitsausführungen enthält detaillierte Informationen zu jeder Fähigkeit, die ausgeführt wurde.

**Hinweis:**
Abgeschlossene Ausführungen werden nach 30 Tagen archiviert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**1.** Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeitsausführungen.**.




**2.** Klicken Sie auf den Link Fähigkeitsausführungen, um zusätzliche Details anzuzeigen.

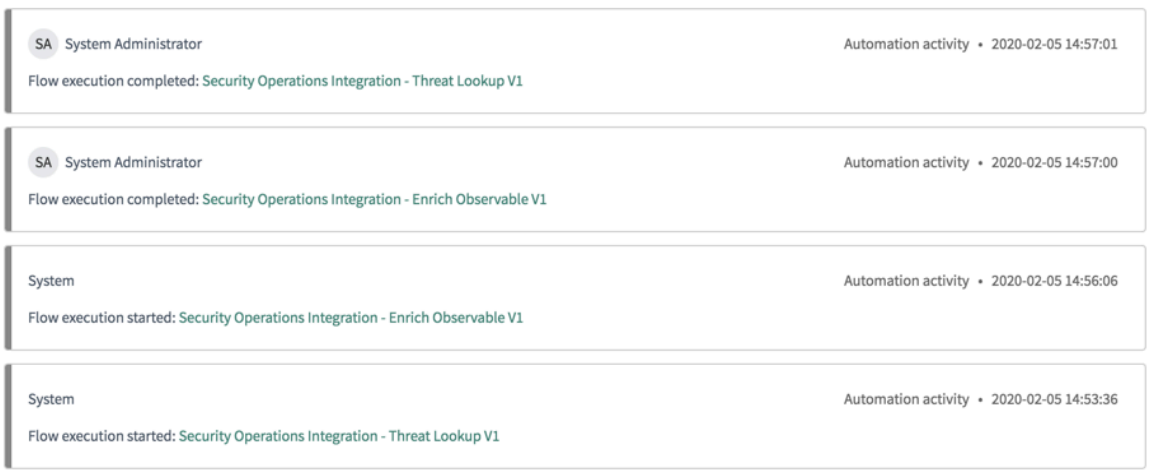
*`Arbeitsnotizen zu Security Incident-Datensatz`*

Wenn einem Security Incident erkennbare Elemente hinzugefügt wurden und die Auslöserbedingung für den Flow erfüllt ist, werden die Subflows „Bedrohungssuche“ und „Erkennbares Element anreichern“ initiiert und die folgenden Arbeitsnotizen werden dem Security Incident hinzugefügt:

- Flow-Ausführung gestartet: Integration von Sicherheitsvorgängen – Erkennbares Element anreichern V1
- Flow-Ausführung abgeschlossen: Integration von Sicherheitsvorgängen – Erkennbares Element anreichern V1
- Flow-Ausführung gestartet: Security Operations Integration – Threat Lookup V1
- Flow-Ausführung abgeschlossen: Security Operations Integration – Threat Lookup V1

Um diese Arbeitsnotizen anzuzeigen, melden Sie sich als Benutzer mit den *`Rollen sn_si.admin`* oder *`sn_si.analyst`*, *`flow_designer`*und *`action_designer an`*.

Navigieren Sie zur Security Incident-Datensatzseite, und klicken Sie auf diese Arbeitsnotizen, um die Details der Flow-Ausführung anzuzeigen.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## REST APIs für die Integration von Drittanbietern mit Security Operations

Das Security Operations -Basissystem enthält eine Reihe von geskripteten REST-APIs, die Kunden und Partnern die einfache Integration in eine vorhandene Security Operations -Bereitstellung ermöglichen. Mit den APIs können Sie Daten von außerhalb Ihres Systems sammeln (z. B. wird ein Python-Skript verwendet, um Daten von VirusTotal zu erhalten) und an Ihre Instanz zurücksenden.

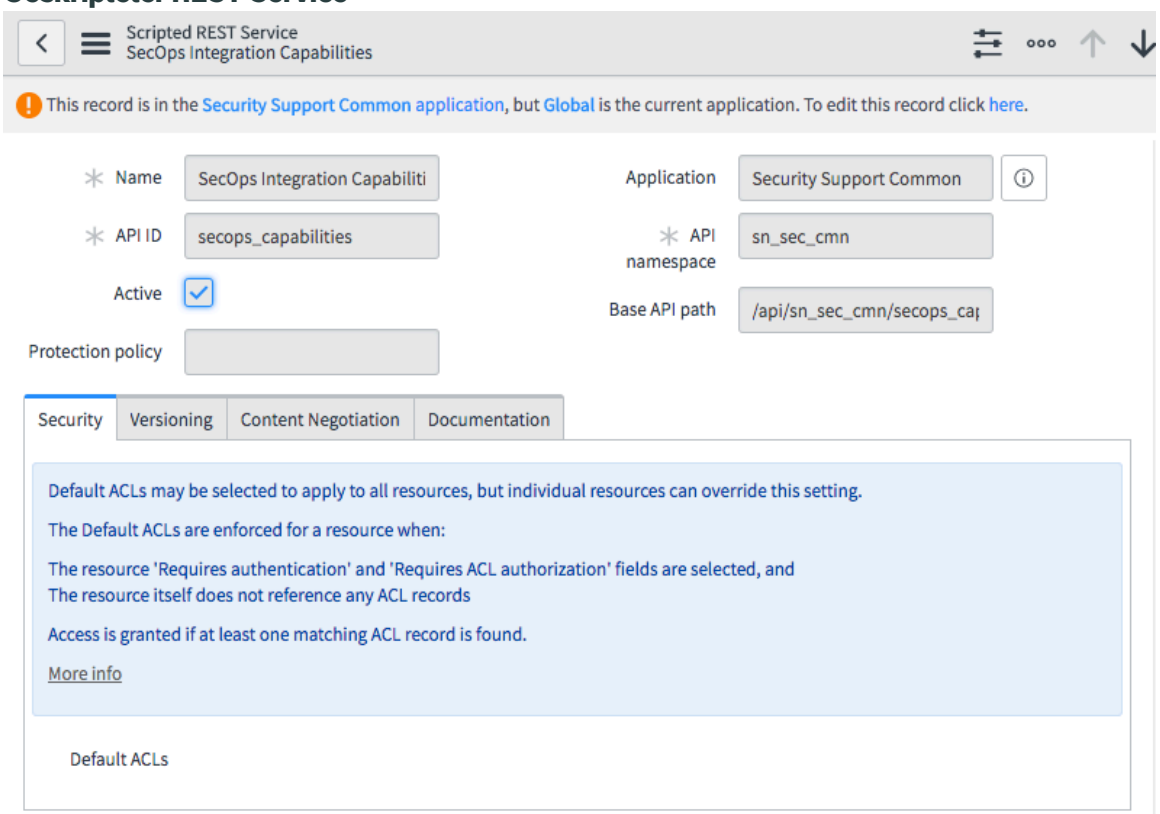
Skripts, die in fast jeder Sprache (z. B. Python) geschrieben sind, können mit den APIs verwendet werden, um kundenspezifische Prozesse auszuführen. Die Skripts müssen in einer Sprache geschrieben sein, die einen nach außen gerichteten HTTP-Post-Aufruf durchführen kann. Wenn Sie beispielsweise eine Java-Anwendung haben, müssen Sie eine Bibliothek wie das Paket `java.net.HttpUrlConnection` verwenden, um einen HTTP-Aufruf zu erstellen und eine JSON-Zeichenfolge als Textkörper für die Nachricht zu übergeben.

Die API wird ausschließlich zum Hinzufügen von Daten verwendet, die außerhalb unseres Systems erfasst wurden. Wenn Sie beispielsweise ein VT-Python-Skript eingegeben und Daten von VT erhalten haben, können Sie diese Daten an die SN-Instanz zurücksenden.

### Authentifizierung

Alle Vorgänge innerhalb der API-Definitionen verwenden die von bereitgestellte Plattformauthentifizierung Scripted REST APIs -Vorgangsfunktion. Um darauf zuzugreifen, navigieren Sie zu **System-Webservices** > **Scripted Web Services** > **Scripted REST APIs** und suchen Sie nach der API **„SecOps Integration Capabilities“**.

**Geskripteter REST-Service**




Der Benutzer und die Domäne des Benutzers sind im Kontext der API leicht verfügbar. Datensätze können an einen Benutzer gebunden, ein Audit-Pfad eingerichtet und die Domänentrennung durchgeführt werden. Da Sie als bestimmter Benutzer authentifiziert sind, können Sie außerdem verwenden Verwenden von GlideRecordSecure , um einen nicht autorisierten Zugriff auf Daten zu verhindern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Autorisierung

Um den Datensatzerstellungsprozess für Benutzer außerhalb der Anwendung Security Operations zu schützen, benötigen Sie die Rolle sn_sec_cmn.api_write. Nur Benutzer mit dieser Rolle können auf die APIs zugreifen.

## Konfigurationsanforderungsparameter

Die folgenden Anforderungsparameter sind verfügbar.

| Name | Standard | Beschreibung |
|---|---|---|
| ignore_mandatory_fields | false | Bei „true“ bleibt der Datensatz erhalten, auch wenn Pflichtfelder nicht ausgefüllt werden. |
| include_wrap | false | Bei „true“ enthält die Antwort den von der Instanz bereitgestellten Standard-Wrapper für Scripted REST APIs. |
| simple_response | false | Bei „true“ enthält die Antwort nur Informationen, ob der Vorgang erfolgreich war. |

## Fehlerantworten

Die folgenden Fehlerantworten können auftreten.

| Fehlermeldung | Wann tritt es auf? | Lösung |
|---|---|---|
| Ungenügender Zugriff | Anwender verfügt nicht über die Rolle sn_sec_cmn.api_write. | Fügen Sie dem Benutzer die Rolle hinzu. |
| Ungültiger Beitragstext | Anforderungstext ist leer oder ein leeres Objekt. | Entspricht der API-Definition. |
| Keine Felder angegeben | Zum Beibehalten bereitgestellte Datenfelder sind leer. | Entspricht der API-Definition. |
| Pflichtfelder fehlen: x, y, z | Pflichtfelder fehlen. | Entsprechen Sie der Tabellendefinition der Zieltabelle, oder legen **Sie ignore_mandatory_fields** auf „true“ fest. |
| Datensatz kann nicht beibehalten werden | Analysierter Datensatz kann nicht beibehalten werden. | GlideRecord insert() fehlgeschlagen, weitere Analyse ist erforderlich. |
| Unbekannter Fehler. | Tritt auf, wenn kein bekannter Fehlerpfad verfolgt wurde. | Weitere Analysen sind erforderlich. |

## Anwendungsfall CI-Ergänzung

Mit Ihren Drittanbieterskripts können Sie zur CI-Anreicherung in die Tabelle „Configuration Item Enrichment“ [sn_sec_cmn_ci_enrichment_result] schreiben. Die Ergänzungsdatensätze basieren auf vorhandenen Fähigkeiten, die detaillierte Informationen zu einem Datensatz aus einer Drittanbieterquelle bereitstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielanforderung und -antworten für den Anwendungsfall der CI-Ergänzung werden hier angezeigt.

**Anforderung für CI-Ergänzung erstellen**


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


**Antwort für CI-Ergänzung erstellen**


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


## Anwendungsfall der Ergänzung erkennbarer Elemente

Mit Ihren Drittanbieterskripts können Sie zur Anreicherung erkennbarer Elemente in die Tabelle „Ergebnis der Anreicherung erkennbarer Elemente“ [sn_ti_observable_enrichment_result] schreiben. Die Ergänzungsdatensätze basieren auf vorhandenen Fähigkeiten, die detaillierte Informationen zu einem Datensatz aus einer Drittanbieterquelle bereitstellen.

Beispielanforderung und -antworten für den Anwendungsfall der Ergänzung erkennbarer Elemente werden hier angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen – Anforderung für Ergänzung erkennbarer Elemente

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

### Erstellen – Antwort für Ergänzung erkennbarer Elemente

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

**Hinweis:**

Zusätzlich zum Anreichern vorhandener Datensätze können Sie Security Operations -Ergänzungsdatenzuordnung auch verwenden, um neue Datensätze zu Tabellen hinzuzufügen, indem Sie eine „ **enrichment_mapping_id** “ für eine vorhandene Ergänzungszuordnung und eine entsprechende **„raw_data“-Zeichenfolge übergeben**, die vom Zuordnungsprozess analysiert werden kann.

## Anwendungsfall für die Bedrohungssuche

Mit Ihren Skripts von Drittanbietern können Sie in die Tabelle „Ergebnis der Bedrohungssuche“ [sn_ti_lookup_result] schreiben, um Ergebnisse der Bedrohungssuche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu erhalten. Die Suchdatensätze basieren auf vorhandenen Funktionen, die detaillierte Informationen zu einem Datensatz aus einer Drittanbieterquelle bereitstellen.

Beispielanforderung und -antworten für den Anwendungsfall „Bedrohungssuche“ werden hier angezeigt.

**Anforderung für Bedrohungssuchen erstellen**

```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Erstellen: Antwort für Bedrohungssuchen**


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


## Integrationsfähigkeiten

Das Framework Integrationsfunktionen bietet eine konsistente Architektur zur Unterstützung der Interoperabilität mit Integrationen von Drittanbietern. Diese abstrahierte Schnittstelle und dieses Datenmodell isolieren Integrationen von Änderungen an der Kernanwendung und stellen eine konsistente Experience für ähnliche Arten von Integrationen sicher.

Jede Integrationsfähigkeit bleibt in der Tabelle „Integrationsfunktion “ [sn_sec_cmn_integration_capability] erhalten. Integrationsfähigkeits-Workflows können nicht einzeln ausgeführt werden und erfordern den Start eines Implementierungs-Workflows. Jedes Plugin, das eine Implementierung der Fähigkeit bereitstellt, fügt seine Implementierung der folgenden untergeordneten Tabelle hinzu: Integration Capability Implementation [sn_sec_cmn_integration_capability_implementation].

Die Implementierung gibt den auszuführenden Workflow, die zugehörige Integration (Plugin-ID) und die implementierte Fähigkeit an. Diese Workflows können mit dem parallelen Workflow-Startprogramm parallel ausgeführt werden. Die sequenzielle Ausführung ist jedoch die Standardeinstellung im Basissystem. Bei Bedarf können Sie die Ausführungsreihenfolge ändern.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Security Operations Integration - Block Request-Fähigkeit

Die Fähigkeit „Aktion blockieren“ blockieren erkennbare Elemente, die einem Security Incident zugeordnet sind an einer Firewall, einem Webproxy oder einem anderen Kontrollpunkt mithilfe von Implementierungsworkflows. Diese Fähigkeit wird während bei

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Die Blockierungsanforderungs-Fähigkeit verfügt über einen Workflow, Workflow „Security Operations Integration - Block Request“., der die zu blockierende Anforderung ausführt. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, findet alle implementierenden Fähigkeiten und führt die Anforderung basierend auf dem konfigurierten Workflow aus.

Die Fähigkeit verwendet auch andere Implementierungen:

- Security Operations Integration Palo Alto Networks Firewall-Startprogramm-Workflow
- Security Operations Palo Alto Networks – Workflow zum Überprüfen und Sperren von Werten

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Blockierungsanforderung ausführen

Blockiert die Kommunikation mit erkennbaren Elementen, die einem Security Incident zugeordnet sind.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Der Workflow „ **Security Operations Integration - Block Request**“ kann über ein Formular für erkennbare Elemente oder über die zugehörige Liste „Erkennbare Elemente für **Security Incident“** für einen Security Incident ausgelöst werden.

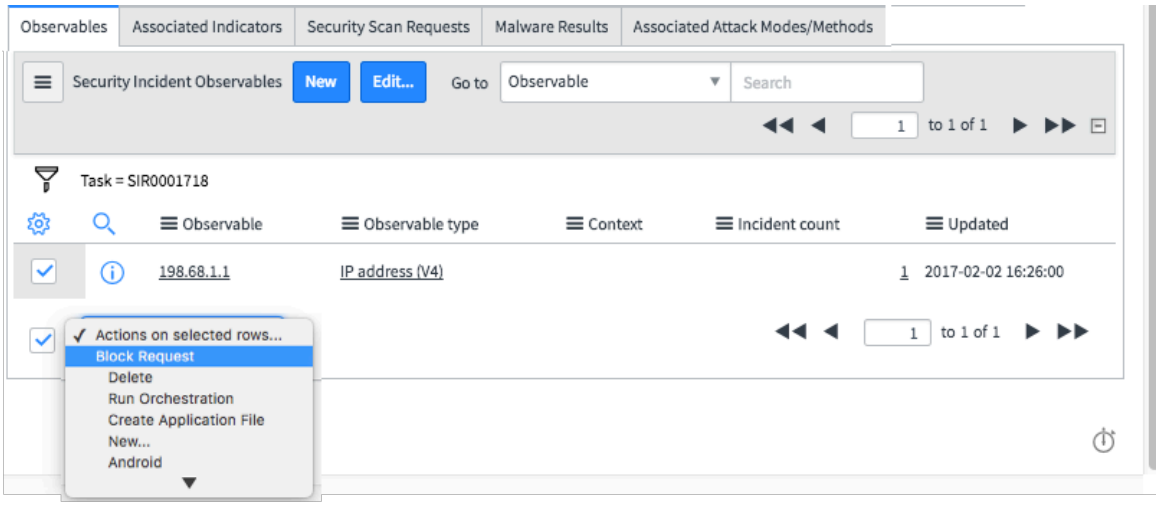
Dieses Beispiel zeigt eine Sperranforderung aus einem Security Incident.

**Prozedur**

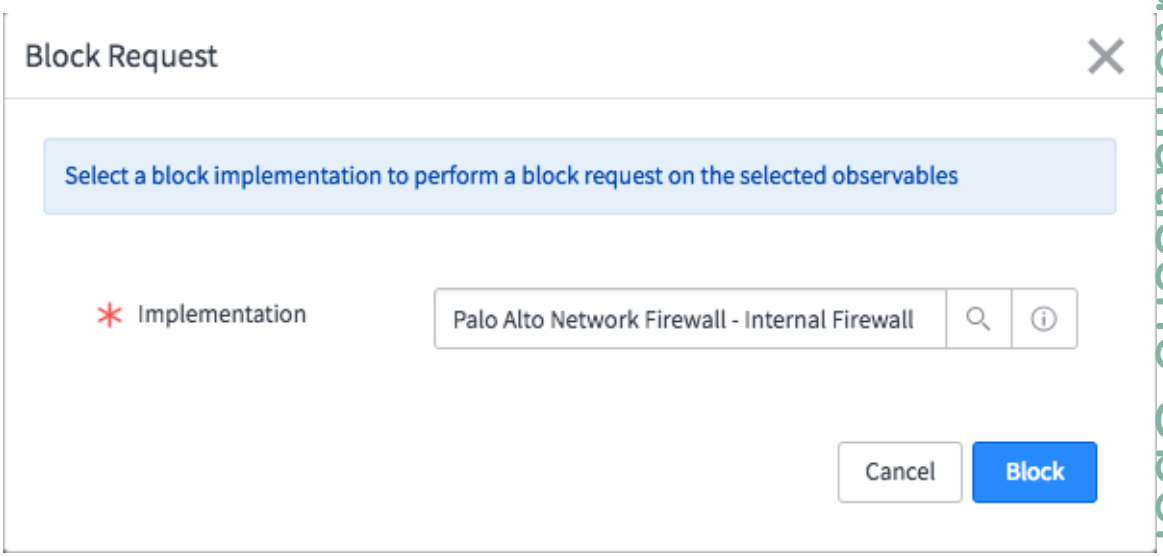
1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie auf der Registerkarte **Zugehörige Liste** erkennbare Elemente aus.
3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen... aufAnforderung** blockieren.

Automatische Übersetzung

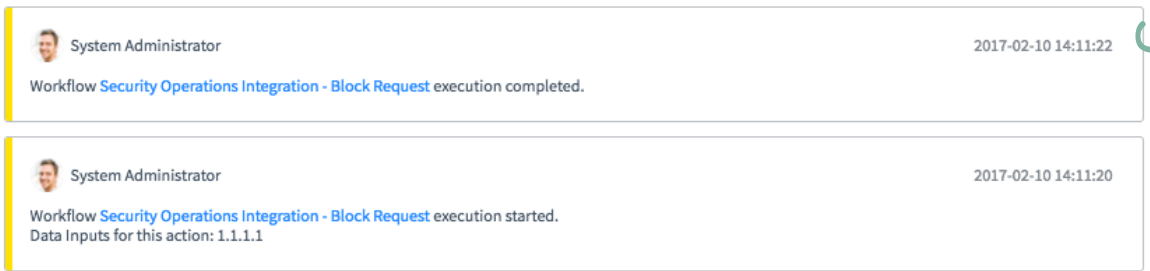
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Dialogfeld wird angezeigt.




4. Wählen Sie die Implementierung aus.
5. Klicken Sie auf **Block**.
   Das Audit der Workflow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.




### Workflow „Security Operations Integration - Block Request“.

Der Workflow „Security Operations Integration - Block Request“ ist ein allgemeiner Workflow, der unabhängig von Integrationen ist. Er blockiert erkennbare Elemente, die einem Security Incident zugeordnet sind. Verwenden Sie es, um eine Integration wie Palo Alto Networks – Firewallzu erfüllen.

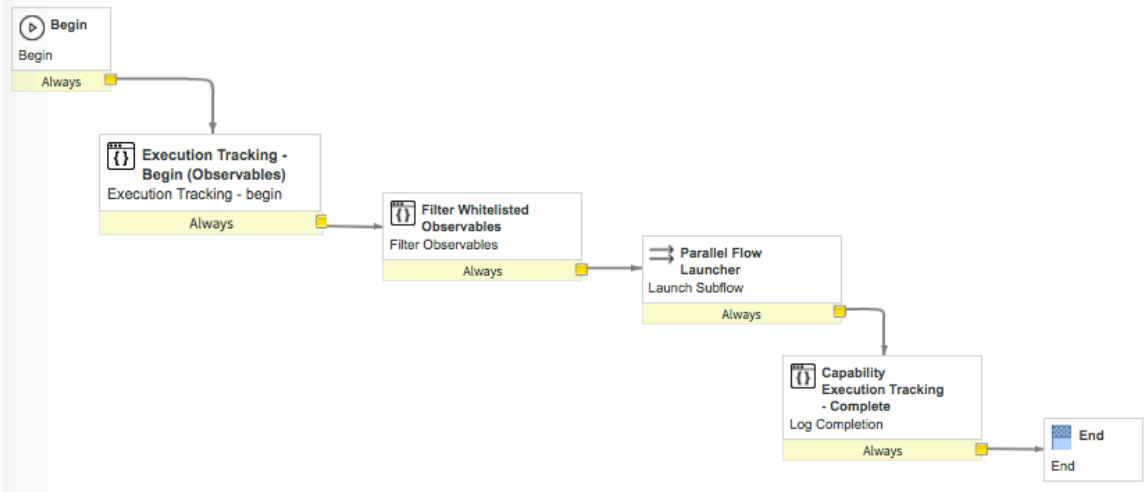
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Der Workflow „ **Security Operations Integration - Block Request**“ kann in einem Formular für erkennbare Elemente oder über die zugehörige Liste „Erkennbare Elemente für **Security Incident** “ für einen Security Incident ausgelöst werden. In einer Liste befindet es sich im Dropdown-Aktionsmenü. In einem Formular handelt es sich um einen zugehörigen Link. Das Blockieren einer Anforderung ist nur verfügbar, wenn Sie eine Implementierung für die Fähigkeit „Anforderung blockieren“ installiert haben.

**Anforderung blockieren**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Erkennbare Elemente auf Allow-Liste filtern“.

Die Workflow-Aktivität Gefilterte erkennbare Elemente auf der Allow-Liste entfernt erkennbare Elemente, die ignoriert werden können, aus der Liste der erkennbaren Elemente. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Erkennbare Elemente auf Allow-Liste filtern“ kann mit jedem Workflow verwendet werden, um erkennbare Elemente zu filtern, bevor eine Aktion ausgeführt wird.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Filterliste erstellt. |
| Fehler | Beim Versuch, die erkennbaren Elemente zu filtern, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Liste der verfügbaren erkennbaren Elemente. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| gefilterteErkennbareElemente | Gefilterte erkennbare Elemente. |

### Security Operations-Integration – E-Mail-Such- und Löschfunktion

Die Funktion „E-Mails suchen und löschen“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche zurück und gibt optional Details für jede gefundene E-Mail zurück. Nach Abschluss der E-Mail-Suche können Sie die E-Mails löschen.

Die Funktion „E-Mails suchen und löschen“ verfügt über einen Workflow, der die Prozesse zum Suchen und Löschen von E-Mails ausführt.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt. Wenn keine der Implementierungen der Fähigkeiten **„E-Mails suchen“ und „Löschen** “ aktiv ist, wird der zugehörige Link „E- **Mail-Suche** “ für einen Security Incident nicht angezeigt.

### Integration von Sicherheitsvorgängen – Workflow „E-Mails suchen und löschen“.

Der Workflow „Security Operations Integration – Email Search and Delete“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche zurück und gibt optional Details für jede gefundene E-Mail zurück. Nach Abschluss der E-Mail-Suche können Sie die E-Mails löschen.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

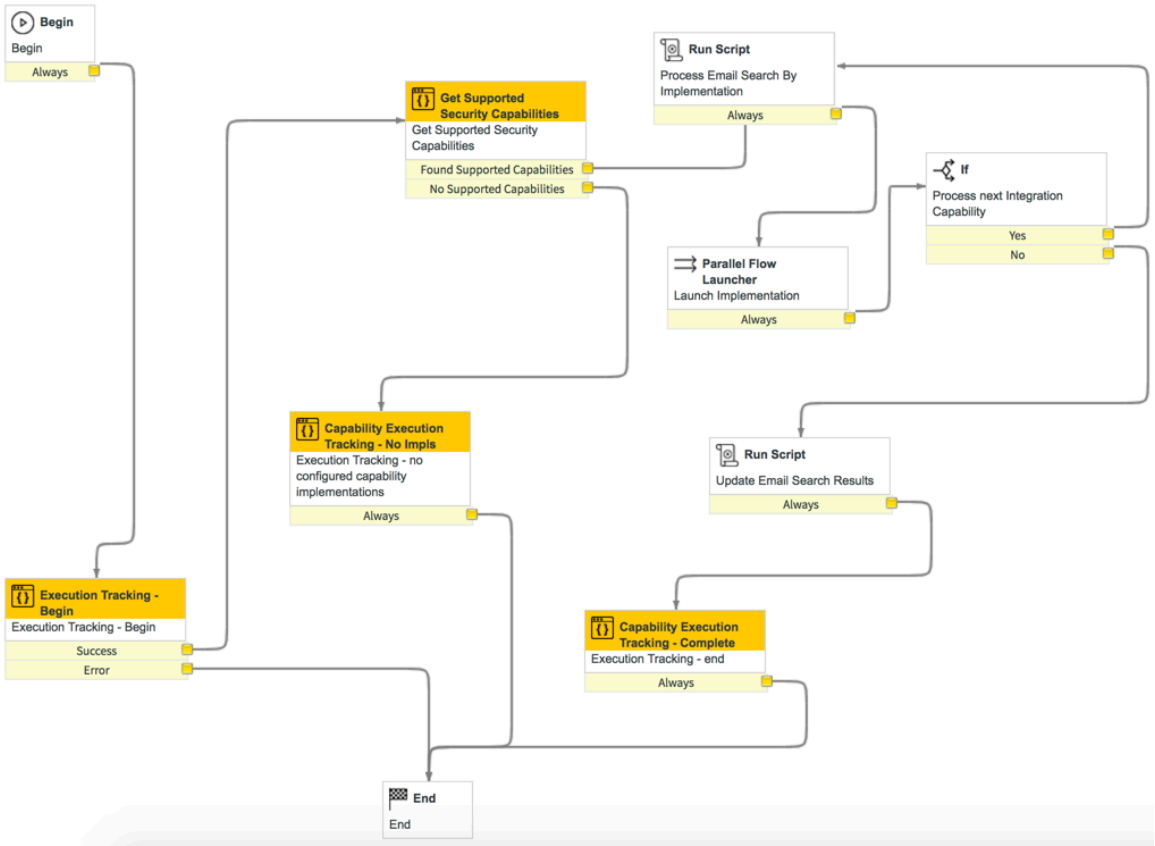
### Warum und wann dieser Vorgang ausgeführt wird
Die Suchabfrage kann einige Zeit in Anspruch nehmen. Nach dem Empfang der Anzahl ist eine Genehmigung erforderlich, um E-Mails von einem E-Mail-Server zu löschen.

Dieser Workflow wird durch die **Schaltflächen Von E-Mail-Servern löschen** und **Auf E-Mail-Servern suchen im Formular „** E-Mail- **Suche** “ in einem Security Incident ausgelöst. Weitere Informationen finden Sie unter Suchen und löschen Sie Phishing-E-Mails.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### E-Mails suchen und löschen




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

#### Aktivität „Beginn der Ausführungsnachverfolgung (Mail Search)“.

Die Ausführungsaktivität „Ausführungsnachverfolgung – Begin (Mail Search)“ erstellt einen Ausführungsnachverfolgungsdatensatz und markiert den Datensatzstatus als Gestartet. Diese Aktivität wird von allen Fähigkeits- und Implementierungs-Workflows verwendet, um ihren Status nachzuverfolgen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ausführungsnachverfolgungsdatensatz wurde erstellt. |
| Fehler | Ausführungsnachverfolgungsdatensatz konnte nicht erstellt werden. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityId | Systembezeichner der ausgeführten Integrationsfähigkeit. |
| implementierungId | Systembezeichner der ausgeführten Implementierung der Integrationsfähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| workflowContextId | Systembezeichner des zugeordneten Workflow-Kontextdatensatzes. Vom System bereitgestellt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| parentCapabilityExcutionId | Systembezeichner des Audit-Datensatzes, der den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows der Integrationsfähigkeit erforderlich, z. B. Splunk, Elasticsearch. |
| emailsearchId | Die sysid des E-Mail-Suchdatensatzes in der E-Mail-Suchtabelle [sn_sec_cmn_email_search]. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner des Ausführungsnachverfolgungsdatensatzes. |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Integration von Security Operations – CI-Fähigkeit ergänzen

Mit der Fähigkeit „CI anreichern“ können Sie Daten für Konfigurationselemente anreichern, die einem Security Incident zugeordnet sind.

Die Fähigkeit „ **CI** anreichern“ verfügt über den Workflow Security Operations Integration - CI-Ergänzungs-Workflow. Wenn der Fähigkeits-Workflow ausgeführt wird, werden zusätzliche Workflows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die zum Anreichern der ausgewählten CIs verwendet werden soll, oder Sie können die Anreicherung mit allen Implementierungen durchführen.

**Hinweis:**
Diese angereicherten Daten sind nicht die Art von Daten, die Sie in Ihrer CMDB speichern möchten, da es sich um forensische Daten handelt, die für eine bestimmte Untersuchung spezifisch sind, z. B. für die Durchführung eines Memdump von einem CI. Stattdessen werden die Daten in der Tabelle „Konfigurationselementanreicherung“ [sn_sec_cmn_ci_enrichment_result] gespeichert.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Security Operations Integration - CI-Ergänzungs-Workflow

Mit dem Workflow „Security Operations Integration - CI Enrichment“ können Sie Daten in Konfigurationselementen (CIs) anreichern, die einem Security Incident zugeordnet sind.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird von Security Incident Response auf zwei Arten ausgelöst.

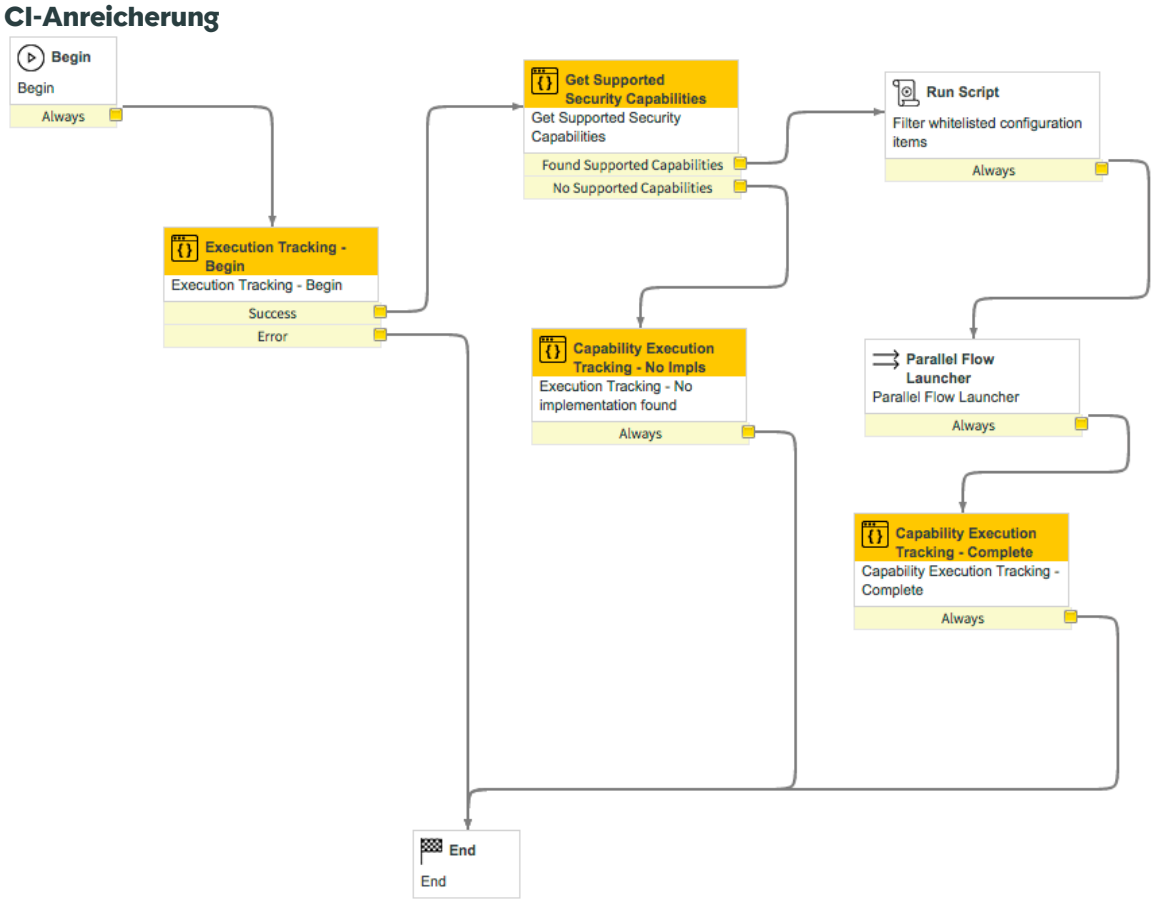
- indem Sie auf der Registerkarte **Konfigurationselemente** (unter dem zugehörigen Link **Betroffene Elemente** ) ein oder mehrere CIs auswählen und in der **Auswahlliste Aktionen für ausgewählte Zeilen** die Option **CI-Ergänzung** ausführen auswählen.
- indem Sie einen CI-Datensatz öffnen und auf den zugehörigen Link **CI** -Ergänzung ausführen klicken.

Mit beiden Methoden können Sie dann angeben, welche Implementierungen zum Anreichern der ausgewählten CIs verwendet werden sollen. Die zugehörigen Implementierungs-Workflows werden ausgeführt, um die Ergänzung durchzuführen.

**Hinweis:**
Das Basissystem enthält keinen Implementierungs-Workflow für diese Fähigkeit. Um CIs anzureichern, müssen Sie Ihren eigenen Implementierungs -Workflow erstellen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Ausführungsnachverfolgung: Beginn der Aktivität

Die Workflow-Aktivität „Execution Tracking – Begin“ (Ausführungsnachverfolgung – Begin) startet den Auditing-Prozess für einen Security Operations -Integrations-Workflow, der für erkennbare Elemente ausgeführt wird.

Die Aktivität „Ausführungsnachverfolgung – Begin“ kann mit jedem Workflow verwendet werden, um mit der Aufzeichnung des Fortschritts des Workflows in einem Audit zu beginnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ein Audit-Datensatz wird erstellt. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityId | Systembezeichner der ausgeführten Integrationsfähigkeit. |
| istImpl | Kennzeichnung, die angibt, ob ein Audit für einen Integration Capability-Workflow oder einen Integration Capability-Implementierungs-Workflow durchgeführt wird. Mögliche Werte sind:<br>• false – bezeichnet die Prüfung eines abstrakten Integration Capability-Workflows wie Sichtungssuche. (Standard)<br>• true – bezeichnet Auditing für einen Integration Capability-Implementierungs-Workflow. Zum Beispiel Splunk oder Elasticsearch. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| erkennbares Element Liste | Eine oder mehrere erkennbare SysIDs zum Ausführen der gewünschten Aktion.<br>Wird als Workflow-Eingabe verwendet. |
| workflowContextId | Systembezeichner des zugeordneten Workflow-Kontextdatensatzes. Vom System bereitgestellt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| parentCapabilityExcutionId | Systembezeichner des Audit-Datensatzes, der den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows von Integration Capability wie Splunk, Elasticsearch und VirusTotal erforderlich. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner des Audit-Datensatzes. |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse (Fortsetzung)

| Ergebnis | Beschreibung |
|---|---|
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Integration von Sicherheitsvorgängen – Fähigkeit „Erkennbares Element anreichern“.

Mit der Fähigkeit „Erkennbares Element anreichern“ können Sie erkennbare Elemente mithilfe von Implementierungs-Workflows mit zusätzlichen Informationen aus verschiedenen Quellen anreichern. Diese Fähigkeit wird während bei der Reaktion auf Incidents während Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Die Fähigkeit „Erkennbares Element anreichern“ verfügt über den Workflow Workflow „Security Operations Integration – Erkennbares Element anreichern“.. Wenn der Fähigkeits-Workflow ausgeführt wird, werden zusätzliche Workflows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die zum Anreichern der ausgewählten erkennbaren Elemente verwendet werden soll, oder Sie können die Anreicherung mit allen Implementierungen durchführen, die den unterstützten erkennbaren Typen entsprechen.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Workflow „Security Operations Integration – Erkennbares Element anreichern“.

Mit dem Workflow „Security Operations Integration – Erkennbares Element anreichern“ können Sie erkennbare Elemente mithilfe von Implementierungsworkflows mit zusätzlichen Informationen aus verschiedenen Quellen anreichern.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

#### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow kann entweder von Security Incident Response oder Threat Intelligence auf zwei Arten ausgelöst werden.

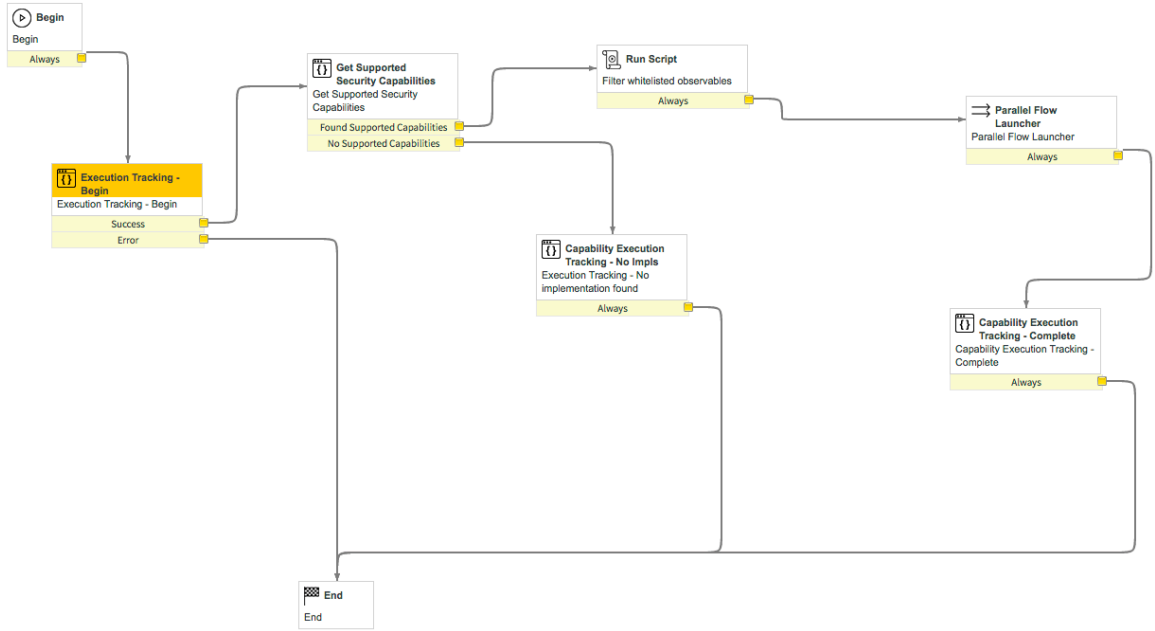
- indem Sie ein oder mehrere erkennbare Elemente aus der Liste „Erkennbare Elemente“ **auswählen** und in der Auswahlliste **Aktionen für ausgewählte Zeilen** die Option Ergänzung erkennbarer Elemente ausführen auswählen.
- indem Sie einen Datensatz für erkennbare Elemente öffnen und auf den zugehörigen Link Ergänzung **erkennbarer Elemente ausführen klicken**.

Mit beiden Methoden können Sie dann angeben, welche Implementierungen zum Anreichern der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Workflows werden ausgeführt, um die Ergänzung durchzuführen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erkennbares Element ergänzen




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

#### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

#### Integration mit Security Operations – Fähigkeit „Netzwerkstatistiken abrufen“.

Die Fähigkeit „Netzwerkstatistiken abrufen“ ruft eine Liste der aktiven Netzwerkverbindungen von einem Host oder Endpunkt ab. Sie kann während Untersuchungen zur Ergänzung von Incidents verwendet werden. Diese Fähigkeit wird automatisch ausgelöst, wenn ein Konfigurationselement zu einem Security Incident hinzugefügt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Fähigkeit „ **Netzwerkstatistiken** abrufen“ verfügt über einen Workflow, Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“., der ein oder mehrere CIs und Aufgaben akzeptiert. Der Workflow durchläuft jede Implementierung und jedes CI und ruft den Implementierungs-Workflow erneut auf.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

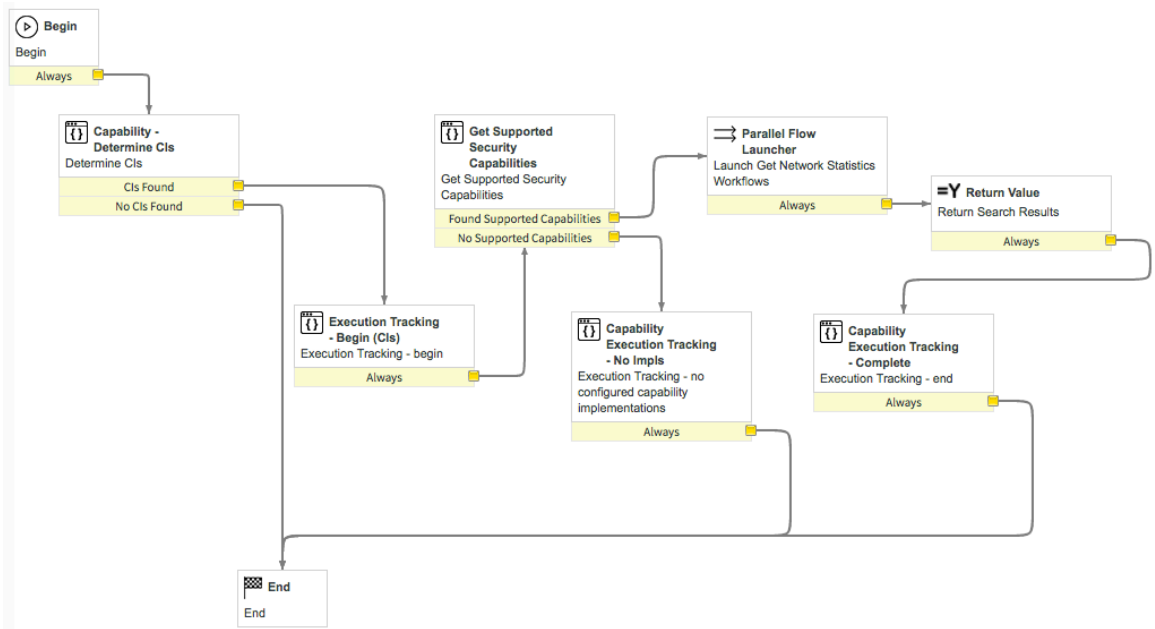
### Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“.

Der Workflow „Security Operations-Integrationen – Netzwerkstatistiken abrufen“ ruft eine Liste der aktiven Netzwerkverbindungen von einem Host oder Endpunkt ab.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird automatisch ausgeführt, wenn ein Konfigurationselement zu einem Security Incident hinzugefügt wird.

**Netzwerkstatistiken abrufen**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Fähigkeit: Bestimmt die CIs-Aktivität

Die Workflow-Aktivität „Fähigkeit – CIs bestimmen“ bestimmt, welche Konfigurationselemente (Configuration Items, CIs) in den Workflow aufgenommen werden sollen.

Die Aktivität „Fähigkeit – CIs bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche CIs in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfigurationselemente gefunden. |
| Fehler | Keine CIs gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |
| cis_affected | Konfigurationselemente. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| cis_affected | Gefilterte CIs |
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |

#### Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.

Die Workflow-Aktivität „ **Ausführungsnachverfolgung – Begin (CIs)** “ startet den Auditing-Prozess für einen Security Operations Integrations-Workflow, der für Konfigurationselemente (CIs) ausgeführt wird.

Die Aktivität „ **Ausführungsnachverfolgung – Begin (CIs)** “ kann mit jedem CI-Workflow verwendet werden, um mit der Aufzeichnung des Fortschritts des Workflows in einem Audit zu beginnen.

### Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ein Audit-Datensatz wird erstellt. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityId | Systembezeichner der ausgeführten Integrationsfähigkeit. |
| istImpl | Kennzeichnung, die angibt, ob ein Audit für einen Integration Capability-Workflow oder einen Integration Capability-Implementierungs-Workflow durchgeführt wird. Mögliche Werte sind:<br>• false – bezeichnet die Prüfung eines abstrakten Integration Capability-Workflows wie Sichtungssuche. (Standard)<br>• true – bezeichnet Auditing für einen Integration Capability-Implementierungs-Workflow. Zum Beispiel Splunk oder Elasticsearch. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| ciListe | Ein oder mehrere Configuration Items (CIs), für die die gewünschte Aktion ausgeführt werden soll, im folgenden Format:<br>`["sysId", "sysId"]`<br>oder<br>`"sysId"`<br>Wird als Workflow-Eingabe verwendet. |
| workflowContextId | Systembezeichner des zugeordneten Workflow-Kontextdatensatzes. Vom System bereitgestellt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| parentCapabilityExcutionId | Systembezeichner des Audit-Datensatzes, der den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows von Integration Capability wie Splunk, Elasticsearch erforderlich. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner des Audit-Datensatzes. |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Workflow „Security Incident Response – Netzwerkstatistiken abrufen“.

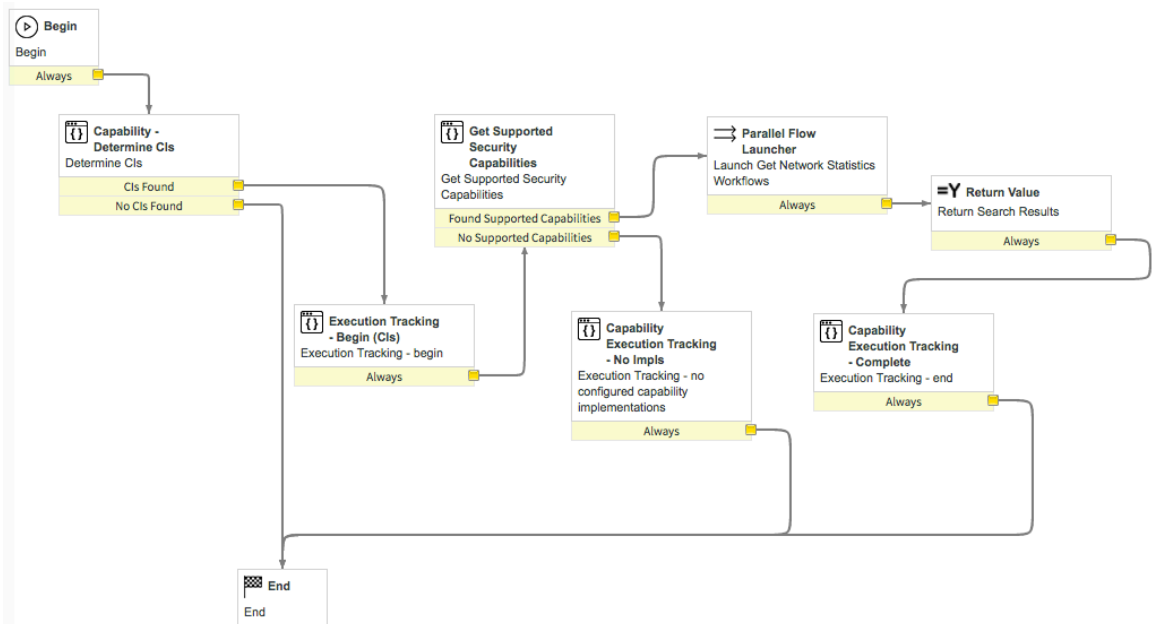
Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** Der Workflow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident im Status **„Analyse“**hinzugefügt wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Workflow automatisch ausgeführt, wenn sich der Status in **Analyse**ändert.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status „ **Analyse** “ befinden und ein neues Konfigurationselement hinzufügen.

**Netzwerkstatistiken abrufen**




Workflow-Prozessaktivitäten umfassen:

Aktivität „FQDN für Konfigurationselement abrufen“.

Bestimmen Sie das Shell-Skript nach Betriebssystem

If-Anweisung wird von PowerShell ausgeführt



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführungsnachverfolgung: Beginn der Aktivität

Ruft Netzwerkstatistiken über die Aktivität „netstat“ ab

Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.

Aktivität „Ergänzungsdatensätze erstellen“.

Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“. Gibt die Ergänzungs-ID zurück.

Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

### Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie den **Status** auf **Analyse**, falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Netzwerkstatistikinformationen im bereit **Zugehörige Links** > **Security Incident-Ergänzungen** Registerkarte. Weitere Informationen finden Sie unter Security Operations -Ergänzungsdatenzuordnung.

Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

#### Aktivität „FQDN für Konfigurationselement abrufen“.

Die zugehörigen Listen namens **Security Common Orchestration** > **Ruft den FQDN des Konfigurationselements ab** Die Workflow-Aktivität ruft den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „FQDN für Konfigurationselement abrufen“ kann mit jedem Workflow verwendet werden, um den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| cmdb_ci.id [Zeichenfolge] | Der Systembezeichner (sys_id) eines Configuration Item-Datensatzes. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| fqdn [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) des Konfigurationselements. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Zusätzliche Hinweise

Das Feld „fqdn“ im Konfigurationselement muss ausgefüllt werden.

### Ruft Netzwerkstatistiken über die Aktivität „netstat“ ab

Die Workflow-Aktivität „Security Common Orchestration – Netzwerkstatistiken über Netstat abrufen“ ruft die Netzwerkstatistiken für eine betroffene Ressource auf einem Windows-basierten System ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Netzwerkstatistiken über netstat abrufen“ kann mit jedem Workflow zum Abrufen von Netzwerkstatistiken von einem Windows-basierten System verwendet werden. Der Computer wird mit dem Befehl **netstat** einschließlich der Parameter **-a** und **-o** abgefragt. Um die Ausgabedaten zu verbessern, wird auch der Befehl **get-process** aufgerufen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Netzwerkstatistiken wurden im JSON-Format abgerufen. |
| Fehler | Beim Versuch, Netzwerkstatistiken abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Ziel [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) oder IP-Adresse des Zielsystems. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Antwort [Zeichenfolge] | Eine JSON-Zeichenfolge, die die aktuell ausgeführten Prozesse auf dem Zielcomputer darstellt.<br><br>JSON-Daten umfassen:<br>**pid**<br>Prozessbezeichner<br>**lokaler _port**<br>Lokaler Port für die Netzwerktransaktion<br>**Status**<br>Status der TCP-Verbindung |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| | **Hinweis:** Dieses Feld ist für UDP-Verbindungen null.<br>**local_address**<br>Lokaler vollständig qualifizierter Domänenname (FQDN) oder IP-Adresse<br>**remote_address**<br>Vollständig qualifizierter Remote-Domänenname (FQDN) oder IP-Adresse<br>**protocol**<br>TCP oder UDP<br>**remote_port**<br>Remote-Port der Netzwerktransaktion<br>**path**<br>Der Dateipfad der ausführbaren Prozessdatei<br>**hash**<br>Der Hashwert der ausführbaren Prozessdatei. Der Hash liegt in SHA-256 für PowerShell V4 oder höher vor. Andernfalls befindet sich der Hash in MD5. |

## Beschränkungen

Der MID Server muss PowerShellunterstützen.

SHA-256-Hash erfordert PowerShell V4.

### Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – Fehler“ zeichnet einen Fehler im Audit-Datensatz auf.

Die Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“ kann mit jedem Workflow verwendet werden, um eine Fehlerbedingung aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Audit-Datensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Dies ist die Ausgabe einer der Auditing-Aktivitäten beginnen. |
| errorMessage | Nachricht, die den Grund für den Fehler angibt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Integration mit Security Operations – Fähigkeit „Laufende Prozesse abrufen“.

Mit der Fähigkeit „Laufende Prozesse abrufen“ wird eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host oder Endpunkt abgerufen. Diese Funktion wird bei Untersuchungen für die Ergänzung von Incidents verwendet.

Die Fähigkeit „Laufende Prozesse abrufen“ verfügt über drei Implementierungs-Workflows von .

- Security Operations Carbon Black Integration - Laufende Prozesse abrufen Workflow
- Workflow „Security Operations System Command Integration – Laufende Prozesse abrufen“.
- Sicherheitsvorgänge Tanium-Integration – Laufende Prozesse abrufen Workflow

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Workflow „Security Operations – Laufende Prozesse abrufen“.

Der Workflow „Security Operations – Laufende Prozesse abrufen“ ist ein allgemeiner Workflow, der unabhängig von Integrationen ist. Sie ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (CI) von einem Host ab. Verwenden Sie es, um eine Integration (z. B. Carbon Black) oder einen Windows-basierten Security Incident zu erfüllen.

#### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

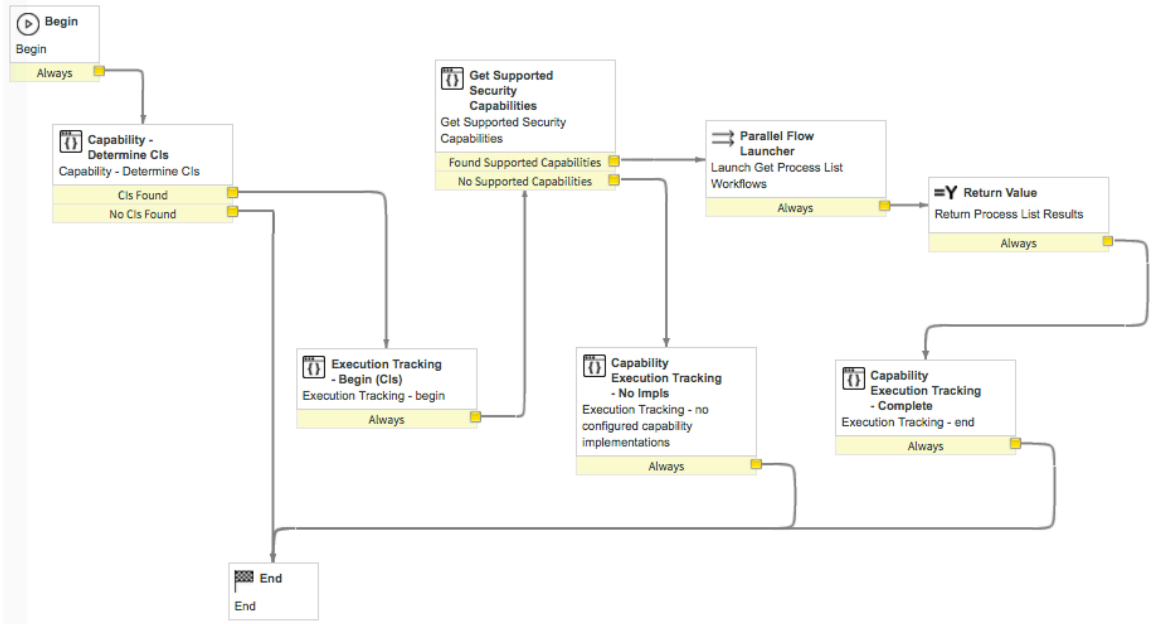
#### Warum und wann dieser Vorgang ausgeführt wird
Workflow-Prozessaktivitäten umfassen:

- Fähigkeit: Bestimmt die CIs-Aktivität
- Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.
- Aktivität „Unterstützte Sicherheitsfunktionen abrufen“
- Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität
- Startprogramm fürparallelen Flow – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Laufende Prozesse abrufen




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Fähigkeit: Bestimmt die CIs-Aktivität

Die Workflow-Aktivität „Fähigkeit – CIs bestimmen“ bestimmt, welche Konfigurationselemente (Configuration Items, CIs) in den Workflow aufgenommen werden sollen.

Die Aktivität „Fähigkeit – CIs bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche CIs in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfigurationselemente gefunden. |
| Fehler | Keine CIs gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |
| cis_affected | Konfigurationselemente. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| cis_affected | Gefilterte CIs |
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Security Operations Carbon Black Integration - Laufende Prozesse abrufen Workflow

„Security Operations Carbon Black Integration - Get Running Processes“ ist die Implementierung für die Carbon Black-Integration, die durch den Workflow „Security Operations Integration - Get Running Process“ gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:

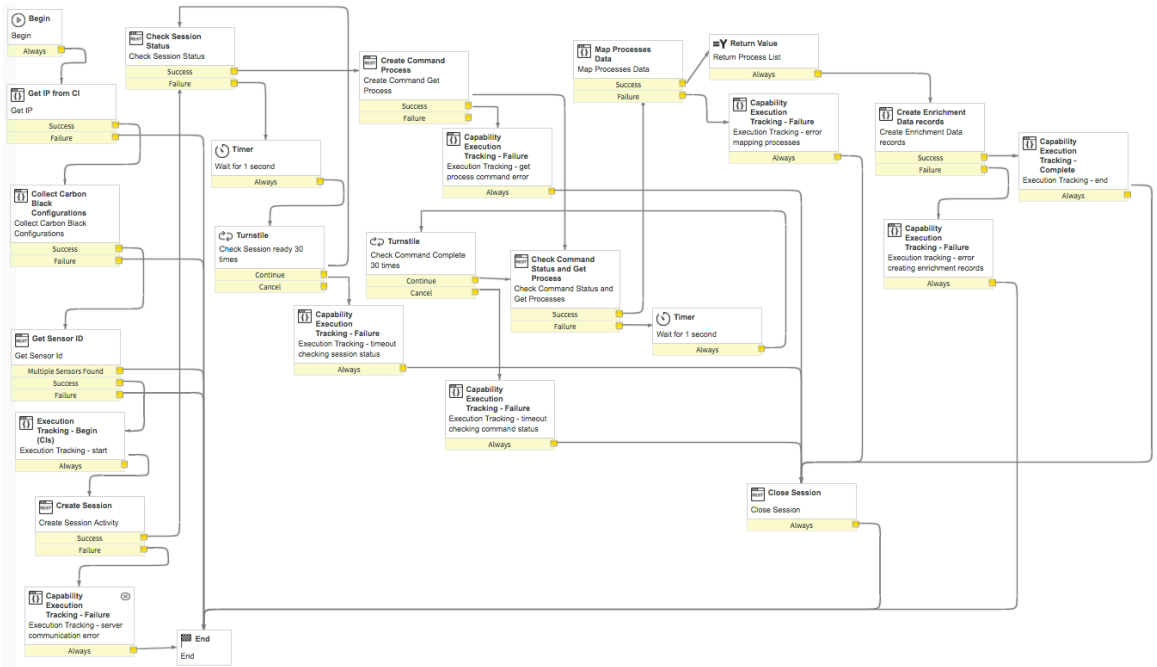
- IP aus CI-Aktivität abrufen
- Aktivität „Carbon Black-Konfigurationen erfassen“
- Aktivität „Sensor-ID abrufen“.
- Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.
- Sitzung erstellen
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivität „Sitzungsstatus überprüfen“.
- Timer-Workflow-Aktivität – Wartet 1 Sekunde
- Workflow-Aktivität für Drehkreuz – 30-mal „Sitzung bereit“ überprüfen
- Aktivität „Befehlsprozess erstellen“
- Überprüfen Sie die Aktivität „Befehlsstatus“ und „Prozess abrufen“.
- Aktivität „Daten zuordnen“. und Prozessliste zurückgeben
- Aktivität „Ergänzungsdatensätze erstellen“.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen
- Aktivität „Sitzung schließen“.

**Carbon Black ruft laufende Prozesse ab**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### IP aus CI-Aktivität abrufen

Die Workflow-Aktivität „IP aus CI abrufen“ erfasst die IP-Adresse aus Konfigurationselementen (CIs), die im Workflow verwendet werden sollen.

Die Aktivität „IP aus CI abrufen“ kann mit jedem Workflow verwendet werden, um Konfigurationselement-IP-Adressen (CIs) zu erfassen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | IP-Adressen gefunden. |
| Fehler | Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| ci_sys_id | Bezeichner des Konfigurationselements. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ip_addr | IP-Adressen |

## Aktivität „Carbon Black-Konfigurationen erfassen“

Die Workflow-Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Konfigurationsinformationen, die im Workflow verwendet werden sollen.

Die Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Carbon Black-Konfigurationsinformationen, die im Workflow verwendet werden sollen.

### Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Für diese Aktivität sind keine Eingabevariablen vorhanden.

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| api_token | API-Schlüssel für Drittpartei-Integrationen. |

### Überprüfen Sie den MID-Server-Status

Bestimmt, ob der im Feld MID Server- **Host der Integrationskonfiguration identifizierte MID Server aktiv** ist. Wenn das Feld auf **Beliebig**festgelegt ist, überprüft die Aktivität, ob ein MID Server ausgeführt wird.

Die Aktivität „MID Server-Status überprüfen“ kann mit jedem Workflow verwendet werden, um zu überprüfen, ob ein MID Server innerhalb des Workflows ausgeführt wird.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sitzungsstatus zurückgegeben. |
| Fehler | Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | ID der ausgeführten Fähigkeit. |
| workflowName | Der Name des ausgeführten Workflows. |
| mid_server_host | Der in der Konfiguration der Integration identifizierte MID Server, i |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| mid_server_live | Gibt an, ob der im Feld **MID Server-Host** der Integrationskonfiguration angegebene MID Server ausgeführt wird. Wenn das Feld auf **Beliebig**festgelegt ist, überprüft die Aktivität, ob ein MID Server ausgeführt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „Sensor-ID abrufen“.

Die Workflow-Aktivität „Sensor-ID abrufen“ erfasst Sensorbezeichner, die im Workflow verwendet werden sollen.

Die Aktivität „Sensor-ID abrufen“ kann mit jedem Workflow verwendet werden, um Sensorinformationen zur Verwendung im Workflow zu sammeln.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sensorbezeichner gefunden. |
| Fehler | Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| ci_ip_address | IP-Adresse des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Array-Elementtyp | API-Variablen |
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

### Ausführungsnachverfolgung: Beginn der Aktivität

Die Workflow-Aktivität „Execution Tracking – Begin“ (Ausführungsnachverfolgung – Begin) startet den Auditing-Prozess für einen Security Operations -Integrations-Workflow, der für erkennbare Elemente ausgeführt wird.

Die Aktivität „Ausführungsnachverfolgung – Begin“ kann mit jedem Workflow verwendet werden, um mit der Aufzeichnung des Fortschritts des Workflows in einem Audit zu beginnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ein Audit-Datensatz wird erstellt. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityId | Systembezeichner der ausgeführten Integrationsfähigkeit. |
| istImpl | Kennzeichnung, die angibt, ob ein Audit für einen Integration Capability-Workflow oder einen Integration Capability-Implementierungs-Workflow durchgeführt wird. Mögliche Werte sind:<br>• false – bezeichnet die Prüfung eines abstrakten Integration Capability-Workflows wie Sichtungssuche. (Standard)<br>• true – bezeichnet Auditing für einen Integration Capability-Implementierungs-Workflow. Zum Beispiel Splunk oder Elasticsearch. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| erkennbares Element Liste | Eine oder mehrere erkennbare SysIDs zum Ausführen der gewünschten Aktion.<br>Wird als Workflow-Eingabe verwendet. |
| workflowContextId | Systembezeichner des zugeordneten Workflow-Kontextdatensatzes. Vom System bereitgestellt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| parentCapabilityExcutionId | Systembezeichner des Audit-Datensatzes, der den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows von Integration Capability wie Splunk, Elasticsearch und VirusTotal erforderlich. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner des Audit-Datensatzes. |

### Aktivität „Sitzung erstellen“.

Die Workflow-Aktivität Sitzung erstellen richtet eine Carbon Black-Sitzung ein, die im Workflow verwendet werden soll.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität Sitzung erstellen kann mit jedem Workflow verwendet werden, um eine Carbon Black-Sitzung innerhalb des Workflows zu erstellen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sitzung erstellt. |
| Fehler | Sitzung nicht erstellt. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| sensor_id | Sensorbezeichner. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Ausgabe | API-Variablen |

### Aktivität „Sitzungsstatus überprüfen“.

Bestimmt den Status einer Carbon Black-Sitzung innerhalb des Workflows.

Die Aktivität „Sitzungsstatus überprüfen“ kann mit jedem Workflow verwendet werden, um den Carbon Black-Sitzungsstatus innerhalb des Workflows zu überprüfen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sitzungsstatus zurückgegeben. |
| Fehler | Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| session_id | Sitzungsbezeichner. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Ausgabe | Informationen zu laufenden Carbon Black-Prozessen. |

#### Aktivität „Befehlsprozess erstellen“

Die Workflow-Aktivität Befehlsprozess erstellen erstellt einen Carbon Black-Befehlsprozess, der im Workflow verwendet werden soll.

Die Aktivität Befehlsprozess erstellen kann mit jedem Workflow verwendet werden, um einen Carbon Black-Befehlsprozess innerhalb des Workflows zu erstellen.

### Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Befehlsprozess erstellt. |
| Fehler | Befehlsprozess nicht erstellt. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| session_id | Sitzungsbezeichner. |
| command_id | Befehlsbezeichner. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Ausgabe | API-Variablen |

### Überprüfen Sie die Aktivität „Befehlsstatus“ und „Prozess abrufen“.

Überprüft den Carbon Black-Befehlsstatus und ruft Prozesse ab, die im Workflow verwendet werden sollen.

Die Aktivität „Befehlsstatus überprüfen und Prozess abrufen“ kann mit jedem Workflow verwendet werden, um den Status eines Carbon Black-Befehls zu überprüfen und Prozesse innerhalb des Workflows abzurufen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Befehlsstatus zurückgegeben und Prozesse erstellt. |
| Fehler | Befehlsstatus oder Prozessfehler. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| session_id | Sitzungsbezeichner. |
| command_id | Befehlsbezeichner. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Ausgabe | API-Variablen |

### Aktivität „Daten zuordnen“.

Die Workflow-Aktivität „Prozessdaten zuordnen“ ordnet Carbon Black-Prozessdaten innerhalb des Workflows zu.

Die Aktivität „Prozessdaten zuordnen“ kann mit jedem Workflow zum Zuordnen von Carbon Black-Prozessen verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Prozesse zugeordnet |
| Fehler | Prozesse nicht zugeordnet. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| impacted_ci | Betroffenes Konfigurationselement. |
| „implementierung_id“. | Implementierungsbezeichner. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Formatierte Rückgabedaten zu laufenden Prozessen, die vom abstrakten Workflow verwendet werden. |
| Prozesse | Liste der Prozesse in einem Array. |

### Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – abgeschlossen“ aktualisiert den Audit-Datensatz, wenn der Workflow abgeschlossen ist.

Die Aktivität „Nachverfolgung der Fähigkeitsausführung – abgeschlossen“ kann mit jedem Workflow verwendet werden, um den Abschluss des Workflows aufzuzeichnen.

**Hinweis:**
Das **Rückgabewert** -Array aus der Kernaktivität des **parallelen Startprogramms** enthält ein Array von Ergebnissen aus allen ausgeführten Integrations-Workflows und meldet den erfolgreichen Abschluss der Ausführungsnachverfolgung.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Audit-Datensatzes wird auf **Abgeschlossen**aktualisiert. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Auditing-Aktivitäten beginnen. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| Nachricht | Abschlussnachricht. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Aktivität „Sitzung schließen“.

Schließt eine Carbon Black-Sitzung innerhalb des Workflows.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität „Sitzung schließen“ kann mit jedem Workflow zum Schließen einer Carbon Black-Sitzung verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sitzung geschlossen. |
| Fehler | Sitzung nicht geschlossen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| session_id | Sitzungsbezeichner. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Ausgabe | API-Variablen |

### Sicherheitsvorgänge Tanium-Integration – Laufende Prozesse abrufen Workflow

**„Security Operations Tanium Integration - Get Running Processes“** ist die Implementierung für die Tanium-Integration, die durch den Workflow „ **Security Operations Integration - Get Running Process** “ gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

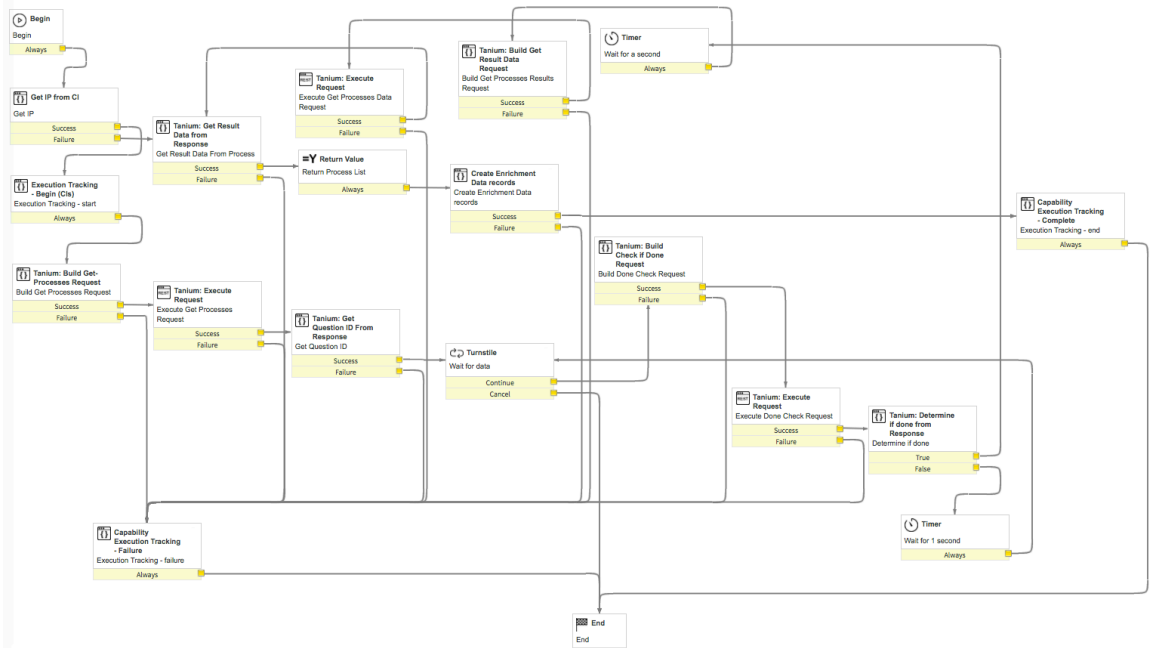
**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP aus CI-Aktivität abrufen
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Tanium: Anforderungsaktivität ausführen
- Tanium: Frage-ID aus Antwortaktivität abrufen
- Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.
- Workflow-Aktivität für Drehkreuz – Auf Daten warten
- Tanium: Aktivität „Überprüfen, ob fertig“ erstellt
- Tanium: Bestimmen Sie, ob dies über die Antwortaktivität erfolgt
- Tanium: Aktivität „Ergebnisdatenanforderung abrufen“ erstellen
- Tanium: Ergebnisdaten aus Antwortaktivität abrufen - Prozessliste zurückgeben
- Aktivität „Ergänzungsdatensätze erstellen“.
- Timer-Workflow-Aktivität – Wartet 1 Sekunde
- Aktivität „Ergänzungsdatensätze erstellen“.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

**Laufende Prozesse abrufen**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### IP aus CI-Aktivität abrufen

Die Workflow-Aktivität „IP aus CI abrufen“ erfasst die IP-Adresse aus Konfigurationselementen (CIs), die im Workflow verwendet werden sollen.

Die Aktivität „IP aus CI abrufen“ kann mit jedem Workflow verwendet werden, um Konfigurationselement-IP-Adressen (CIs) zu erfassen, die im Workflow verwendet werden sollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | IP-Adressen gefunden. |
| Fehler | Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| ci_sys_id | Bezeichner des Konfigurationselements. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| ip_addr | IP-Adressen |

### Tanium: Aktivität „Anforderung für Get-Prozesse erstellen“

Die Workflow-Aktivität Tanium: Get Result Data from Response (Tanium: Ergebnisdaten aus Antwort abrufen) erstellt eine Anforderung für Prozesse, die im Workflow verwendet werden sollen.

Die Aktivität „Tanium: Build Get Processes Request“ kann mit jedem Workflow verwendet werden, um eine Prozessanforderung zu erstellen, die im Workflow verwendet werden soll.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Prozessanforderung erstellt. |
| Fehler | Prozessanforderung fehlgeschlagen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| ci_ip_address | IP-Adresse des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint | Gibt den zu verwendenden verschlüsselten SOAP-Endpunkt an. |
| request_body | Verschlüsselte SOAP-Anforderungsinhalte. |
| http_timeout | Ganzzahl in Sekunden. |
| use_mid | Legt fest, ob der MID-Server verwendet werden soll. |

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Frage-ID aus Antwortaktivität abrufen

Diese Workflow-Aktivität verarbeitet den Antworttext, um die Frage-ID zu erhalten.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der SOAP-Antworttext. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Tanium-Server zurückgegebene Frage-ID. |

### Tanium: Aktivität „Überprüfen, ob fertig“ erstellt

Diese Workflow-Aktivität erstellt eine Anforderung des Tanium -Servers, um zu überprüfen, ob die Datenerfassung für die Frage abgeschlossen ist. Sie gibt die verschlüsselte Anforderung und andere Komponenten zurück, die zum Ausführen der Anforderung erforderlich sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| question_id [Ganzzahl] | Die vom Server Tanium zurückgegebene Frage-ID. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Bestimmen Sie, ob dies über die Antwortaktivität erfolgt

Diese Workflow-Aktivität bestimmt basierend auf dem Antworttext, ob eine Anforderung abgeschlossen wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| response_body [Zeichenfolge] | Der von Tanium zurückgegebene SOAP-Anforderungstext. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| fertig [Boolean] | Gibt „true“ zurück, wenn die Anforderungsverarbeitung abgeschlossen ist. |

### Tanium: Aktivität „Ergebnisdatenanforderung abrufen“ erstellen

Dieser Workflow erstellt eine Anforderung zum Sammeln aller Daten, die von Tanium als Antwort auf eine Frage zurückgegeben werden. Er verwendet eine Frage-ID als Eingabe und stellt die Ausgabe zur Ausführung der Anforderung bereit, einschließlich einer verschlüsselten SOAP-Umschlagnutzlast.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| question_id [Zeichenfolge] | Frage-ID der an Tanium gestellten Frage |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. |
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |
| use_mid [Boolean] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Tanium: Anforderungsaktivität ausführen

Diese Workflow-Aktivität führt eine HTTP-Anforderung aus. Die Eingaben definieren den Endpunkt und den erwarteten Anforderungstext. Der Anforderungstext selbst ist der verschlüsselte SOAP-Umschlag.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| request_body [Verschlüsselt] | Der SOAP-Anforderungstext. Dieses Eingabefeld ist ein Pflichtfeld. |
| use_mid [Boolesch] | Eine boolesche Kennzeichnung, die angibt, ob der MID Server verwendet werden soll. |
| Endpunkt [Zeichenfolge] | Der verschlüsselte Endpunkt aus der Datenbank. Dieses Eingabefeld ist ein Pflichtfeld. |
| http_timeout [Ganzzahl] | Der HTTP-Zeitüberschreitungswert in Sekunden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code [Ganzzahl] | Standard-HTTP-Statuscodes. |
| Header [Zeichenfolge] | Die SOAP-Kopfzeile. |
| Textkörper [Zeichenfolge] | Der SOAP-Text. |
| Fehler [Zeichenfolge] | Alle vom Server bereitgestellten Fehler. |

### Tanium: Ergebnisdaten aus Antwortaktivität abrufen

Die Workflow-Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ verarbeitet den Antworttext aus den Ergebnisdaten und gibt ein Array von JSON-Objekten aus, die die Ergebnisse von Tanium darstellen.

Die Aktivität „Tanium: Ergebnisdaten aus Antwort abrufen“ kann mit jedem Workflow verwendet werden, um Ergebnisdaten abzurufen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergebnisdaten abgerufen. |
| Fehler | Keine Daten abgerufen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| response_body | Verschlüsselte SOAP-Antwortinhalte |
| „implementierung_id“. | Implementierungsbezeichner. |
| impacted_ci | Betroffenes Konfigurationselement. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| result_data | Array-Elementtyp von API-Variablen. Jedes Array enthält Schlüssel-Wert-Paare, die aus der Spalte und den vom Server zurückgegebenen Werten bestehen. Wenn keine Daten vom Server empfangen werden, ist die Ausgabe ein leeres Array. |
| Ausgabe | Formatierte Rückgabedaten zu laufenden Prozessen, die vom abstrakten Workflow verwendet werden. |

### Workflow „Security Operations System Command Integration – Laufende Prozesse abrufen“.

Der Workflow „Security Operations System Command Integration - Get Running Processes“ ruft die laufenden Prozesse eines Konfigurationselements ab, wenn ein Windows- oder Unix-basierter Security Incident im Status **„Analyse“**hinzugefügt oder aktualisiert wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Bei neuen Security Incidents wird der Workflow automatisch ausgeführt, wenn Sie den Incident mit einem ausgewählten Konfigurationselement übermitteln und sich der Status automatisch in **Analyse**ändert. Wenn er im Status **Entwurf** bleibt, wird er nicht ausgeführt.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich im Status „ **Analyse** “ befinden und ein neues Konfigurationselement hinzufügen.

Workflow-Prozessaktivitäten umfassen:

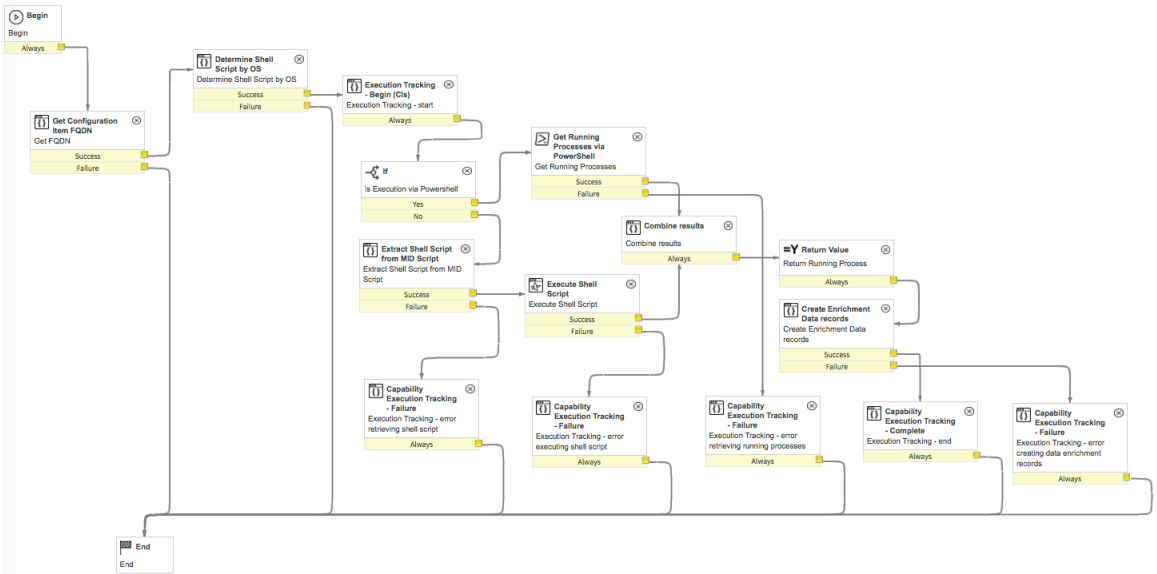
- Aktivität „FQDN für Konfigurationselement abrufen“.
- Bestimmen Sie das Shell-Skript nach Betriebssystemaktivität
- Ausführungsnachverfolgung: Beginn der Aktivität



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ruft laufende Prozesse über PowerShell ab
- Aktivität „Shell-Skript ausführen“.
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Aktivität „Shell-Skript aus MID-Skript extrahieren“
- Kombinieren Sie Ergebnisseund Rückgabewerte in einem Array
- Aktivität „Ergänzungsdatensätze erstellen“.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

**Laufende Prozesse abrufen**




## Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie den **Status** auf **Analyse**, falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration stellt Informationen zum laufenden Prozess in der bereit **Zugehöriger Link** > **Security Incident-Ergänzungen**Registerkarte. Weitere Informationen finden Sie unter Security Operations -Ergänzungsdatenzuordnung.

   Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „FQDN für Konfigurationselement abrufen“.

Die zugehörigen Listen namens **Security Common Orchestration** > **Ruft den FQDN des Konfigurationselements ab** Die Workflow-Aktivität ruft den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „FQDN für Konfigurationselement abrufen“ kann mit jedem Workflow verwendet werden, um den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| cmdb_ci.id [Zeichenfolge] | Der Systembezeichner (sys_id) eines Configuration Item-Datensatzes. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| fqdn [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) des Konfigurationselements. |

## Zusätzliche Hinweise

Das Feld „fqdn“ im Konfigurationselement muss ausgefüllt werden.

#### Bestimmen Sie das Shell-Skript nach Betriebssystemaktivität

Die Workflow-Aktivität „Shell-Skript nach Betriebssystem bestimmen“ bestimmt, welches Betriebssystem im Workflow verwendet werden soll

Die Aktivität „Shell-Skript nach Betriebssystem bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welches Shell-Skript basierend auf dem Betriebssystem ausgeführt werden soll, das auf dem System ausgeführt wird, das das Konfigurationselement enthält.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Betriebssystem gefunden. |
| Fehler | Kein Betriebssystem gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| ciSysId | Systembezeichner des Konfigurationselements. |
| processType | Interner Bezeichner, der definiert, welches Skript aus der Tabelle abgerufen werden soll. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| processScript | ECC-Agent, der den laufenden Prozess erfasst. |
| Ausführungsvorlage | Bestimmt, ob das Skript über eine Probe oder mit PowerShell ausgeführt wird. |
| anreicherungMappingId | Systembezeichner der Ergänzungszuordnung, die zum Transformieren der Antwortdaten verwendet wird. |

### Aktivität „Laufende Prozesse über PowerShell abrufen“.

Die Workflow-Aktivität „Sensor-ID abrufen“ erfasst laufende Prozesse mit PowerShell, um sie im Workflow zu verwenden.

Die Workflow-Aktivität „Laufende Prozesse über PowerShell abrufen“ kann mit jedem Workflow verwendet werden, um Prozesse abzurufen, die in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Prozesse gefunden |
| Fehler | Keine Prozesse gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Ziel | IP oder vollständig qualifizierter Domänenname (FQDN) des Ziel-CI |
| processingScript | ECC-Skript, das auf einem Windows-basierten System ausgeführt wird. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Rohausgabe. Die Ausführung verarbeitet Daten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „Shell-Skript aus MID-Skript extrahieren“

Die Workflow-Aktivität Shell-Skript aus MID-Skript extrahieren ruft ein MID-Server-Shell-Skript ab, das mit im Workflow verwendet werden soll.

Die Aktivität Shell-Skript aus MID-Skript extrahieren kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript zu extrahieren, das in den Workflow aufgenommen werden soll.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Shell-Skript gefunden |
| Fehler | Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| sysId | Systembezeichner |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| scriptValue | Skript als Zeichenfolgenwert, ausgeführt auf einem Unix-System. |

### Aktivität „Shell-Skript ausführen“.

Die Workflow-Aktivität „Shell-Skript ausführen“ führt ein MID Server-Shell-Skript innerhalb des Workflows aus.

Die Aktivität „Shell-Skript ausführen“ kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Shell-Skript gefunden |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ergebnisse (Fortsetzung)

| Ergebnis | Beschreibung |
|---|---|
| Fehler | Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Ziel | IP oder vollständig qualifizierter Domänenname (FQDN) des Ziel-CI |
| scriptValue | Skript als Zeichenfolgenwert, ausgeführt auf einem Unix-System. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Rohausgabe. Die Ausführung verarbeitet Daten. |

### Aktivität „Ergebnisse kombinieren“.

Die Workflow-Aktivität Ergebnisse kombinieren führt die Ergebnisse von Drittanbieterintegrationen zusammen, um sie im Workflow zu verwenden.

Die Aktivität Ergebnisse kombinieren kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergebnisse kombiniert. |
| Fehler | Kombination fehlgeschlagen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| inputA | Ergebnissatz A |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| inputB | Ergebnissatz B |
| „implementierung_id“. | Implementierungsbezeichner. |
| impacted_ci | Konfigurationselement |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis | Ergebnissatz A oder Ergebnissatz B, je nachdem, welcher ausgefüllt ist. |

### Security Operations Integration - Host-Fähigkeit isolieren

Die Fähigkeit „ **Host** isolieren“ schränkt Systemverbindungen zu anderen Geräten ein. „Host isolieren“ wird für ein Konfigurationselement (CI) ausgeführt.

Die Fähigkeit „ **Host** isolieren“ verfügt über einen Workflow Workflow „Security Operations – Host isolieren“., der ein oder mehrere CIs und optional eine Implementierung akzeptiert. Sie können eine Implementierung angeben, die zum Isolieren des Hosts verwendet werden soll, oder für den Workflow angeben, dass versucht werden soll, den Host mithilfe aller Implementierungen zu isolieren.

**Hinweis:**
Security Operations Carbon Black-Integration – Hostisolierung entfernen ist zwar nicht in eine Fähigkeit, einen Workflow integriert, aber für die Orchestration verfügbar, um die Kommunikation mit einem isolierten Host wiederherzustellen.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Führen Sie „Host isolieren“ aus

**„Host isolieren** “ schränkt Systemverbindungen zu anderen Geräten ein.

### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Der Workflow „ **Security Operations Integration - Host or Endpoint**isolieren“ kann über die zugehörige Liste für einen Security Incident ausgelöst werden.

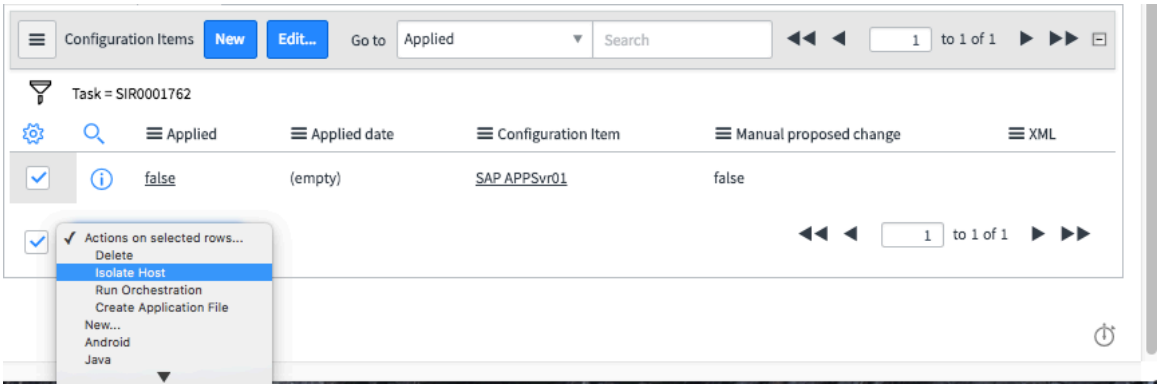
### Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie **Konfigurationselemente** auf der Registerkarte **Zugehörige Liste** aus.

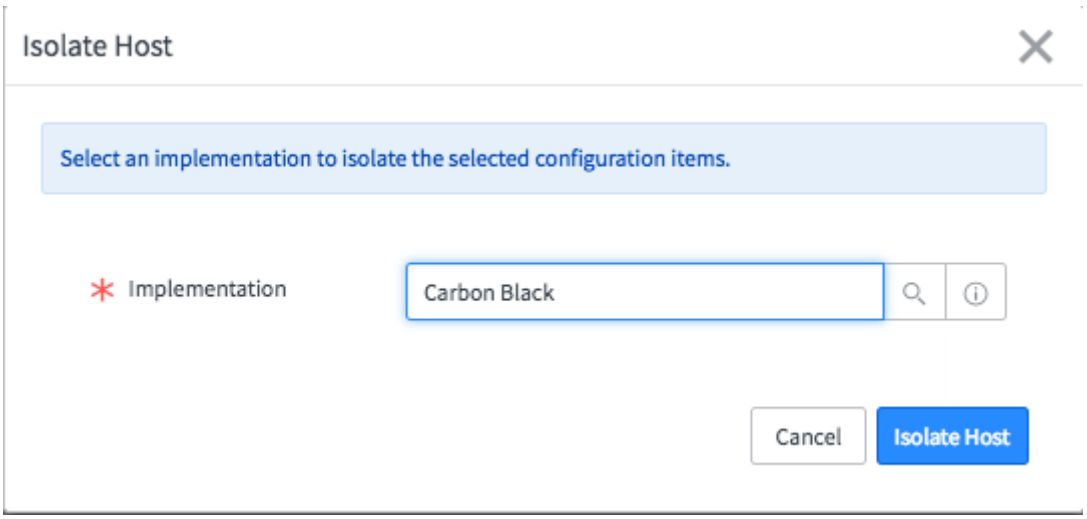


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen... aufHost** isolieren.




Das Dialogfeld wird angezeigt.




4. Wählen Sie die Implementierung aus.
5. Klicken Sie **auf Host isolieren**.
   Das Audit der Workflow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.

### Workflow „Security Operations – Host isolieren“.

Der Workflow **„Security Operations – Host** isolieren“ ist ein allgemeiner Workflow, der unabhängig von Integrationen ist. Sie verwendet die konfigurierten Abfragen, um nach einer Reihe von Konfigurationselementen zu suchen. Verwenden Sie es, um eine Integration zu erfüllen, z. B. Carbon Black.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

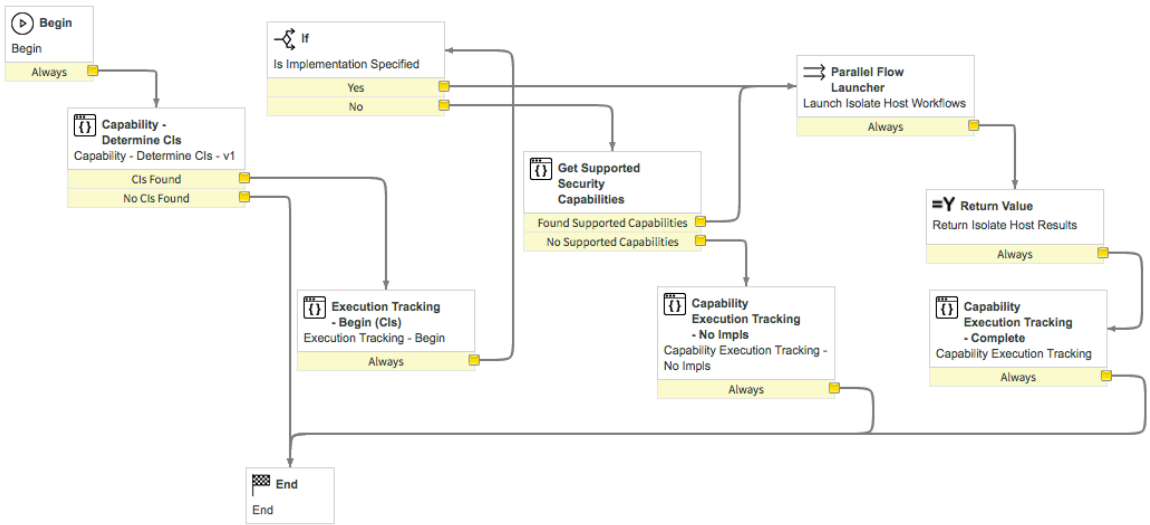
**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow wird über die Registerkarte **Konfigurationselemente** in einer zugehörigen Liste für Security Incidents ausgelöst.

Workflow-Prozessaktivitäten umfassen:

- Fähigkeit: Bestimmt die CIs-Aktivität
- Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.
- Aktivität „Unterstützte Sicherheitsfunktionen abrufen“
- Startprogrammfür parallele Flows : Starten Sie den entsprechenden Workflow. Speichern Sie die Ergebnisse in einem Array.
- Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.

**Host isolieren**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Fähigkeit: Bestimmt die CIs-Aktivität

Die Workflow-Aktivität „Fähigkeit – CIs bestimmen“ bestimmt, welche Konfigurationselemente (Configuration Items, CIs) in den Workflow aufgenommen werden sollen.

Die Aktivität „Fähigkeit – CIs bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche CIs in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfigurationselemente gefunden. |
| Fehler | Keine CIs gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |
| cis_affected | Konfigurationselemente. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| cis_affected | Gefilterte CIs |
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident CIs zu). |

## Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

### Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Operations Carbon Black Integration - Host-Workflow isolieren

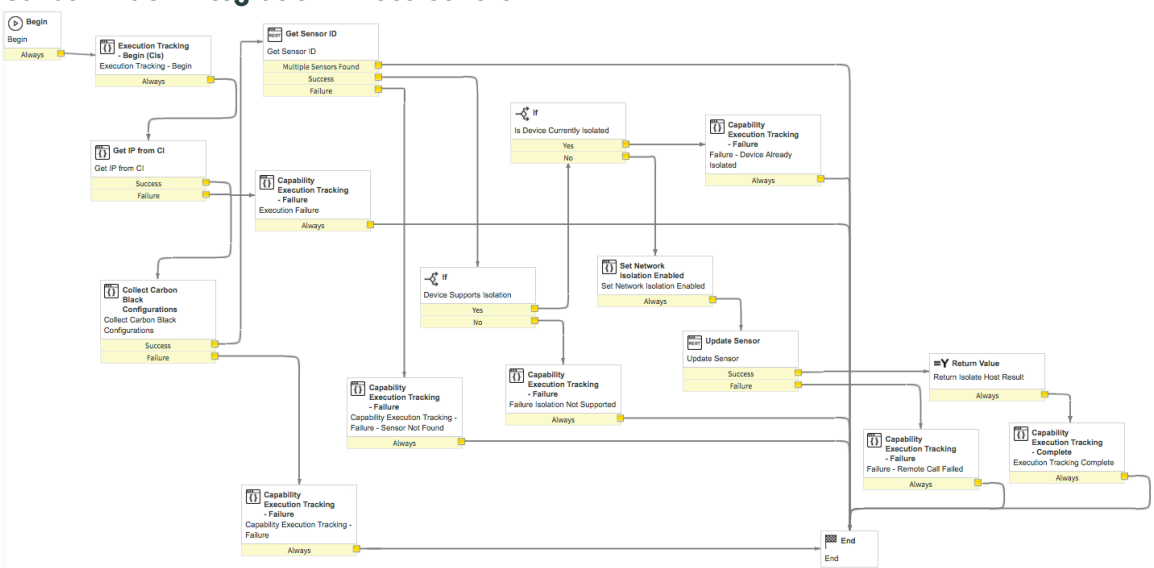
„Security Operations Carbon Black Integration - Isolate Host“ ist die Implementierung für die Carbon Black-Integration, die durch den Workflow „Security Operations Integration - Isolate Host“ gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:

- Aktivität „Ausführungsnachverfolgung – Beginn (CIs)“.
- IP von CI abrufen
- Erfasst Carbon Black-Konfigurationen
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Sensor-ID abrufen
- Festlegen der Netzwerkisolierung aktiviert
- Sensor aktualisieren: Gibt das Ergebnis „Host isolieren“ zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

**Carbon Black-Integration – Host isolieren**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### IP aus CI-Aktivität abrufen

Die Workflow-Aktivität „IP aus CI abrufen“ erfasst die IP-Adresse aus Konfigurationselementen (CIs), die im Workflow verwendet werden sollen.

Die Aktivität „IP aus CI abrufen“ kann mit jedem Workflow verwendet werden, um Konfigurationselement-IP-Adressen (CIs) zu erfassen, die im Workflow verwendet werden sollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | IP-Adressen gefunden. |
| Fehler | Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| ci_sys_id | Bezeichner des Konfigurationselements. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ip_addr | IP-Adressen |

### Aktivität „Carbon Black-Konfigurationen erfassen“

Die Workflow-Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Konfigurationsinformationen, die im Workflow verwendet werden sollen.

Die Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Carbon Black-Konfigurationsinformationen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Für diese Aktivität sind keine Eingabevariablen vorhanden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| api_token | API-Schlüssel für Drittpartei-Integrationen. |

### Aktivität „Sensor-ID abrufen“.

Die Workflow-Aktivität „Sensor-ID abrufen“ erfasst Sensorbezeichner, die im Workflow verwendet werden sollen.

Die Aktivität „Sensor-ID abrufen“ kann mit jedem Workflow verwendet werden, um Sensorinformationen zur Verwendung im Workflow zu sammeln.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sensorbezeichner gefunden. |
| Fehler | Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| ci_ip_address | IP-Adresse des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Array-Elementtyp | API-Variablen |
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

### Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest

Die Workflow-Aktivität „Netzwerkisolierung aktivieren“ aktiviert die Netzwerkisolierung.

Die Aktivität „Netzwerkisolierung aktivieren“ kann mit jedem Workflow verwendet werden, um die Netzwerkisolierung zu aktivieren.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Netzwerkisolierung aktiviert. |
| Fehler | Netzwerkisolierung kann nicht aktiviert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |
| Deaktivieren | Bestimmt, ob der Host isoliert ist, oder entfernt die Hostisolierung.<br>True = Isolierung deaktivieren<br>False = Isolierung bleibt aktiviert |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktualisieren Sie die Sensoraktivität

Die Workflow-Aktivität „Sensor aktualisieren“ aktualisiert den Sensor, um Hosts oder Endpunkte zu isolieren.

Die Aktivität „Sensor aktualisieren“ kann mit jedem Workflow verwendet werden, um Hosts oder Endpunkte zu isolieren.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Aktualisierter Sensor. |
| Fehler | Sensor kann nicht aktualisiert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| sensor_id | Sensorbezeichner. |
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |

### Security Operations Carbon Black-Integration – Hostisolierung entfernen

Der Workflow „ **Carbon Black Integration - Remove Host Isolation“ von Security Operations** gibt die Kommunikation mit einem angegebenen Host oder Endpunkt in einem Carbon Black-System frei.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

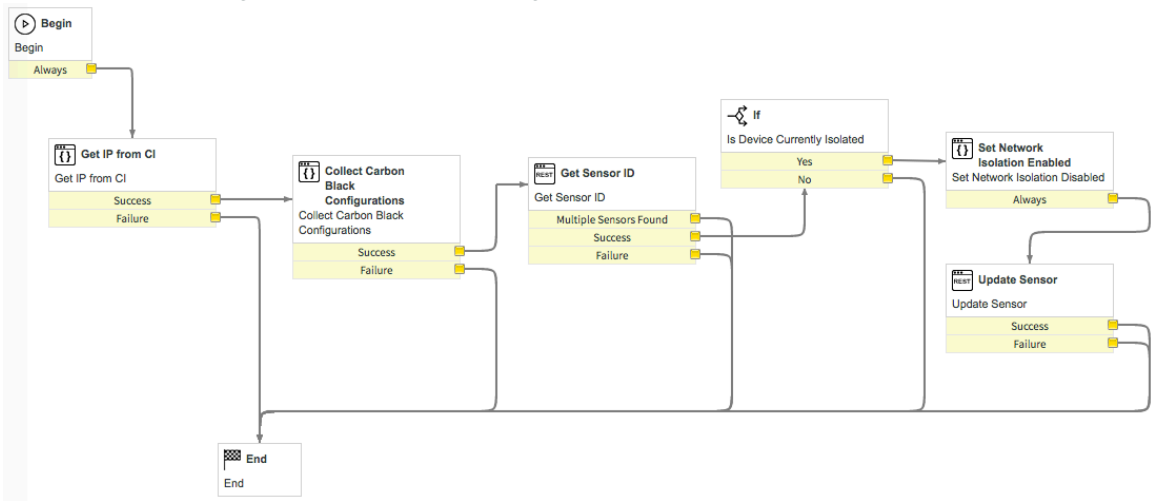
### Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow ist nicht Teil einer Fähigkeit und erfordert eine benutzerdefinierte Orchestrierung, um ausgeführt zu werden.

Workflow-Prozessaktivitäten umfassen:

- IP von CI abrufen
- Wenn erfolgreich: Carbon Black-Konfigurationen erfassen
- Sensor-ID abrufen
- Wenn das Gerät die Isolierung unterstützt und das Gerät nicht isoliert ist,legen Sie „Netzwerkisolierung aktiviert“ auf „deaktiviert“ fest.
- Sensor aktualisieren: Gibt das Ergebnis „Host isolieren“ zurück.

**Carbon Black-Integration – Hostisolierung entfernen**




### IP aus CI-Aktivität abrufen

Die Workflow-Aktivität „IP aus CI abrufen“ erfasst die IP-Adresse aus Konfigurationselementen (CIs), die im Workflow verwendet werden sollen.

Die Aktivität „IP aus CI abrufen“ kann mit jedem Workflow verwendet werden, um Konfigurationselement-IP-Adressen (CIs) zu erfassen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | IP-Adressen gefunden. |
| Fehler | Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| ci_sys_id | Bezeichner des Konfigurationselements. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ip_addr | IP-Adressen |

### Aktivität „Carbon Black-Konfigurationen erfassen“

Die Workflow-Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Konfigurationsinformationen, die im Workflow verwendet werden sollen.

Die Aktivität „Carbon Black-Konfigurationen erfassen“ erfasst Carbon Black-Konfigurationsinformationen, die im Workflow verwendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Für diese Aktivität sind keine Eingabevariablen vorhanden.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| api_token | API-Schlüssel für Drittpartei-Integrationen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „Sensor-ID abrufen“.

Die Workflow-Aktivität „Sensor-ID abrufen“ erfasst Sensorbezeichner, die im Workflow verwendet werden sollen.

Die Aktivität „Sensor-ID abrufen“ kann mit jedem Workflow verwendet werden, um Sensorinformationen zur Verwendung im Workflow zu sammeln.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Sensorbezeichner gefunden. |
| Fehler | Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| ci_ip_address | IP-Adresse des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |
| Array-Elementtyp | API-Variablen |
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

### Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest

Die Workflow-Aktivität „Netzwerkisolierung aktivieren“ aktiviert die Netzwerkisolierung.

Die Aktivität „Netzwerkisolierung aktivieren“ kann mit jedem Workflow verwendet werden, um die Netzwerkisolierung zu aktivieren.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Netzwerkisolierung aktiviert. |
| Fehler | Netzwerkisolierung kann nicht aktiviert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |
| Deaktivieren | Bestimmt, ob der Host isoliert ist, oder entfernt die Hostisolierung.<br>True = Isolierung deaktivieren<br>False = Isolierung bleibt aktiviert |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

### Aktualisieren Sie die Sensoraktivität

Die Workflow-Aktivität „Sensor aktualisieren“ aktualisiert den Sensor, um Hosts oder Endpunkte zu isolieren.

Die Aktivität „Sensor aktualisieren“ kann mit jedem Workflow verwendet werden, um Hosts oder Endpunkte zu isolieren.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Aktualisierter Sensor. |
| Fehler | Sensor kann nicht aktualisiert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| api_token | Carbon Black-API-Schlüssel. |
| use_mid_server | Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht. |
| endpoint_base | Basis-URL der Carbon Black-API. |
| sensor_id | Sensorbezeichner. |
| sensor_detail | Beschreibung des Carbon Black-Sensors im JSON-Format. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| status_code | Ermittelt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt. |

### Integration von Sicherheitsvorgängen – Fähigkeit „In Beobachtungsliste veröffentlichen“.

Die Fähigkeit „In Beobachtungsliste veröffentlichen“ fügt erkennbare Elemente und Indikatoren, die einem Security Incident zugeordnet sind, einer Drittanbieter-Beobachtungsliste hinzu, die Sicherheits-Ereignisse überwacht und Warnungen generiert. Diese Funktion wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Workflow „Security Operations Integration - Publish to Watchlist“ (In Beobachtungsliste veröffentlichen).

Der Workflow **„Security Operations Integrations - Publish to Watchlist** “ (In Beobachtungsliste veröffentlichen) ist ein allgemeiner Workflow, der unabhängig von Integrationen ist. Sie fügt Beobachtungslisten von Drittanbietern, die die Fähigkeit unterstützen, erkennbare Elemente hinzu. Verwenden Sie es, um eine Integration zu erfüllen.

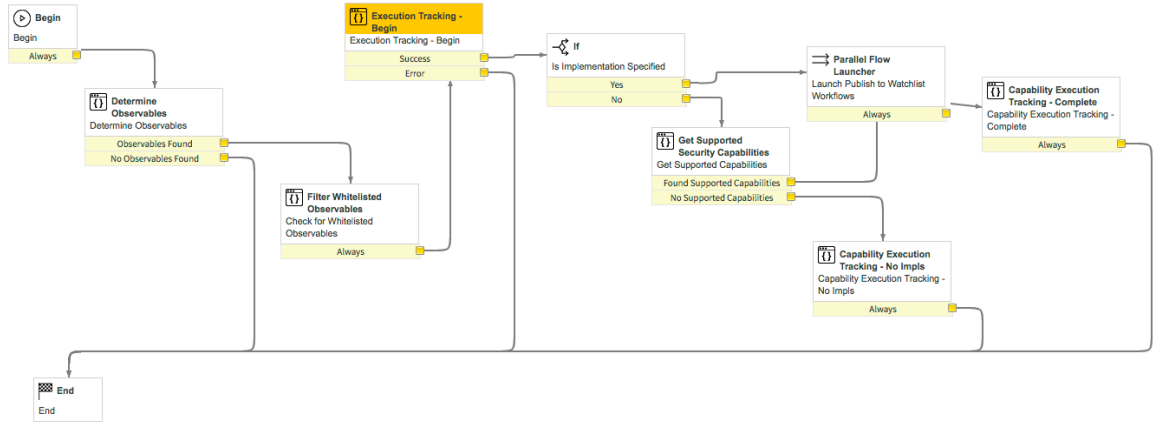
**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow ist sichtbar und wird nur ausgeführt, wenn eine Integration verfügbar ist. Sie wird über die Registerkarte „Erkennbare Elemente“ oder „ **ZugeordneteIndikatoren“** bei einem Security Incident ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### In Beobachtungsliste veröffentlichen




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Bestimmen Sie die Aktivität „Erkennbare Elemente“.

Die Workflow-Aktivität **„Erkennbare** Elemente bestimmen“ bestimmt, welches erkennbare Element in den Workflow aufgenommen werden soll

Die Aktivität „ **Erkennbare Elemente bestimmen** “ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente gefunden |
| Fehler | Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu). |
| Erkennbare Elemente | IP-Adressen, Hash, URLs, Domänennamen. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Gefilterte erkennbare Elemente |

### Aktivität „Erkennbare Elemente auf Allow-Liste filtern“.

Die Workflow-Aktivität Gefilterte erkennbare Elemente auf der Allow-Liste entfernt erkennbare Elemente, die ignoriert werden können, aus der Liste der erkennbaren Elemente. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Erkennbare Elemente auf Allow-Liste filtern“ kann mit jedem Workflow verwendet werden, um erkennbare Elemente zu filtern, bevor eine Aktion ausgeführt wird.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Filterliste erstellt. |
| Fehler | Beim Versuch, die erkennbaren Elemente zu filtern, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Liste der verfügbaren erkennbaren Elemente. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| gefilterteErkennbareElemente | Gefilterte erkennbare Elemente. |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Integration von Sicherheitsvorgängen – Sichtungssuchfunktion

Die Fähigkeit „ **Sichtungssuche** “ akzeptiert eine Reihe von erkennbaren Elementen, findet alle Integrationen, die eine Sichtungssuche unterstützen, und führt diese Suchen dann aus.

Die Fähigkeit „Sichtungssuche“ verfügt über den Workflow Security Operations Integration - Sichtungssuch-Workflow, der die Sichtungssuche ausführt. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchen basierend auf dem konfigurierten Workflow aus. Sobald die Suche abgeschlossen ist, wird den Arbeitsnotizen des Incident eine Notiz hinzugefügt, die angibt, ob und wie viele Sichtungen gefunden wurden.

Um Konfigurationen der Sichtungssuche anzuzeigen, navigieren Sie zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfigurationen**.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

### Erstellen Sie Konfigurationsdatensätze für die Sichtungssuche

Erstellen Sie mehrere Konfigurationsdatensätze für die Sichtungssuche, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter ändern.

#### Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss in der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für die Splunk-Integration unterstützt.

#### Warum und wann dieser Vorgang ausgeführt wird
Sie können auch Konfigurationsdatensätze für Sichtungssuchen erstellen, um gespeicherte Suchen im Protokollspeicher von Splunk Enterprise aufzurufen.

**Hinweis:**
Die Suchkonfigurationsabfragen stützen sich auf Splunk-Protokolldaten, um mit Splunk Common Information Model (CIM) konform zu sein.

Mit gespeicherten Suchkonfigurationen können Sie:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie benutzerdefinierte Suchen, die mehrere Event-Datensätze kombinieren.
- Designeffiziente und effektive Suchvorgänge.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das Basissystem enthält die in der folgenden Abbildung gezeigten Beispielkonfigurationen:

**Gespeicherte Suchkonfigurationen**

| Name | Observable type | Search | Is saved search |
|---|---|---|---|
| Search | Search | Search | Search |
| Default Proofpoint Inplace Search-Emails | Email | tag=email [\| search tag="email" AND (sub... | false |
| Default Saved Search - Emails | Email | args.email.subject=${email.subject}&args... | true |
| Default PAN Inplace Search - URLs | URL | tag=network url=${observable} \| table us... | false |

Die gespeicherten Such- und Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der gespeicherten Konfiguration übereinstimmen, die in Ihrer Splunk-Instanz definiert ist. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

**Hinweis:**
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Searches, Reports, and Alerts (Suchen, Berichte und Warnungen), und suchen Sie nach Ihrer gespeicherten Suchabfrage. Klicken Sie auf den Link **Berechtigungen**, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie das Optionsfeld **Alle Apps** aus, und aktivieren Sie die Option **Leseberechtigung** für **Jeder**. Dadurch wird der Wert der Spalte „Freigabe“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn diese Option nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**.
2. Ändern Sie den **App-Kontext** in **Alle**.

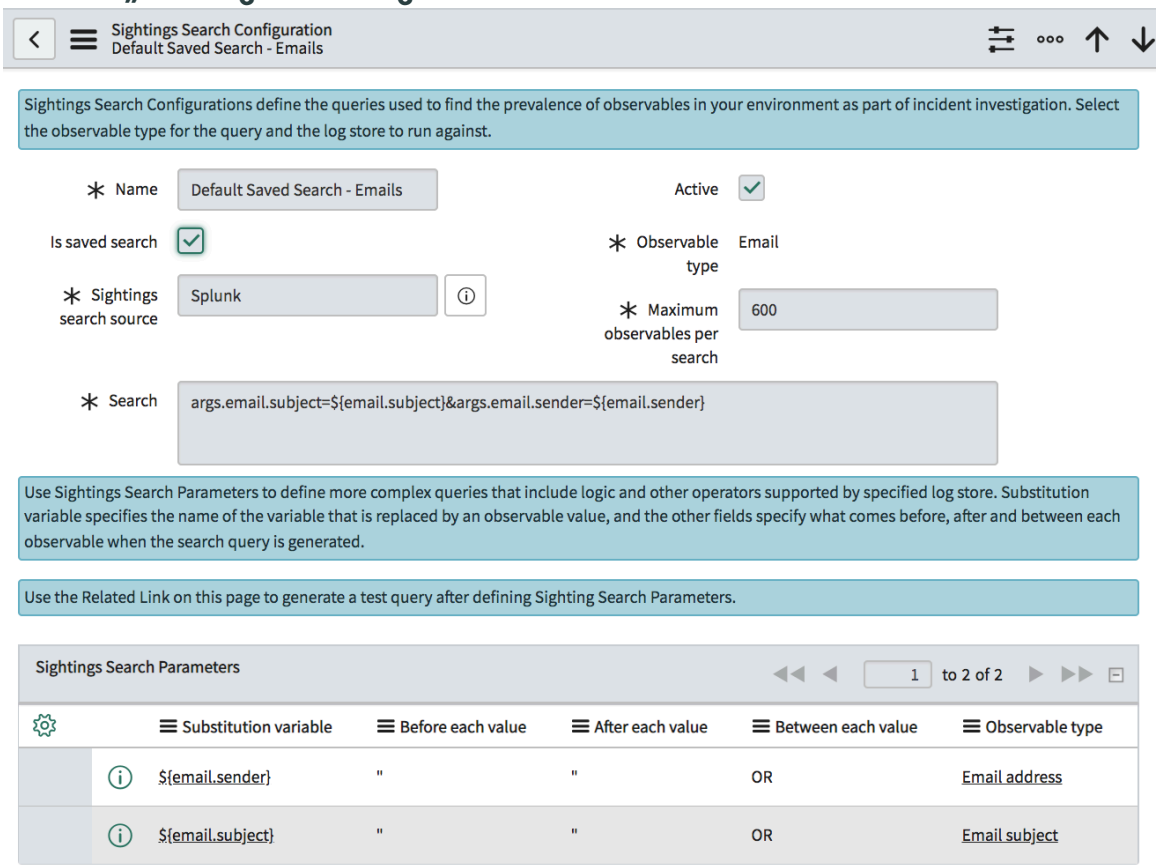
   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Beispielsweise enthält das Formular „Sichtungssuchkonfiguration“ die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „Sichtungssuchkonfiguration“**




Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit demselben Namen, Standardmäßige gespeicherte Suche – E-Mails, und denselben Suchparametern für die E-Mail-Adresse und den E-Mail-Betreff. Wenn der Name und die Suchparameter nicht identisch sind, generiert die Sichtungssuche kein genaues Ergebnis.

## Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

**Formular „Sichtungssuchkonfiguration“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Konfiguration |
| Ist gespeicherte Suche | Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt. |
| Sichtungssuchquelle | Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus. |
| Aktiv | Option für den gespeicherten Suchstatus. Für die Suche nach Sichtungen können nur aktive Suchkonfigurationen verwendet werden. |
| Erkennbarer Typ | Erkennbarer Typ kann ein beliebiger erkennbarer Typ sein, z. B. IP, Hash-Wert, URL, Domänenname usw. |
| Maximale erkennbare Elemente pro Suche | Maximale Anzahl der erkennbaren Elemente, die von der Suche zurückgegeben werden sollen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Suchen | Die Standardsuchzeichenfolge ist `$(observable)`, Sie können jedoch eine eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden. |

2. Klicken Sie auf **Absenden**.

### Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

### Nächste Maßnahme
Klicken Sie nach dem Definieren der Suchabfrage auf **Testabfrage für Sichtungssuche generieren**, und geben Sie eine Liste von Werten für erkennbare Elemente an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

## Führen Sie eine Sichtungssuche aus

Bestimmen Sie die Verbreitung einer Bedrohung im Laufe der Zeit, oder testen Sie Korrektur- oder Beseitigungsmaßnahmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Die Ergebnisse sind in der zugehörigen Liste **„Erkennbare Security Incident-Elemente“** enthalten.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird
Die Fähigkeit „Sichtungssuche“ verfügt über den Workflow Security Operations Integration - Sichtungssuch-Workflow, der die Sichtungssuche ausführt. Dieser Workflow akzeptiert eine Liste von erkennbaren Elementen, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchen basierend auf dem konfigurierten Workflow aus.

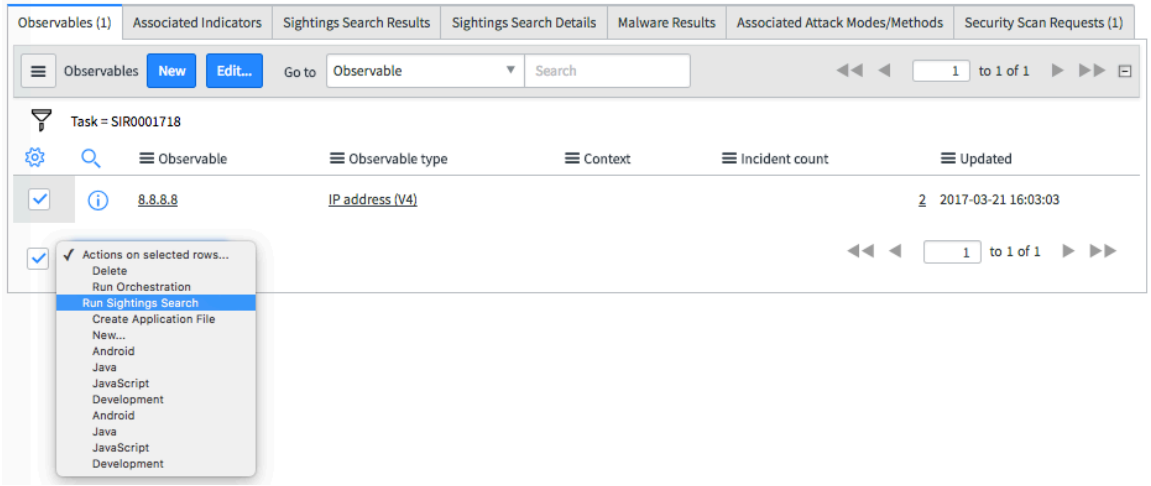
**Hinweis:**
Eine aktive Implementierung muss konfiguriert sein. Sichtungssuche unterstützt Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger und QRadar-Incident-Ergänzung. Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen wie **„Sichtungssuche**ausführen“ nicht in Produktmenüs angezeigt.

### Prozedur

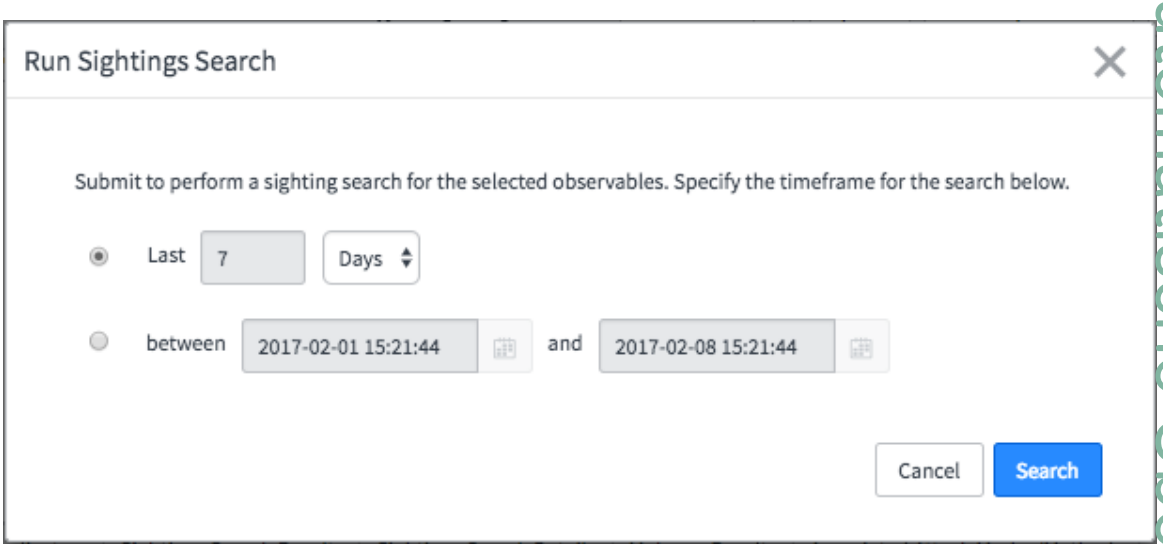
1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf den zugehörigen Link **IoC anzeigen**.
3. Wählen Sie auf der Registerkarte „Zugehörige Liste“ die Option Erkennbare **Elemente** aus.
4. Wählen Sie die erkennbaren Elemente aus, für die Sie eine Sichtungssuche durchführen möchten.
5. Klicken Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen... aufSichtungssuche** ausführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Das Dialogfeld „Sichtungssuche ausführen“ wird geöffnet.




**Hinweis:**
Die im Dialogfeld eingegebenen Werte überschreiben die Fähigkeitskonfigurationswerte für diese Ausführung.

6. Wählen Sie die Anzahl der Tage oder einen Datumsbereich für die Suche nach Daten aus.

| Option | Bezeichnung |
|---|---|
| **Letzte** | Die Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents.<br>Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage. |
| **zwischen** | Zu durchsuchender Datumsbereich. Standarddaten:<br>Datum und Uhrzeit, zu der der Incident geöffnet wurde.<br>Datum und Uhrzeit sieben Tage vor Eröffnung des Incidents. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
**Zuletzt** ist die Anzahl der Stunden oder Tage vor der Erstellung des zu durchsuchenden Incidents. Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage.

7. Klicken Sie auf **Suche**.
Ein Sichtungssuchdatensatz wird erstellt. Zusammengefasste und zugehörige Sichtungsdaten werden im Security Incident auf den Registerkarten **Sichtungssuchergebnisse** und **Sichtungssuchdetails** angezeigt.

**Hinweis:**
Sichtungssuchergebnisdaten können mit Trusted Security Circlegeteilt werden, mit Ausnahme von Rohdaten bei Implementierungen, die für die Einbeziehung von Rohdaten konfiguriert sind.

### Ergebnisse von Sightings Search

| Ergebnis | Beschreibung |
|---|---|
| Nummer | Bezeichner für die Sichtungssuche. |
| Anzahl der erkennbaren Elemente | Anzahl der per Abfrage gesuchten erkennbaren Elemente. |
| Interne Sichtungen | Anzahl der internen Sichtungen. |
| Externe Sichtungen | Anzahl der externen Sichtungen. (Erhalten aus Bedrohungsfreigabe.) |
| Übereinstimmende Konfigurationselemente | Anzahl der Konfigurationselemente, die mit einem vorhandenen Datensatz in Ihrer CMDB für jedes in Ihrer Umgebung gefundene erkennbare Element übereinstimmten. |
| Startdatumsbereich | Zeit, um mit der Suche nach Sichtungen zu beginnen. |
| Enddatumsbereich | Zeit, um die Suche nach Sichtungen zu beenden. |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung. |

Hinweis: Wenn die für die Sichtungssuche verwendete Implementierung so konfiguriert ist, dass sie Rohdaten enthält, und mindestens eine Sichtung gefunden wird, wird oben im Security Incident ein Anhang mit Rohdatenbeispielen angezeigt.

### Sichtungssuchdetails

| Detail | Beschreibung |
|---|---|
| Sichtungssuche | Bezeichner für die Sichtungssuche. |
| Erkennbares Element | Erkennbares Element, nach dem per Abfrage gesucht wird. |
| Erkennbarer Typ | Typ des erkennbaren Elements, nach dem per Abfrage gesucht wird. |
| Interne Sichtungen | Aggregierte Anzahl der internen Sichtungen. |
| Externe Sichtungen | Aggregierte Anzahl der externen Sichtungen. (Erhalten aus Bedrohungsfreigabe.) |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung. |

### Security Operations Integration - Sichtungssuch-Workflow

Der Workflow**„Security Operations Integration - Sichtungssuche** “ ist ein allgemeiner Workflow, der unabhängig von Integrationen ist. Sie verwendet die konfigurierten Abfragen, um basierend auf den konfigurierten Integrationen, die die Fähigkeit unterstützen, nach



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einer Reihe von erkennbaren Elementen zu suchen. Verwenden Sie es, um eine Integration wie Splunk oder Elasticsearch zu erfüllen.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

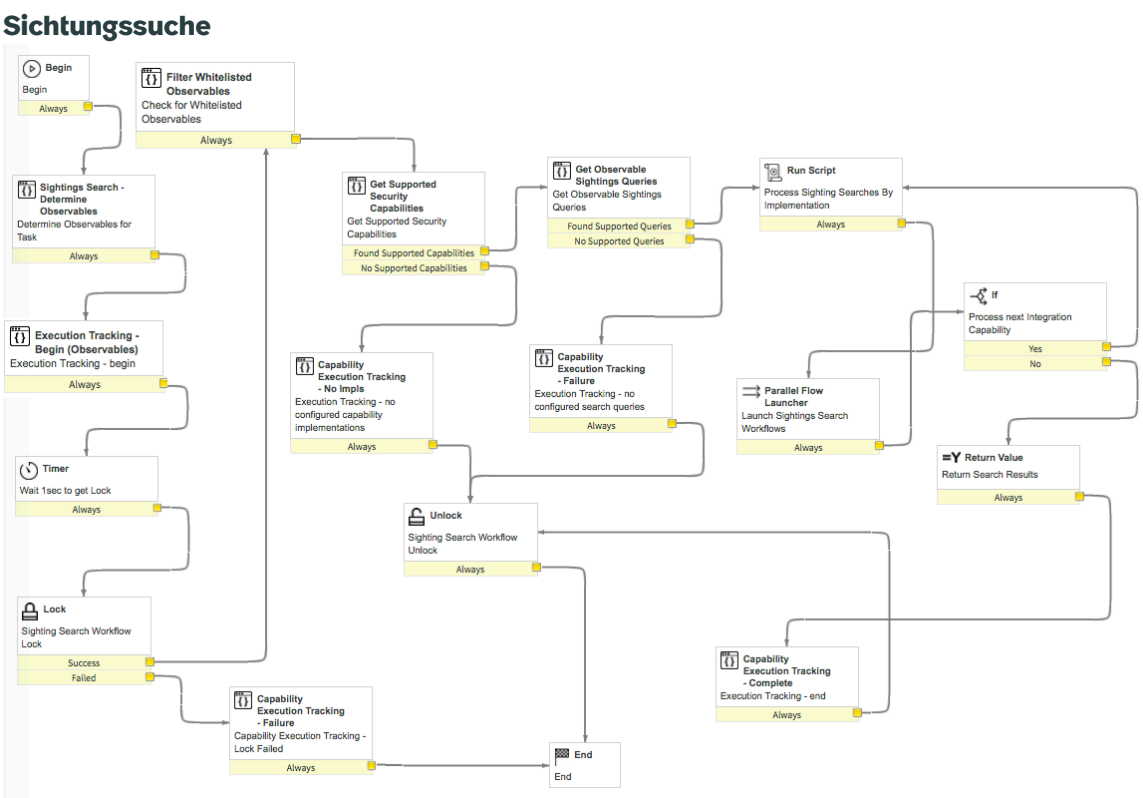
**Warum und wann dieser Vorgang ausgeführt wird**
Wenn einem Security Incident ein erkennbares Element zugeordnet ist, wird dieser Workflow ausgelöst, wenn Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen...** auf der Registerkarte Erkennbare Elemente des **Security Incident** auf **Sichtungssuche ausführen** klicken.

Workflow-Prozessaktivitäten umfassen:

- Bestimmen Sie die Aktivität „Erkennbare Elemente“.
- Ausführungsnachverfolgung: Beginn der Aktivität
- Timer-Workflow-Aktivität – Wartet eine Sekunde, um eine Sperre zu erhalten.
- Workflow-Aktivität sperren
- Filtern Sie aufgelistete erkennbare Elemente
- Aktivität „Unterstützte Sicherheitsfunktionen abrufen“
- Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität
- Entsperren Workflow Aktivität
- Aktivität „Abfragen erkennbarer Sichtungen abrufen“.
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Skript ausführen Workflow Aktivität
- Startprogramm für parallele Flows
- Wenn Workflow-Aktivität Wenn Workflow-Aktivität – Iterieren, bis alle entsprechenden Workflows ausgeführt wurden, und die Ergebnisse in einem Array speichern.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Sichtungssuche – Aktivität „Erkennbare Elemente bestimmen“.

Die Workflow-Aktivität **„Sichtungssuche – Erkennbare Elemente** bestimmen“ bestimmt, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

Die Aktivität „ **Sichtungssuche – Erkennbare Elemente bestimmen** “ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente gefunden |
| Fehler | Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| task_sys_id | Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu). |
| Erkennbare Elemente | IP-Adressen, Hash, URLs, Domänennamen. |
| workflow_current_sys_id | Systembezeichner des aktuellen Datensatzes. (Nur verwendet, wenn `task_sys_id`, Eingaben für erkennbare Elemente sind nicht verfügbar. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Gefilterte erkennbare Elemente |

### Aktivität „Erkennbare Elemente auf Allow-Liste filtern“.

Die Workflow-Aktivität Gefilterte erkennbare Elemente auf der Allow-Liste entfernt erkennbare Elemente, die ignoriert werden können, aus der Liste der erkennbaren Elemente. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Erkennbare Elemente auf Allow-Liste filtern“ kann mit jedem Workflow verwendet werden, um erkennbare Elemente zu filtern, bevor eine Aktion ausgeführt wird.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Filterliste erstellt. |
| Fehler | Beim Versuch, die erkennbaren Elemente zu filtern, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Liste der verfügbaren erkennbaren Elemente. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| gefilterteErkennbareElemente | Gefilterte erkennbare Elemente. |

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Aktivität „Abfragen erkennbarer Sichtungen abrufen“.

Die Workflow-Aktivität „Abfragen **erkennbarer Sichtungen** abrufen“ ruft Abfragen aus der Integrationskonfiguration ab.

Die Aktivität „ **Abfragen erkennbarer Sichtungen abrufen** “ kann mit jedem Workflow verwendet werden, um Abfragen abzurufen, die mithilfe des **Parallel Flow-Startprogramms**an die angegebene Implementierung gesendet werden sollen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Abfragen gefunden. |
| Fehler | Beim Versuch, Abfragen abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Liste der gefilterten erkennbaren Elemente. |
| capabilities | Liste der unterstützten Fähigkeiten. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| queries | Suchzeichenfolge. |
| queryCount | Anzahl der auszuführenden Abfragen. |

### Security Operations – Arcsight Logger Sichtungs-Workflow

Der Workflow**„Security Operations – ArcSight Logger – Sichtungssuche“** ist die Implementierung für die Splunk-Integration, die vom **Workflow „Security Operations Integration – Sightings Search**“ gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si_analyst

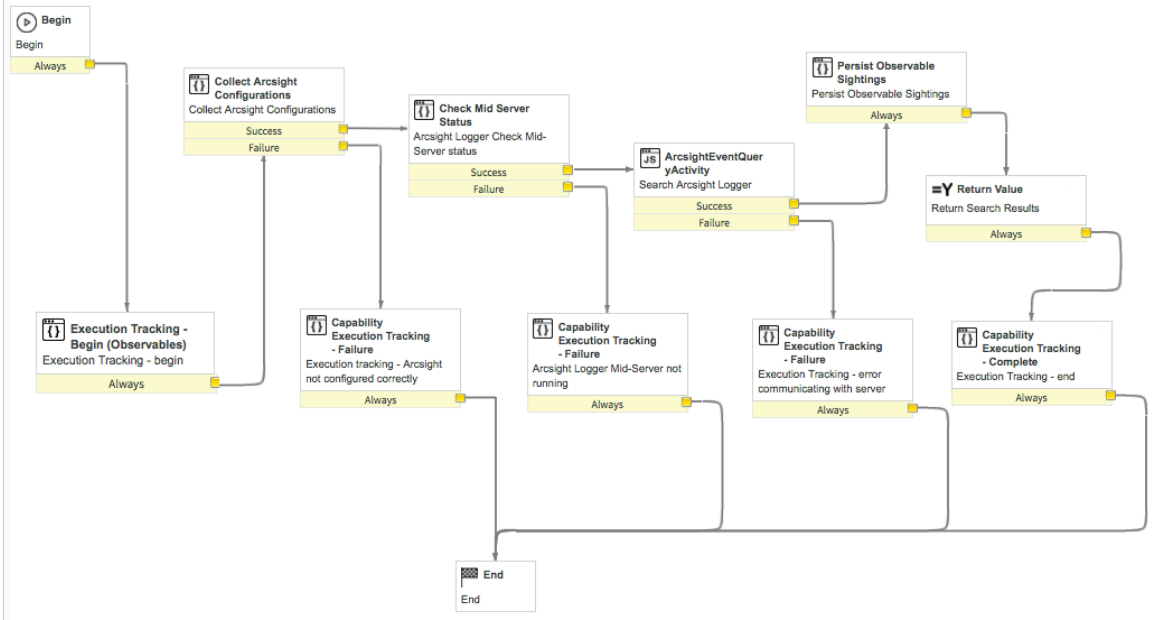
**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung: Beginn der Aktivität
- Aktivität „ArcSight-Konfigurationen erfassen“
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Aktivität „ArcSight Event-Abfrage“.
- Überprüft, ob der MID-Server ausgeführt wird oder nicht.
- Aktivität „ArcSight Event-Abfrage“.
- Aktivität „Persistierende Sichtungen erkennbarer Elemente“ – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Arcsight Logger Sichtungssuche




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

#### Aktivität „ArcSight-Konfigurationen erfassen“

Die Workflow-Aktivität **„ArcSight-Konfigurationen erfassen“ erfasst Konfigurationsinformationen**, die im Workflow verwendet werden sollen.

Die Aktivität „ **ArcSight-Konfigurationen erfassen** “ kann mit jedem Workflow verwendet werden, um die Konfigurationseinstellungen für HPE Security ArcSight Logger zu erfassen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Trusted Security Circle oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| link_endpoint_base | Link zu einer ArcSight Logger-Suchschnittstelle, falls verfügbar. |
| use_default_workflows | Bestimmt die Verwendung des Workflows, der mit dem Plugin installiert wurde. Mögliche Werte sind:<br>• true – Workflow verwenden<br>• false – Workflow nicht verwenden |
| „arcsight_username“. | Benutzername für HPE Security ArcSight Logger |
| „arcsight_password“. | Passwort für HPE Security ArcSight Logger |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. an. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |
| all_peers | Legt fest, ob alle anderen mit dem Netzwerk verbundenen Protokollierungen durchsucht werden sollen. |

### Aktivität „ArcSight Event-Abfrage“.

Die Workflow-Aktivität „ **ArcSight-Event-Abfrage“** durchsucht die ArcSight-Event-Protokolle nach schädlichen Indikatoren.

Die Aktivität „ **ArcSight Event-Abfrage** “ kann mit jedem Workflow zum Durchsuchen der HPE Security ArcSight Logger-Ereignisprotokolle verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Abfrage erfolgreich. |
| Fehler | Beim Versuch, die Abfrage zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Anwender | Benutzername für das HPE Security ArcSight Logger-System. |
| Kennwort | Passwort für das HPE Security ArcSight Logger-System. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| base_url | Basis-URL der Drittpartei-Integrations-API. |
| link_base_url | Link zu einer ArcSight Logger-Suchschnittstelle, falls verfügbar. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |
| all_peers | Legt fest, ob alle anderen mit dem Netzwerk verbundenen Protokollierungen durchsucht werden sollen. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Ausgabe der Abfrage im JSON-Format. |

### Aktivität „Persistierende Sichtungen erkennbarer Elemente“

Die Workflow-Aktivität **„Persistente Sichtungen erkennbarer Elemente** “ ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die Aktivität „ **Persistente Sichtungen** erkennbarer Elemente“ kann mit jedem Workflow verwendet werden, um in der Drittanbieterintegration gefundene erkennbare Elemente aufzuzeichnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente abgerufen. |
| Fehler | Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| SichtungenAntwort | |
| Aufgaben-ID | Aufgabenbezeichner. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | |

### Security Operations – Elasticsearch-Sichtungssuch-Workflow

**Security Operations - Elasticsearch-Sichtungssuch-** Workflow ist die Elasticsearch-Implementierung, die vom **Security Operations-Integration - Sichtungssuch-** Workflow gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst

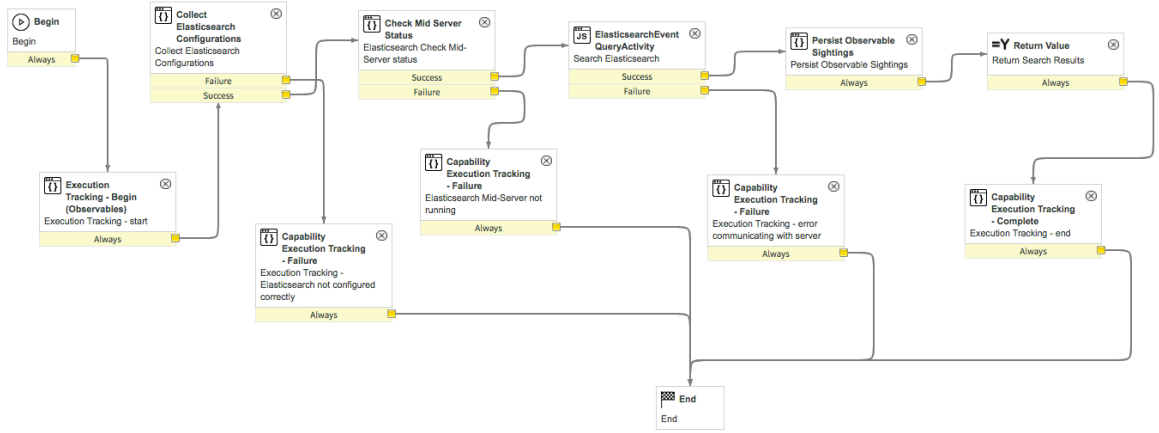
**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung: Beginn der Aktivität
- Aktivität „Elasticsearch-Konfigurationen erfassen“
- Überprüft, ob der MID-Server ausgeführt wird oder nicht.
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Elasticsearch Event QueryActivity-Aktivität
- Aktivität „Persistierende Sichtungen erkennbarer Elemente“ – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Elasticsearch-Sichtungssuche




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Elasticsearch-Konfigurationen erfassen“

Die Workflow-Aktivität **Elasticsearch-Konfigurationen sammeln erfasst Konfigurationsinformationen**, die im Workflow verwendet werden sollen.

Die Aktivität **Elasticsearch-Konfigurationen erfassen** kann mit jedem Workflow zum Erfassen der Elasticsearch-Konfigurationseinstellungen verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. an. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| link_endpoint_base | [Optional] Link zu einer Kibana-Instanz, falls verfügbar. |
| use_default_workflows | Bestimmt die Verwendung des Workflows, der mit dem Plugin installiert wurde. Mögliche Werte sind:<br>• true – Workflow verwenden<br>• false – Workflow nicht verwenden |
| Elastic_username | Elasticsearch-Benutzername |
| Elastic_password | Elasticsearch-Passwort |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. an. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Elasticsearch Event QueryActivity-Aktivität

Die Workflow-Aktivität **Elasticsearch Event Query** durchsucht die Elasticsearch-Ereignisprotokolle nach schädlichen Indikatoren.

Die **Elasticsearch Event QueryActivity-** Aktivität kann mit jedem Workflow zum Durchsuchen der Elasticsearch-Event-Protokolle verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Abfrage erfolgreich. |
| Fehler | Beim Versuch, die Abfrage zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Anwender | Benutzername für das Elasticsearch-System. |
| Kennwort | Passwort für das Elasticsearch-System. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| base_url | Basis-URL der Drittpartei-Integrations-API. |
| link_base_url | [Optional] Link zu einer Kibana-Instanz, falls verfügbar. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. $(observable) ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Ausgabe der Abfrage im JSON-Format. |

### Aktivität „Persistierende Sichtungen erkennbarer Elemente“

Die Workflow-Aktivität **„Persistente Sichtungen erkennbarer Elemente** “ ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die Aktivität „ **Persistente Sichtungen** erkennbarer Elemente“ kann mit jedem Workflow verwendet werden, um in der Drittanbieterintegration gefundene erkennbare Elemente aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente abgerufen. |
| Fehler | Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| SichtungenAntwort | |
| Aufgaben-ID | Aufgabenbezeichner. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | |

### Workflow „Security Operations – McAfee ESM-Sichtungssuche“.

Der Workflow „**Security Operations – McAfee ESM – Sichtungssuche** “ ist die Implementierung für die Splunk-Integration, die vom **Workflow „Security Operations Integration – Sightings Search**“ gestartet wird.

### Vorbereitungen

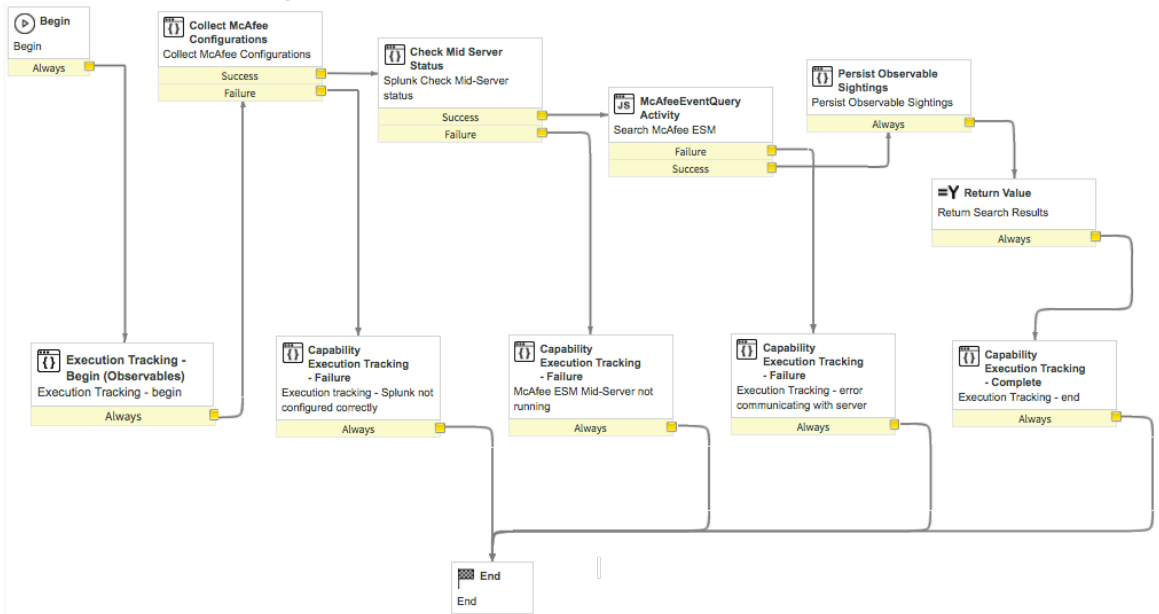
Erforderliche Rolle: sn_si_analyst

### Warum und wann dieser Vorgang ausgeführt wird

Workflow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung: Beginn der Aktivität
- Aktivität „McAfee-Konfigurationen erfassen“
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Aktivität „McAfee ESM Event-Abfrage“.
- Überprüft, ob der MID-Server ausgeführt wird.
- Aktivität „Persistierende Sichtungen erkennbarer Elemente“ – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

### McAfee ESM-Sichtungssuche




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „McAfee-Konfigurationen erfassen“

Die Workflow-Aktivität „ **McAfee-Konfigurationen** erfassen“ erfasst Konfigurationsinformationen, die im Workflow verwendet werden sollen.

Die Aktivität „ **McAfee-Konfigurationen** erfassen“ kann mit jedem Workflow zum Erfassen der McAfee ESM-Konfigurationseinstellungen verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. an. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| link_endpoint_base | Link zu einer McAfee-Webschnittstelle, falls verfügbar. |
| use_default_workflows | Bestimmt die Verwendung des Workflows, der mit dem Plugin installiert wurde. Mögliche Werte sind: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen (Fortsetzung)

| Variable | Beschreibung |
|---|---|
| | • true – Workflow verwenden<br>• false – Workflow nicht verwenden |
| Elastic_username | McAfee-Benutzername |
| Elastic_password | McAfee-Passwort |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. an. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

### Aktivität „McAfee ESM Event-Abfrage“.

Die Workflow-Aktivität „ **McAfee ESM Event-Abfrage** “ durchsucht die McAfee ESM-Ereignisprotokolle nach schädlichen Indikatoren.

Die Aktivität „ **McAfee ESM Event-Abfrage** “ kann mit jedem Workflow zum Durchsuchen der HPE Security ArcSight Logger-Ereignisprotokolle verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Abfrage erfolgreich. |
| Fehler | Beim Versuch, die Abfrage zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Anwender | Benutzername für das McAfee ESM-System. |
| Kennwort | Passwort für das McAfee ESM-System. |
| Erkennbare Elemente | Suchsyntax. `$(observable)` ist der Standardwert. |
| base_url | Basis-URL der Drittpartei-Integrations-API. |
| link_base_url | Link zu einer McAfee-Webschnittstelle, falls verfügbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Ausgabe der Abfrage im JSON-Format. |

### Aktivität „Persistierende Sichtungen erkennbarer Elemente“

Die Workflow-Aktivität **„Persistente Sichtungen erkennbarer Elemente** “ ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die Aktivität „ **Persistente Sichtungen** erkennbarer Elemente“ kann mit jedem Workflow verwendet werden, um in der Drittanbieterintegration gefundene erkennbare Elemente aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente abgerufen. |
| Fehler | Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| SichtungenAntwort | |
| Aufgaben-ID | Aufgabenbezeichner. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | |

### Workflow „Security Operations – QRadar-Sichtungssuche“.

Der Workflow**„Security Operations – QRadar-Sichtungssuche“** ist die Implementierung für die IBM QRadar-Integration, die vom **Workflow „Security Operations Integration – Sightings Search**“ gestartet wird.

### Vorbereitungen

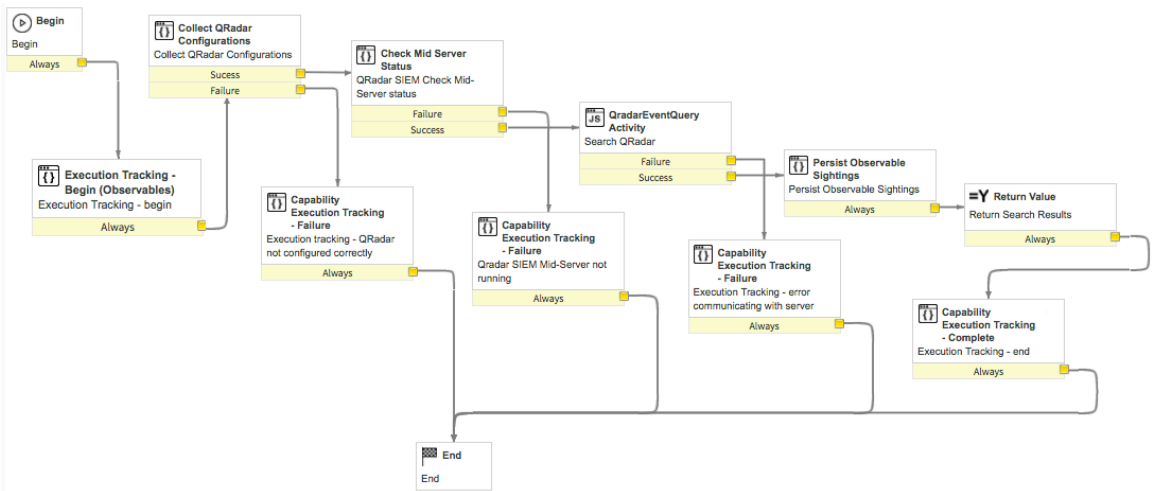
Erforderliche Rolle: sn_si_analyst

### Warum und wann dieser Vorgang ausgeführt wird

Workflow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung: Beginn der Aktivität
- Aktivität „QRadar-Konfigurationen erfassen“
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Überprüft, ob der MID-Server ausgeführt wird.
- QRadar-Event-QueryActivity-Aktivität
- Aktivität „Persistierende Sichtungen erkennbarer Elemente“ – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

### QRadar-Sichtungssuche




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „QRadar-Konfigurationen erfassen“

Die Workflow-Aktivität **QRadar-Konfigurationen sammeln erfasst Konfigurationsinformationen**, die im Workflow verwendet werden sollen.

Die Aktivität **QRadar-Konfigurationen erfassen** kann mit jedem Workflow zum Erfassen der IBM QRadar-Konfigurationseinstellungen verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. an. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| link_endpoint_base | Link zu einer IBM QRadar -Instanz, falls verfügbar. |
| use_default_workflows | Bestimmt, ob der mit dem Plugin installierte Workflow verwendet werden soll oder nicht. Mögliche Werte sind „true“ und „false“.an. |
| Elastic_username | QRadar-Benutzername |
| Elastic_password | QRadar-Passwort |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. an. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

### QRadar-Event-QueryActivity-Aktivität

Die Workflow-Aktivität **QRadar-Event-Abfrage** durchsucht die QRadar-Event-Protokolle nach schädlichen Indikatoren.

Die Aktivität **QRadar Event QueryActivity** kann mit jedem Workflow zum Durchsuchen der Elasticsearch-Ereignisprotokolle verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Abfrage erfolgreich. |
| Fehler | Beim Versuch, die Abfrage zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Anwender | Benutzername für das QRadar-System. |
| Kennwort | Passwort für das QRadar-System. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Vertrauenswürdige Sicherheitskreise oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| base_url | Basis-URL der Drittpartei-Integrations-API. |
| link_base_url | Link zu einer IBM QRadar -Instanz, falls verfügbar. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Ausgabe der Abfrage im JSON-Format. |

### Aktivität „Persistierende Sichtungen erkennbarer Elemente“

Die Workflow-Aktivität **„Persistente Sichtungen erkennbarer Elemente** “ ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die Aktivität „ **Persistente Sichtungen** erkennbarer Elemente“ kann mit jedem Workflow verwendet werden, um in der Drittanbieterintegration gefundene erkennbare Elemente aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente abgerufen. |
| Fehler | Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| SichtungenAntwort | |
| Aufgaben-ID | Aufgabenbezeichner. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Security Operations Integration - Splunk-Sichtungssuch-Workflow

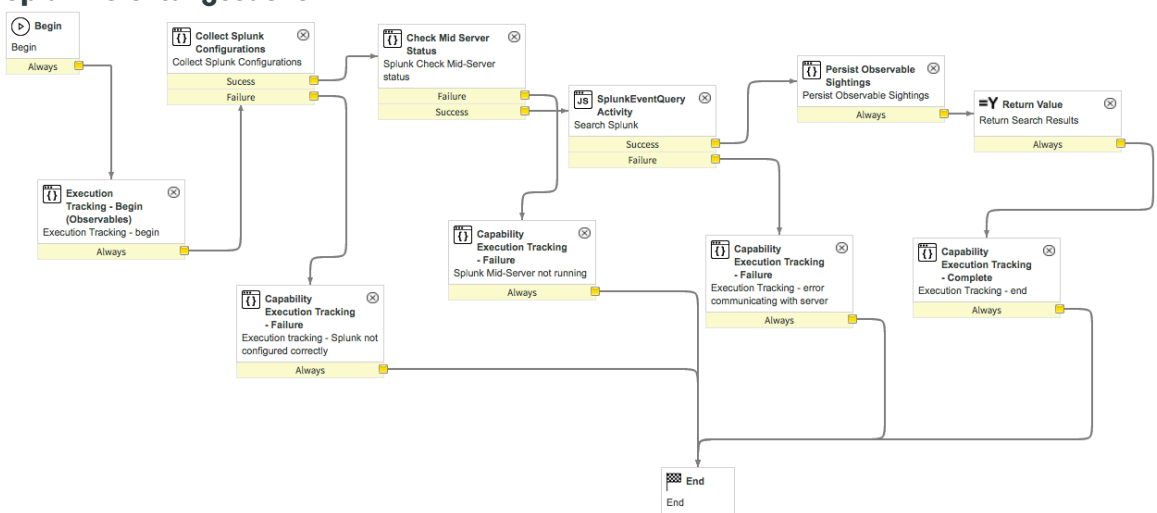
Der Workflow**„Security Operations – Splunk-Sichtungssuche“** ist die Implementierung für die Splunk-Integration, die durch den **Workflow „Security Operations Integration – Sightings Search**“ gestartet wird.

**Vorbereitungen**
Erforderliche Rolle: sn_si_analyst

**Warum und wann dieser Vorgang ausgeführt wird**
Workflow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung: Beginn der Aktivität
- Aktivität „Splunk-Konfigurationen erfassen“
- Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler“.
- Überprüft, ob der MID-Server ausgeführt wird oder nicht.
- Aktivität „Splunk Event-Abfrage“.
- Aktivität „Persistierende Sichtungen erkennbarer Elemente“ – gibt Suchergebnisse in einem Array zurück.
- Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

**Splunk-Sichtungssuche**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Splunk-Konfigurationen erfassen“

Die Workflow-Aktivität **„Splunk-Konfigurationen erfassen“ erfasst Konfigurationsinformationen**, die im Workflow verwendet werden sollen.

Die Aktivität „ **Splunk-Konfiguration erfassen** “ kann mit jedem Workflow zum Erfassen der Splunk-Konfigurationseinstellungen verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Konfiguration erfolgreich. |
| Fehler | Beim Versuch, die Konfiguration zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Trusted Security Circle oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| query | Suchsyntax. `$(observable)` ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| endpoint_base | Basis-URL der Drittpartei-Integrations-API. |
| link_endpoint_base | Links zur Webschnittstelle Splunk, sofern verfügbar. |
| use_default_workflows | Bestimmt die Verwendung des Workflows, der mit dem Plugin installiert wurde. Mögliche Werte sind:<br>• true – Workflow verwenden<br>• false – Workflow nicht verwenden |
| Elastic_username | Splunk-Benutzername. |
| Elastic_password | Splunk-Passwort. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Ausgabevariablen (Fortsetzung)**

| Variable | Beschreibung |
|---|---|
| query | Suchsyntax. $(observable) ist der Standardwert. |

### Aktivität „Splunk Event-Abfrage“.

Die Workflow-Aktivität „ **Splunk-Event-Abfrage“** durchsucht die Splunk-Event-Protokolle nach schädlichen Indikatoren.

Die Aktivität **„Splunk Event QueryActivity** “ kann mit jedem Workflow zum Durchsuchen der Splunk-Event-Protokolle verwendet werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Splunk |
| Fehler | Beim Versuch, die Splunk-Abfrage zu überprüfen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| Anwender | Benutzername für das Splunk-System. |
| Kennwort | Passwort für das Splunk-System. |
| Erkennbare Elemente | Die Liste der erkennbaren Elemente aus Trusted Security Circle oder die Security Incident-Aufgabe, nach der gesucht werden soll. Wird im JSON-Format zurückgegeben. |
| base_url | URL des Splunk-Integrationsendpunkts. |
| link_base_url | Link zur Webschnittstelle Splunk, sofern verfügbar. |
| Quelle | Quelle der Anforderung zum Ausführen des Workflows. Unterstützte Eingaben sind: Vertrauenswürdige Sicherheitskreise oder Security Incident-Aufgabe. |
| max_rows | Maximale Anzahl von Zeilen, die von der Abfrage zurückgegeben werden sollen. Der Grenzwert hängt von der Drittanbieterintegration ab. |
| days_to_search | Tage, die ab dem aktuellen Tag rückwärts durchsucht werden sollen. Der Standardwert ist 7. |
| query | Suchsyntax. $(observable) ist der Standardwert. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ausgabe | Ausgabe der Abfrage im JSON-Format. |

### Aktivität „Persistierende Sichtungen erkennbarer Elemente“

Die Workflow-Aktivität **„Persistente Sichtungen erkennbarer Elemente** “ ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die Aktivität „ **Persistente Sichtungen** erkennbarer Elemente“ kann mit jedem Workflow verwendet werden, um in der Drittanbieterintegration gefundene erkennbare Elemente aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Erkennbare Elemente abgerufen. |
| Fehler | Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| SichtungenAntwort | |
| Aufgaben-ID | Aufgabenbezeichner. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | |

### Sichtungssuchergebnisse anzeigen

Sie können die Ergebnisse der Sichtungssuche auf interne und externe schädliche Indikatoren überprüfen.

**Vorbereitungen**
Erforderliche Rolle: sn_si.analyst



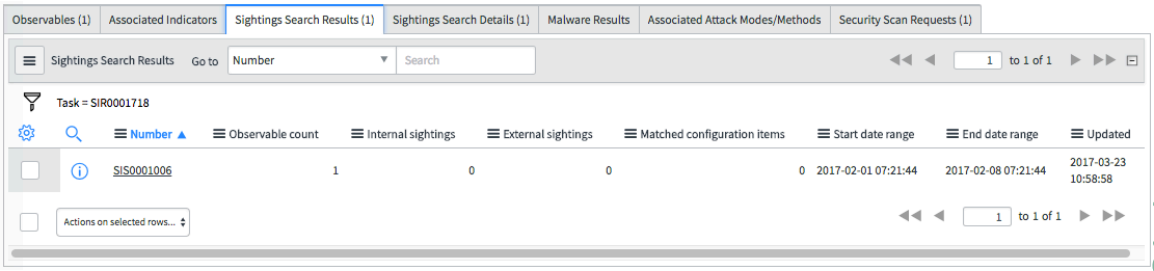
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Warum und wann dieser Vorgang ausgeführt wird

.

## Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie in der Gruppe „Zugehörige **IoC** -Liste anzeigen“ die Registerkarte **Sichtungssuchergebnisse** aus, um die Liste der Sichtungssuchen anzuzeigen.




**Hinweis:**
Diese Daten können mit Trusted Security Circlegeteilt werden.

### Ergebnisse von Sightings Search

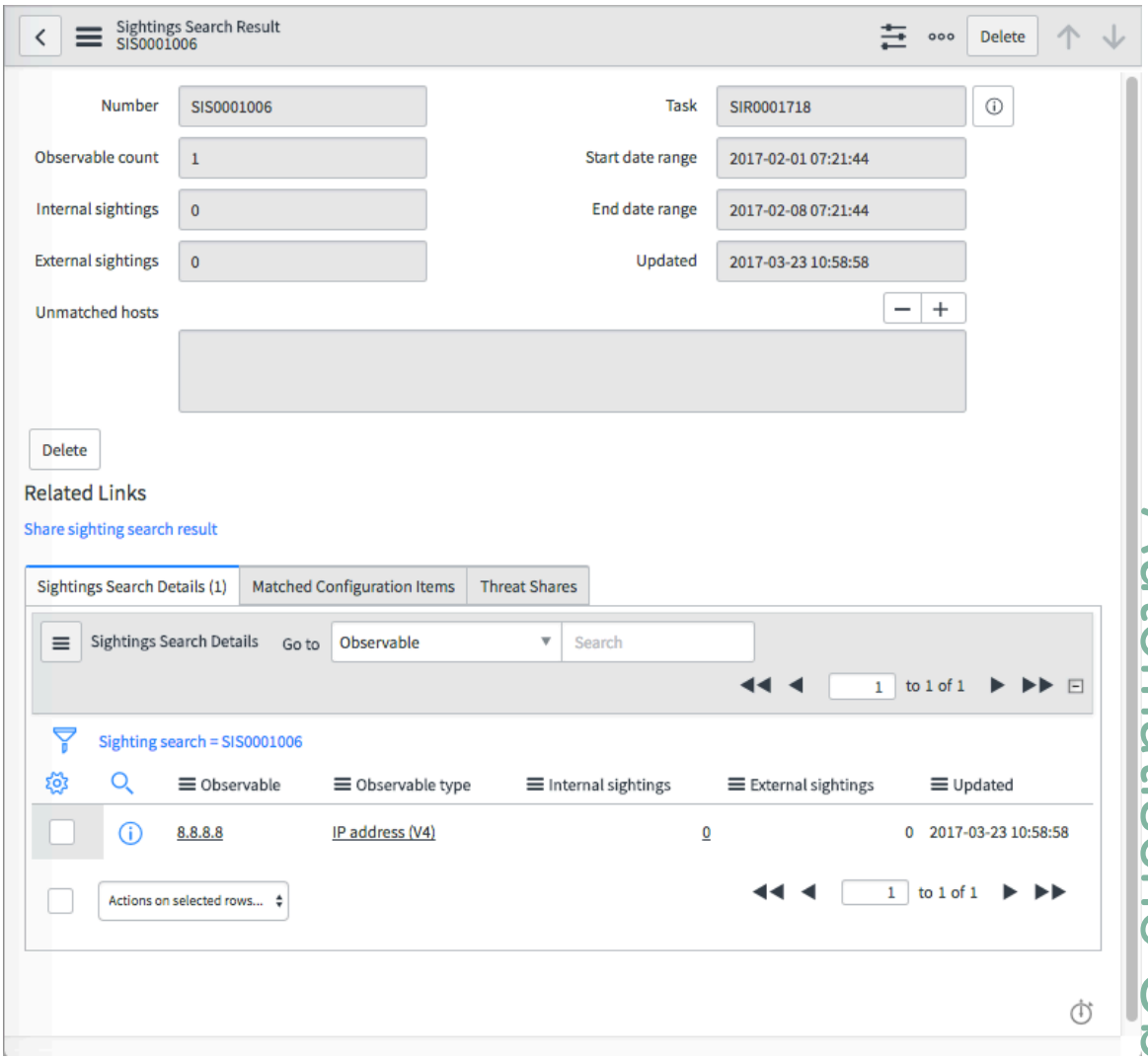
| Ergebnis | Beschreibung |
|---|---|
| Nummer | Sichtungssuchbezeichner. |
| Anzahl der erkennbaren Elemente | Anzahl der gesuchten erkennbaren Elemente. |
| Interne Sichtungen | Aggregierte Anzahl der internen Sichtungen. |
| Externe Sichtungen | Aggregierte Anzahl der externen Sichtungen. (Erhalten aus Bedrohungsfreigabe.) |
| Übereinstimmende Konfigurationselemente | Aggregierte Anzahl der Konfigurationselemente, die einem vorhandenen Datensatz in Ihrer CMDB entsprechen. |
| Startdatumsbereich | Zeit, um mit der Suche nach Sichtungen zu beginnen. |
| Enddatumsbereich | Zeit, um die Suche nach Sichtungen zu beenden. |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung. |

So zeigen Sie die Details einer einzelnen Suche an:

3. Klicken Sie in der Liste **„Sichtungssuchergebnisse** “ auf eine Sichtungssuche.
Das Formular „Sichtungssuchergebnis“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




**Formular „Sichtungssuchergebnisse“.**

| Detail | Beschreibung |
|---|---|
| Nummer | Bezeichner der internen Sichtungssuche. |
| Anzahl der erkennbaren Elemente | Anzahl der von dieser Abfrage gesuchten erkennbaren Elemente. |
| Interne Sichtungen | Anzahl der internen Sichtungen für diese Suche. |
| Externe Sichtungen | Anzahl der externen Sichtungen für diese Suche. (Erhalten von Trusted Security Circle.) |
| Nicht übereinstimmende Hosts | Liste der potenziellen Konfigurationselemente für diese Suche, die mit keinem Datensatz in Ihrer CMDB abgeglichen wurden. |
| Aufgabe | Bezeichner der Security Incident-Aufgabe |
| Startdatumsbereich | Zeit, zu der die Sichtungssuche gestartet wurde. |
| Enddatumsbereich | Zeitpunkt, zu dem die Sichtungssuche beendet wurde. |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung. |
| Details einer Sichtungssuche | Typ, Anzahl der Sichtungen und Änderungsdatum. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Detail | Beschreibung |
|---|---|
| Übereinstimmende Konfigurationselemente | Anzahl der Konfigurationselemente, die einem vorhandenen Datensatz in Ihrer CMDB entsprechen. Listet das CI und die Sichtung auf. |
| Bedrohungsfreigaben | Liste der für Trusted Security Circlefreigegebenen Bedrohungen. |

### Freigeben von Sichtungssuchergebnissen

Sie können lokale Sichtungsdetails oder Ergebnisse, die einer bestimmten Suche zugeordnet sind, mit Ihrem vertrauenswürdigen Sicherheitskreis teilen.

## Vorbereitungen

Erforderliche Rolle: sn_si.analyst

## Warum und wann dieser Vorgang ausgeführt wird

Die Freigabe kann mithilfe der folgenden Security Incident Response **-Eigenschaften**automatisiert werden.

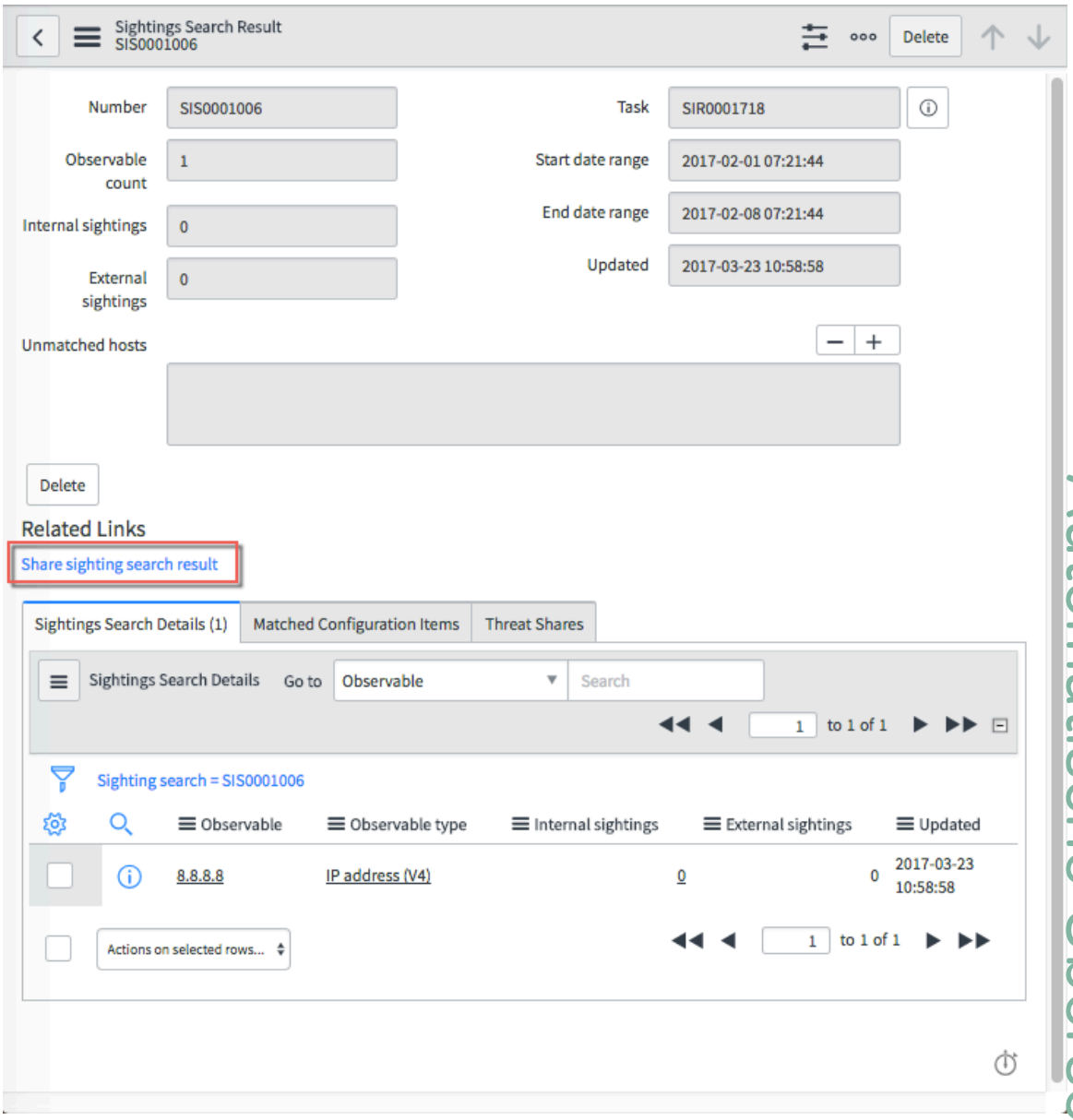
- Geben Sie die Ergebnisse einer Sichtungssuche automatisch an den standardmäßigen vertrauenswürdigen ServiceNow-Kreis weiter
- Beziehen Sie erkennbare Elemente ohne lokale Sichtungen ein, wenn Sie Sichtungssuchergebnisse automatisch freigeben
- Reagieren Sie mit lokalen Sichtungen, wenn eine Bedrohungsfreigabe von einem vertrauenswürdigen Kreis empfangen wird

## Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf die zugehörige Liste **IoC** anzeigen, und wählen Sie die Registerkarte **Sichtungssuchergebnisse** aus, um die Liste der Sichtungssuchen anzuzeigen.
3. Klicken Sie auf ein Sichtungssuchergebnis.



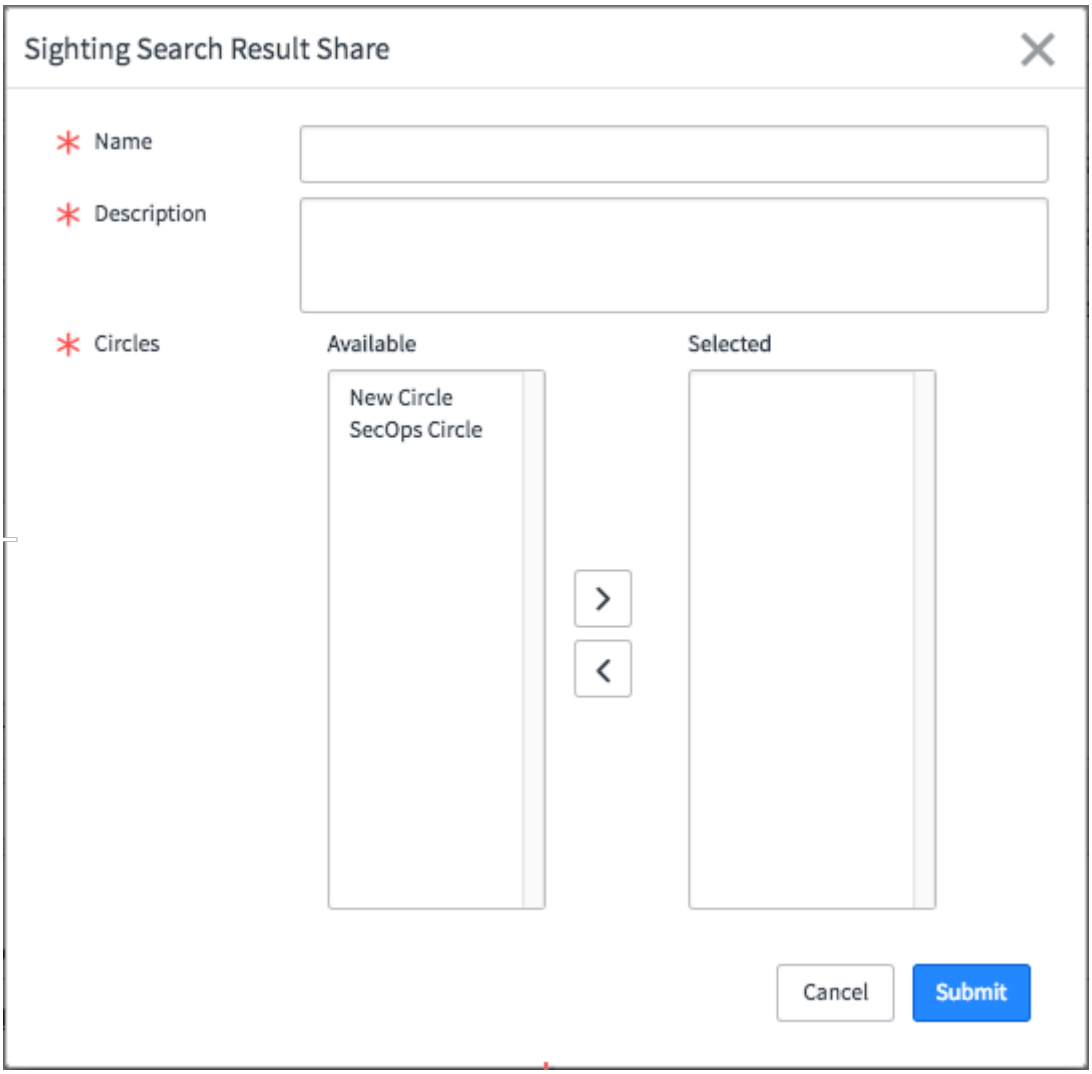
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. **Klicken**Sie im Formular „Sichtungssuchergebnis“ auf den zugehörigen Link **Sichtungssuchergebnis** freigeben.
   Das Dialogfeld „Sichtungssuchergebnis – Freigabe“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Geben Sie einen **Namen** für diesen freigegebenen Datensatz für erkennbare Elemente ein.
6. Geben Sie eine **Beschreibung**der erkennbaren Elemente ein, die freigegeben werden sollen.
7. Wählen Sie **Kreise** aus, um die erkennbaren Elemente für freizugeben.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.

### Erkennbare Elemente aus einem Security Incident freigeben

Erkennbare Elemente können von einem Security Incident in Security Incident Response an Mitglieder in Ihrem vertrauenswürdigen Kreis weitergegeben werden.

#### Vorbereitungen

Erforderliche Rolle: sn_si.analyst

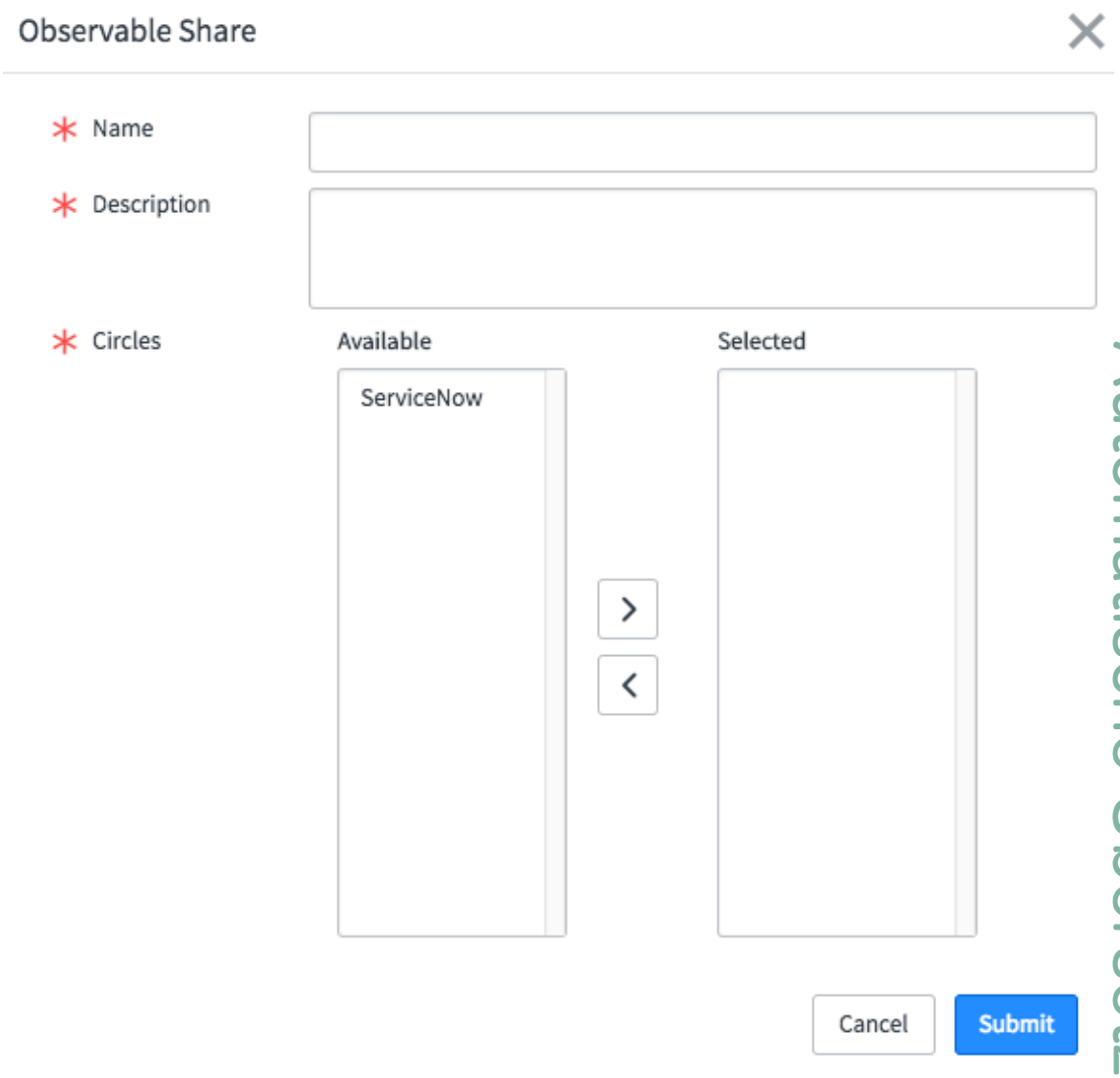
#### Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie in der Gruppe „Zugehörige **IoC** -Liste anzeigen“ die Registerkarte „ **Erkennbare** Elemente“ aus.
3. Klicken Sie auf ein erkennbares Element.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Klicken** Sie im Formular „Erkennbares Element“ auf den zugehörigen Link **Erkennbares** Element freigeben.
   Das Dialogfeld „Freigabe erkennbarer Elemente“ wird angezeigt.




5. Geben Sie einen **Namen** für diesen Bedrohungsfreigabe-Datensatz ein.
6. Geben Sie eine **Beschreibung**der ausgewählten erkennbaren Elemente ein.
7. Wählen Sie **Kreise** aus, um die erkennbaren Elemente für freizugeben.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.
9. Sie können die Datensätze für Bedrohungsfreigaben anzeigen, indem Sie auf die Registerkarte „ **Bedrohungsfreigaben** “ klicken.
10. Wenn eines der freigegebenen erkennbaren Elemente Sichtungen enthält, werden die Sichtungen ebenfalls freigegeben und können durch Klicken auf die Registerkarte **Sichtungen** angezeigt werden.

### Sichtungssuchdetails anzeigen

Überprüfen Sie die zusammengefassten Details aller Sichtungssuchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_si.analyst

### Warum und wann dieser Vorgang ausgeführt wird
.

### Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie in der Gruppe „Zugehörige **IoC** -Liste anzeigen“ die Registerkarte **Sichtungssuchdetails** aus, um die Liste der Sichtungssuchen anzuzeigen.

**Hinweis:**
Diese Daten können mit Trusted Security Circlegeteilt werden.

#### Details einer Sichtungssuche

| Detail | Beschreibung |
|---|---|
| Erkennbares Element | Liste aller erkennbaren Elemente, nach denen per Abfrage gesucht wurde. |
| Erkennbarer Typ | |
| Interne Sichtungen | Anzahl der internen Sichtungen für alle Suchvorgänge. |
| Externe Sichtungen | Anzahl der externen Sichtungen für alle Suchen. (Erhalten aus Bedrohungsfreigabe.) |
| Sichtungssuche | Sichtungssuchbezeichner. |
| Aktualisiert | Datum und Uhrzeit der letzten Änderung. |

## Security Operations-Integration – Funktion „Bedrohungssuche“.

Die Fähigkeit „Bedrohungssuchen“ führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein oder mehrere **erkennbare Elemente** bekannten Sicherheitsbedrohungen zugeordnet sind.

Die Fähigkeit **„Bedrohungssuche“** verfügt über den Workflow Security Operations-Integration – Workflow „Bedrohungssuche“.. Wenn der Fähigkeits-Workflow ausgeführt wird, werden zusätzliche Workflows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die für die Suche nach den ausgewählten erkennbaren Elementen verwendet werden soll, oder Sie können die Suche mit allen Implementierungen durchführen.

**Hinweis:**
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

## Security Operations-Integration – Workflow „Bedrohungssuche“.

Der Workflow „ **Security Operations Integration - Threat Lookup** “ greift auf verfügbare Implementierungen der Bedrohungssuche zu und führt die zugehörigen Implementierungs-Workflows aus, um Bedrohungssuchen für ausgewählte erkennbare Elemente durchzuführen.

### Vorbereitungen
Erforderliche Rolle: sn_ti.write

### Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow kann auf folgende Arten ausgelöst werden.

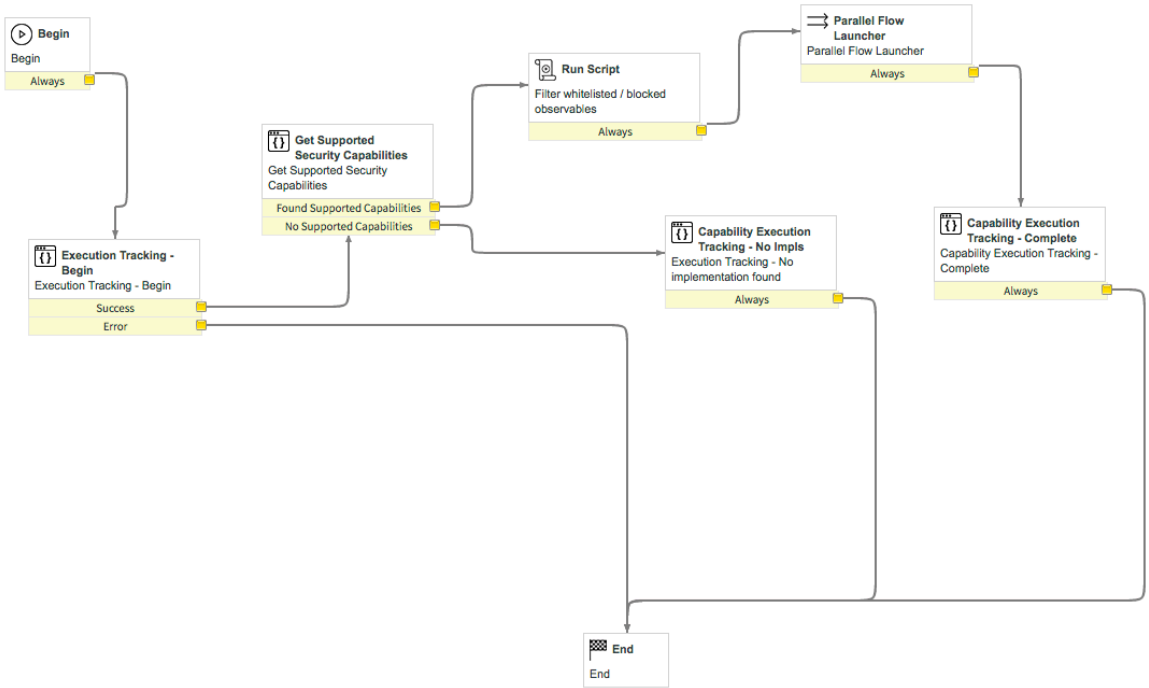


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- indem Sie ein oder mehrere erkennbare Elemente aus der Liste „Erkennbare Elemente“ auswählen und in der Auswahlliste **Aktionen für ausgewählte Zeilen** die Option **Bedrohungssuche ausführen** auswählen.
- indem Sie einen erkennbaren Datensatz öffnen und auf den zugehörigen Link **Bedrohungssuche ausführen** klicken.
- Über die zugehörige Liste „Erkennbare Elemente“ in einem Security Incident

Mit jeder Methode können Sie dann angeben, welche Suchimplementierungen zum Scannen der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Workflows werden ausgeführt, um die Suchvorgänge durchzuführen.

**Bedrohungssuche**




Spezifische Aktivitäten für diesen Workflow werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Integrations-Workflow-Aktivitäten.

### Aktivität „Unterstützte Sicherheitsfunktionen abrufen“

Die Workflow-Aktivität „Unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktivität Unterstützte Fähigkeiten abrufen kann mit jedem Workflow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Integration, die die gefundene Fähigkeit unterstützt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse (Fortsetzung)

| Ergebnis | Beschreibung |
|---|---|
| Fehler | Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityName | Name der Fähigkeit. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| domainId | Systembezeichner für eine beliebige Domäne, die dem Workflow zugeordnet ist. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| unterstützteFähigkeiten | Liste der Integrationen, die die Fähigkeit unterstützen. |
| capabilityCount | Anzahl der Integrationen, die die Fähigkeit unterstützen. |

### Nachverfolgung der Fähigkeitsausführung – keine implementierte Aktivität

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktivität „Fähigkeitsausführungsnachverfolgung – keine Implementierungen“ kann mit jedem abstrakten Integrationsfähigkeits-Workflow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Ausführungsnachverfolgungsdatensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Ausgabe der Aktivität, die zum Starten der Ausführungsverfolgung verwendet wird. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

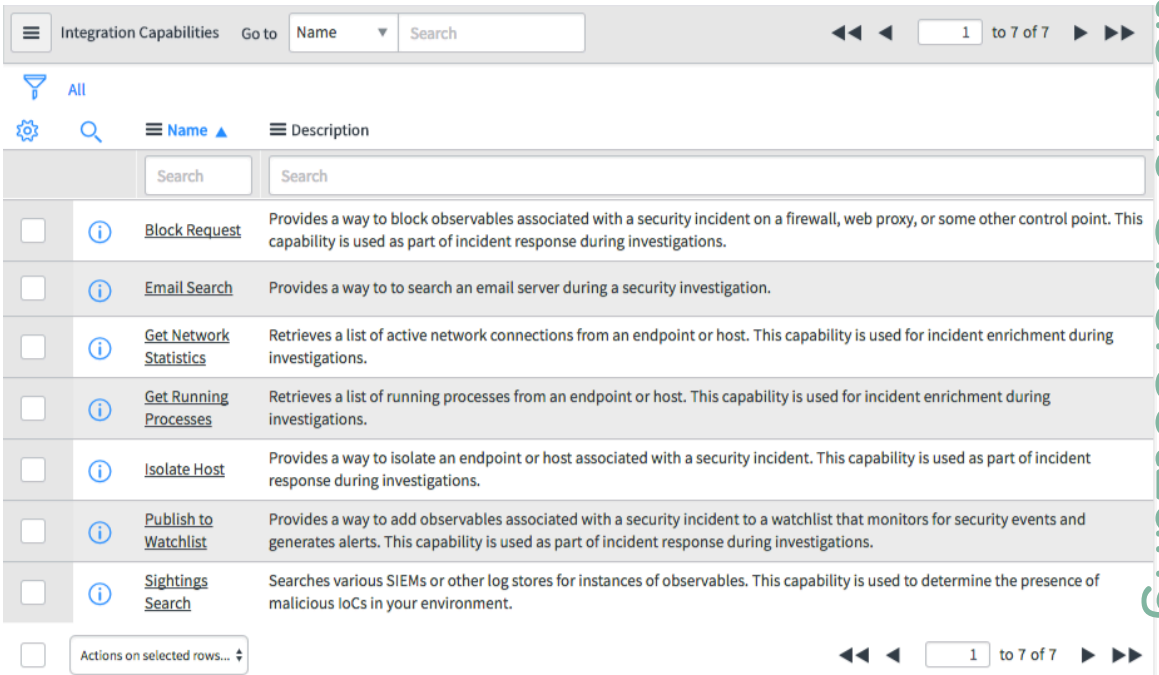
### Ändern Sie die Reihenfolge der Workflow-Ausführung

Implementierungen der Integrationsfähigkeit geben den auszuführenden Workflow an. Im Basissystem werden Workflows nacheinander in der in der Implementierung angegebenen Reihenfolge ausgeführt. Sie können die Reihenfolge nach Bedarf ändern.

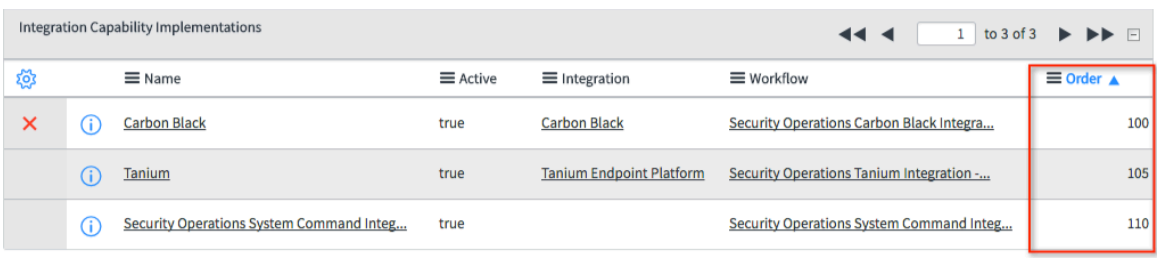
**Vorbereitungen**
Erforderliche Rolle: sn_sec_cmn.write

**Prozedur**

**1.** Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationsfunktionen**.



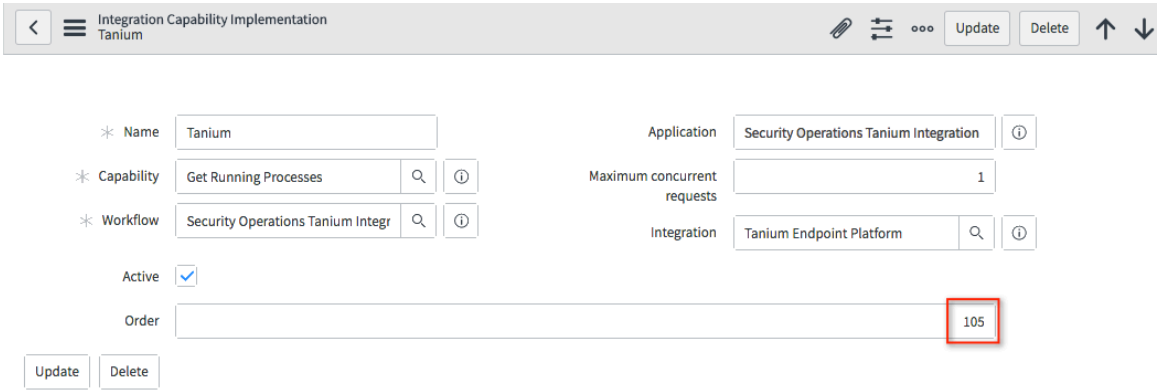

**2.** Wählen Sie die Integrationsfähigkeit aus, für die Sie die Ausführungsreihenfolge ändern möchten.




**3.** Wählen Sie die Implementierung aus, die Sie ändern möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




4. Ändern Sie die **Reihenfolge** in eine höhere oder niedrigere Zahl.
   Niedrigere Zahlen haben eine höhere Ausführungspriorität.
5. Klicken Sie auf **Absenden**.

## Allgemeine Integrations-Workflow-Aktivitäten

Viele der mit Drittanbieterintegrationen verknüpften Workflows umfassen dieselben Aktivitäten. Zum Beispiel Aktivitäten zum Starten und Abschließen der Verarbeitung.

### Ausführungsnachverfolgung: Beginn der Aktivität

Die Workflow-Aktivität „Execution Tracking – Begin“ (Ausführungsnachverfolgung – Begin) startet den Auditing-Prozess für einen Security Operations -Integrations-Workflow, der für erkennbare Elemente ausgeführt wird.

Die Aktivität „Ausführungsnachverfolgung – Begin“ kann mit jedem Workflow verwendet werden, um mit der Aufzeichnung des Fortschritts des Workflows in einem Audit zu beginnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ein Audit-Datensatz wird erstellt. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityId | Systembezeichner der ausgeführten Integrationsfähigkeit. |
| istImpl | Kennzeichnung, die angibt, ob ein Audit für einen Integration Capability-Workflow oder einen Integration Capability-Implementierungs-Workflow durchgeführt wird. Mögliche Werte sind: |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| | • false – bezeichnet die Prüfung eines abstrakten Integration Capability-Workflows wie Sichtungssuche. (Standard)<br>• true – bezeichnet Auditing für einen Integration Capability-Implementierungs-Workflow. Zum Beispiel Splunk oder Elasticsearch. |
| Aufgaben-ID | Systembezeichner für eine Aufgabe, die dem Workflow zugeordnet ist. |
| erkennbares Element Liste | Eine oder mehrere erkennbare SysIDs zum Ausführen der gewünschten Aktion.<br>Wird als Workflow-Eingabe verwendet. |
| workflowContextId | Systembezeichner des zugeordneten Workflow-Kontextdatensatzes. Vom System bereitgestellt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| parentCapabilityExcutionId | Systembezeichner des Audit-Datensatzes, der den Implementierungs-Workflow gestartet hat. Nur für Implementierungs-Workflows von Integration Capability wie Splunk, Elasticsearch und VirusTotal erforderlich. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner des Audit-Datensatzes. |

### Nachverfolgung der Fähigkeitsausführung: Aktivität abschließen

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – abgeschlossen“ aktualisiert den Audit-Datensatz, wenn der Workflow abgeschlossen ist.

Die Aktivität „Nachverfolgung der Fähigkeitsausführung – abgeschlossen“ kann mit jedem Workflow verwendet werden, um den Abschluss des Workflows aufzuzeichnen.

**Hinweis:**
Das **Rückgabewert** -Array aus der Kernaktivität des **parallelen Startprogramms** enthält ein Array von Ergebnissen aus allen ausgeführten Integrations-Workflows und meldet den erfolgreichen Abschluss der Ausführungsnachverfolgung.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Audit-Datensatzes wird auf **Abgeschlossen**aktualisiert. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Auditing-Aktivitäten beginnen. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |
| Nachricht | Abschlussnachricht. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler".

Die Workflow-Aktivität „Fähigkeitsausführungsnachverfolgung – Fehler" zeichnet einen Fehler im Audit-Datensatz auf.

Die Aktivität „Nachverfolgung der Fähigkeitsausführung – Fehler" kann mit jedem Workflow verwendet werden, um eine Fehlerbedingung aufzuzeichnen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Der Status des Audit-Datensatzes wird auf **Fehler** gesetzt, und eine Meldung mit der Angabe des Fehlers wird aufgezeichnet. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| capabilityExecutionId | Systembezeichner für den Audit-Datensatz. Dies ist die Ausgabe einer der Auditing-Aktivitäten beginnen. |
| errorMessage | Nachricht, die den Grund für den Fehler angibt. |
| workflowName | Name des Workflows. Vom System bereitgestellt. |

## Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

### Aktivität „Ergänzungsdatensätze erstellen".

Die Workflow-Aktivität Ergänzungsdatensätze **erstellen** erstellt oder aktualisiert Ergänzungsdatensätze, die im Workflow verwendet werden sollen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität **Ergänzungsdatensätze erstellen** kann mit jedem Workflow verwendet werden, um Ergänzungsdatensätze im Workflow zu aktualisieren.

### Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergänzungsdatensatz aktualisiert. |
| Fehler | Ergänzungsdatensatz nicht aktualisiert. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_id | Aufgabenbezeichner. |
| content | Rohinhalt (laufende Prozessdaten). |
| enreicherung_mapping_id | Identifier der Ergänzungszuordnung. |
| ci_id | Bezeichner des Konfigurationselements. |
| Referenzwert | Nicht verwendet. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Ergebnis | Mit dem EnrichmentUtils-Skript erstellte GlideRecords. |

## Security Operations Workflow-Auslöser

Security Operations Workflow-Auslöser enthalten eine Bedingung für eine Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist.

### Erstellen Sie Security Operations Workflow-Auslöser

Erstellen Sie einen Workflow-Auslöser, der eine Bedingung für eine Tabelle enthält.

#### Vorbereitungen

Security Operations enthält mehrere Workflow-Auslöser im Basissystem:

**Konfigurationselement ändert sich bei einem aktiven Security Incident**



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendet die Integration, um CI-bezogene Daten anzureichern, wenn sich Konfigurationselemente ändern.

**Angreifbare Gruppe erneut scannen**

Scannt eine angreifbare Gruppe erneut mit Scan-Schwachstellen-Workflow, wenn Sie die Gruppe **schließen/ignorieren**.

**Scannen Sie das angreifbare Element erneut**

Scannt ein angreifbares Element erneut und verwendet Workflow zum Scannen angreifbarer Elemente, wenn Sie das Element **schließen/ignorieren**.

Erforderliche Rollen:

- Zum Lesen: sn_sec_cmn.read
- Zum Erstellen oder Aktualisieren von: sn_sec_cmn.write
- Zu löschen: sn_sec_cmn.admin

## Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Workflow-Auslöser**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

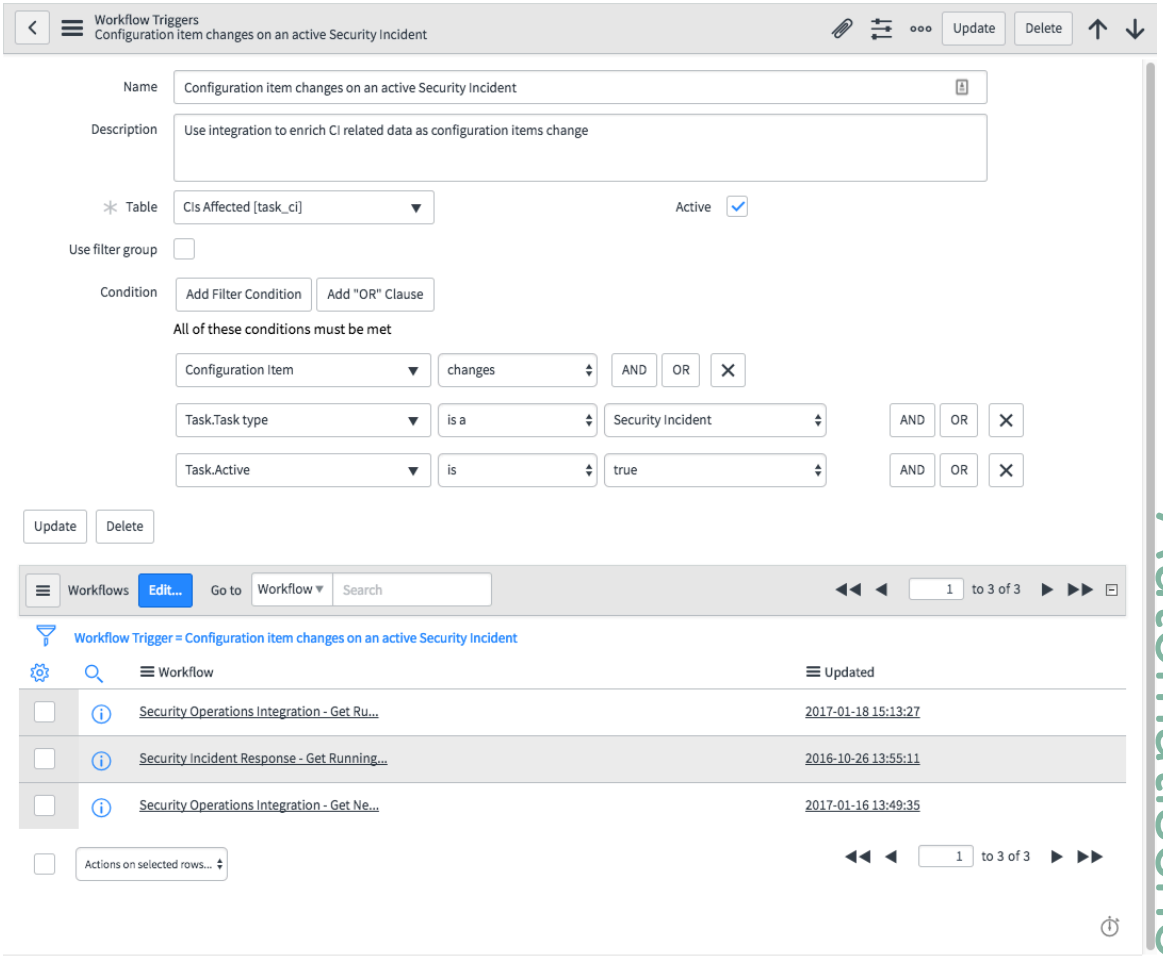
### Workflow-Auslöser

| Feld | Beschreibung |
|---|---|
| Name | Der Name des Workflow-Auslösers. |
| Beschreibung | Geben Sie eine Beschreibung für den Workflow-Auslöser ein. |
| Tabelle | Die Tabelle, die den Workflow-Auslöser enthält.<br><br>Wenn Sie das Kontrollkästchen **Filtergruppe verwenden** aktiviert und eine Filtergruppe ausgewählt haben, wird in diesem Feld standardmäßig die Tabelle verwendet, die der ausgewählten Filtergruppe zugeordnet ist. |
| Bedingung | Verwenden Sie den Bedingungsgenerator, um die Kriterien für den Workflow-Auslöser zu definieren.<br><br>Wenn Sie das Kontrollkästchen Filtergruppe **verwenden** aktiviert und eine Filtergruppe ausgewählt haben, werden die **Bedingungsfelder** nicht angezeigt. |
| Aktiv | Aktivieren Sie diese Checkbox, um den Workflow-Auslöser zu aktivieren. |
| Filtergruppe verwenden | Aktivieren Sie diese Checkbox, um eine vordefinierte Filtergruppe zu verwenden, oder erstellen Sie eine neue Filtergruppe, um die Workflow-Auslöserkriterien zu definieren. |
| Filtergruppe | Wählen Sie die Filtergruppe aus, die zum Definieren von Workflow-Auslösern verwendet werden soll.<br><br>Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Filtergruppen verwenden** aktiviert ist. |

4. Wenn Sie Ihre Eingaben abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formular-Header, und wählen **Sie Speichern**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




Die Registerkarte **Workflows** wird angezeigt. Sie enthält Workflows, die ausgeführt werden, wenn alle Filterbedingungen oder Filtergruppenbedingungen erfüllt sind.

5. Führen Sie die folgenden Schritte aus, um Workflows hinzuzufügen.
   a. Klicken Sie auf der Registerkarte **Workflows** auf **Bearbeiten**.
   b. Verwenden Sie bei Bedarf den Bedingungsgenerator, um die Workflows zu finden, die Sie auswählen möchten, oder verwenden Sie den Slushbucket, um Workflows auszuwählen und in die Workflow-Liste zu verschieben.
   c. Klicken Sie auf **Speichern**.
   Die ausgewählten Workflows werden hinzugefügt.
6. Klicken Sie auf **Aktualisieren**.

## Orchestration für Security Operations

Benutzer können mit Daten aus Windows- oder UNIX-basierten Systemen und Umgebungen mithilfe von Aktivitätenpaketen und Workflows in Security Operations Orchestrationinteragieren und Daten abrufen.

Security Operations Orchestration spart Zeit, indem manuelle Prozesse eliminiert und kontextbezogene Informationen zur Behebung von Incidents eingeholt werden. Die Produkte Security Operations verfügen über Standard-Aktivitätenpakete und -Workflows, die in jedem der Plugins enthalten und aktiviert sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um zusätzliche Orchestration-Aktivitäten zu erstellen und darauf zuzugreifen, die mit den Produkten des Standardangebots Security Operations nicht verfügbar sind, erwerben Sie eine vollständige Orchestration-Lizenz.

- Security Incident Response Orchestration -Workflows:
  - Workflow „Security Incident Response – Netzwerkstatistiken abrufen“.
  - Workflow „Security Operations System Command Integration – Laufende Prozesse abrufen“.
  - Workflow „Suchanforderung für IoC-Änderungen erstellen“.
  - Integration von Sicherheitsvorgängen – Workflow „E-Mails suchen und löschen“.
- Threat Intelligence Orchestration -Workflows:
  - Threat Intelligence IoC-Such-Workflow ausführen
  - Security Incident mit Suchergebnis-Workflow aktualisieren
- Vulnerability Response Orchestration -Workflows:
  - Scan-Schwachstellen-Workflow
  - Workflow zum Scannen angreifbarer Elemente

## Orchestration-Workflows für Security Operations

Security Operationsenthält mehrere Workflows.

### Scan-Schwachstellen-Workflow

Die zugehörigen Listen namens **Vulnerability Response** > **Scan-Schwachstelle** Der Workflow scannt eine Korrekturaufgabe erneut.

**Vorbereitungen**
Erforderliche Rolle: keine

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow wird durch **„Angreifbare Gruppe erneut scannen“** während einer Aktion „ **Schließen/Ignorieren** “ ausgelöst.

Workflow-Prozessaktivitäten umfassen:

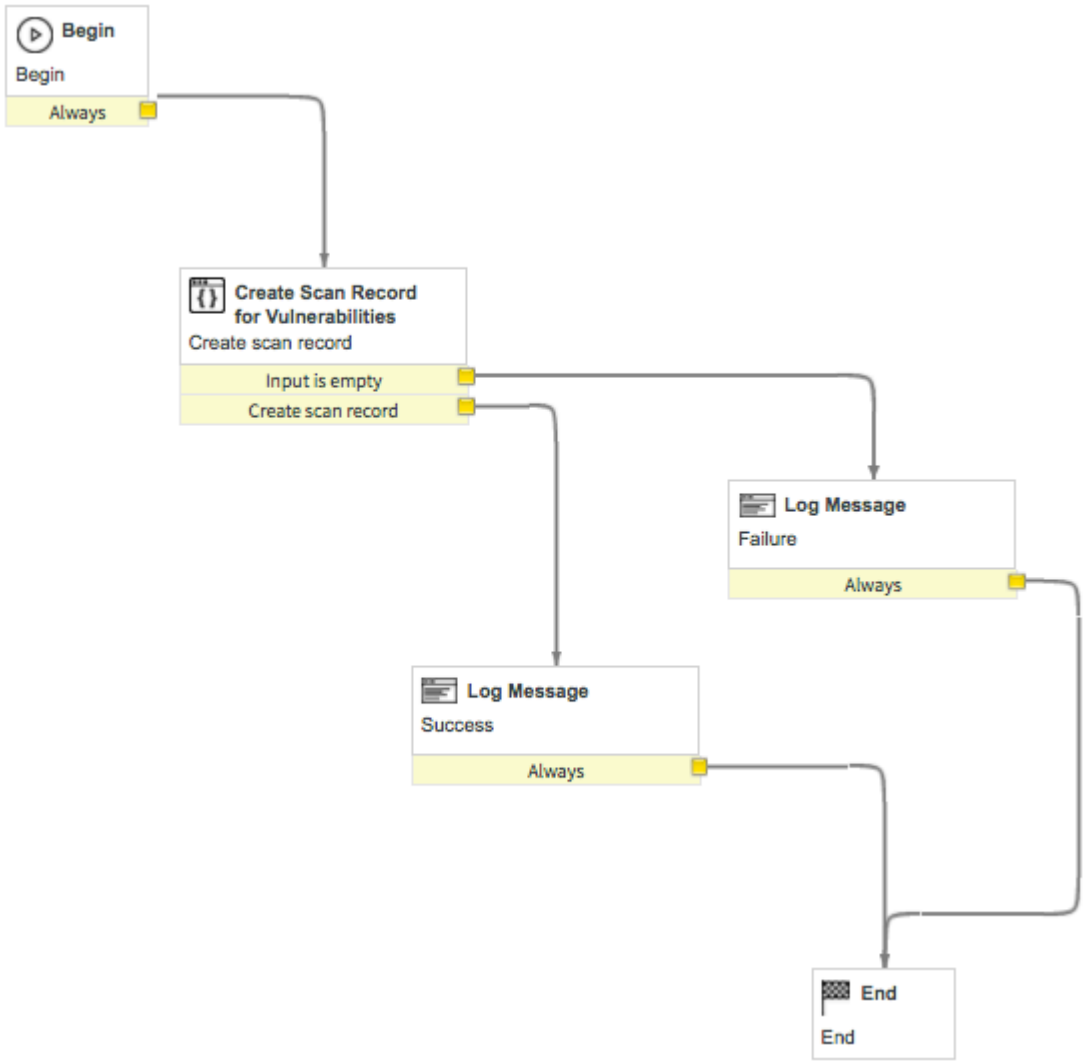
Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Protokollnachricht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Scan-Schwachstellen-Workflow






## Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**.
2. Öffnen Sie einen Aufgabendatensatz (VUL).
3. Klicken Sie auf **Schließen**.
4. Wählen Sie **Geschlossen** für **Gewünschter Zustand**.
5. Wählen Sie **Fest** für den **Substatus**.
6. Wählen Sie **Warten auf Bestätigung beim nächsten Scan** für **Jetzt schließen?**
   Für die Korrekturaufgabe und angreifbaren Elemente ändert sich der **Status** in „ **Bestätigung ausstehend**“, der **Substatus** ändert sich in „ **Festgelegt**“, und ein erneuter Scan wird ausgeführt.

### Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Schwachstellenprüfungen für einzelne oder mehrere angreifbare Elemente können mit der Workflow-Aktivität **Scan-Datensatz für Schwachstellen erstellen** ausgeführt werden, die im Basissystem enthalten ist. Wenn die Eingabe an die Aktivität übergeben wird, wird ein Scan-Datensatz erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Aufgaben-IDs [Zeichenfolge] | Eine Zeichenfolge von durch Kommas getrennten sysIds, die die erwarteten Eingaben definieren. Dieses Feld ist ein Pflichtfeld. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| scanResult [Boolesch] | Gibt „True“ zurück, wenn die Eingabe nicht leer ist. Für die taskIds wird ein Scan-Datensatz erstellt. |

### Workflow zum Scannen angreifbarer Elemente

Die zugehörigen Listen namens**Vulnerable Response** > **Angreifbares Element scannen** Der Workflow scannt ein angreifbares Element erneut.

**Vorbereitungen**
Erforderliche Rolle: keine

**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow wird durch **Rescan Schwachstelle**(Rescan Schwachstelle) während einer Aktion **Schließen/Ignorieren** ausgelöst.

Workflow-Prozessaktivitäten umfassen:

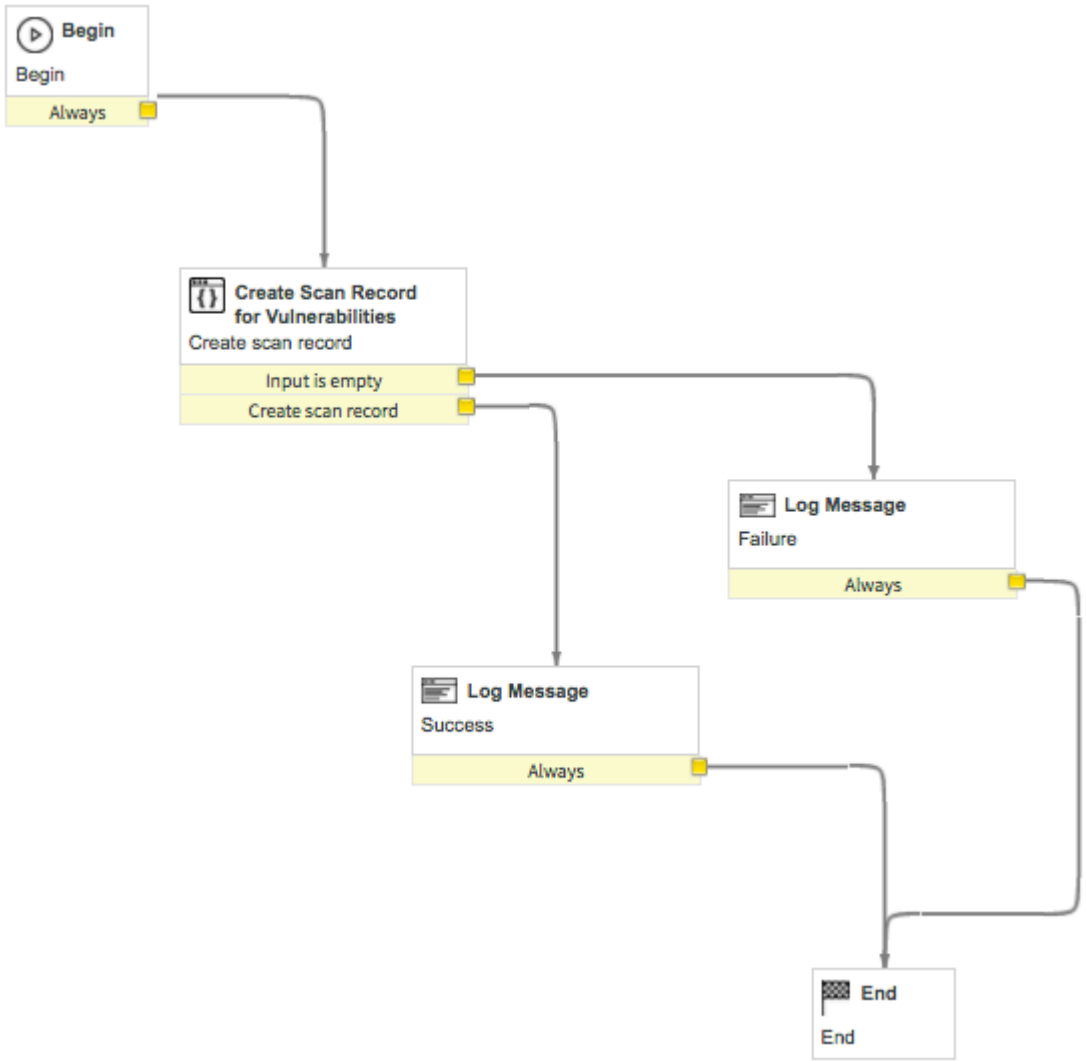
Variablen für die Aktivität „Scan-Datensatz für Schwachstellen erstellen“.

Protokollnachricht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Scan-Schwachstellen-Workflow






**Prozedur**

1. Navigieren zu **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie auf **Schließen/Ignorieren**.
4. Wählen Sie **Geschlossen**für **Gewünschter Zustand**.
5. Wählen Sie **Fest** für den **Substatus**.
   Der **Status** der Gruppe ändert sich in **Bestätigung ausstehend**, der **Substatus** ändert sich in **Festgelegt**, und ein erneuter Scan wird ausgeführt.

### Security Incident mit Suchergebnis-Workflow aktualisieren

Der Workflow Security Incident **mit Suchergebnissen** aktualisieren aktualisiert vorhandene Security Incidents mit Suchergebnissen.

**Vorbereitungen**
Erforderliche Rolle: sn_si.basic

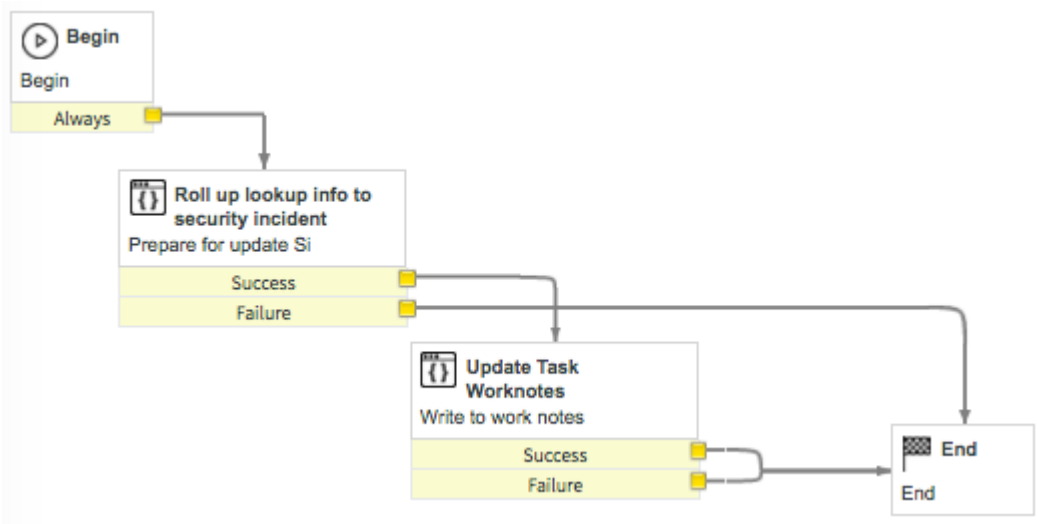
**Warum und wann dieser Vorgang ausgeführt wird**
Dieser Workflow wird durch eine Geschäftsregel in der Suchtabelle ausgelöst, die überwacht, wenn sich das Feld **Ergebnis** in Fehlgeschlagen ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Prozessaktivitäten umfassen:

Rollup-Suchinformationen zur Security Incident-Aktivität

Aktivität „Aufgabenarbeitsnotizen aktualisieren“.




## Orchestration-Aktivitäten von Security Operations

Security Operations enthält viele Aktivitäten zur Verwendung in Workflows.

### Aktivität „Ergänzungsdatensätze erstellen“.

Die Workflow-Aktivität Ergänzungsdatensätze **erstellen** erstellt oder aktualisiert Ergänzungsdatensätze, die im Workflow verwendet werden sollen.

Die Aktivität **Ergänzungsdatensätze erstellen** kann mit jedem Workflow verwendet werden, um Ergänzungsdatensätze im Workflow zu aktualisieren.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Ergänzungsdatensatz aktualisiert. |
| Fehler | Ergänzungsdatensatz nicht aktualisiert. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| task_id | Aufgabenbezeichner. |
| content | Rohinhalt (laufende Prozessdaten). |
| enreicherung_mapping_id | Identifier der Ergänzungszuordnung. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Variable | Beschreibung |
|---|---|
| ci_id | Bezeichner des Konfigurationselements. |
| Referenzwert | Nicht verwendet. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Ergebnis | Mit dem EnrichmentUtils-Skript erstellte GlideRecords. |

### Aktivität „FQDN für Konfigurationselement abrufen“.

Die zugehörigen Listen namens **Security Common Orchestration** > **Ruft den FQDN des Konfigurationselements ab** Die Workflow-Aktivität ruft den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „FQDN für Konfigurationselement abrufen“ kann mit jedem Workflow verwendet werden, um den vollständig qualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| cmdb_ci.id [Zeichenfolge] | Der Systembezeichner (sys_id) eines Configuration Item-Datensatzes. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| fqdn [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) des Konfigurationselements. |

## Zusätzliche Hinweise

Das Feld „fqdn“ im Konfigurationselement muss ausgefüllt werden.

### Erstellen Sie eine Compliance-Suchaktivität

Die Aktivität „Compliance-Suche erstellen“ erstellt eine Compliance-Suche für E-Mails auf den angegebenen Exchange-Servern unter Verwendung der definierten Suchabfragen und gibt den Namen der erstellten Compliance-Suche zurück.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| search_query | Obligatorische Suchabfrage, die verwendet wird, um E-Mails in Exchange Server in allen Postfächern zu finden. |
| Exchange-Standort | Obligatorisches Standortfeld, das für die Suche innerhalb des definierten Standorts verwendet wird. Werte sind:<br>• Alle<br>• Name des spezifischen Postfachs |
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Name der erstellten Compliance-Suche. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Fehler beim Erstellen der Suche | Wenn die Sucherstellung aufgrund einer Ausnahme auf dem Exchange-Server fehlschlägt. |
| Suche erfolgreich erstellt | Wenn die Sucherstellung erfolgreich ist. |
| Fehler beim Erstellen der Suche aufgrund eines Analysefehlers | Wenn die Sucherstellung aufgrund eines Analyseproblems fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |

### IP aus CI-Aktivität abrufen

Diese Workflow-Aktivität bestimmt die IPv4-Adresse, die einem Konfigurationselement (CI) zugeordnet ist.

Die Aktivität **IP aus CI** abrufen kann mit jedem Workflow verwendet werden, um die IPv4-Adresse eines CI abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| ci_sys_id [Zeichenfolge] | Systembezeichner des Konfigurationselements |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| ip_addr [Zeichenfolge] | IPv4-Adresse Wenn die IP-Adresse nicht bestimmt werden kann, ist dieser Wert leer. |

## Austrittsbedingungen

Mögliche Ergebnisse für diese Aktivität sind:

#### Bedingungen

| Bedingung | Beschreibung |
|---|---|
| Erfolg | Eine IPv4-Adresse wurde zurückgegeben. |
| Fehler | Es konnte keine IPv4-Adresse ermittelt werden. |

### Ruft Netzwerkstatistiken über die Aktivität „netstat“ ab

Die Workflow-Aktivität „Security Common Orchestration – Netzwerkstatistiken über Netstat abrufen“ ruft die Netzwerkstatistiken für eine betroffene Ressource auf einem Windows-basierten System ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Netzwerkstatistiken über netstat abrufen“ kann mit jedem Workflow zum Abrufen von Netzwerkstatistiken von einem Windows-basierten System verwendet werden. Der Computer wird mit dem Befehl **netstat** einschließlich der Parameter **-a** und **-o** abgefragt. Um die Ausgabedaten zu verbessern, wird auch der Befehl **get-process** aufgerufen.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

#### Ergebnisse

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Netzwerkstatistiken wurden im JSON-Format abgerufen. |
| Fehler | Beim Versuch, Netzwerkstatistiken abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Ziel [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) oder IP-Adresse des Zielsystems. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Antwort [Zeichenfolge] | Eine JSON-Zeichenfolge, die die aktuell ausgeführten Prozesse auf dem Zielcomputer darstellt.<br><br>JSON-Daten umfassen:<br><br>**pid**<br>Prozessbezeichner<br><br>**lokaler _port**<br>Lokaler Port für die Netzwerktransaktion<br><br>**Status**<br>Status der TCP-Verbindung<br><br>**Hinweis:**<br>Dieses Feld ist für UDP-Verbindungen null.<br><br>**local_address**<br>Lokaler vollständig qualifizierter Domänenname (FQDN) oder IP-Adresse<br><br>**remote_address**<br>Vollständig qualifizierter Remote-Domänenname (FQDN) oder IP-Adresse<br><br>**protocol**<br>TCP oder UDP<br><br>**remote_port**<br>Remote-Port der Netzwerktransaktion<br><br>**path**<br>Der Dateipfad der ausführbaren Prozessdatei<br><br>**hash**<br>Der Hashwert der ausführbaren Prozessdatei. Der Hash liegt in SHA-256 für PowerShell V4 oder höher vor. Andernfalls befindet sich der Hash in MD5. |

## Beschränkungen

Der MID Server muss PowerShellunterstützen.

SHA-256-Hash erfordert PowerShell V4.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ruft laufende Prozesse über die WMI-Aktivität ab

Die Workflow-Aktivität „**Laufende Prozesse** abrufen“ ruft die laufenden Prozesse eines Konfigurationselements auf einem Windows-basierten System ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „ **Laufende Prozesse über WMI** abrufen“ kann mit jedem Workflow verwendet werden, um laufende Prozesse auf einem Windows-basierten System abzurufen.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

#### Eingabevariablen

| Variable | Beschreibung |
|---|---|
| Ziel [Zeichenfolge] | Vollständig qualifizierter Domänenname (FQDN) oder IP-Adresse des Zielsystems. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

#### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| Antwort [Zeichenfolge] | Eine JSON-Zeichenfolge, die die aktuell ausgeführten Prozesse auf dem Zielsystem darstellt.<br>JSON-Daten umfassen:<br>**pid**<br>Der Prozessbezeichner<br>**Name**<br>Der Name des Prozesses<br>Außerdem, falls verfügbar:<br>**Verantwortlicher**<br>Der Name des Prozessverantwortlichen<br>**owner_sid**<br>Der Systembezeichner des Prozessverantwortlichen<br>**owner_domain**<br>Die Domäne des Prozessverantwortlichen<br>**path**<br>Der Dateipfad der ausführbaren Prozessdatei<br>**hash**<br>Der Hashwert der ausführbaren Prozessdatei. Der Hash liegt in SHA-256 für PowerShell V4 oder höher vor. Andernfalls befindet sich der Hash in MD5. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Beschränkungen

Der MID Server muss **PowerShell**unterstützen.

SHA-256-Hash erfordert PowerShell V4.

### Aktivität „Compliance-Suchstatus überprüfen“.

Die Aktivität „Compliance-Suchstatus überprüfen“ überprüft den Status der erstellten Compliance-Suche auf dem Exchange-Server. Wenn der Status abgeschlossen ist, werden die Informationen zur E-Mail-Suche zurückgegeben, die für die Compliance-Suche gefunden wurden.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

| Variable | Beschreibung |
|---|---|
| targetId | Obligatorisches Bezeichnerfeld für den Zielhost, in dem sich der Exchange-Server befindet. |
| Suchname | Obligatorischer Name der auf dem Exchange-Server erstellten Compliance-Suche. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

### Ausgabevariablen

| Variable | Beschreibung |
|---|---|
| response | Enthält den Status der Compliance-Suche und die Anzahl der auf dem Exchange-Server gefundenen E-Mails für die Compliance-Suche. |

## Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktivität sind:

### Austrittsbedingungen

| Variable | Beschreibung |
|---|---|
| Suche wird ausgeführt | Wenn der Status der Compliance-Suche in Bearbeitung ist. |
| Suche abgeschlossen – keine Bedrohungs-E-Mails gefunden | Wenn der Status der Compliance-Suche abgeschlossen ist und im Rahmen der Compliance-Suche keine E-Mails gefunden werden. |
| Suche abgeschlossen – Bedrohungs-E-Mails gefunden | Wenn der Status der Compliance-Suche abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden. |
| Fehler beim Überprüfen des Status | Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt. |
| Fehler | Wenn eine Ausnahme in der Workflow-Aktivität auftritt. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Aktivität „Aufgabenarbeitsnotizen aktualisieren“.

Die Workflow-Aktivität **Security Common Orchestration - Update Task Worknotes** aktualisiert den Abschnitt „ **Aktivität** “ (Arbeitsnotizen) eines Aufgabendatensatzes. Dies ist nützlich für die Protokollierung von Informationen.

Die Aktivität „ **Aufgabenarbeitsnotizen aktualisieren** “ kann mit jedem Workflow verwendet werden, um die Arbeitsnotizen eines beliebigen Aufgabendatensatzes zu aktualisieren.

## Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| task_id [Zeichenfolge] | Der Systembezeichner (sys_id) eines Aufgabendatensatzes. |
| Inhalt [Zeichenfolge] | Die Daten, die in die Arbeitsnotizen einer Aufgabe geschrieben werden. |

## Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob die Aktualisierung erfolgreich war. |

### Rollup-Suchinformationen zur Security Incident-Aktivität

Die Aktivität „ **Rollup für Suchinformationen zu Security Incident** “ durchführen kann mit jedem Workflow verwendet werden, um Informationen aus einer Bedrohungssuche zu sammeln und eine Zusammenfassung des Inhalts sowie die ID des ursprünglichen Security Incident in Aufgaben-Arbeitsnotizen auszugeben.

## Ergebnisse

Mögliche Ergebnisse für diese Aktivität sind:

**Ergebnisse**

| Ergebnis | Beschreibung |
|---|---|
| Erfolg | Suchberichtszusammenfassung, für die ein Rollup zum Security Incident durchgeführt wurde. |
| Fehler | Ursprungsaufgabe und Suchzusammenfassungsbericht sind leer. |

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| scanID[Zeichenfolge] | Suchbezeichner. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| siId[Zeichenfolge] | Security Incident-Bezeichner. |
| Antwort [Zeichenfolge] | Zusammenfassung der Suchergebnisse, einschließlich: IoC-Wert, Ergebnis, Fehlergrund, Suchreferenz usw. |

#### Schreiben Sie Inhalte, die als Anhangsaktivität aufgezeichnet werden sollen

Diese Aktivität schreibt den aus einer Eingabe übergebenen Inhalt und erstellt einen bestimmten Anhang zu einem bestimmten Datensatz.

Die Aktivität **Inhalt in Datensatz als Anhang** schreiben kann mit jedem Workflow verwendet werden, um Inhalte zu schreiben und an einen Datensatz anzuhängen.

### Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

**Eingabevariablen**

| Variable | Beschreibung |
|---|---|
| Tabellenname [Zeichenfolge] | Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld. |
| sysid [Zeichenfolge] | Der Systembezeichner (sys_id) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld. |
| Nutzlast | Der Nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld. |
| filename | Name der Anhangdatei. |

### Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

**Ausgabevariablen**

| Variable | Beschreibung |
|---|---|
| Ergebnis [Zeichenfolge] | Gibt an, ob die Aktualisierung erfolgreich war. |

## Data Loss Prevention Incident Response

Mit der Anwendung Data Loss Prevention Incident Response (DLP IR) können Sie den Korrektur-Workflow von DLP-Incidents aus mehreren Quellen überprüfen und verwalten, z. B. Endpunkt, Netzwerk, E-Mail und Cloud.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

**Data Loss Prevention Incident Response**

| | | |
|---|---|---|
| **Erkunden**<br>Erfahren Sie, wie Analysten und Administratoren DLP Incident Response verwenden | **Installieren und konfigurieren Sie**<br>Installation und Konfiguration der Anwendung DLP Incident Response | **Verwalten**<br>Administrationsaufgaben zum Verwalten der DLP-Incidents in der Now Platform |
| **Verwenden**<br>Aktualisieren und verwalten Sie Incidents mithilfe des DLP-Endbenutzerportals, des DLP Ops-Portals und des DLP-Dashboards. | **integrieren**<br>Erweitern Sie die DLP-Fähigkeiten durch die Integration mit Anwendungen von Drittparteien | |

## Data Loss Prevention Incident Response erkunden

Erkunden Sie die Anwendung Data Loss Prevention Incident Response, um zu erfahren, wie Sie vertrauliche Informationen für Ihre Kunden verwalten, z. B. Finanz- und Unternehmensdaten, Gesundheitsdatensätze oder Sozialversicherungsnummern.

Datenverlust tritt auf, wenn vertrauliche oder vertrauliche Informationen das Unternehmensnetzwerk aufgrund nicht autorisierter Kommunikation verlassen. Mit der DLP-Anwendung können Sie Datenverlustkanäle erkennen, darauf reagieren und sie schützen.

Durch die Verwendung der Anwendung Data Loss Prevention Incident Response hat Ihre Organisation die folgenden wichtigen Vorteile:

- Integrieren Sie mehrere DLP-Lösungen von Drittparteien, um eine einheitliche Ansicht der Incidents in Now Platformzu erhalten.
- Überwachen und weisen Sie Incidents den Endbenutzern zu, damit Sie das DLP-Incident-Management optimieren können.
- Coachen Sie Ihre Mitarbeiter mithilfe der benutzerdefinierten E-Mail-Vorlagen und Benachrichtigungen, die für jeden Incident gesendet werden, sowie in Form eines Digest.
- Eskalieren Sie die überfälligen DLP-Incidents von den Endbenutzern an die Manager.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

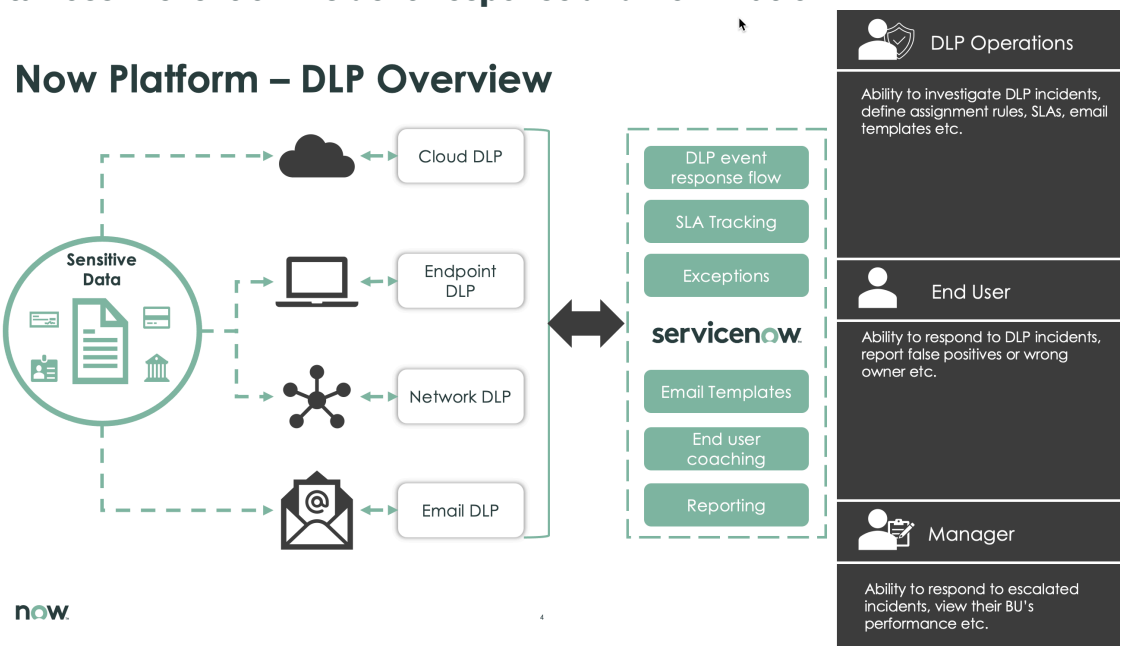
- Zeigen Sie Zusammenfassungsberichte offener Incidents nach Richtlinie, Schweregrad, Top-Tätern usw. an.
- Verfolgen Sie DLP-Incident-Trends, falsch positive Trends und Korrekturtrends nach.

In diesem Abschnitt erfahren Sie mehr über die wichtigsten Funktionen und die verschiedenen Rollen, die bei der Arbeit mit DLP-Incidents eine Rolle spielen.

## DLP Incident Response – Übersicht

Erfahren Sie, wie Sie die Anwendungen Now Platform und Data Loss Prevention Incident Response (DLP IR) verwenden können. Verwalten Sie vertrauliche Informationen für Ihre Kunden, z. B. Finanz- und Unternehmensdaten, Gesundheitsdatensätze oder Sozialversicherungsnummern. Automatisieren Sie die Fehlerkorrektur-Workflows mit der Anwendung DLP Incident Response.

## Data Loss Prevention Incident Response und Now Platform




Die Anwendung Data Loss Prevention Incident Response umfasst die folgenden Funktionen:

- Einen Endbenutzer-Arbeitsbereich, in dem Ihre Endbenutzer oder Mitarbeiter die zugewiesenen DLP-Incidents überprüfen und darauf reagieren können.
- Ein Manager Workspace, in dem ein Manager die eskalierten DLP-Incidents überprüfen und angemessen darauf reagieren kann.
- Ein einheitlicher Arbeitsbereich, in dem Ihr DLP-Betriebsteam die Trends bei offenen Incidents, häufigsten Straftätern und Incidents nach Scan-Quelle nachverfolgen und die DLP-Incidents für mehrere Quellen (Endpunkte, Netzwerke und E-Mail) anzeigen, bearbeiten, zuweisen und schließen kann.
- Administrative Steuerungen, die die E-Mail-Vorlagen für das Coaching und die Kommunikation von Endbenutzern, Zuweisungsregeln für die automatische Zuweisung von Incidents, Regeln für die automatische Eskalation und Delegierung für die Reaktion auf Incidents definieren.

## Erste Schritte mit DLP Incident Response

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihrer Anwendung Data Loss Prevention Incident Response (DLP IR) beginnen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste**

| Setupaufgabe | Beschreibung |
| --- | --- |
| Vergewissern Sie sich, dass Sie die erforderlichen Rollen Now Platform und DLP zugewiesen haben. | DLP Incident Response unterstützt die folgenden Rollen:<br>• Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow Store und weist den DLP-Administrator (sn_dlir.admin) zu.<br>• sn_dlir.admin<br>• sn_dlir.analyst |
| Vergewissern Sie sich, dass die Kernanwendungen ServiceNow, die zur Unterstützung der Anwendung Data Loss Prevention Incident Response erforderlich sind, installiert und aktiviert sind. | Das Plugin Data Loss Prevention Incident Response (com.snc.data_loss_incident) ist zur Unterstützung des Produkts Data Loss Prevention Incident Response erforderlich.<br>Vergewissern Sie sich, dass die folgenden Security Operations -Anwendungen über ServiceNow Store] installiert und aktiviert wurden. Wenn nicht installiert ist, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation zu gewährleisten:<br>• Data Loss Prevention Incident Response (com.snc.data_loss_incident)<br>• Security Support Common<br>Weitere Informationen zum Einrichten Ihrer Now Platform -Instanz für die Integration finden Sie unter Berechtigungen für ein Security Operations-Produkt oder eine Security Operations-Anwendung erhalten oder ServiceNow Store-Anwendungen aktivieren. |
| Domänentrennung | Überprüfen Sie das Thema Domänentrennung und DLP-Reaktion auf Incidents, wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten. |

## DLP IR Incident Response installieren und konfigurieren

Laden Sie die Anwendung Data Loss Prevention Incident Response (DLP IR) aus dem ServiceNow Store herunter, und installieren Sie sie in Ihrer Instanz.

Bevor Sie die Workflows für die Integration aufrufen, installieren und konfigurieren Sie die Anwendung Data Loss Prevention Incident Response aus ServiceNow Store in Ihrer Instanz von Now Platform.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Installieren und konfigurieren Sie die Anwendung DLP Incident Response

Verwalten Sie vertrauliche Informationen, und automatisieren Sie die Nachbesserungs-Workflows mithilfe der Anwendung Data Loss Prevention Incident Response (DLP IR) in Ihrer Instanz Now Platform.

### Vorbereitungen

Bevor Sie die Konfigurationsschritte abschließen können, müssen Sie die Anwendung aus dem ServiceNow Store herunterladen und in Ihrer Instanz installieren.

Erforderliche Rolle: admin und sn_dlir.admin

### Prozedur

1. Befolgen Sie die Anweisungen zum Herunterladen einer Anwendung aus dem ServiceNow Store.
2. Nachdem Sie die Anwendung **DLP Incident Response** und alle zugehörigen Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **DLP-Administration** > **Standardkonfiguration** , um den Rest der Anwendungskonfigurationabzuschließen.

## Domänentrennung und DLP-Reaktion auf Incidents

Sie können die Domänentrennung mit DLP Incident Response verwenden, um die Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen zu unterteilen, die als Domänen bezeichnet werden. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

### Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

## Funktionsweise der Domänentrennung mit DLP Incident Response

- Erstellen Sie einen Benutzer mit den erforderlichen Rollen sn_dlir.admin und sn_dlir.analyst in der jeweiligen Domäne.
- Führen Sie die DLP-Konfigurationen für Incident Response in der entsprechenden Domäne aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

# DLP-Administration für Incident Response

Sie können Regeln einrichten und zuweisen, Fälligkeitsregeln konfigurieren, E-Mail-Vorlagen verwenden, Endbenutzer-Antwortaktionen konfigurieren und vieles mehr, um die Data Loss Prevention Incident Response (DLP IR) Incidents auf der Now Platformzu verwalten.

Mit der Anwendung Data Loss Prevention Incident Response können Sie die folgenden Konfigurationen durchführen.

## DLP-Standardkonfigurationseinstellungen

Definieren Sie die Standardkonfigurationseinstellungen für Data Loss Prevention Incident Response (DLP IR) Incidents, um die Einstellungen für Incident-Benachrichtigungen und Incident-Zuweisungen für Ihre Endbenutzer zu identifizieren und einzurichten.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses Modul verwenden, um die Standardkonfigurationseinstellungen zu definieren, wenn die zentralen Zuweisungsregeln und Bezeichnerregeln ausgeschöpft sind und keiner Bedingung oder keinem Benutzer zugeordnet werden können. Sie können Endbenutzersuchregeln und Zuweisungsregeln auch definieren und erneut auf vorhandene aktive DLP-Incidents anwenden.

Mit der Endbenutzer-Incident-Benachrichtigung können Sie die Häufigkeit angeben, mit der E-Mail-Benachrichtigungen an Ihre Endbenutzer gesendet werden. Sie können beispielsweise Benachrichtigungseinstellungen so einrichten, dass Incidents gesammelt und einmal pro Woche eine E-Mail-Zusammenfassung gesendet wird. Durch die Zuweisung eines Incident können Sie angeben, welcher Gruppe Sie die DLP-Incidents anfänglich zuweisen. Sie können auch angeben, wie die Endbenutzer vom DLP-Betriebsteam weiter identifiziert werden.

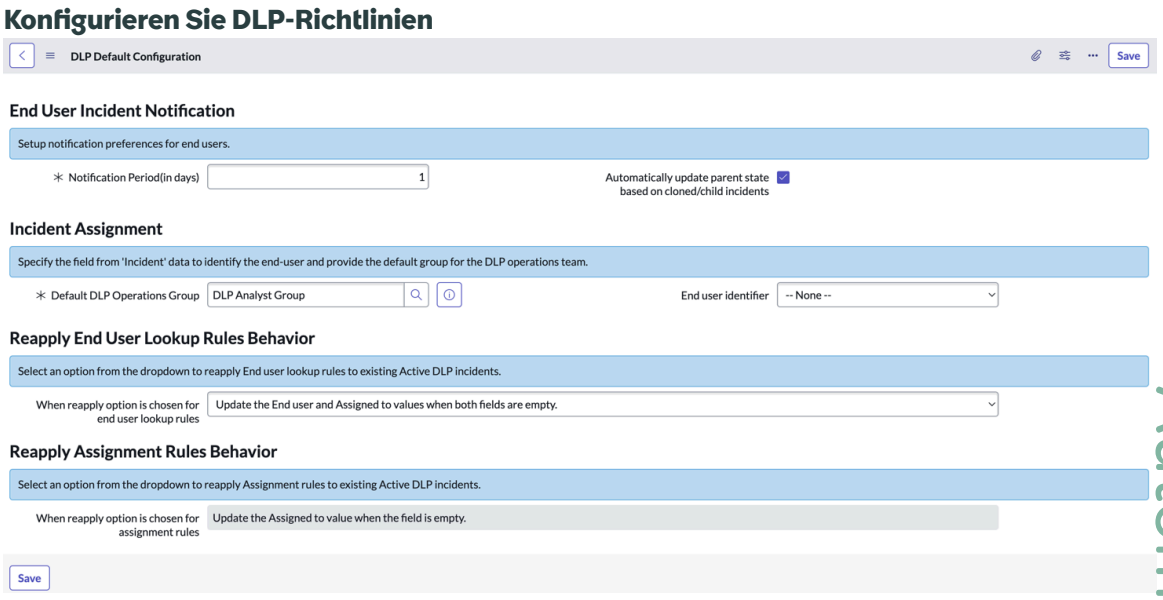
Angenommen, ein Benutzer hat Kreditkarteninformationen in einer Datei in einem Netzwerk gespeichert. Wenn das DLP-Integrationsprodukt einer Drittpartei einen Incident für einen Verstoß gegen die Richtlinie für vertrauliche Daten erstellt, enthalten die von Now Platform DLP erfassten Incident-Daten Informationen über den Endbenutzer. Sie können den Incident dann dem richtigen Endbenutzer zuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Standardkonfiguration**.




2. Füllen Sie die Felder des Formulars aus.

### Formular „DLP-Standardkonfiguration“

| Konfigurationsname | Feld | Beschreibung |
|---|---|---|
| Endbenutzer-Incident-Benachrichtigung | Benachrichtigungszeitraum (Tage) | Definieren Sie die Anzahl der Tage, nach denen eine E-Mail-Benachrichtigung an den Endbenutzer gesendet werden soll. Die Anzahl der Tage muss zwischen 1 und 60 Tagen liegen. |
| | Übergeordneten Status basierend auf geklonten/ untergeordneten Incidents automatisch aktualisieren | Option zum automatischen Aktualisieren des übergeordneten Status-Incident basierend auf den geklonten oder untergeordneten Incidents. |
| Incident-Zuweisung | Standardmäßige DLP-Vorgangsgruppe | Standardgruppe, der alle DLP-Incidents zugewiesen sind.<br>**Hinweis:**<br>Sie können nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde. |
| | Bezeichner des Endbenutzers | Geben Sie das Feld an, das aus Incident-Daten zum Identifizieren des Endbenutzers verwendet werden soll. Mögliche Werte:<br>○ **E-Mail-Adresse des Datenbesitzers**<br>○ **Ziel**<br>○ **Datei erstellt von**<br>○ **Datei geändert von** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Konfigurationsname | Feld | Beschreibung |
|---|---|---|
| | | ○ **Dateibesitzer**<br>○ **FTP-Benutzername**<br>○ **Absender** |
| Wenden Sie das Verhalten der Endbenutzer-Suchregeln erneut an | Wenn die Option „Erneut anwenden“ für Endbenutzer-Suchregeln ausgewählt ist | Option zum erneuten Anwenden von Endbenutzer-Suchregeln auf vorhandene aktive DLP-Incidents. Sie können eine der folgenden Optionen auswählen, um sie erneut anzuwenden:<br>○ **Endbenutzerwert aktualisieren, wenn das Feld leer ist**: Aktualisiert den Endbenutzerwert der vorhandenen aktiven DLP-Incidents, wenn dieses Feld leer ist.<br>○ **Endbenutzerwert aktualisieren**: Aktualisiert den Endbenutzerwert der vorhandenen aktiven DLP-Incidents.<br>○ **Werte für „Endbenutzer“ und „Zugewiesen an“ aktualisieren, wenn beide Felder leer sind**: Aktualisiert die Werte für „Endbenutzer“ und „Zugewiesen an“ der vorhandenen aktiven DLP-Incidents, wenn beide Felder leer sind.<br>**Hinweis:** Wenn diese Option ausgewählt ist, wird die Option **Wert für Zugewiesen an aktualisieren, wenn das Feld leer ist** im Abschnitt „Verhalten der Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt.<br>○ **Werte für Endbenutzer und Zugewiesen an für alle aktiven DLP-Incidents**aktualisieren: Aktualisiert die Werte für Endbenutzer und |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Konfigurationsname | Feld | Beschreibung |
|---|---|---|
| | | Zugewiesen an für alle aktiven DLP-Incidents.<br><br>**Hinweis:**<br>Wenn diese Option ausgewählt ist, wird die Option **Wert für „Zugewiesen an“ für alle aktiven DLP-Incidents** aktualisieren im Abschnitt „Verhalten der Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt. |
| Verhalten von Zuweisungsregeln erneut anwenden | Wenn die Option „Erneut anwenden“ für Zuweisungsregeln ausgewählt ist | Option zum erneuten Anwenden von Zuweisungsregeln auf vorhandene aktive DLP-Incidents. Sie können eine der folgenden Optionen auswählen, um sie erneut anzuwenden:<br>○ **Aktualisieren Sie den Wert Zugewiesen an, wenn das Feld leer ist.**<br>○ **Aktualisieren Sie den Wert Zugewiesen an für alle aktiven DLP-Incidents.** |

3. Klicken Sie auf **Speichern**.

## Konfigurieren Sie Suchregeln für Endbenutzer

Sie können Suchregeln für Endbenutzer erstellen und konfigurieren und die DLP-Incidents basierend auf diesen Regeln den jeweiligen Endbenutzern zuweisen.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Endbenutzer-Suchregeln, um die Endbenutzer DLP-Incidents automatisch nur über das Endbenutzerfeld zuzuweisen. Mit der DLP-Endbenutzer-Suchregel können Sie den Endbenutzer für DLP-Incidents basierend auf Endbenutzer-Bezeichner, benutzerdefinierten Attributen oder Skript zuweisen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Endbenutzer-Suchregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „DLP-Endbenutzer-Suchregel“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Endbenutzer-Suchregel. |
| Aktiv | Option, um anzugeben, ob die Endbenutzer-Suchregel aktiv ist. |
| Ausführungsbefehl | Die Suchregelpriorität des Endbenutzers.<br>Dieses Feld gibt die Reihenfolge an, in der die Endbenutzer-Suchregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen.<br><br>Die Endbenutzer-Suchregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw.<br><br>Der Standardwert ist 100. |
| Beschreibung | Eindeutige Beschreibung für die Endbenutzer-Suchregel. |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Endbenutzer-Suchregel zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>Sie können beispielsweise die Bedingungen für diese Endbenutzer-Suchregel festlegen, indem Sie die Bedingung als **Integration Source**, **enthält**, **Symantec**auswählen.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |



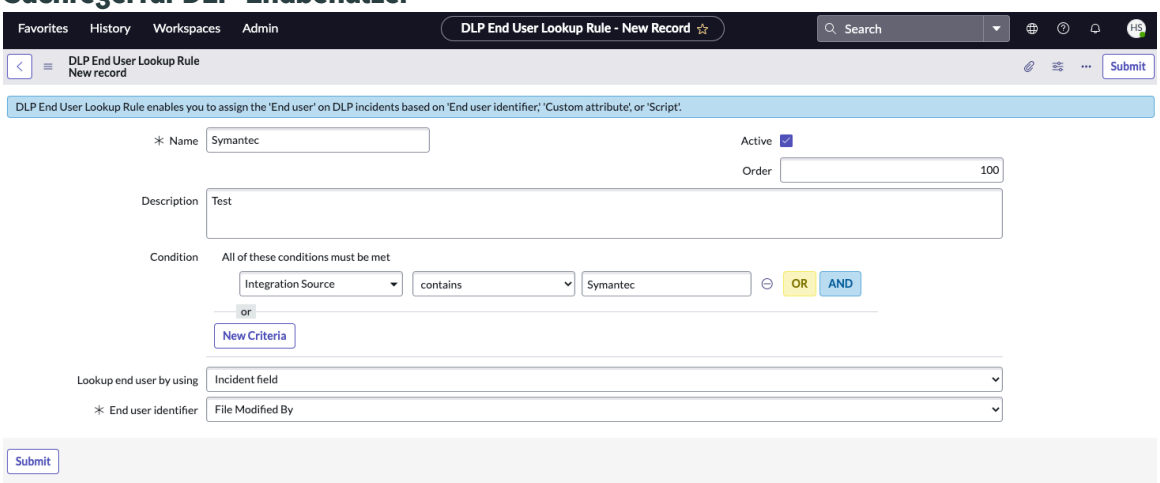
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Suchen Sie mithilfe von nach dem Endbenutzer | Option zum Suchen des Endbenutzers mithilfe des **Incident-Felds** oder des **Skripts**. |
| Bezeichner des Endbenutzers | Der Endbenutzerbezeichner des DLP-Incidents. Dieses Feld wird angezeigt, wenn das **Feld Incident aus dem FeldEndbenutzersuche mit** ausgewählt wird. Sie können einen der folgenden Endbenutzerbezeichner auswählen:<br>○ **E-Mail-Adresse des Datenbesitzers**<br>○ **Ziel**<br>○ **Datei erstellt von**<br>○ **Datei geändert von**<br>○ **Dateibesitzer**<br>○ **FTP-Benutzername**<br>○ **Absender**<br>○ **Benutzerdefinierter Benutzer aus Incident** |
| Benutzerdefiniertes Attribut | Option zum Angeben eines benutzerdefinierten Attributs aus dem Incident, der den Verweis auf einen Benutzer enthält. Dieses Feld wird nur angezeigt, wenn **Benutzerdefinierter Benutzer aus Incident** im Feld **Endbenutzer-Bezeichner** ausgewählt wird. |
| Skript | Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Endbenutzer-Suchregeln anzupassen und zu formatieren. Beispielsweise können Sie das E-Mail-Adressfeld verwenden, um den Endbenutzer zu identifizieren. |

### Example

Das folgende Beispiel zeigt eine Endbenutzer-Suchregel mit dem Namen Symantec. Der Bedingungsgenerator erfordert, dass die „Integrationsquelle“ „Symante“ ist. Die Option „ **Endbenutzer suchen mit** “ ist auf „Incident-Feld“ festgelegt, und die Option „ **Endbenutzer-Bezeichner** “ ist auf „Datei geändert von“ festgelegt.

**Suchregel für DLP-Endbenutzer**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Endbenutzer-Suchregeln auszuwählen und auf alle vorhandenen DLP-Incidents erneut anzuwenden.
5. Um eine Endbenutzer- **Suchregel**auf alle vorhandenen DLP-Incidents erneut anzuwenden, klicken Sie auf Erneut anwenden.

## Erstellen Sie eine Zuweisungsregel für Ihre Data Loss Prevention Incident Response Incidents

Erstellen und aktivieren Sie die Zuweisungsregeln. Weisen Sie dann die Incidents Data Loss Prevention Incident Response (DLP IR) Benutzergruppen, Endbenutzern, Managern oder Benutzern aus dem Incident zu.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Sie können Zuweisungsregeln verwenden, um DLP-IR-Incidents Benutzergruppen, Endbenutzern oder Managern zuzuweisen. Die Zuweisung der DLP-Incidents erfolgt, wenn die Bedingungen in der Zuweisungsregel erfüllt sind.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Zuweisungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „DLP-Zuweisungsregel“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Zuweisungsregel. |
| Aktiv | Option, um anzugeben, ob die Zuweisungsregel aktiv ist. |
| Ausführungsbefehl | Die Priorität der Zuweisungsregel. Dieses Feld gibt die Reihenfolge an, in der die Zuweisungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen.<br><br>Die Zuweisungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw.<br><br>Der Standardwert ist 100. |
| Beschreibung | Eindeutige Beschreibung für diese Zuweisungsregel. |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Um eine Bedingung für die Zuweisungsregel zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>Angenommen, Sie erstellen eine DLP-Zuweisungsregel für einen Endpunkt. Sie können angeben, dass die Quelle des Bedingungsscans ein Endpunkt-Dateisystem ist, das erfüllt sein muss, bevor ein Incident zugewiesen wird.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Zuweisen an | Zuweisung zu einem der folgenden:<br>○ Benutzergruppe<br>○ Endbenutzer<br>○ Manager<br>○ Benutzer aus Incident<br>Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind. |
| Benutzergruppe | Option zum Suchen und Auswählen einer Benutzergruppe, der die DLP-Incidents zugewiesen werden sollen. Dieses Feld wird angezeigt, wenn **Benutzergruppe** im Feld **Zuweisen an** ausgewählt wird.<br><br>**Hinweis:**<br>Sie können nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde. |
| Endbenutzer | Option zum Zuweisen des DLP-Incidents an den Endbenutzer. Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Zuweisen mithilfe von Manager-Feldern | Manager des Endbenutzers. Dieses Feld wird angezeigt, wenn **Manager** im Feld **Zuweisen an** ausgewählt wird.<br><br>Sie können die DLP-Incidents einem bestimmten Manager zuweisen, indem Sie eines der Manager-Felder auswählen, z. B. Nachname, E-Mail, Stadt, Mitarbeiternummer. |
| Benutzerbezeichner | Der Benutzerbezeichner des Incident. Dieses Feld wird angezeigt, wenn im Feld **Zuweisen an** die Option **Benutzer aus Incident** ausgewählt wird. Sie können einen der folgenden Benutzerbezeichner auswählen:<br>○ **E-Mail-Adresse des Datenbesitzers**<br>○ **Ziel**<br>○ **Datei erstellt von**<br>○ **Datei geändert von**<br>○ **Dateibesitzer**<br>○ **FTP-Benutzername**<br>○ **Absender**<br>○ **Benutzerdefinierter Benutzer aus Incident** |
| Benutzerdefiniertes Attribut | Option zum Angeben eines benutzerdefinierten Attributs aus dem Incident, der den Verweis auf einen Benutzer enthält. Dieses Feld wird nur angezeigt, wenn **Benutzerdefinierter Benutzer aus Incident** im Feld **Benutzerbezeichner** ausgewählt wird. |
| Bewertung anhängen | Option, um anzugeben, ob Sie dem Incident eine Bewertung anfügen möchten. |
| Status der Vorbewertungsantwort | Option, um auszuwählen, in welchem Status sich der Incident befinden soll, bevor der Endbenutzer reagiert. Es kann sich auch um einen benutzerdefinierten Status handeln.<br><br>Der Standardwert ist Ausstehende Bewertung. |
| Status der Antwort nach der Bewertung | Option zum Auswählen des Status des DLP-Incident, nachdem der Benutzer geantwortet hat.<br><br>Der Standardwert ist „Bewertung abgeschlossen“. |
| Erweitert | Erweiterte Option zum Identifizieren des Endbenutzers. Dieses Feld wird nur angezeigt, wenn **Benutzerdefinierter Benutzer aus Incident** im Feld **Benutzerbezeichner** ausgewählt wird. |



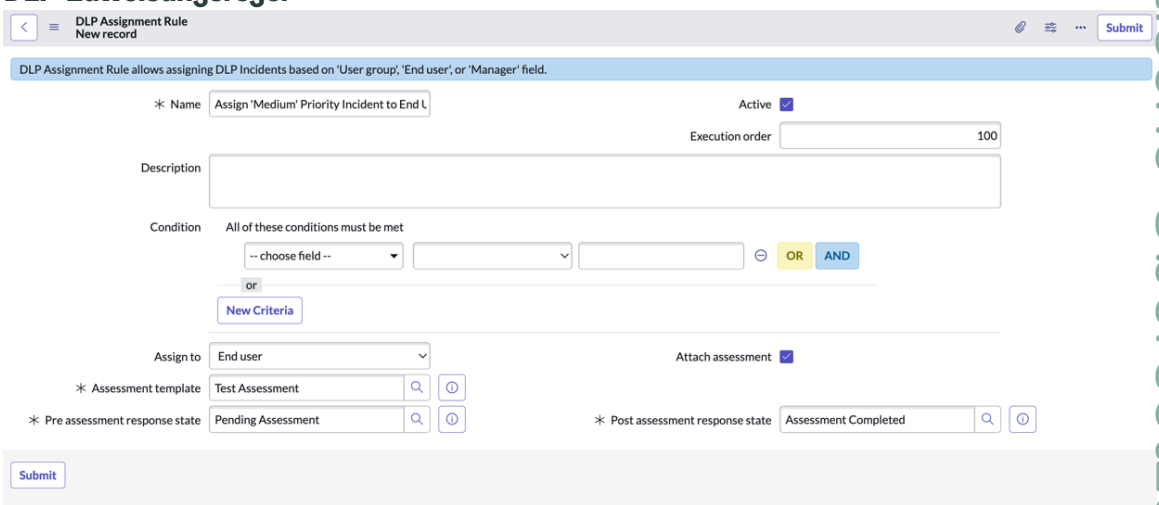
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Zuweisungsregel anzupassen und zu formatieren, um den Endbenutzer zu identifizieren. Anschließend wählen Sie aus, wem Sie den DLP-Incident zuweisen möchten. Dabei kann es sich um einen Endbenutzer oder den Manager des Endbenutzers handeln.<br><br>Beispielsweise können Sie das E-Mail-Adressfeld verwenden, um den Endbenutzer zu identifizieren. |

**Example**

Das folgende Beispiel zeigt eine Zuweisungsregel mit dem Namen Incident mit Priorität „Mittel“ an Endbenutzer zuweisen. Der Bedingungsgenerator erfordert, dass die Scan-Quelle Endbenutzer Incident 'Mittlere' Priorität zuweisenund das Feld Zuweisen an auf Endbenutzerfestgelegt ist. Anschließend können Sie nach der E-Mail-Adresse des Endbenutzers suchen.

**DLP-Zuweisungsregel**




4. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Zuweisungsregeln auszuwählen und auf alle vorhandenen DLP-Incidents erneut anzuwenden.
5. Um eine Zuweisungsregel auf alle vorhandenen DLP-Incidents erneut anzuwenden, klicken Sie auf **Erneut anwenden**.

## Konfigurieren Sie Incident-Konsolidierungsregeln, um Ihre DLP-Incidents zu konsolidieren

Konfigurieren Sie die Incident-Konsolidierungsregel, um mehrere Incidents ähnlicher Art unter einem übergeordneten Incident zu konsolidieren.

**Vorbereitungen**

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen
- sn_dlir.analyst und sn_dlir.analyst_read – Anzeigen (schreibgeschützt)

### Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Incident-Konsolidierungsregeln, um DLP-Incidents gleicher Art automatisch unter einem übergeordneten Incident zu konsolidieren. Mit der Konsolidierungsregel für DLP-Incidents können Sie die DLP-Incidents basierend auf der für Konsolidierungsdauer und Konsolidierungsidentifizierung angegebenen Konfiguration konsolidieren.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Incident-Konsolidierungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „DLP-Zuweisungsregel“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Incident-Konsolidierungsregel. |
| Aktiv | Option, um anzugeben, ob die Incident-Konsolidierungsregel aktiv ist. |
| Ausführungsbefehl | Die Priorität der Incident-Konsolidierungsregel. Dieses Feld gibt die Reihenfolge an, in der die Incident-Konsolidierungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen.<br><br>Die Incident-Konsolidierungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw.<br><br>Der Standardwert ist 100. |
| Beschreibung | Eindeutige Beschreibung für die Incident-Konsolidierungsregel. |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Incident-Konsolidierungsregel zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung als **Integration Source**, **enthält**, **Symantec**auswählen.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Konsolidierungsdauer | Option zum Festlegen der Dauer für die Incident-Konsolidierung.<br><br>Incidents in diesem Zeitraum mit denselben Werten für die ausgewählten Felder werden unter dem ersten Incident konsolidiert. Der erste Incident, der dieser Regel entspricht, ist der übergeordnete Incident, die restlichen Incidents sind untergeordnete Incidents. |
| Konsolidieren Sie Incidents nach | Wählen Sie das DLP-Incident-Feld aus, um die Incidents zu konsolidieren, wenn im ausgewählten Feld für verschiedene Incidents derselbe Wert vorhanden ist.<br><br>Wählen Sie mindestens ein Feld aus.<br>Wählen Sie mindestens ein Feld aus. |

Das folgende Beispiel zeigt eine Incident-Konsolidierungsregel mit dem Namen Incidents für Symantec-Integration konsolidieren. Der Bedingungsgenerator erfordert die Integrationsquelle als Symantec. Die Option **Bedingungsdauer** ist auf 1 Stunde festgelegt, und die Option Richtlinienname ist für **Incident konsolidieren nach**ausgewählt.

Zum Zeitpunkt der Symantec DLP-Incident-Erfassung wird diese Regel ausgeführt. Wenn mehrere Incidents denselben Richtliniennamen haben, wird der Incident unter dem ersten erfassten Incident konsolidiert, der dieser Regel entspricht.

4. Klicken Sie auf **Absenden**.
   Incidents, die basierend auf der Konsolidierungsregel konsolidiert wurden, sind in der Liste der untergeordneten Incidents im DLP-Analystenarbeitsbereich verfügbar.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Richten Sie die Fälligkeitsdatumsregeln für Ihre DLP-Incidents ein

Richten Sie die Regeln für das Fälligkeitsdatum der Antwort ein, um die Zeit zu bestimmen, in der die Endbenutzer auf die zugewiesenen Data Loss Prevention Incident Response (DLP-IR) Incidents reagieren können.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses Modul verwenden, um die Regeln für das Fälligkeitsdatum der Antwort für die verschiedenen Arten von DLP-Incidents und die Regeln zum Starten der Zählung des Fälligkeitsdatums zu definieren. Nach Ablauf des Fälligkeitsdatums werden die Benutzer über den überfälligen Incident benachrichtigt. Sie haben auch die Möglichkeit, den überfälligen Incident an einen der folgenden Orte zu eskalieren:

- Manager
- Benutzerdefinierter Benutzer aus Incident
- Benutzergruppe

Zum Beispiel, wenn Sie den überfälligen Incident an einen Manager eskalieren und maximal drei Eskalationsebenen angegeben haben. Die erste Ebene des Managers wird zuerst benachrichtigt. Wenn der Incident erneut überfällig ist, wird die zweite Ebene des Managers benachrichtigt, gefolgt von der dritten Ebene, wenn der Incident noch überfällig ist. Wenn der Manager einen Delegierten hat, hat der Manager die Möglichkeit, die Eskalation oder den überfälligen Incident dem Delegierten zuzuweisen.

Sie haben auch die Möglichkeit, mehrere Fälligkeitsdatumsregeln für Antworten zu erstellen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Regeln für Antwortfälligkeitsdatum**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular Antwortfälligkeitsdatum – Regel**

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel für das Fälligkeitsdatum der Antwort. |
| Aktiv | Option, um anzugeben, ob die Regel für das Fälligkeitsdatum der Antwort aktiv ist. |
| Fällig in (Tage) | Anzahl der fälligen Tage. |
| Fälligkeitsdatum ab | Startdatum, das zur Berechnung des Fälligkeitsdatums verwendet wird. Das Fälligkeitsdatum kann entweder ab dem Zeitpunkt berechnet werden, zu dem der Benutzer über den Incident benachrichtigt wurde, oder ab dem Datum der Incident-Zuweisung. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Notify vor dem Fälligkeitsdatum | Option, um den Endbenutzer vor dem Fälligkeitsdatum über den DLP-Incident zu benachrichtigen. |
| Notify am (Tage vor dem Fälligkeitsdatum) | Anzahl der Tage vor dem Fälligkeitsdatum, wenn die Regel eine Benachrichtigung an den Endbenutzer auslöst. |
| Beschreibung | Eindeutige Beschreibung für diese Regel für das Fälligkeitsdatum der Antwort. |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Regel für das Fälligkeitsdatum der Antwort zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Eskalation | Option zur Eskalation des DLP-Incident an jemanden, wenn das Fälligkeitsdatum der Antwort nicht eingehalten wurde. Weitere Informationen finden Sie unter Fügen Sie mehrere Benutzer hinzu, um auf DLP-Incidents zuzugreifen |
| Überfälligen Incident an eskalieren | Option, um anzugeben, ob der Incident an einen Manager, einen benutzerdefinierten Benutzer oder eine Benutzergruppe eskaliert werden soll.<br><br>Dieses Feld wird nur angezeigt, wenn die Option **Eskalieren** aktiviert ist. |
| Zuweisen mit | Geben Sie an, wie ein Manager identifiziert werden soll.<br><br>Dieses Feld wird nur angezeigt, wenn **Manager** im Feld **Überfälligen Incident eskalieren an** ausgewählt wird. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Maximale Eskalationsebenen | Option zum Definieren der maximalen Anzahl von Eskalationsstufen für einen Manager und einen benutzerdefinierten Benutzer.<br><br>Als Manager oder benutzerdefinierter Benutzer können Sie eine beliebige Anzahl von Eskalationsebenen definieren. Standardmäßig werden drei Eskalationsebenen bereitgestellt.<br><br>○ Als Manager können Sie eine beliebige Anzahl von Eskalationsebenen definieren, indem Sie den Wert in diesem Feld aktualisieren.<br>○ Als benutzerdefinierter Benutzer können Sie das Symbol + verwenden, um eine beliebige Anzahl von Eskalationsebenen zu definieren. |
| Benutzerdefiniertes Attribut | Option zum Angeben eines benutzerdefinierten Attributs aus dem Incident, der den Verweis auf einen Benutzer enthält.<br><br>Dieses Feld wird nur angezeigt, wenn **Benutzerdefinierter Benutzer aus Incident** im **Feld Überfälligen** Incident eskalieren an ausgewählt wird. |
| Benutzergruppe | Option zum Suchen und Auswählen einer Benutzergruppe, an die DLP-Incidents eskaliert werden sollen.<br><br>Dieses Feld wird nur angezeigt, wenn **Benutzergruppe** im Feld **Überfälligen Incident eskalieren an** ausgewählt wird.<br><br>**Hinweis:**<br>Sie können nur Gruppen anzeigen und auswählen, denen die Rolle sn_dlir.analyst zugewiesen wurde. |

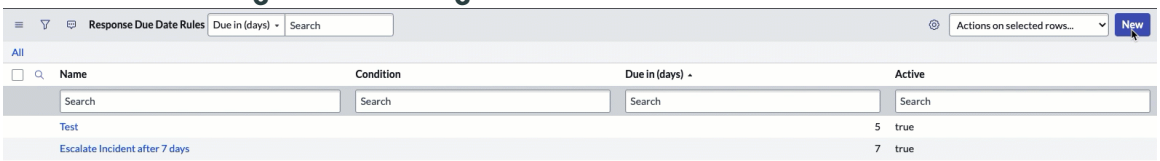


**Example**

Das folgende Beispiel zeigt die Regel für das Fälligkeitsdatum der Antwort, um zu bestimmen, wie viel Zeit Sie Ihren Endbenutzern geben möchten, um auf die zugewiesenen Data Loss Prevention Incident Response (DLP) Incidents zu reagieren. Nach der ersten Benachrichtigung des Endbenutzers liegt das Fälligkeitsdatum der Antwort in zwei Tagen. Der Condition Builder zeigt an, dass die Scan-Quelle mit dem Endpunkt-Dateisystem übereinstimmen muss, um mit der Erstellung des Fälligkeitsdatums der Antwort fortzufahren. Die Eskalationsoption ist ausgewählt. Der Incident wird an den Manager eskaliert, wenn das Fälligkeitsdatum der Antwort nicht eingehalten wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Richten Sie die Fälligkeitsdatumsregeln für Antworten ein




4. Klicken Sie auf **Absenden**.

### Fügen Sie mehrere Benutzer hinzu, um auf DLP-Incidents zuzugreifen

Verwenden Sie die Eskalationskettenfunktion, um allen an dem Incident beteiligten Benutzern den Zugriff auf die DLP-Incidents über die Listenansicht zu ermöglichen, auch wenn der Incident einem anderen Benutzer zugewiesen ist.

#### Vorbereitungen

Erforderliche Rolle:

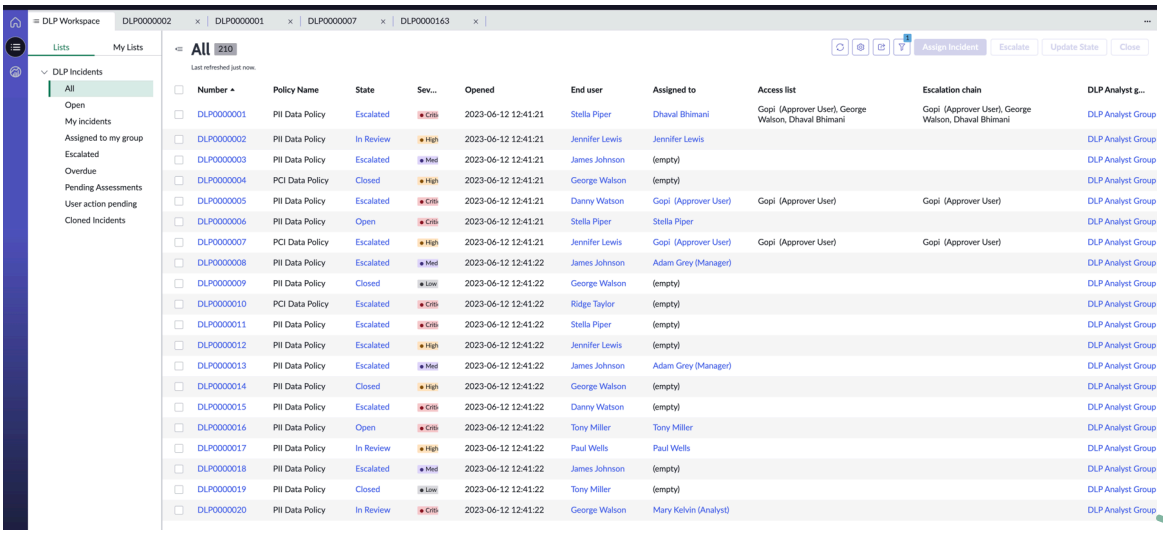
- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.read, sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

#### Prozedur

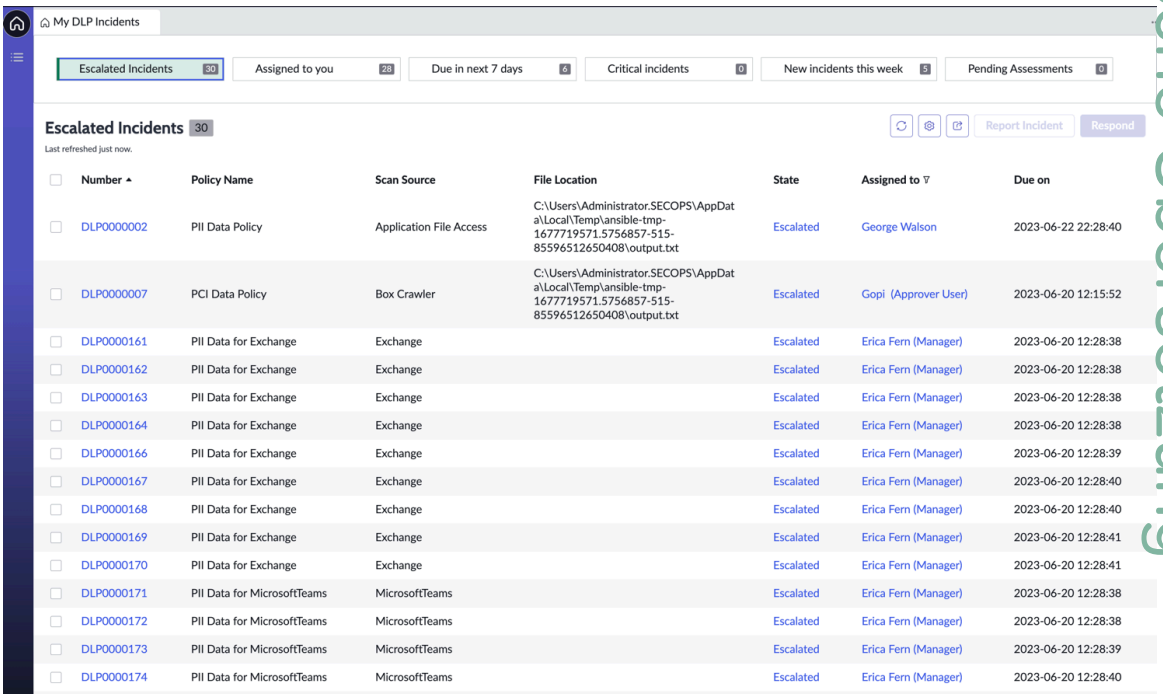
1. Navigieren zu **DLP** > **DLP-Analyst-Arbeitsbereich**.
   In der Listenansicht sollten die Benutzer und ihre Delegierten den DLP-Incident auf der Registerkarte **„Eskalierte** Incidents“ im Endbenutzerportal anzeigen können.
2. Öffnen Sie einen beliebigen Incident.
3. Klicken Sie auf die Schaltfläche **Eskalieren**, um einen Incident zu eskalieren.
4. Wählen Sie den Benutzer oder die Benutzergruppe aus der Dropdown-Liste aus.
   Sie können der Eskalationskette mehrere Benutzer hinzufügen. Alle Benutzer, die Zugriff haben, werden im Detailbereich der Formularansicht und auf der Registerkarte **Alle** Incidents aufgelistet. Die Eskalationskette wird basierend auf den Konfigurationseinstellungen angezeigt. Weitere Informationen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Data Loss Prevention Incident Response



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung wird der Incident einem Manager zugewiesen, der Endbenutzer kann den Incident jedoch weiterhin anzeigen.
6. Um dies zu überprüfen, navigieren Sie als Endbenutzer zum **DLP** -Benutzerarbeitsbereich.
   Alle Incidents, die dem Endbenutzer zugewiesen sind, werden angezeigt.
7. Zeigen Sie die Liste der eskalierten Incidents im Abschnitt **„Eskalierte Incidents** “ an.




Sie können die Benutzerzugriffsliste auch in der Listenansicht in der Spalte **Eskalationskette**anzeigen.

8. Öffnen Sie einen beliebigen Incident.
9. **Klicken** Sie auf die Schaltfläche Antworten, um die Antwort auf den Incident zu übermitteln.
10. Wählen Sie die Antwort aus der Dropdown-Liste aus.
11. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Konfigurieren Sie Genehmigungsregeln

Richten Sie Genehmigungsregeln ein, um Genehmigungen von verschiedenen Ebenen von Genehmigerbenutzern einzuholen, wenn eine erweiterte Antwortoption ausgewählt wird.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Genehmigungsregeln, um die Einwilligung zu von Endbenutzern gestellten Anforderungen für die Genehmigung des erweiterten Antworttyps zu erteilen. Der DLP-Administrator kann hier auch mehrere Genehmigungsebenen definieren.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Genehmigungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „DLP-Zuweisungsregel“.**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Genehmigungsregel. |
| Aktiv | Option, um anzugeben, ob die Genehmigungsregel aktiv ist. |
| Ausführungsbefehl | Priorität der Genehmigungsregel. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen.<br><br>Die Genehmigungsregel mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200, 300 usw.<br><br>Der Standardwert ist 100. |
| Beschreibung | Eindeutige Beschreibung für die Genehmigungsregel. |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Genehmigungsregel zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br>Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung als **Integrationsquelle**, **enthält**, **Microsoft**auswählen. |
| Gilt für Antwortoptionen | Option zur Auswahl der Antwortoption vom Typ „Erweitert“.<br>Sie können mehrere Antwortoptionen auswählen. |
| Genehmigende Person | Wählen Sie aus, welchen Typ des genehmigenden Benutzers Sie festlegen möchten.<br>○ **Benutzertabelle**: Wählen Sie diese Option aus, wenn Sie den genehmigenden Benutzer aus der Benutzertabelle (sys_user) auswählen möchten.<br>○ **Benutzerdefinierte Genehmigungsliste**: Wählen Sie diese Option aus, wenn Sie mehrere benutzerdefinierte Genehmigerebenen für eine einzelne Anforderung konfigurieren möchten |
| Bezeichner des Genehmigers | Dieses Feld wird angezeigt, wenn **Benutzertabelle** für die **Genehmigeroption** ausgewählt ist.<br>Wählen Sie das Feld aus, um den Genehmiger aus der Benutzertabelle (sys_user) zu identifizieren. |
| Anzahl der Ebenen | Dieses Feld wird angezeigt, wenn **Benutzertabelle** für die **Genehmigeroption** ausgewählt ist.<br>Endnummer in diesem Feld, um die Genehmigungsebenen zu definieren.<br>Beispiel: Wenn im Feld „Anzahl der Ebenen“ 3 hinzugefügt wird und im Feld „Genehmigerbezeichner“ die Option „Manager“ ausgewählt wird, durchläuft |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | die Genehmigungsanforderung drei Genehmigungsebenen. |

Das folgende Beispiel zeigt die Genehmigungsregel, die für eine der erweiterten Antwortoptionen erstellt wurde. Die Bedingung erfordert, dass der Name der Integrationsquelle das Microsoft-Schlüsselwort enthält, das dann diese Konfiguration auslöst.

4. **Wählen** Sie für die Option Genehmiger die Option **Benutzerdefinierte Genehmigungsliste**aus.
5. Klicken Sie auf **Absenden**.
6. Die zugehörige Liste „**Genehmigungsebenen** “ wird in der Formularansicht ausgefüllt.
7. Klicken Sie im Abschnitt **Genehmigungsebenen** auf **Neu**.
8. Füllen Sie die Felder des Formulars aus.

**Formular „Genehmigungsebene“**

| Feld | Beschreibung |
|---|---|
| Name | Name für die Genehmigungsebene. |
| Aktiv | Option, um anzugeben, ob die Genehmigungsebene aktiv ist. |
| level | Die Ebene für die Genehmigungsregel. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsebenen ausgeführt werden, wenn zwei oder mehr Ebenen konfiguriert sind.<br><br>Die Genehmigungsebene mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Geben Sie einen Wert ein, um die Vorgangsebene festzulegen. Zum Beispiel 100, 200, 300 usw.<br><br>Der Standardwert ist 100. |
| Genehmigungsregel | Genehmigungsregel, für die Sie diese Konfiguration definieren möchten.<br><br>Dies ist ein schreibgeschütztes Feld. |
| Beschreibung | Eindeutige Beschreibung für die Genehmigungsregel. |
| Genehmigungen erforderlich | Wählen Sie diese Option aus, um zu definieren, ob die Genehmigung von allen konfigurierten Benutzern/Gruppen oder nur von einem Benutzer erforderlich ist. |
| Genehmiger | Option zum Auswählen der Genehmiger. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **a.** Benutzer und Gruppen:<br>**i. Benutzer**: Klicken Sie auf das hinzufügen“, um einen bestimmten Benutzer aus der Liste hinzuzufügen. Sie können einen Benutzer auch über seine E-Mail-Adresse oder Suchoption hinzufügen.<br>Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das hinzufügen.<br>**ii. Gruppen**: Klicken Sie auf<add_icon> Symbol, um eine bestimmte Gruppe aus der Liste hinzuzufügen. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen.<br>**b. Suchen mit Skript**: Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Genehmigungsebene anzupassen und zu formatieren. Beispielsweise können Sie das E-Mail-Adressfeld verwenden, um den genehmigenden Benutzer zu identifizieren. |

**9.** Klicken Sie auf **Absenden**.

## Erstellen und verwalten Sie Benutzeranweisungen für DLP-Incidents

Erstellen und verwalten Sie Vorlagen für Benutzeranweisungen für DLP-Incidents, damit die Benutzer die Anweisungen zur Lösung von Incidents und die nächsten Schritte des Lösungsprozesses verstehen.

### Vorbereitungen

Die Kartenvorlage „Benutzeranweisungen“ zeigt zwei verschiedene Header an, die weitere Informationen zu einem bestimmten Incident in der Formularansicht enthalten.

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Wenn dem Endbenutzer ein Incident zugewiesen wird, muss der Benutzer möglicherweise die zusätzlichen Anweisungen zur Reaktion auf die Incidents kennen, die Benutzer in die Terminologie einführen und zusätzliche Informationen zum Incident bereitstellen. Diese Vorlagen können die Benutzer anleiten, um eine genaue Antwort auf die DLP-Incidents bereitzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Vorlagen für Benutzeranweisungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

#### DLP-Incident-Bewertung

| Feld | Beschreibung |
|---|---|
| Name | Name der Benutzeranweisungsvorlage. |
| Kurzbeschreibung | Eindeutige Beschreibung dieser Benutzeranweisungsvorlage. |
| Aktiv | Option, um anzugeben, ob die Benutzeranweisungsvorlage aktiv ist. |
| Ausführungsbefehl | Priorität der Incident-Benutzeranweisungsvorlage. Dieses Feld gibt die Reihenfolge an, in der die Reihenfolge ausgeführt wird, um die Benutzeranweisungsvorlage auszuwerten, wenn ein Incident erstellt wird.<br>Die Option mit der niedrigsten Nummer hat die höchste Priorität.<br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl.<br>Der Standardwert ist 100. |
| Incidents, die der Bedingung entsprechen | Incidents, die den im Bedingungsgenerator definierten Bedingungen entsprechen, werden angezeigt.<br>Diese Bedingungen basieren auf den DLP-Incident-Daten. Um eine Bedingung für eine Benutzeranweisung zu erstellen, wählen Sie eines der Incident-Felder aus.<br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder ODER:<br>Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt sein. Wenn OR ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Betrifft | Wählen Sie den Benutzer oder die Benutzergruppen aus, für die die Vorlage gilt. Die anderen verfügbaren Optionen sind:<br>○ **Alle Endbenutzer**: Aktivieren Sie dieses Kontrollkästchen, wenn die Anweisungsvorlage für alle Benutzer gilt.<br>○ **Alle Prüfer eskalierter Incidents**: Aktivieren Sie dieses Kontrollkästchen, wenn die Vorlage für alle Prüfer der eskalierten Incidents gilt.<br>○ **Bestimmte Benutzer**: Klicken Sie auf das Symbol, um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den die DLP-Incident-Bedingungen gelten. Sie können einen Benutzer auch über seine E-Mail-Adresse oder Suchoption hinzufügen. Beispiel: Manager der Rechtsabteilung.<br>Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das Symbol **Mich** hinzufügen.<br>○ **Bestimmte Benutzergruppen**: Klicken Sie auf das Symbol, um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die die DLP-Incident-Bedingungen gelten. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller. |
| Anweisungen Vorlage: Anweisungen | Fügen Sie Anweisungen im Rich-Text-Editor mit Variablen hinzu, die auf Incident-Ebene verfügbar sind. |

4. Führen Sie einen Drilldown zum Abschnitt „ **Anweisungsvorlage** “ durch, geben Sie die Vorlagenanweisung ein, und fügen Sie bei Bedarf Informationen auf Incident-Ebene in diesem Abschnitt hinzu.
5. Verschieben Sie die erforderlichen Variablen per Drag-and-Drop, um bestimmte Felder dynamisch anzuzeigen.
6. Klicken Sie auf **Absenden**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Benutzeranweisungensvorlagen werden jetzt erstellt, und Sie können auf eine beliebige Benutzeranweisungskopfzeile klicken, um die zusätzlichen Details eines DLP-Incidents zu erfahren.

Weitere Informationen finden Sie unter Data Loss Prevention Incident Response Benutzerarbeitsbereich.

### Konfigurieren Sie DLP-UI-Benutzeranweisungen

Konfigurieren Sie die System-UI-Nachrichten, um nach Bedarf detaillierte Benutzeranweisungen hinzuzufügen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren zu **Alle** > **System-UI** > **Nachrichten**.
2. Suchen Sie nach **user_instruction_card_heading**.

   Standardmäßig sind user_instruction_card_heading und user_instruction_modal_window_heading die beiden UI-Nachrichtenkonfigurationen, die den Benutzern bereitgestellt werden.
3. Klicken Sie auf eine der Benutzeranweisungen, um sie zu aktualisieren oder zu ändern.

## Erstellen und verwalten Sie E-Mail-Vorlagen für Ihre DLP-Incidents

Erstellen und verwalten Sie die vorkonfigurierten E-Mail-Vorlagen zum Senden von Benachrichtigungen an Endbenutzer, Benutzergruppen oder Manager. Mit diesen Vorlagen können Sie Ihre Endbenutzer über die Incidents von Data Loss Prevention Incident Response (DLP IR) beraten und mit ihnen kommunizieren.

**Vorbereitungen**
Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

> **Wichtig:**
> Damit Analysten die E-Mail-Kommunikation eines DLP-Incident im Aktivitätenstrom anzeigen können, sollten Sie die Rolle „sn_dlir.analyst“ in der globalen Systemeigenschaft glide.ui.activity.email_roleshinzufügen oder anfügen.

**Warum und wann dieser Vorgang ausgeführt wird**
E-Mail-Benachrichtigungen werden nach Incident-Benachrichtigungen, die an die Endbenutzer gesendet werden, Eskalationsbenachrichtigungen, die an die Manager gesendet werden, oder Fälligkeitsdatumsbenachrichtigungen kategorisiert. Sie können E-Mail-Benachrichtigungen über die Fälligkeitsdaten für DLP-Incidents senden oder die Endbenutzer darüber informieren, was zu tun ist, wenn bestimmte Bedingungen im E-Mail-Bedingungsfilter erfüllt sind.
Mit DLP-E-Mail-Vorlagen können Sie die E-Mail-Benachrichtigung für Endbenutzer, Manager und Analysten senden. Sie können die Vorlagen so konfigurieren, dass sie pro Incident oder als Digest gesendet werden. Betreff und Text Ihrer E-Mail können Variablen enthalten, sodass Sie Ihren vorhandenen Inhalt wiederverwenden können.

DLP stellt basierend auf den Kategorien die folgenden vorkonfigurierten E-Mail-Vorlagen bereit:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **DLP-E-Mail-Vorlage – Pro Incident-Genehmigungsbenachrichtigung:** Benachrichtigen Sie Benutzer über die Genehmigung ihrer Anforderungen.
- **DLP-E-Mail-Vorlage – Eskalationsbenachrichtigung:** Senden Sie Eskalationsbenachrichtigungen in Form von Digests an Manager.
- **DLP-E-Mail-Vorlage – Benachrichtigung über ausstehende Genehmigung:** Benachrichtigen Sie Genehmiger über ausstehende Elemente.
- **DLP-E-Mail-Vorlage – Stornierungsbenachrichtigung pro Incident-Genehmigungsanforderung:**Benachrichtigt Benutzer über eine Genehmigungsanforderung, die vom DLP-Analystenteam abgebrochen wurde.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Abschluss der Benutzerantwort:** Benachrichtigen Sie das DLP-Analystenteam über die von Benutzern übermittelte Antwort.
- **DLP-E-Mail-Vorlage – Anwender-Incident-Benachrichtigung:**Dies ist eine Standardvorlage für Anwender-Digest-Benachrichtigungen. Senden Sie Incident-Benachrichtigungen alle paar Tage in Form von Digests an die Endbenutzer, auch wenn keine neuen Incidents vorhanden sind, um die Benutzer über die Gesamtzahl der Incidents im Namen des jeweiligen Benutzers zu informieren. Sie können auch Digest-Benachrichtigungen senden, um die Benutzer über die nächsten bevorstehenden Fälligkeitsdaten von DLP-Incidents mit dem Schweregrad „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ zu informieren.
- **DLP-E-Mail-Vorlage – Pro Incident-**Benachrichtigung über ausstehende Genehmigung: Benachrichtigen Sie Genehmiger über ausstehende Genehmigungen.
- **DLP-E-Mail-Vorlage – Ablehnungsbenachrichtigung:** Senden Sie die Ablehnungsbenachrichtigung an die anfordernde Person.
- **DLP-E-Mail-Vorlage – Fälligkeitsdatumsbenachrichtigung:** Senden Sie eine Benachrichtigung über das Fälligkeitsdatum für Incidents. Wenn dem Endbenutzer ein DLP-Incident zugewiesen wird und der Endbenutzer vor dem Fälligkeitsdatum keine Maßnahmen ergriffen hat, wird eine E-Mail-Benachrichtigung an den Endbenutzer gesendet. Sie haben auch die Möglichkeit, den DLP-Incident an einen Manager, einen benutzerdefinierten Benutzer oder eine Benutzergruppe zu eskalieren, wenn das Fälligkeitsdatum der Antwort nicht eingehalten wurde.

  **Hinweis:**
  Fälligkeitsdatumsbenachrichtigungen müssen in Form von Digests vorliegen.

- **DLP-E-Mail-Vorlage – Benachrichtigung über Benutzerantwort pro Incident:** Benachrichtigen Sie Analysten über die von Benutzern übermittelte Antwort pro Incident.
- **DLP-E-Mail-Vorlage – Pro Incident-Eskalationsbenachrichtigung:** Benachrichtigen Sie Manager über Eskalationen pro Incident.
- **DLP-E-Mail-Vorlage – Benachrichtigung pro Incident-Benutzer:** Benachrichtigt Benutzer über die Zuweisung pro Incident.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **E-Mail-Vorlagen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Formular „DLP-E-Mail-Vorlage“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der E-Mail-Vorlage. |
| Aktiv | Option, um anzugeben, ob die DLP-E-Mail-Vorlage aktiv ist. Wenn diese Option nicht aktiviert ist, werden für diese E-Mail-Vorlage keine Benachrichtigungen gesendet. |
| Kategorie | E-Mail-Benachrichtigungskategorie. DLP unterstützt die folgenden Optionen:<br>○ **Incident-Benachrichtigung an Endbenutzer**: Wird gesendet, wenn die Incidents den Endbenutzern zugewiesen werden.<br>○ **Eskalationsbenachrichtigung an Manager**: Wird gesendet, wenn das Fälligkeitsdatum der Antwort überschritten wird, oder dem Manager manuell über das DLP Ops-Portal zugewiesen werden.<br>○ **Benachrichtigung über Fälligkeitsdatum**: Wird gesendet, wenn das Fälligkeitsdatum der Antwort überschritten wird.<br>○ **Benutzerantwortbenachrichtigung an Analysten**: Wird gesendet, wenn der Endbenutzer eine Aktion für den DLP-Incident durchführt.<br>○ Benachrichtigung über ausstehende**Genehmigungen**: Benachrichtigen Sie Genehmiger über ausstehende Elemente.<br>○ **Genehmigungsbenachrichtigung an die anfordernde**Person: Benachrichtigen Sie Benutzer über die Genehmigung ihrer Anforderungen.<br>○ **Benachrichtigung an anfordernde**Person ablehnen: Benachrichtigen Sie Benutzer über die Ablehnung ihrer Anforderungen.<br>○ Stornierungsbenachrichtigung an**anfordernde**Person: Benachrichtigt Benutzer über die Stornierung ihrer Anforderungen. |
| Typ | Option, um anzugeben, ob die E-Mail pro Incident oder als Digest gesendet wird.<br>**Hinweis:**<br>Wenn Sie im Feld **Kategorie** die Option **Fälligkeitsdatumsbenachrichtigung** ausgewählt haben, können Sie nur Digests verwenden. Wählen Sie diese Option aus. |
| Beschreibung | Eindeutige Beschreibung für diese E-Mail-Vorlage. |
| Ausführungsbefehl | E-Mail-Vorlagenpriorität. Dieses Feld gibt die Reihenfolge an, in der die E-Mail-Vorlagen ausgeführt werden, wenn zwei oder mehr E-Mail-Vorlagen die Auslösebedingungen gemeinsam nutzen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Die E-Mail-Vorlage mit der niedrigsten Nummer hat die höchste Priorität. Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl. Der Standardwert ist 100. |
| Vorlagenbedingung | Optionen in den Vorlagenbedingungen, die auf der DLP-Incident-Tabelle basieren. Sie können eines der Incident-Felder zum Erstellen der Auslöserbedingung für die E-Mail-Vorlage auswählen.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Zielbenutzer | Zielbenutzer für die Vorlage, wenn die Bedingungen erfüllt sind. Die Zielbenutzer können eine der folgenden sein:<br>○ **Alle Empfänger**: Senden Sie die E-Mail an Zielbenutzer.<br>○ **Empfänger in der Gruppe:** Senden Sie die E-Mail mithilfe der Filteroption nur an Empfänger innerhalb einer bestimmten Gruppe.<br>○ **Empfänger, die den Kriterien entsprechen**: Senden Sie die E-Mail an Zielbenutzer, die die Kriterien erfüllen. Sie können den Filter verwenden, um Zielbenutzer basierend auf den Bedingungen aufzuschlüsseln. Beispiel: Stadt. |
| E-Mail-Vorlage | E-Mail-Vorlage, die Sie auswählen können. Sie können die Variablen definieren, um vorhandene Inhalte wiederzuverwenden und der E-Mail-Benachrichtigung hinzuzufügen.<br><br>Die Felder **Kategorie** und **Typ** bestimmen die Variablen, die zur Auswahl verfügbar sind. Angenommen, die E-Mail-Kategorie ist auf Incident-Benachrichtigung festgelegt und der E-Mail-Typ ist ein Digest. Die |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Variablen für die Auswahl sind Digest-Felder, um die Anhäufung mehrerer DLP-Incidents zu berücksichtigen.<br><br>Hier ist ein E-Mail-Text-HTML-Beispiel für jede E-Mail-Vorlage:<br><br>○ **Standardvorlage für Pro Incident-Genehmigungsbenachrichtigung**:<br><br>`Dear ${respondent.first_name},`<br><br>`Your request "${end_user_response}" on the incident ${number} has been approved.`<br><br>`- Date protection team`<br><br>○ **Benachrichtigung über Stornierung pro Incident-Genehmigungsanforderung**<br><br>`Dear ${respondent.first_name},`<br><br>`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`<br><br>`No action is required from you at this point. Data protection team will contact you for any further information required.`<br><br>`- Data protection team`<br><br>○ **Standardvorlage für Fälligkeitsdatumsbenachrichtigung**:<br><br>`Dear ${target_user.name},`<br><br>`Following incidents require your response.`<br><br>`${due_days_table}`<br><br>`- Data protection team`<br><br>○ **Standardvorlage für Benutzerbenachrichtigung pro Incident**:<br><br>`Dear ${assigned_to.name},`<br><br>`DLP Incident ${number} is assigned to you.`<br><br>`Please review and submit your response.`<br><br>`- Data protection team`<br><br>○ **Standardvorlage für Benutzer-Incident-Benachrichtigung**:<br><br>`Hello ${target_user.name},` |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication.<br><br>Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}.<br><br>Please log in to the ${link_to_dlp_portal} and submit your response.<br><br>- Data protection team |
| | ○ **Standardvorlage für Eskalation – Digest**:<br>Hi ${target_user.name},<br><br>The following data security incidents have been escalated to you due to lack of response from the assignees.<br><br>Please login to the incident response workspace to review the incidents and submit your response.<br><br>${overdue_table}<br><br>- Data protection team |
| | ○ **Standardvorlage für Eskalation – Pro Incident**:<br>Dear ${assigned_to.name},<br><br>Data security incident ${number} has been escalated to you.<br><br>Please review and submit your response or assign the incident back to the user.<br><br>- Data protection team |
| | ○ **Standardvorlage für Benachrichtigung über ausstehende Genehmigung**:<br>Dear ${approver.first_name},<br><br>Your approval is required for a few requests on data security incidents.<br><br>Please login to the workspace here and review the requests.<br><br>- Data protection team |
| | ○ **Standardvorlage für Benachrichtigungen über ausstehende Genehmigung pro Incident**: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Dear ${Approver},<br><br>Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}.<br><br>Please visit this here to approve or reject the request.<br><br>- Data Protection Team<br><br>○ **Standardvorlage für Pro Incident-Ablehnungsbenachrichtigung**:<br><br>Dear ${respondent.first_name} ${respondent.last_name},<br><br>This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected.<br><br>Please review the incident here.<br><br>- Data protection team<br><br>○ **Standardvorlage für Pro Incident-Anwenderantwortbenachrichtigung**:<br><br>Hi ${assigned_to.name},<br><br>This is to inform you that a response has been submitted for the DLP Incident ${number}.<br><br>○ **Standardvorlage für Benachrichtigung über Abschluss der Benutzerantwort**:<br><br>Hello ${target_user.name},<br><br>This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication.<br><br>Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}. |

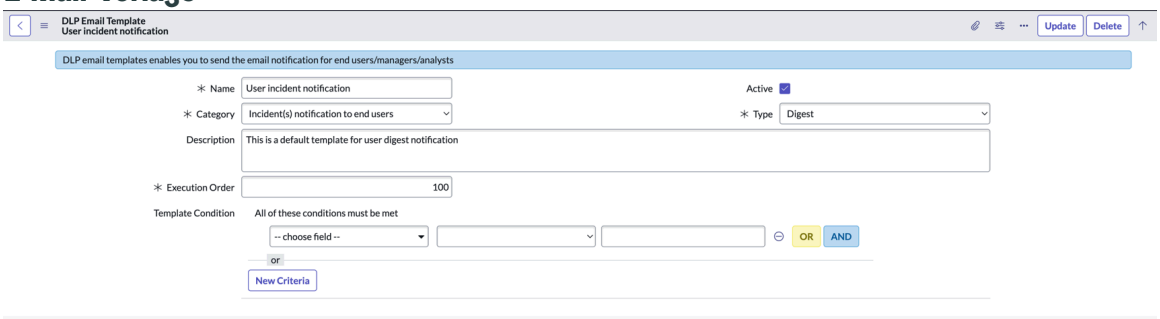
**Example**

Das folgende Beispiel zeigt die DLP-E-Mail-Vorlage mit den Zielbenutzern, die als alle Empfänger definiert sind.

Automatische Übersetzung

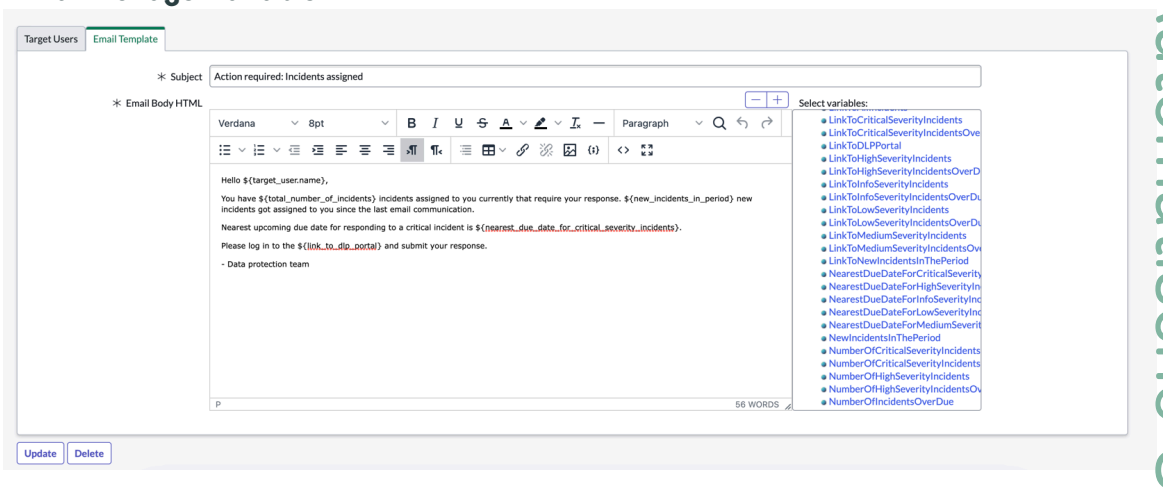
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**E-Mail-Vorlage**




Das folgende Beispiel zeigt eine E-Mail-Vorlage mit dem Betreff „Benutzer-Incident-Benachrichtigung“ und einer Variablen *new_incidents_in_period*. Der E-Mail-Text enthält mehrere Variablen, die aus der Spalte Variablen auswählen hinzugefügt werden.

**E-Mail-Vorlagenvariablen**




4. Klicken Sie auf **Absenden**.

### Ergebnisse

Der Endbenutzer erhält eine Digest-Benachrichtigung per E-Mail mit allen ausgewählten Variablenfeldern in der Vorlage.

## Erstellen und verwalten Sie Bewertungen für DLP-Incidents

Erstellen und verwalten Sie Bewertungen, damit Endbenutzer auf DLP-Incidents reagieren können. Sie können die Bewertungen verwenden, um Informationen über die vertraulichen Daten zu sammeln, die in den DLP-Incidents verfügbar gemacht wurden oder durch die sie weitergegeben wurden.

Bewertungen für DLP-Incidents

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

DLP-Incident-Bewertungen helfen Ihnen, potenzielle Bedrohungen und Schwachstellen für Ihre Daten basierend auf der Reaktion des Endbenutzers zu identifizieren. Sie können diese

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen verwenden, um die vorhandenen Lücken, Bedenken und Erwartungen Ihrer Endbenutzer zu ermitteln.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Bewertungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**DLP-Incident-Bewertung**

| Feld | Beschreibung |
|---|---|
| Name | Name der DLP-Incident-Bewertung. |
| Aktiv | Option, um anzugeben, ob die DLP-Incident-Bewertung aktiv ist. |
| Beschreibung | Eindeutige Beschreibung für diese DLP-Incident-Bewertung. |
| Einführung in die Bewertung | Geben Sie eine Einführung oder einen Kontext für Ihre Bewertung an. Sie können auch Variablen aus dem Abschnitt Variablen auswählen verwenden, um bestimmte Felder dynamisch anzuzeigen. |

4. Klicken Sie auf **Absenden**.
5. Öffnen Sie nach dem Erstellen einer Bewertung die Bewertung, und klicken Sie auf **Bewertungsdesigner**.
6. Wählen Sie im Abschnitt „Neue Bewertung“ im Abschnitt „Steuerungen“ einen Typ von Bewertungsfrage aus.
7. Verschieben Sie den erforderlichen Bewertungsfragetyp per Drag-and-Drop in den Abschnitt Neue Bewertung.
   Beispielsweise können Sie das Auswahlsteuerelement per Drag-and- **Drop** unter den Abschnitt „Neue Bewertung“ oder „Neue Kategorie“ verschieben.
8. Um weitere Kategorien für die Bewertung hinzuzufügen, klicken Sie auf das hinzufügen.
9. Um eine vorhandene Kategorie zu ändern, klicken Sie auf das hinzufügen.
10. Nachdem Sie die verschiedenen Bewertungsfragen zum ersten Mal erstellt haben, klicken Sie auf **Speichern**und dann auf **Veröffentlichen**.

## Richten Sie Optionsregeln für die Reaktion auf Incidents für Ihre DLP-Incidents ein

Richten Sie die Optionsregeln für die Reaktion auf Incidents ein, die Endbenutzer oder Analysten bei der Reaktion auf einen Incident verwenden können.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Sie können die Art der Reaktion konfigurieren, die ein Endbenutzer basierend auf der Art des DLP-Incident ausführen soll. Die Basissystem-Anwendung „DLP Incident Response“ bietet die folgenden Antwortoptionen für Benutzer:

- Bewertung abgeschlossen
- Gelöschter Inhalt
- Gelöschte Datei
- Verschlüsselte Datei
- Maskierter Inhalt
- Falsch positives Ergebnis melden
- Falschen Besitzer melden
- Erforderlich für Geschäftsprozess
- Überprüfte Berechtigungen

Angenommen, ein Endbenutzer meldet einen DLP-Incident als falsch positiv. Der Status für diesen Incident wird dann automatisch als „Geschlossen“ markiert, da der von Ihnen konfigurierte Zielstatus „Geschlossen“ ist.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Optionsregeln für die Reaktion auf Incidents**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Optionsregeln für Reaktion auf Incidents“**

| Feld | Beschreibung |
|---|---|
| Name | Name der Option zur Reaktion auf Incidents. |
| Aktiv | Option, um anzugeben, ob die Option zur Reaktion auf Incidents aktiv ist. |
| Ausführungsbefehl | Priorität der Option zur Reaktion auf Incidents. Dieses Feld gibt die Reihenfolge an, in der die Incident-Antwortoptionen ausgeführt werden, wenn zwei oder mehr Incident-Antwortoptionen die Auslösebedingungen gemeinsam nutzen.<br><br>Die Incident-Antwortoption mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl.<br><br>Der Standardwert ist 100. |
| Beschreibung | Eindeutige Beschreibung für diese Option zur Reaktion auf Incidents. |
| Standardmäßiger Zielstatus | Der von Ihnen konfigurierte Standardzielstatus. |

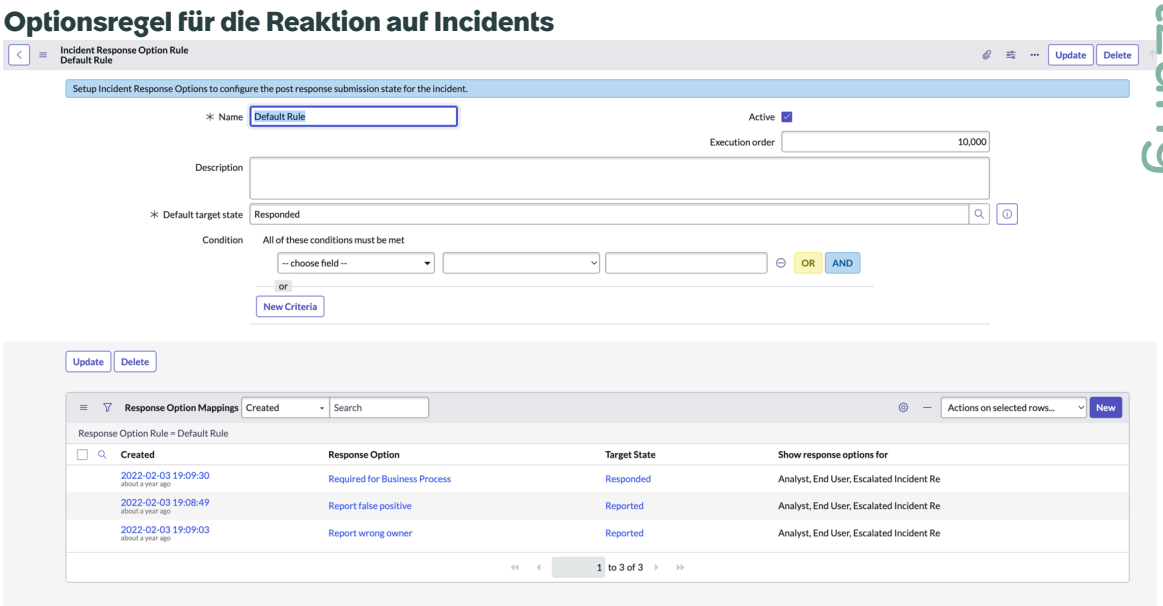


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Bedingung | Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Incident-Antwortoptionen zu erstellen, wählen Sie eines der Incident-Felder aus.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**:<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |

### Example

Das folgende Beispiel zeigt die Konfiguration der Endbenutzeraktion für einen Endpunkt. Die Bedingung erfordert, dass die Scan-Quelle ein Endpunkt-Dateisystem ist, das dann diese Endbenutzeraktionskonfiguration auslöst. Die Zuordnung zeigt, dass die Antwortoptionen für den Endbenutzerfalscher Besitzer des Berichts, falsch positiver Bericht und gelöschte Datei sind.






© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie im Abschnitt **Antwortoptionszuordnungen** auf **Neu**.
5. Füllen Sie die Felder des Formulars aus.

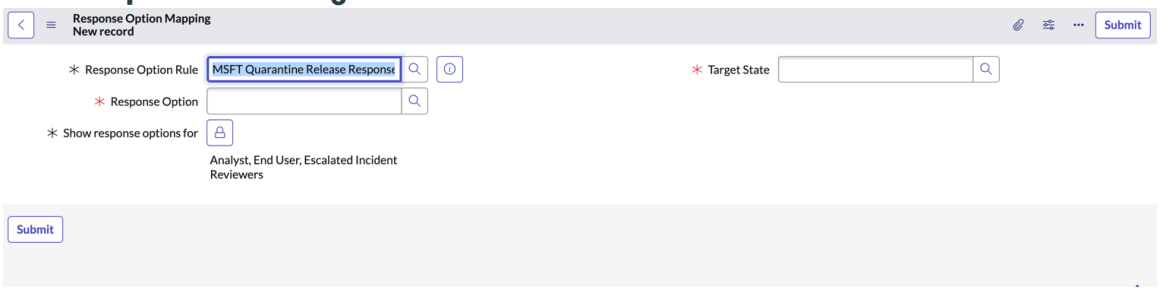
**Formular „Antwortoptionszuordnung“.**

| | |
|---|---|
| Antwortoptionsregel | Name der Optionsregel für die Reaktion auf Incidents. Zum Beispiel impliziert SharePoint, dass die Scan-Quelle SharePoint ist. Sie können entweder den Namen der Incident-Antwort eingeben oder mithilfe der Suche nachschlagen. |
| Antwortoption | Option zur Auswahl der Antwortoption. Sie können entweder die Antwortoption eingeben oder mithilfe der Suche nachschlagen. |
| Zielstatus | Der Zielstatus des DLP-Incident, nachdem der Endbenutzer die entsprechende Aktion ausgewählt hat.<br>**Hinweis:**<br>a. Das Feld Zielstatus wird nur **angezeigt**, wenn Sie **Antwortoption** auswählen, deren Typ den **Typ: Standard**hat. Weitere Informationen zur Konfiguration der Zielstatustypen finden Sie unter Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents.<br>b. Wenn eine Antwortoption vom **Typ „Erweitert** “ ausgewählt ist, können Sie den Zielstatus nicht festlegen und wird ausgeblendet. Der Zielstatus wird basierend auf dem benutzerdefinierten Status zugewiesen, der im Flow Designer-Subflow konfiguriert wurde. |
| Antwortoptionen für anzeigen | Option zum Bestimmen der Benutzerrollen, für die die Antwortoptionen angezeigt werden sollen.<br>Mit der Option zum Entsperren können Sie zwischen **Analyst**, **Endbenutzer**und **eskalierten Analystenüberprüfern** wählen. Sie können eine oder alle Rollen auswählen. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Antwortoptionszuordnungsaktion**




6. Klicken Sie auf **Absenden**.

### Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents

Verwenden Sie diese Funktion, um die Art der Antwort zu konfigurieren, die ein Endbenutzer oder Analyst ausführen soll.

**Vorbereitungen**

Die Basissystem-Anwendung „DLP Incident Response“ bietet die folgenden Antwortoptionen:

1. Bewertung abgeschlossen
2. Gelöschter Inhalt
3. Gelöschte Datei
4. Verschlüsselte Datei
5. Maskierter Inhalt
6. Falsch positives Ergebnis melden
7. Falschen Besitzer melden
8. Fordern Sie die E-Mail-Freigabe aus der Quarantäne an

   **Hinweis:**
   Diese Option ist für die DLP Microsoft Exchange-Datensätze verfügbar.

9. Erforderlich für Geschäftsprozess
10. Überprüfte Berechtigungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

**Prozedur**

1. Navigieren zu **Alle** > **DLP-Administration** > **Antwortoptionen**.

   Standardmäßig bietet das Basissystem zwei Arten von Antwortoptionen:

   a. **Einfach**: Eine manuelle Antwortoption, die vom Benutzer übermittelt wird.

   b. **Erweitert**: Eine automatisierte Antwortoption löst einen Flow Designer-Subflow aus, wenn der Benutzer die Antwortoption übermittelt.

2. Klicken Sie auf **Neu**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**3.** Füllen Sie die Felder des Formulars aus.

### Antwortoptionsformular vom Typ: Standard

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie den Namen der Option für die Reaktion auf Incidents ein. |
| Typ | Option zum Auswählen des Antwortoptionstyps. |

### Antwortoptionsformular vom Typ: Erweitert

| Feld | Beschreibung |
|---|---|
| Name | Geben Sie den Namen der Option für die Reaktion auf Incidents ein. |
| Typ | Option zur Auswahl der Antwortoption. Standardmäßig werden in diesem Feld die folgenden zwei Arten von Optionen angezeigt:<br>○ **Einfach**: Wenn Sie diese Option beim Erstellen einer neuen Antwortoption auswählen, müssen Sie möglicherweise einen Antwortoptionsnamen und den Typ hinzufügen.<br>○ **Erweitert**: Wenn Sie diese Option auswählen, können Sie die folgenden Felder auswählen:<br>▪ **Flow**: Wählen Sie den Flow Designer-Subflow aus.<br>▪ **MID-Server erforderlich**: Aktivieren Sie dieses Kontrollkästchen, wenn der ausgewählte Flow den MID-Server verwendet. |
| Flow | Wählen Sie den erforderlichen Flow Designer-Flow aus, um die MID-Anwendung und die MID-Fähigkeit zu aktivieren.<br>Wenn Sie einen Subflow für die Antwortoption erstellen, fügen Sie die folgenden Subflow-Eingaben hinzu:<br>**a. Name**:<br>▪ dlp_incident<br>▪ mid_server_capability<br>▪ mid_server_application<br>**b. Typ**:<br>▪ Referenz (zur DLP-Incident-Tabelle)<br>▪ Sys-ID für MID Server-Anwendung und MID Server-Fähigkeit |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

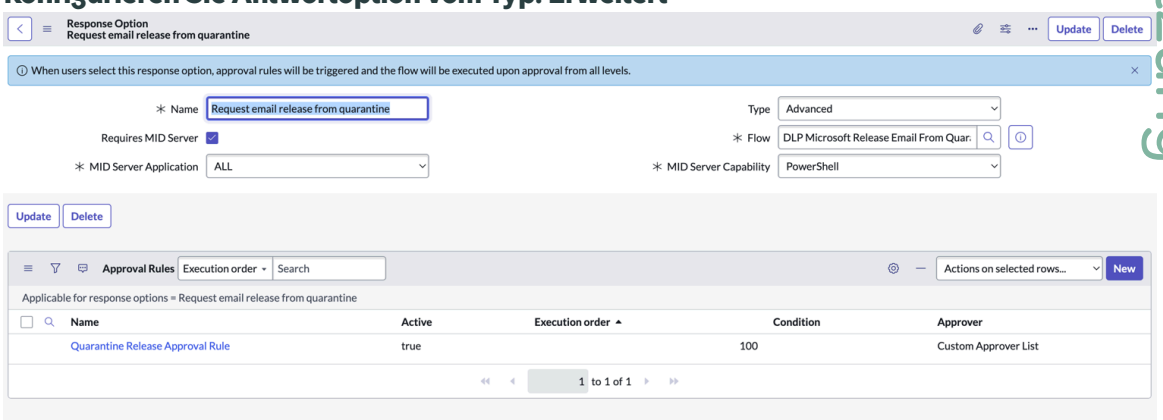
| Feld | Beschreibung |
|---|---|
| Erfordert MID-Server | Option zum Bestimmen der MID-Server-Konfiguration. Durch Aktivieren der Felder **Erfordert MID Server** -Kontrollkästchen **MID Server-Anwendung** und **MID Server-Fähigkeit** können Sie die MID-Anwendung und die MID-Fähigkeit konfigurieren.<br>**Hinweis:** Basierend auf der MID-Server-Anwendungs- und MID-Server-Fähigkeitskonfiguration und wenn ein MID ausgeführt wird, ist nur die Antwortoption im Arbeitsbereich sichtbar. |
| MID-Server-Anwendung | Wählen Sie die erforderliche MID Server-Anwendung aus der Dropdown-Liste aus. |
| MID-Server-Fähigkeit | Wählen Sie die erforderliche MID Server-Fähigkeit aus der Dropdown-Liste aus. |

**Hinweis:**
Wenn für die ausgewählte MID Server-Fähigkeit kein MID Server verfügbar ist, ist die Antwortoption nicht sichtbar. Wenn Sie einen bestimmten MID-Server aus der Liste auswählen möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Anschließend muss mindestens ein konfigurierter MID-Server in den ausgewählten MID-Anwendungen ausgeführt werden und über verfügen ausgewählte MID Server-Fähigkeit.

4. Klicken Sie auf **Absenden**.

**Hinweis:**
Wenn Sie eine **erweiterte** Antwortoption erstellen, wird die zugehörige Liste „**Genehmigungsregeln" ausgefüllt**, damit Sie die Genehmigungsregel für diese neue Antwortoption konfigurieren können. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln.

**Konfigurieren Sie Antwortoption vom Typ: Erweitert**




## Konfigurieren Sie das Altersdiagramm für Ihre DLP-Incidents

Konfigurieren Sie das Altersdiagramm, das im Ops-Portal von Data Loss Prevention Incident Response (DLP IR) angezeigt wird. Dieses Diagramm zeigt die Anzahl der offenen Incidents nach Anzahl der Tage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Konfiguration des Altersdiagramms**.
2. Überprüfen Sie die Altersdiagrammeinträge in der folgenden Tabelle, und passen Sie die Einträge für Ihre Umgebung an.

**Formular „DLP-Altersdiagrammkonfigurationen“**

| Name | Bedingung |
|---|---|
| 0–30 Tage | Alter des offenen Incident, das zwischen 0 und 30 Tagen liegt. |
| 31–60 Tage | Alter des offenen Incident, der zwischen 31 und 60 Tagen liegt. |
| 61–90 Tage | Alter des offenen Incident, der zwischen 61 und 90 Tagen liegt. |
| Über 90 Tage | Alter des offenen Incident, der über 90 Tage liegt |

3. Fügen Sie eine neue Altersdiagrammkonfiguration hinzu, indem Sie auf **Neu**klicken.
4. Geben Sie im Feld Name einen **Namen** für die DLP-Altersdiagrammkonfiguration ein.
5. Legen Sie die Bedingungen für die Konfiguration des DLP-Altersdiagramms fest.
   a. Um Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**.
      - Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.
      - Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.

      **Hinweis:**
      Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

   b. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.
6. Klicken Sie auf **Absenden**.

## Konfigurieren Sie, wie Endbenutzeraktionen delegiert werden

Verhindern Sie, dass bestimmte Führungskräfte in der Organisation Benachrichtigungen über die ihnen zugewiesenen oder eskalierten Incidents erhalten.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie sich ein Szenario vor, in dem die Führungskraft ein Benutzer ist, der zu einer Führungsebene oder Führungskraftgruppe gehört. Der Führungskraft sollten keine E-Mails über die Zuweisung oder Eskalation von Incidents gesendet werden. Ein delegierter Benutzer kann dann die erforderliche Aktion im Namen der Führungskraft ausführen.

Sobald ein Benutzer eine bestimmte Person, Henry, als Delegierten zugewiesen hat, kann ein anderer Benutzer Henry nicht erneut als Delegierten zuweisen. Ebenso kann ein Delegierter keinen anderen Benutzer als Delegierten zuweisen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Delegierten-Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Delegierten-Konfiguration“**

| Feld | Beschreibung |
|---|---|
| Benutzer | Name des Benutzers, der einen Delegierten für DLP-Incidents benötigt. |
| Delegierter | Name des Benutzers, der im Namen des ursprünglichen Endbenutzers auf den DLP-Incident reagieren kann. |

4. Klicken Sie auf **Absenden**.

## Konfigurieren Sie Regeln zur Identifizierung von Wiederholungstätern

Konfigurieren Sie die Identifizierungsregeln für Wiederholungstäter, um Benutzer zu identifizieren, die dasselbe Problem mehrmals wiederholen.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Sie können Wiederholungstäter anhand bestimmter Regeln oder Kriterien identifizieren. Data Loss Prevention Incident Response stellt Felder bereit, mit denen Sie Wiederholungstäter identifizieren können.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Regeln zur Identifizierung von Wiederholungstätern**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Regeln zur Identifizierung von Wiederholungstätern“

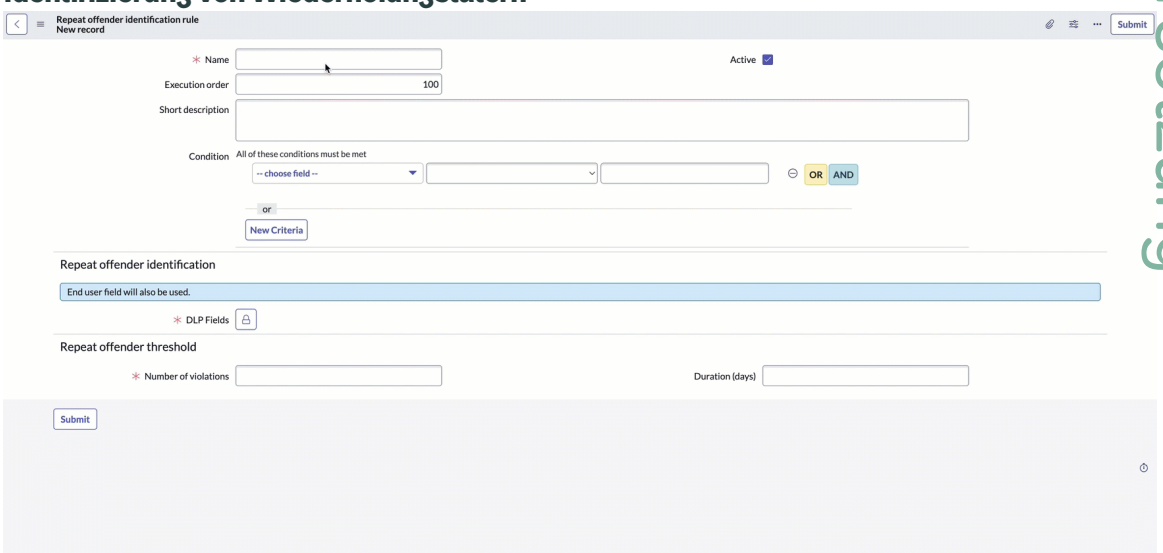
| Feld | Beschreibung |
|---|---|
| Name | Name der Regel zur Identifizierung von Wiederholungstätern. |
| Ausführungsbefehl | Priorität der Regeln zur Identifizierung von Wiederholungstätern. Dieses Feld gibt die Reihenfolge an, in der die Regeln zur Identifizierung von Wiederholungstätern ausgeführt werden, wenn zwei oder mehr Regeln die Auslösebedingungen gemeinsam nutzen.<br><br>Die Regel zur Identifizierung von Wiederholungstätern mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl. Der Standardwert ist 100. |
| Kurzbeschreibung | Eindeutige Beschreibung für diese Regel zur Identifizierung von Wiederholungstätern. |
| Bedingung | Bedingungen im Bedingungsgenerator, die auf der DLP-Incident-Tabelle basieren. Sie können eines der Incident-Felder auswählen, um die Auslöserbedingung für die Regel zur Identifizierung von Wiederholungstätern zu erstellen.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen.<br><br>Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**:<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| DLP-Felder | Identifizieren Sie Wiederholungstäter basierend auf den erforderlichen DLP-Feldern. Klicken Sie auf das neben den DLP-Feldern, um die Liste der verfügbaren DLP-Felder anzuzeigen. Wählen Sie die DLP-Felder, die Sie verwenden möchten, aus der |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt.<br><br>Sie können beispielsweise die Felder**Dateiname** und **Dateibesitzer** aus der Spalte Verfügbar auswählen und in die Spalte Ausgewählt verschieben. Anschließend können Sie die Wiederholungstäter anhand der Felder **Dateiname** und **Dateibesitzer** identifizieren.<br><br>Wenn also ein Benutzer den Schwellenwert für Wiederholungstäter (Anzahl der Verstöße und Dauer) überschreitet und derselbe Benutzer mit den DLP-Feldern übereinstimmt, wird dieser bestimmte Benutzer als Wiederholungstäter identifiziert. |
| Anzahl der Verstöße | Definieren Sie den Schwellenwert für Wiederholungstäter. Nachdem der Benutzer dieselben Aktionen wiederholt und gegen die angegebene Anzahl von Verstößen verstoßen hat, wird der Benutzer als Wiederholungstäter identifiziert. |
| Dauer (in Tagen) | Definieren Sie den Schwellenwert für Wiederholungstäter in Tagen. Nachdem der Benutzer dieselben Aktionen wiederholt und die Schwellenwertdauer überschritten hat, wird der Benutzer als Wiederholungstäter identifiziert. |

**Identifizierung von Wiederholungstätern**




4. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erstellen Sie benutzerdefinierte Status für Ihre DLP-Incidents

Erstellen und konfigurieren Sie Ihre eigenen benutzerdefinierten Status für die Incidents DLP IR.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig bietet Ihnen die Anwendung Data Loss Prevention Incident Response die folgenden Status:

- Geschlossen
- Offen
- Wird überprüft
- Eskaliert
- Überfällig
- Beantwortet
- Entwurf
- Gemeldet

Sie können einen der Standardstatus oder Ihre benutzerdefinierten Status basierend auf den DLP-Incidents auswählen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Benutzerdefinierte Status**.
2. Um einen benutzerdefinierten Status zu erstellen, klicken Sie auf **Neu**.
3. **Geben Sie** im Feld Status einen Namen für den benutzerdefinierten Status ein.
4. Klicken Sie auf **Absenden**.

## Erstellen Sie benutzerdefinierte Felder für Ihre DLP-Incidents

Erstellen und konfigurieren Sie Ihre benutzerdefinierten Felder für die DLP-Incidents. Sie können verschiedene Arten von benutzerdefinierten Feldern erstellen, z. B. Zeichenfolge, Nummer, Kontrollkästchen, Auswahl, Datum und Uhrzeit, und sie in den DLP-Incident-Formularen verwenden.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

**Wichtig:**
Benutzerdefinierte Felder für DLP-Incidents werden nur ab der Version San Diego unterstützt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Warum und wann dieser Vorgang ausgeführt wird

Benutzerdefinierte Felder sind Einschränkungen auf Feldebene zugeordnet. Wenn also Einschränkungen auf Feldebene vorhanden sind, gelten sie für benutzerdefinierte Felder im DLP Ops-Portal und im Endbenutzerportal.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Benutzerdefinierte Felder**.
2. Erstellen Sie ein benutzerdefiniertes Feld, indem Sie auf **Neu**klicken.
3. Füllen Sie die Felder des Formulars aus.

**Formular „Benutzerdefiniertes DLP-Feld".**

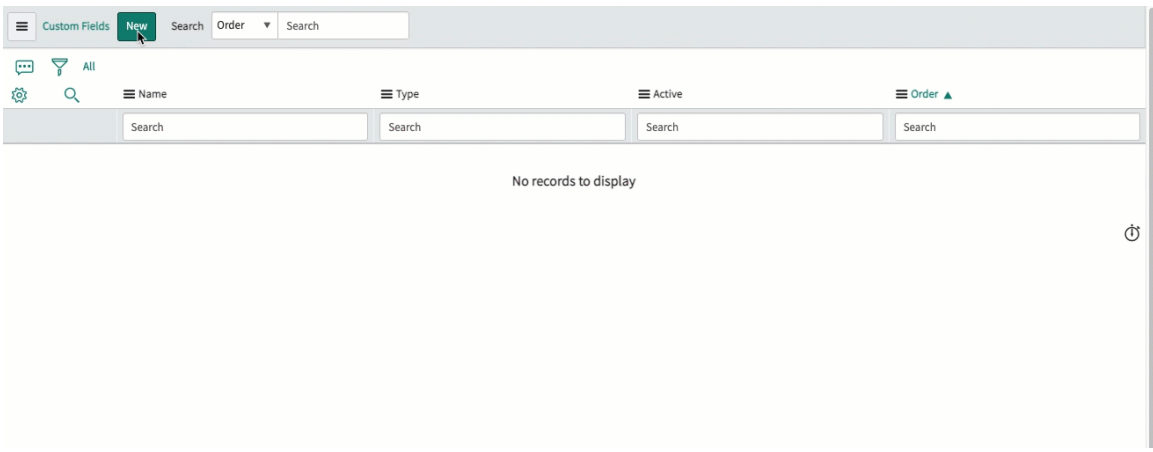
| Feld | Beschreibung |
|---|---|
| Name | Name des benutzerdefinierten Felds. |
| Typ | Option zum Auswählen des Typs des benutzerdefinierten Felds. Sie können einen der folgenden Typen auswählen:<br>○ **Zeichenfolge**<br>○ **Nummer**<br>○ **Checkbox**<br>○ **Auswahl**<br>Wenn Sie den benutzerdefinierten Feldtyp als **Auswahl**auswählen, können Sie nach dem Erstellen des benutzerdefinierten Felds die Auswahloptionen für das benutzerdefinierte Feld definieren.<br>So erstellen Sie eine Auswahloption für ein benutzerdefiniertes Feld:<br>**a.** Öffnen Sie das erforderliche benutzerdefinierte Feld.<br>**b.** Klicken Sie im Abschnitt Benutzerdefinierte Auswahlfeldoptionen auf **Neu**.<br>**c.** Definieren Sie im Feld Optionsname den erforderlichen Optionsnamen.<br>**d.** Klicken Sie auf **Absenden**.<br>○ **Datum**<br>○ **Datum/Uhrzeit**<br>**Hinweis:**<br>Nachdem Sie einen Typ für Ihr neues benutzerdefiniertes Feld ausgewählt haben, dürfen Sie es nicht mehr ändern. Wenn Sie den Typ ändern möchten, müssen Sie erneut ein neues benutzerdefiniertes Feld mit dem erforderlichen Typ erstellen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Reihenfolge | Option zur Auswahl der Reihenfolge, in der die benutzerdefinierten Felder angezeigt werden sollen. Sie können den Reihenfolgenwert für jedes benutzerdefinierte Feld definieren. Die benutzerdefinierten Felder werden basierend auf den von Ihnen definierten Reihenfolgenwerten sortiert.<br><br>Standardmäßig werden die benutzerdefinierten Felder in aufsteigender Reihenfolge sortiert. Sie können die benutzerdefinierten Felder in absteigender Reihenfolge sortieren, indem Sie auf die Spalte **Reihenfolge** klicken. |
| Aktiv | Option, um anzugeben, ob das benutzerdefinierte Feld aktiv ist. |
| Beschreibung | Beschreibung für das benutzerdefinierte Feld, das Sie erstellt haben. |

**Benutzerdefiniertes DLP-Feld**




4. Klicken Sie auf **Absenden**.

## Konfigurieren Sie erweiterte Einstellungen für Data Loss Prevention Incident Response

Konfigurieren Sie die erweiterten Einstellungen, damit Sie unter anderem die Felder im Incident zum Identifizieren der Endbenutzer festlegen können.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Die Konfiguration erweiterter Einstellungen für Data Loss Prevention Incident Response ist optional. Einige erweiterte Einstellungen umfassen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definieren Sie die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können.
- Aktivieren Sie den Schnellmodus, um E-Mails schneller zu senden.
- Bestimmen Sie die Protokollausführlichkeit der Anwendung.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**.
2. Füllen Sie die Felder des Formulars aus.

**Formular „Erweiterte Einstellungen“**

| Feld | Beschreibung |
|---|---|
| Sollen die vertraulichen Daten, die den Verstoß verursacht haben, im Incident angezeigt werden? | Option, um auszuwählen, ob Sie die vertraulichen Daten anzeigen möchten, die den Verstoß im DLP-Incident verursacht haben.<br>Standardmäßig ist diese Option aktiviert. |
| Sollen die vertraulichen Daten, die den Verstoß verursacht haben, auch in den untergeordneten Incidents angezeigt werden? | Option, um auszuwählen, ob Sie die vertraulichen Daten, die den Verstoß verursacht haben, auch im untergeordneten DLP-Incident anzeigen möchten.<br>Standardmäßig ist diese Option deaktiviert. |
| Liste der Felder im Incident, die zum Identifizieren des Endbenutzers verwendet werden | Die Liste der Felder im Incident des Moduls „Zuweisungsregel“, die zum Identifizieren des Endbenutzers verwendet werden. Sie können auch eigene benutzerdefinierte Attribute angeben, um den Endbenutzer zu identifizieren. |
| Maximale Anzahl von Incidents in einer Digest-E-Mail | Die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können.<br>Standardmäßig ist der Wert 100. |
| Maximale Dauer des Wiederholungsvergehens (in Tagen) | Die maximale Dauer, um einen Wiederholungstäter zu identifizieren.<br>Standardmäßig beträgt der Wert 90 Tage. |
| Schnellmodus zum Senden von E-Mails | Option zum Validieren von E-Mails und Identifizieren von Problemen. Sie können die Validierung durchführen, indem Sie die Option **Ja** aktivieren.<br>Standardmäßig ist diese Option aktiviert. |
| Diese Eigenschaft wird verwendet, um die Protokollausführlichkeit der Anwendung festzulegen | Die Ausführlichkeitsstufe des Protokolls der Anwendung, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren:<br>○ **Fehler**<br>○ **warnen** |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ **Info**<br>○ **debuggen**<br><br>Standardmäßig ist der Wert **info**. |
| Schließen Sie geklonte und untergeordnete Incidents aus Berichten aus | Option zum Ausschließen geklonter und untergeordneter Incidents aus den Berichten.<br><br>Standardmäßig ist diese Option **Ja**. |
| Wartezeit in Tagen für das Löschen von Übereinstimmungsinhalten im Cloud-Speicher, nachdem der Incident geschlossen wurde | Option zur Auswahl der Anzahl der Wartetage zum Bereinigen des Übereinstimmungsinhalts der Incidents, die für eine bestimmte Zeitdauer inaktiv sind.<br><br>Standardmäßig ist der Wert 90. Wenn der DLP-Incident nach 90 Tagen inaktiv ist, wird der Übereinstimmungsinhalt aus dem Cloud-Speicher bereinigt. |
| Incident der DLP-Analystengruppe nach der letzten Eskalationsstufe zuweisen | Aktivieren Sie dieses Kontrollkästchen, um den Incident dem Analysten nach der letzten Eskalationsstufe zuzuweisen. |
| Ermöglichen Sie Benutzern den Zugriff auf Incidents nach der Eskalation | Aktivieren Sie dieses Kontrollkästchen, damit die zugewiesenen Benutzer nach der Eskalation auf den Incident bzw. die Incidents zugreifen können.<br><br>Wenn Sie diese Option auswählen, können alle Benutzer, die der Eskalationskettenliste hinzugefügt wurden, auf den Incident bzw. die Incidents zugreifen. |
| Zulassen, dass Analysten abgeschlossene Bewertungen bearbeiten | Aktivieren Sie diese Checkbox, damit der Analyst die abgeschlossene Bewertung bearbeiten kann.<br><br>Wenn Sie diese Option auswählen, können Analysten die Bewertungen bearbeiten. Wenn diese Option deaktiviert ist, können Sie die Bewertungen im schreibgeschützten Modus anzeigen. |

3. Klicken Sie auf **Speichern**.

## Überwachen Sie den Microsoft DLP-Integrationsausführungsprozess

Verfolgen und überwachen Sie den laufenden Erfassungsprozess. Die Integrationsausführungsprozesse enthalten die Statistiken darüber, wie viele Daten verarbeitet wurden, und den Integrationsstatus.

Erforderliche Rolle: sn_dlir.admin.

Der Integrationsausführungsprozess listet die Details dazu auf, wie viele Datensätze erfasst werden. Beispiel:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. In Symantec enthält der Prozess sowohl untergeordnete als auch übergeordnete Integrationsausführungen. Der übergeordnete Datensatz gibt die Erfassungsdaten an, und der untergeordnete Datensatz gibt die Ergänzungsaufrufe und benutzerdefinierten Attributdatensätze an.
2. In Microsoft muss nur der übergeordnete Datensatzerfassungsprozess ausgeführt werden.

**DLP-Integrationsausführungsprozesse**: Zeigt die Warteschlangeneinträge, den Status der Warteschlangeneinträge und die abgerufenen Datensätze an.

Die Integrationsausführung enthält die Quelle, für die das Integrationsprofil und der Integrationsausführungsdatensatz erstellt werden, Profilabfrageintervalle, Erfassungsstatus und -substatus sowie die Incident-Anzahl, die die Anzahl der erfassten Datensätze angibt.

1. Navigieren zu **DLP-Administration** > **Integrationsausführungen**.
2. Wählen Sie die Integrationsausführung aus der Liste aus.
3. Navigieren Sie zu **DLP-Integration Prozess ausführen**.
4. Zeigen Sie den Warteschlangeneintragsstatus des Datensatzes an.

## DLP-Incident-Zugriffsbeschränkungen

Verwalten Sie die Transparenz eines bestimmten DLP-Incident, der vertrauliche Informationen enthält. Sie können Zugriffsbeschränkungen für Incidents verwenden, um zu definieren, wer auf einen bestimmten DLP-Incident zugreifen kann, und den Zugriff bestimmter Benutzer oder Gruppen auf diesen Incident auszuschließen.

### Richten Sie Einschränkungen auf Feldebene für Ihre DLP-Incidents ein

Legen Sie Einschränkungen auf Feldebene in DLP-Incidents fest, um vertrauliche Informationen vor der Offenlegung zu schützen. Sie können Einschränkungen auf Feldebene verwenden, um die Benutzer oder Gruppen zu steuern, die in den DLP-Incidents auf bestimmte Felder zugreifen können.

#### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

#### Warum und wann dieser Vorgang ausgeführt wird

Mit Einschränkungen auf Feldebene können Sie nur bestimmte Felder für bestimmte Benutzer oder Gruppen anzeigen, wodurch Sie die Daten, auf die ein Benutzer zugreifen kann, granularer steuern können. Sie können eine Einschränkung auf Feldebene erstellen, indem Sie die DLP-Incident-Übereinstimmungsbedingungen definieren, die Benutzer oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Felder auswählen, die diese Benutzer oder Gruppen anzeigen können.

#### Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Feldebene**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „DLP-Feldebenenbeschränkung“

| Feld | Beschreibung |
|---|---|
| Name | Name der Einschränkung auf Feldebene. |
| Aktiv | Option, um anzugeben, ob die Einschränkung auf Feldebene aktiv ist. |
| Ausführungsbefehl | Priorität der Einschränkungen auf Feldebene. Dieses Feld gibt die Reihenfolge an, in der die Einschränkungen auf Feldebene ausgeführt werden, wenn zwei oder mehr Einschränkungen auf Feldebene die Auslösebedingungen gemeinsam nutzen.<br><br>Die Einschränkung auf Feldebene mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl. Der Standardwert ist 100. |
| Kurzbeschreibung | Eindeutige Beschreibung für diese Einschränkung auf Feldebene. |
| Incident-Übereinstimmungsbedingung | Optionen im Incident, die den definierten Bedingungen entsprechen. Sie können eines der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Feldebene zu definieren.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**:<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>Beispielsweise können Sie das Feld als `Richtliniennameauswählen` und die Bedingung `auf`, und `Name der Richtlinie`festlegen.<br><br>**Hinweis:**<br>Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. |
| Betrifft | Option zum Anwenden der Incident-Übereinstimmungsbedingungen auf bestimmte Benutzer oder Gruppen. Sie können die Bedingungen auf Folgendes anwenden:<br>○ **Alle Endbenutzer**: Option zum Auswählen aller Endbenutzer, für die die DLP-Incident-Bedingungen gelten.<br>○ **Alle Prüfer eskalierter Incidents**: Option zur Auswahl aller Prüfer eskalierter Incidents, für die die DLP- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

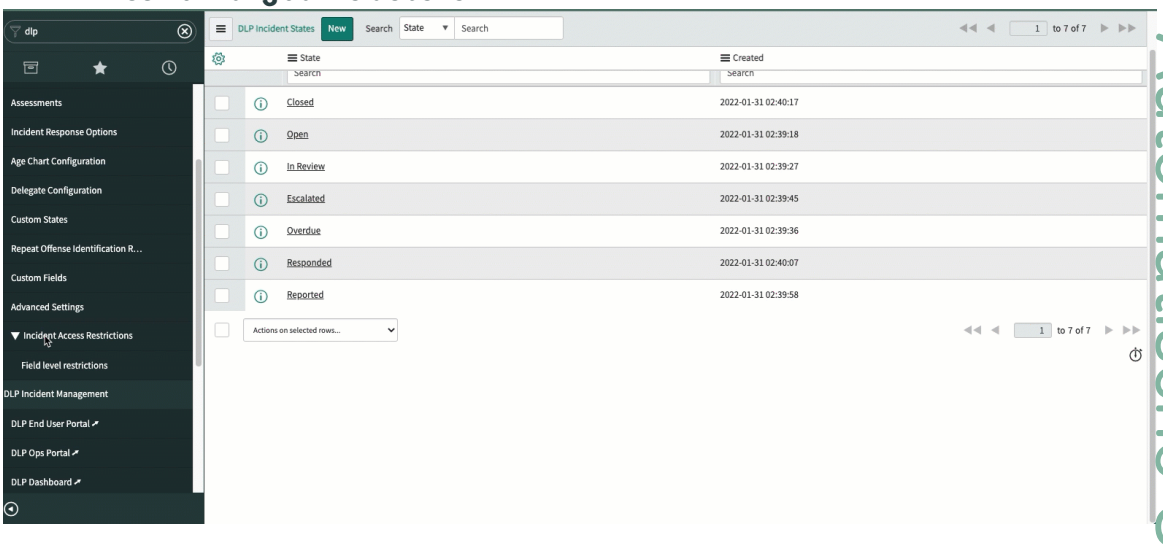
| Feld | Beschreibung |
| --- | --- |
| | Incident-Bedingungen gelten. Dies bezieht sich auf alle DLP-Incidents, die an den Manager eskaliert wurden.<br>○ **Benutzer**: Sie auf das Schlosssymbol, um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den die DLP-Incident-Bedingungen gelten. Sie können einen Benutzer auch über seine E-Mail-Adresse oder Suchoption hinzufügen. Beispiel: Manager der Rechtsabteilung.<br>Um sich selbst als Benutzer hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf das hinzufügen<br>○ **Gruppen**: Klicken Sie auf das , um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die die DLP-Incident-Bedingungen gelten. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller. |
| Nur Zugriff auf folgende Felder zulassen | ○ **DLP-Felder**: Option zum Definieren der DLP-Felder, für die Sie den Zugriff für die ausgewählten Benutzer oder Gruppen zulassen möchten. Wählen Sie die DLP-Felder, auf die Sie Zugriff gewähren möchten, aus der Spalte Verfügbar aus, und verschieben Sie sie in die Spalte Ausgewählt.<br>**Hinweis:**<br>Die ausgewählten Benutzer oder Gruppen können nur auf die ausgewählten DLP-Felder zugreifen.<br>Sie können beispielsweise die Felder**Zugewiesen an** und **Geöffnet** aus der Spalte Verfügbar auswählen und in die Spalte Ausgewählt verschieben. Dann haben die ausgewählten Benutzer oder Gruppen nur Zugriff auf die Felder Zugewiesen an und Geöffnet.<br>○ **Anhänge**hochladen: Option, um anzugeben, ob die ausgewählten Benutzer oder Gruppen Anhänge hochladen dürfen.<br>○ **Benutzerdefinierte Felder**: Option zum Definieren der benutzerdefinierten Felder, die den ausgewählten Benutzern oder Gruppen den Zugriff ermöglichen sollen. Sie können die benutzerdefinierten Felder, die Sie erstellt haben, in der Spalte Verfügbar anzeigen.<br>Wählen Sie in der Spalte Verfügbar die benutzerdefinierten Felder aus, auf die Sie Zugriff |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | gewähren möchten, und verschieben Sie sie in die Spalte Ausgewählt.<br><br>**Wichtig:**<br>▪ Benutzerdefinierte Felder für DLP-Incidents werden nur ab der Version San Diego unterstützt.<br>▪ Die ausgewählten Benutzer oder Gruppen können nur auf die ausgewählten benutzerdefinierten Felder zugreifen. |

**DLP – Einschränkung auf Feldebene**




4. Klicken Sie auf **Absenden**.

## Richten Sie Einschränkungen auf Datensatzebene für Ihre DLP-Incidents ein

Legen Sie Einschränkungen auf Datensatzebene in DLP-Incidents fest, um vertrauliche Datensätze vor der Offenlegung zu schützen. Sie können Einschränkungen auf Datensatzebene verwenden, um die Benutzer oder Gruppen zu steuern, die in den DLP-Incidents auf bestimmte Datensätze zugreifen können.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – Erstellen, Bearbeiten und Löschen.
- sn_dlir.analyst und sn_dlir.analyst_read – Ansicht (schreibgeschützt).

### Warum und wann dieser Vorgang ausgeführt wird

Mit Einschränkungen auf Datensatzebene können Sie den Zugriff auf Datensätze nur für bestimmte Benutzer oder Gruppen gewähren, wodurch Sie die Datensätze, auf die ein Benutzer zugreifen kann, präziser steuern können. Sie können eine Einschränkung auf Datensatzebene erstellen, indem Sie die DLP-Incident-Übereinstimmungsbedingungen definieren, die Benutzer oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Datensätze auswählen, die diese Benutzer oder Gruppen anzeigen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Datensatzebene**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

**Formular „DLP-Datensatzebenenbeschränkung“.**

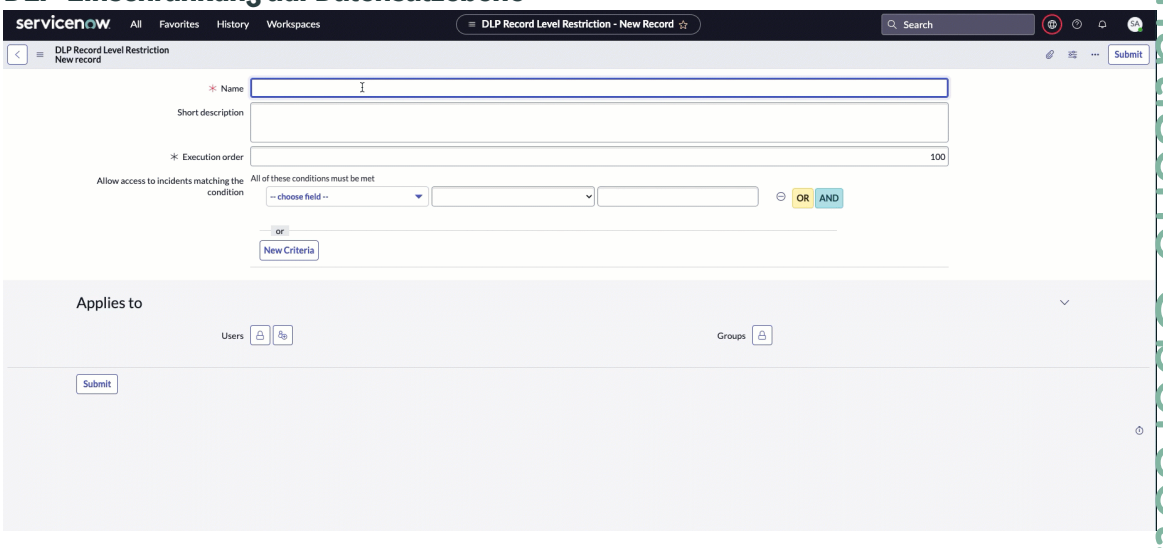
| Feld | Beschreibung |
|---|---|
| Name | Name der Einschränkung auf Datensatzebene. |
| Kurzbeschreibung | Eindeutige Beschreibung für diese Einschränkung auf Datensatzebene. |
| Ausführungsbefehl | Priorität der Einschränkungen auf Datensatzebene. Dieses Feld gibt die Reihenfolge an, in der die Einschränkungen auf Datensatzebene ausgeführt werden, wenn zwei oder mehr Einschränkungen auf Datensatzebene die Auslösebedingungen gemeinsam nutzen.<br><br>Die Einschränkung auf Datensatzebene mit der niedrigsten Nummer hat die höchste Priorität.<br><br>Um die Reihenfolge des Vorgangs festzulegen, geben Sie einen Wert ein. Zum Beispiel 100, 200 oder eine andere Zahl. Der Standardwert ist 100. |
| Erlauben Sie den Zugriff auf Incidents, die der Bedingung entsprechen | Optionen ermöglichen den Zugriff auf die Incidents, die den definierten Bedingungen entsprechen. Sie können eines der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Datensatzebene zu definieren.<br><br>Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**:<br>○ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>○ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br><br>Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**.<br><br>**Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.<br><br>Sie können beispielsweise das Feld als `Aktiv`auswählen und die Bedingung auf `ist`, und `true`festlegen. |
| Betrifft | Option zum Anwenden von Einschränkungen auf Datensatzebene auf bestimmte Benutzer oder Gruppen. Sie können die Bedingungen wie folgt anwenden: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | ○ **Benutzer**: Sie auf das Schlosssymbol, um einen bestimmten Benutzer aus der Liste hinzuzufügen, für den der ausgewählte Datensatz gilt. Sie können einen Benutzer auch über seine E-Mail-Adresse oder Suchoption hinzufügen. Beispiel: Manager der Rechtsabteilung.<br><br>Um sich selbst als Benutzer hinzuzufügen, für den der Datensatz gilt, klicken Sie auf das hinzufügen. Beispiel: Systemadministrator.<br><br>○ **Gruppen**: Klicken Sie auf das , um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die der ausgewählte Datensatz gilt. Sie können eine Gruppe auch mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller. |

**DLP-Einschränkung auf Datensatzebene**




4. Klicken Sie auf **Absenden**.

## Archivierung von DLP-Incidents

Data Loss Prevention Incident Response wird mit einer Archivierungsregel im Basissystem für die DLP-Incident-Tabelle bereitgestellt. Die zugehörigen Datensätze werden auch im Basissystem der DLP-Incident-Archivregel hinzugefügt.

### Vorbereitungen

Erforderliche Rolle: admin

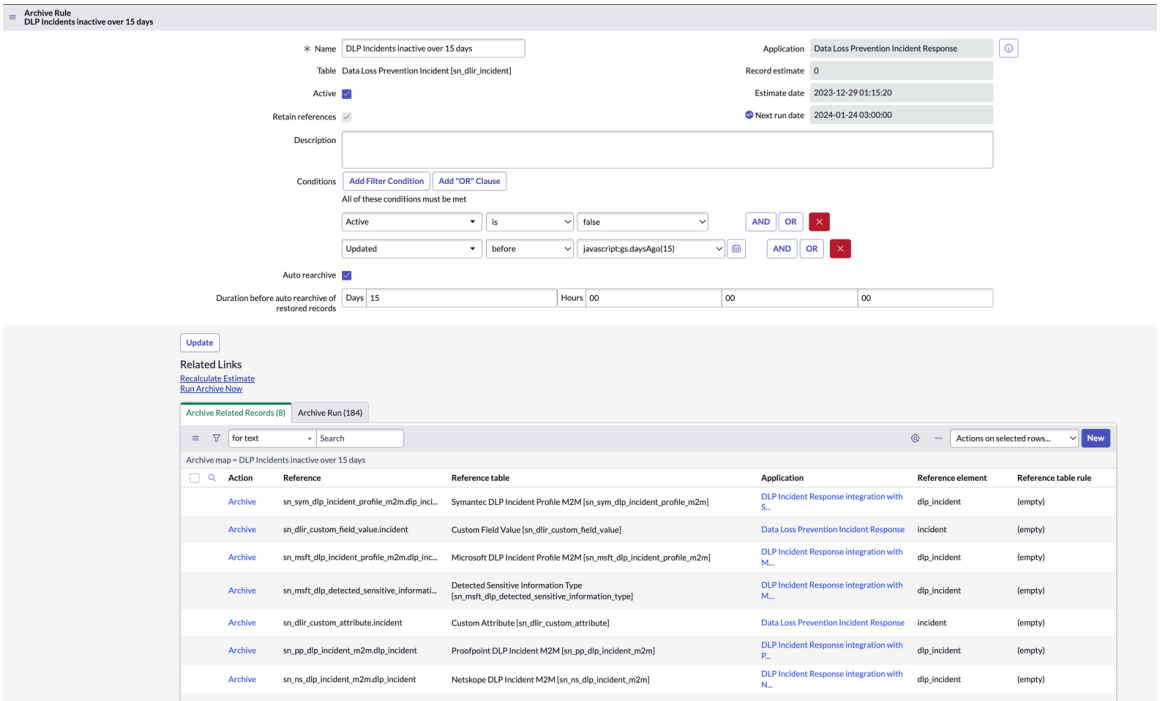
### Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
   Die Systemarchivierungsregeln, die sich im Basissystem befinden, werden angezeigt.
2. Zeigen Sie die DLP-Archivierungsregel an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
„**DLP-Incidents inaktiv über 15 Tage** “ ist die standardmäßige Basissystem-Archivierungsregel für DLP-Incidents. Sie können die Archivierungsregel bei Bedarf ändern. Diese Regel bedeutet, dass Incidents, die länger als 15 Tage inaktiv sind, automatisch archiviert werden.




**Hinweis:**
Informationen dazu, wie die Archivierungsregeln erstellt werden, finden Sie unter Archivierungsregeln erstellen .

3. **Aktualisieren Sie** die Regel, falls erforderlich.

### Archivieren Sie zugehörige DLP-Datensätze

Verwenden Sie die zugehörige Liste Zugehörige Datensätze archivieren für DLP-Incidents, um die zugehörigen Datensätze der Archivregel hinzuzufügen.

**Vorbereitungen**
Erforderliche Rolle: admin

**Prozedur**

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**.
2. Wählen Sie die Archivierungsregel **DLP-Incidents inaktiv über 15 Tage aus**.
3. Wechseln Sie zur zugehörigen Liste **Zugehörige Datensätze** archivieren.
4. Zeigen Sie die zugehörigen DLP-Datensätze an.

| Anwendung | Referenztabelle |
|---|---|
| DLP Incident Response Integration with Symantec | Symantec DLP-Incident-Profil M2M [sn_sym_dlp_incident_profile_m2m] |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Anwendung | Referenztabelle |
|---|---|
| Data Loss Prevention Incident Response | Benutzerdefinierter Feldwert [sn_dlir_custom_field_value] |
| DLP Incident Response integration with Microsoft | Microsoft DLP-Incident-Profil M2M [sn_msft_dlp_incident_profile_m2m] |
| DLP Incident Response integration with Microsoft | Typ der erkannten vertraulichen Informationen [sn_msft_dlp_detected_sensitive_information_type] |
| Data Loss Prevention Incident Response | Benutzerdefiniertes Attribut [sn_dlir_custom_attribute] |
| DLP Incident Response integration with Proofpoint | Proofpoint-DLP-Incident M2M [sn_pp_dlp_incident_m2m] |
| DLP Incident Response integration with Netskope | Netskope-DLP-Incident M2M [sn_ns_dlp_incident_m2m] |
| DLP Incident Response Integration with Symantec | Typ der erkannten vertraulichen Informationen [sn_sym_dlp_detected_sensitive_information_type] |

**Hinweis:**
Alle Systemtabellen wie E-Mails, Bewertungen und Anhänge werden automatisch zum archivierten DLP-Datensatz weitergeleitet.

5. Wählen Sie die archivbezogene Datensatzregel aus, die Sie archivieren möchten.

**Hinweis:**
Weitere Informationen zum Hinzufügen weiterer zugehöriger Datensätze finden Sie unter DLP-bezogene Datensätze archivieren auf Now Platform.

## Data Loss Prevention Incident Response Incident-Management

Verwenden Sie Data Loss Prevention Incident Response Incident Management, um Incidents mithilfe des DLP-Benutzerarbeitsbereichs, des DLP-Analystenarbeitsbereichs und des DLP-Dashboards zu aktualisieren und zu verwalten.

### Data Loss Prevention Incident Response Benutzerarbeitsbereich

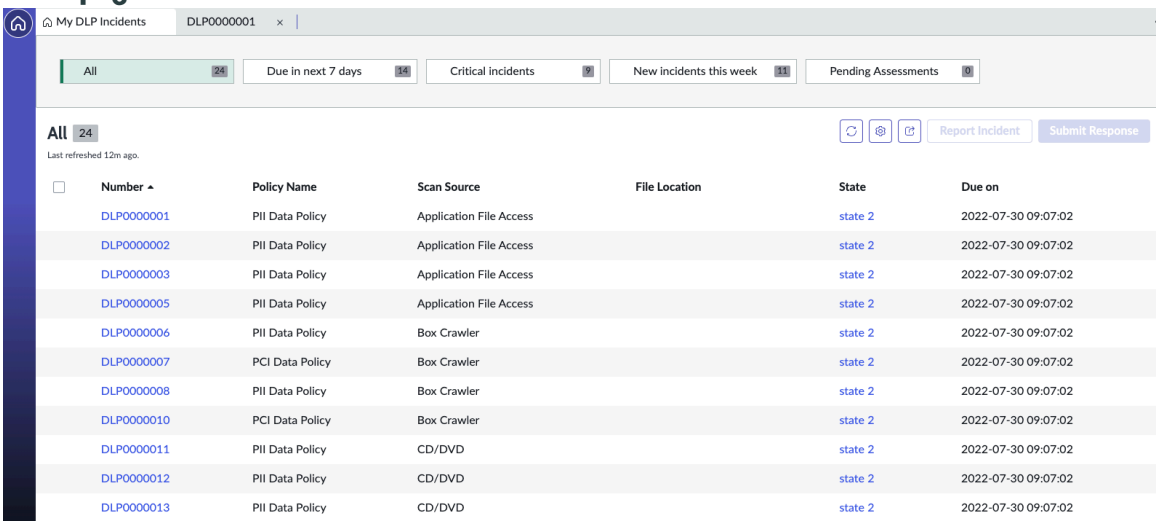
Der Benutzerarbeitsbereich Data Loss Prevention Incident Response (DLP IR) ist ein Arbeitsbereich, in dem Endbenutzer, Manager und Genehmiger auf die zugewiesenen DLP-Incidents reagieren können. Die Endbenutzer, Manager und Genehmiger können dann auf die Incidents reagieren, indem sie die richtigen Aktionen angeben.

Sie können auch Bewertungen erstellen und verwalten, damit Endbenutzer auf DLP-Incidents reagieren können. Der Arbeitsbereich besteht aus einer Zielseite und Listenansichten, in denen Sie die zugewiesenen DLP-Incidents anzeigen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Homepage des DLP-Benutzerarbeitsbereichs**




## DLP-Incidents melden oder darauf reagieren

Greifen Sie auf den Benutzerarbeitsbereich Data Loss Prevention Incident Response (DLP) zu, überprüfen Sie die zugewiesenen DLP-Incidents, und melden oder reagieren Sie auf die Incidents.

### Vorbereitungen

Erforderliche Rolle:

- Beliebiger gültiger Benutzer/Mitarbeiter

### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Benutzerarbeitsbereich**.
   Die Seite „Meine DLP-Incidents“ wird in einer neuen Registerkarte geöffnet.
2. Klicken Sie auf eine Listenansicht, um die Ihnen zugewiesenen Incidents zu überprüfen.

| Listenansicht | Beschreibung |
|---|---|
| Alle | Zeigen Sie alle zugewiesenen Incidents an. |
| In den nächsten 7 Tagen fällig | Zeigen Sie alle Incidents an, die in den nächsten 7 Tagen fällig sind. |
| Kritische Incidents | Zeigen Sie alle Incidents mit der Schweregradbezeichnung „Kritisch“ an. |
| Neue Incidents diese Woche | Zeigen Sie alle Incidents an, die diese Woche zugewiesen sind. |
| Ausstehende Bewertungen | Zeigen Sie alle noch ausstehenden Bewertungen an. |

3. Sie können die DLP-Incidents auf zwei Arten überprüfen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und auf das Kontrollkästchen neben den Incidents zu klicken.

   b. Wählen Sie die für Sie geeignete Option aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

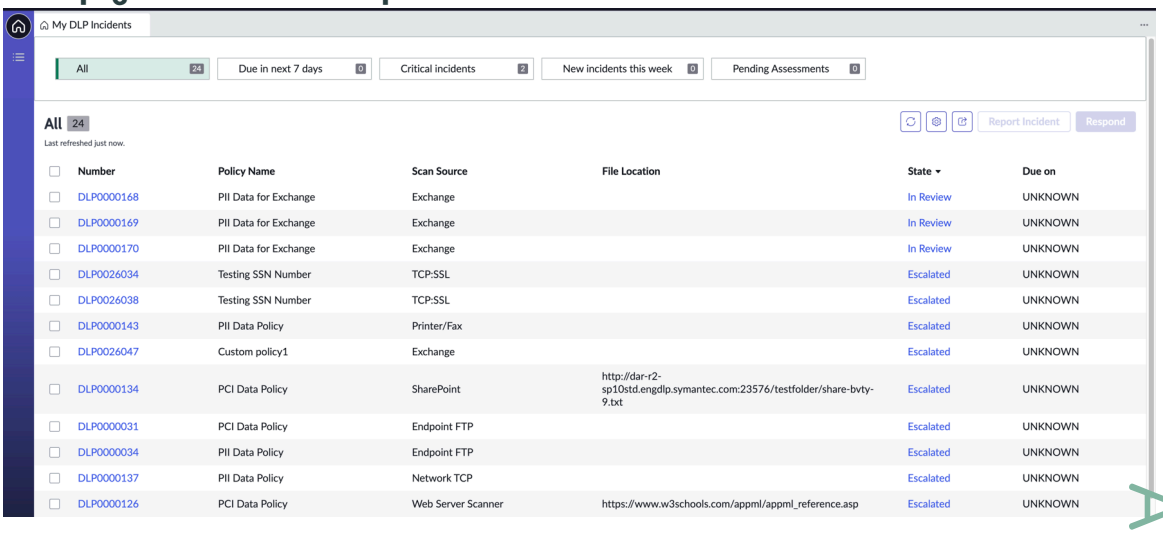
### Homepage des DLP-Endbenutzerportals

| Option | Beschreibung |
|---|---|
| Liste neu laden | Option zum Aktualisieren der Liste der DLP-Incidents, wenn Sie eine Aktualisierung vorgenommen haben. |
| Listenaktionen | Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt:<br>▪ **Speichern unter**<br>▪ **Spalten bearbeiten**<br>▪ **Breiten zurücksetzen**<br>**Hinweis:**<br>Wenn Sie eine eigene benutzerdefinierte Liste haben, die im Abschnitt „ **Meine Listen** “ für Ihren Arbeitsbereich erstellt wird, können Sie auch die folgenden zusätzlichen Listenaktionen ausführen:<br>▪ **Umbenennen**<br>▪ **Speichern**<br>▪ **Löschen** |
| URL kopieren für Alle | Option zum Kopieren der URLs aller DLP-Incidents. |
| Incident melden | Aktion, um den Incident als falsch positiv oder als falscher Besitzer zu melden. Sie können beispielsweise einen falschen Besitzer melden und einen anderen Besitzer vorschlagen oder den Incident als falsch positiv melden. |
| Beantworten | Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Benutzer beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann der Benutzer die Option **Gelöschte Datei** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare angeben.<br>Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Homepage des DLP-Benutzerportals**




**c.** Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen. Auf der Registerkarte **Details** werden die folgenden Abschnitte angezeigt:

- Details: Sie können die Details des DLP-Incident anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname.
- Verfassen: Um Kommentare zum DLP-Incident hinzuzufügen, die für alle sichtbar sind, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.
- Aktivität: Sie können die Details der verschiedenen Aktivitäten im DLP-Incident anzeigen.
- Anhänge: Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen**, und wählen Sie den Anhang auf Ihrem lokalen Laufwerk aus.

  Auf der Registerkarte **Zusätzliche Details** werden alle zusätzlichen Informationen zum DLP-Incident angezeigt, einschließlich benutzerdefinierter Felder.

  **Wichtig:**

  - Benutzerdefinierte Felder für DLP-Incidents werden nur ab der Version San Diego unterstützt.
  - Wenn für einen bestimmten DLP-Incident benutzerdefinierte Felddaten verfügbar sind, können Sie sie auf der Registerkarte **Zusätzliche Details** anzeigen. Wenn keine benutzerdefinierten Felder für den DLP-Incident vorhanden sind, wird eine leere Seite angezeigt.

- **Typ**der erkannten vertraulichen Informationen: Zeigt die erkannten vertraulichen Informationen des Incident an.

  **Hinweis:**
  Diese zugehörige Liste ist nur für die DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Im Incident-Datensatz von Microsoft oder Symantec wird immer dann, wenn der Benutzer auf den Datensatz des erkannten vertraulichen Informationstyps zugreift, der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

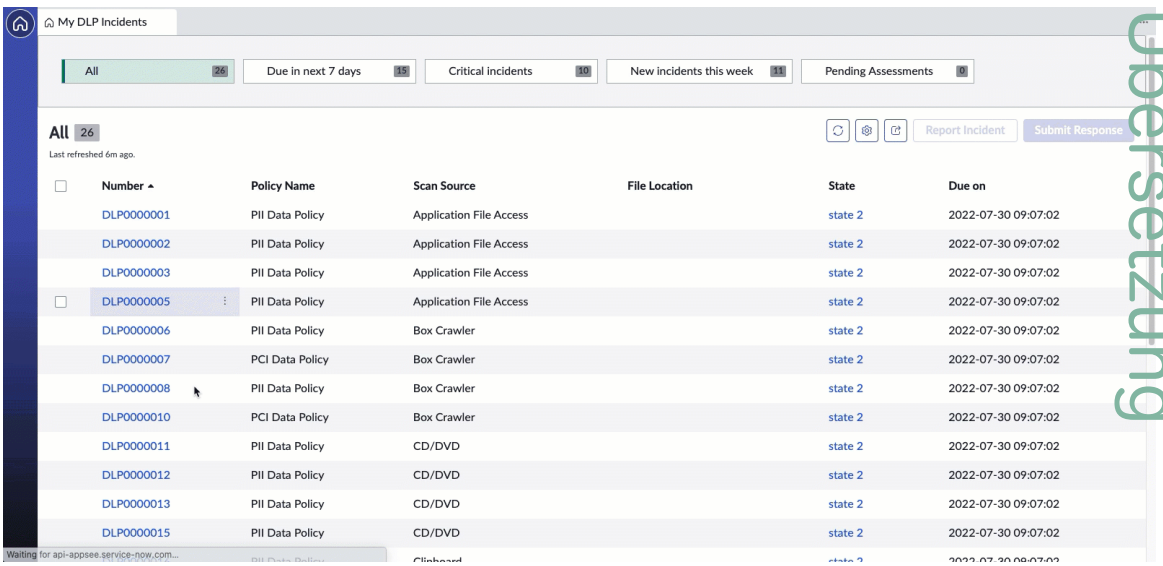
**d.** Wählen Sie die für Sie geeignete Option aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| Falsch positives Ergebnis melden | Aktion zum Melden, dass der DLP-Incident fälschlicherweise ausgelöst oder erstellt wurde. Sie können die Details dazu angeben, warum Sie den Incident als falsch positiv im Feld Kommentare markiert haben. |
| Falschen Besitzer melden | Aktion, um zu melden, dass der DLP-Incident dem falschen Benutzer zugewiesen wurde. Wenn Sie den richtigen Besitzer für den Incident kennen, können Sie den Namen des Besitzers im Feld Besitzer vorschlagen auswählen. Um zusätzliche Details hinzuzufügen, verwenden Sie das Feld Kommentare. |
| Beantworten | Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Benutzer beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann der Benutzer die Option **Gelöschte Datei** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare angeben.<br><br>Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**. |

**DLP-Incident-Aktionen**




**4.** Um Bewertungen vorzunehmen, wählen Sie die **Listenansicht Ausstehende Bewertungen** aus.

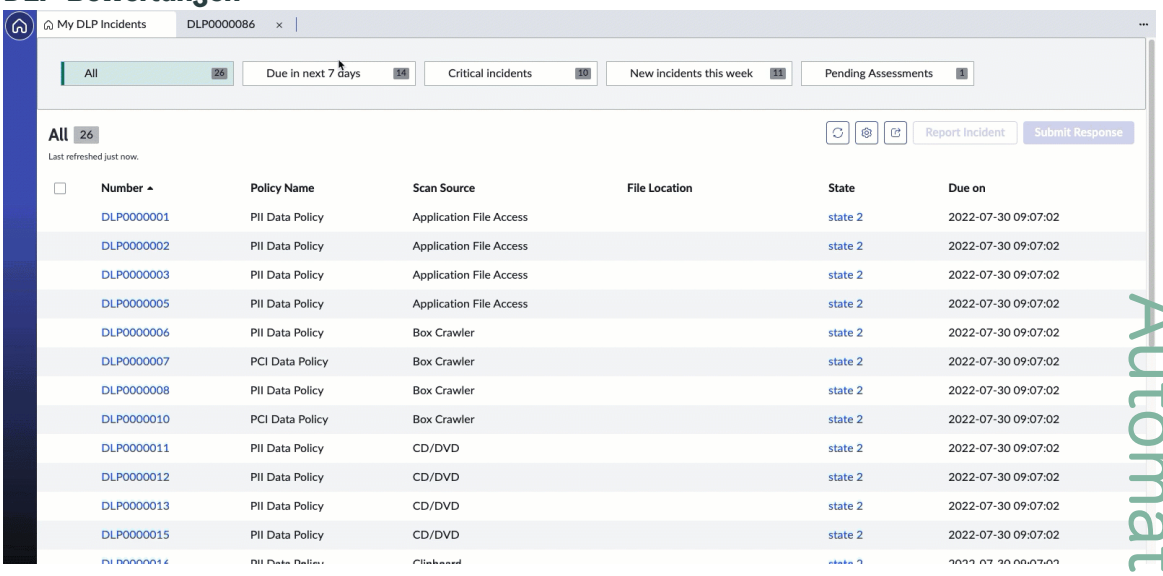
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**a.** Klicken Sie auf eine bestimmte Bewertungsnummer, um sie zu öffnen.

**b.** Beantworten Sie die Bewertungsfragen, und klicken Sie je nach Anforderungen auf **Speichern** oder **Absenden**.

**DLP-Bewertungen**




5. Klicken Sie auf den Kartenabschnitt **Anweisungen**, der über allen Feldern in der DLP-Incident-Formularansicht angezeigt wird, um zusätzliche Informationen zu einem bestimmten Incident anzuzeigen.

> **Hinweis:**
> Dieser Abschnitt im Arbeitsbereich führt die Benutzer zu den Incident-Informationen, die zum Verständnis der nächsten Schritte der Incident-Lösung beitragen.
>
> Auf der Karte „Benutzeranweisungen“ werden zwei verschiedene Header angezeigt, die weitere Informationen zu einem bestimmten Incident in der Formularansicht enthalten. Klicken Sie auf eine beliebige Benutzeranweisungskopfzeile, um die zusätzlichen Details zu erfahren.

Weitere Informationen finden Sie unter Erstellen und verwalten Sie Benutzeranweisungen für DLP-Incidents und Konfigurieren Sie DLP-UI-Benutzeranweisungen.

### Arbeiten mit meinem Genehmigungsmodul

Das Modul „Meine Genehmigungen“ ist im DLP-Benutzerarbeitsbereich für angemeldete Benutzer verfügbar. Benutzer können die Zuweisungsgenehmigungsanforderungen hier genehmigen oder ablehnen.

**Vorbereitungen**
Erforderliche Rolle:

- Endbenutzer
- Manager
- Genehmigende Person

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Benutzerarbeitsbereich**.
   Die Seite „ **Meine DLP-Incidents** “ wird auf einer neuen Registerkarte angezeigt.
2. Klicken Sie auf das Modul „ **Meine Genehmigungen** “ unter dem Modul „ **Meine DLP-Incidents** “.
   Die Listenansicht „Meine Genehmigungen“ wird angezeigt.

   Genehmiger können die Anforderungen in der Listenansicht der Seite „ **Meine Genehmigungen** “ genehmigen oder ablehnen. Sie können mehrere Anforderungen in der Listenansicht genehmigen oder ablehnen.

   Genehmiger können die Details der zugewiesenen Anforderung in der Formularansicht anzeigen. Durch Klicken auf die Aktion **Genehmigen** oder **Ablehnen** in der Formularansicht kann die individuelle Anforderung genehmigt oder abgelehnt werden.

**Hinweis:**

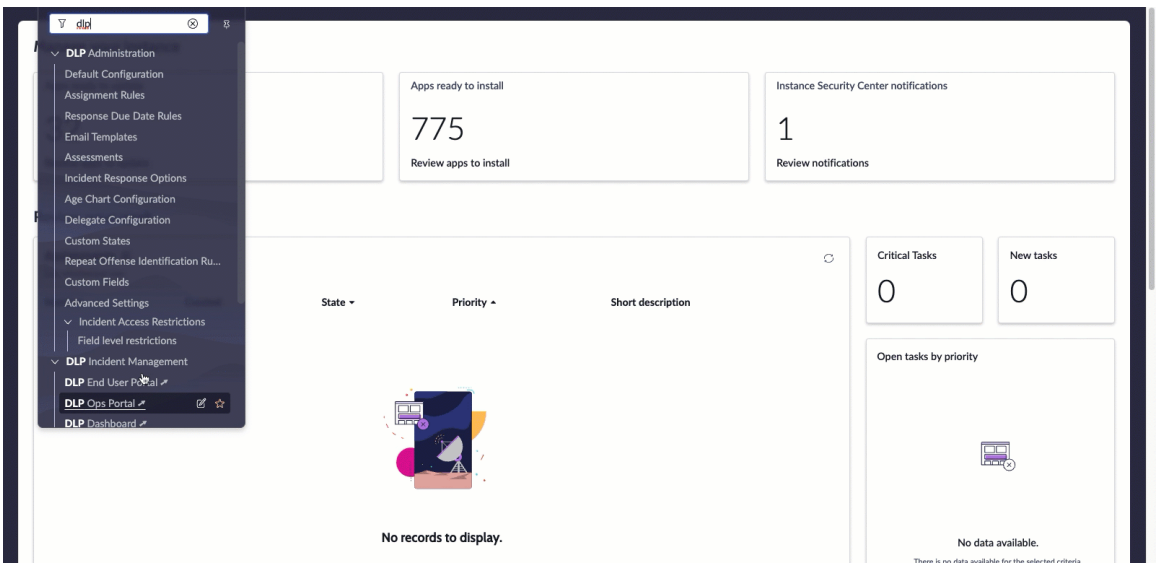
Um die DLP-Incident-Details anzuzeigen, klicken Sie auf das Symbol „ ⓘ “ im Feld **„Genehmigen“**.

## Data Loss Prevention Incident Response Arbeitsbereich für Analysten

Verwenden Sie den Analyst Workspace Data Loss Prevention Incident Response (DLP IR), um die DLP-Incidents anzuzeigen. Weisen Sie die Incidents Endbenutzern zur Lösung usw. zu.

Der DLP-Arbeitsbereich besteht aus einer Homepage mit Dashboards, Listenansichten und Formularansichten, mit denen Sie DLP-Incidents überwachen können.

### Übersichtsseite des DLP-Arbeitsbereichs




### Überprüfen und weisen Sie Ihre DLP-Incidents zu

Greifen Sie auf den Analyst Workspace Data Loss Prevention Incident Response (DLP IR) zu, um die DLP-Incidents zu überprüfen und zuzuweisen oder zu lösen. Sie können Trends für Incidents nach Schweregrad, häufigsten Straftätern, Incidents nach Scan-Quelle und Incidents nach Richtlinie nachverfolgen.

DLP-Arbeitsbereichs-Homepage

DLP-Arbeitsbereich – Übersicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst – DLP-Incidents bearbeiten und anzeigen.
- sn_dlir.analyst_read und sn_dlir.read – DLP-Incidents anzeigen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Analyst-Arbeitsbereich**.
   Die Listenseite „Meine Incidents“ des DLP-Arbeitsbereichs wird auf einer neuen Registerkarte geöffnet.
2. Klicken Sie auf das Homepage-Symbol des **DLP-Arbeitsbereichs**, um die Homepage-Ansicht des Arbeitsbereichs anzuzeigen.
3. Überprüfen Sie die Dashboard-Widgets, um Trends nach Incidents nach Schweregrad, häufigsten Straftätern, Incidents nach Scan-Quelle und Incidents nach Richtlinie zu identifizieren.
4. Klicken Sie auf der Homepage auf die entsprechenden Filter, um die Widgets nach ihren verschiedenen Kategorien anzuzeigen.

| Filter | Beschreibung |
|---|---|
| Offene Incidents | Zeigen Sie alle offenen Incidents an. |
| Überfällige kritische Incidents | Zeigen Sie die Incidents an, die den Schweregrad „Kritisch“ aufweisen und überfällig sind. |
| Incidents, die Endbenutzern zugewiesen sind | Zeigen Sie die Incidents an, die Endbenutzern zugewiesen sind. |

5. Sie können die DLP-Incidents auf zwei Arten überprüfen und zuweisen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und auf das Kontrollkästchen neben den Incidents zu klicken.

   b. Wählen Sie die für Sie geeignete Option aus.

| Option | Beschreibung |
|---|---|
| Liste neu laden | Option zum Aktualisieren der Liste der DLP-Incidents, wenn Sie eine Aktualisierung vornehmen. |
| Listenaktionen | Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt:<br>▪ **Speichern unter**<br>▪ **Spalten bearbeiten**<br>▪ **Breiten zurücksetzen** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>Wenn Sie eine eigene benutzerdefinierte Liste haben, die im Abschnitt „ **Meine Listen** “ für Ihren Arbeitsbereich erstellt wird, können Sie auch die folgenden zusätzlichen Listenaktionen ausführen:<br>▪ **Umbenennen**<br>▪ **Speichern**<br>▪ **Löschen** |
| URL kopieren für Alle | Option zum Kopieren der URLs aller DLP-Incidents. |
| Filterbereich anzeigen | Option, um die erforderlichen Incidents mithilfe der Filteroption aufzuschlüsseln.<br>**i.** Klicken Sie oben links auf der Seite auf den Filter und wählen Sie **Erweiterte Ansicht aus**.<br>**ii.** Verwenden Sie einen vorhandenen Filter, oder erstellen Sie einen eigenen, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und Werte enthalten.<br>**iii.** Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** oder **ODER**:<br>▪ Wenn **UND** ausgewählt ist, müssen alle Bedingungen erfüllt sein.<br>▪ Wenn **OR** ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.<br>**iv.** Klicken Sie auf **Aktualisieren**. |
| Incident zuweisen | Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt:<br>▪ **Incident**zuweisen an: Option, um den Incident einem Analysten, Endbenutzer oder einer anderen Person zuzuweisen.<br>▪ **Benutzer**: Option, um zu bestimmen, welchem Benutzer der Incident zugewiesen werden soll.<br>▪ **Incident-Status Vorbenutzerantwort**: Option, um zu bestimmen, in welchem Status sich der Incident befinden soll, bevor der Benutzer antwortet. Es kann sich auch um einen benutzerdefinierten Status handeln.<br>▪ **Bewertung**anhängen: Option, um anzugeben, ob Sie dem Incident eine |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
|---|---|
| | Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar:<br>▪ **Bewertungsvorlage**: Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident.<br>▪ **Incident-Status nach Benutzerantwort** Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Benutzer reagiert hat. |
| Beantworten | Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Benutzer beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann der Benutzer die Option **Gelöschte Datei** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare angeben.<br>Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern**. |
| Eskalation | Aktion zum Eskalieren des Incident. Sie können den Incident eskalieren, indem Sie den Benutzer auswählen, an den er eskaliert werden soll. Sie können auch zusätzliche Informationen im Feld Kommentare eingeben. |
| Status aktualisieren | Aktion zum Aktualisieren des Status des Incident. Sie können den Status des Incident aktualisieren, indem Sie einen der Status aus den Dropdown-Optionen auswählen. Es kann sich auch um einen benutzerdefinierten Status handeln. |
| Schließen | Aktion zum Schließen des Incident. Sie können auch zusätzliche Kommentare hinzufügen, bevor Sie den Incident schließen. |

**c.** Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen.

- Registerkarte „**Details** “: Zeigt die folgenden Abschnitte an:
  - **Details**: Sie können die Details des DLP-Incident anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname usw. Sie haben auch die Möglichkeit, die Felder Schweregrad, Status, Endbenutzer und DLP-Analystengruppe zu ändern und zu speichern.
  - **Verfassen**: Um Kommentare zum DLP-Incident hinzuzufügen, die für alle sichtbar sind, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Aktivität**: Sie können die Details der verschiedenen Aktivitäten im DLP-Incident anzeigen.
- **Anhänge**: Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen**, und wählen Sie den Anhang auf Ihrem lokalen Laufwerk aus.

- Registerkarte**Zusätzliche Details** : Zeigt alle zusätzlichen Informationen zum DLP-Incident an, einschließlich benutzerdefinierter Felder.

**Wichtig:**

- Benutzerdefinierte Felder für DLP-Incidents werden nur ab der Version San Diego unterstützt.
- Sie können die Registerkarte **Zusätzliche Details** verwenden, um festzustellen, ob benutzerdefinierte Felder für einen bestimmten DLP-Incident erstellt wurden.

- Registerkarte**Benutzerdefinierte Attribute** : Zeigt die Liste der benutzerdefinierten Attribute an, die sich auf den DLP-Incident beziehen.
- **Andere Incidents vom Endbenutzer**: Zeigt den Incident desselben Endbenutzers an. Sie können Incidents konsolidieren, indem Sie die Aktion **Als untergeordneten Incident** hinzufügen aus dieser zugehörigen Liste ausführen.
- **Typ**der erkannten vertraulichen Informationen: Zeigt die erkannten vertraulichen Informationen des Incident an.

**Hinweis:**
Diese zugehörige Liste ist nur für die DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Im Incident-Datensatz von Microsoft oder Symantec wird immer dann, wenn der Benutzer auf den Datensatz des erkannten vertraulichen Informationstyps zugreift, der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

- **Untergeordnete Incidents**: Zeigt die untergeordneten Incidents an, die manuell (durch Ausführen der Aktion „Als untergeordneten Incident hinzufügen“ ) oder aus den DLP-Konsolidierungsregeln erstellt wurden. Sie können die Verknüpfung des Nachfolge-Incident aufheben, indem Sie in dieser zugehörigen Liste „Verknüpfung des Nachfolge-Incident aufheben“ ausführen.
- **Geklonte Incidents**: Zeigt die geklonten Incidents aus dem übergeordneten Incident an. Durch Klicken auf die Aktion **Incident** klonen der Formularansicht können Sie einen neuen geklonten Incident erstellen.
- Registerkarte „**Bewertungen** “: Zeigt die Liste der Bewertungen an, die dem DLP-Incident zugewiesen sind.

**d.** Wählen Sie die für Sie geeignete Option aus.

| Option | Beschreibung |
|---|---|
| Incident zuweisen | Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | ▪ **Incident**zuweisen an: Option, um den Incident einem Analysten, Endbenutzer oder einer anderen Person zuzuweisen.<br>▪ **Benutzer**: Option zum Auswählen des Benutzers, dem der Incident zugewiesen werden soll.<br>▪ **Incident-Status Vorbenutzerantwort**: Option zum Auswählen des Status, in dem sich der Incident befinden soll, bevor der Benutzer antwortet. Es kann sich auch um einen benutzerdefinierten Status handeln.<br>▪ **Bewertung**anhängen: Option, um anzugeben, ob Sie dem Incident eine Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar:<br>  ▪ **Bewertungsvorlage**: Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident.<br>  ▪ **Incident-Status nach Benutzerantwort**: Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Benutzer geantwortet hat. |
| Genehmigung abbrechen | Aktion zum Abbrechen der Genehmigungsanforderung.<br><br>Diese Aktion ist für Analysten in der Formularansicht nur sichtbar, wenn sich der DLP-Incident im Status **„Genehmigung ausstehend** “ befindet. Verfügbare Optionen:<br><br>▪ **Incident**zuweisen an: Option, um den Incident niemandem, einem Analysten oder einer anderen Person zuzuweisen.<br>▪ **Benutzer**: Option zum Auswählen des Benutzers, dem der Incident zugewiesen werden soll.<br>▪ **Incident-Status**nach Abbruch: Option zum Auswählen des Status, in dem sich der Incident nach Abbruch der Anforderung befinden soll.<br>▪ **Kommentare**: Zur Bereitstellung zusätzlicher Details für die Stornierung. |
| Bewertung zuweisen | Aktion zum Anfügen einer Bewertung bei der Zuweisung des Incident. Auswahlmöglichkeiten: |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | ▪ **Bewertungsvorlage**: Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident.<br>▪ **Incident-Status nach Benutzerantwort**: Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Benutzer geantwortet hat. |
| Datei herunterladen | Aktion zum Herunterladen der Datei oder E-Mail mit dem Verstoßinhalt. Diese Aktion kann für Incidents ausgeführt werden, die für Microsoft OneDrive, SharePoint Online oder Exchange Online erstellt wurden. |
| Speichern | Aktion zum Speichern der von Ihnen vorgenommenen Änderungen. Sie haben die Möglichkeit, die Felder Schweregrad, Status und Endbenutzer des DLP-Incident zu ändern und zu speichern. |
| Beantworten | Reagieren Sie auf einen Incident, indem Sie eine Option zur Reaktion auf Incidents auswählen. Wenn ein Benutzer beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann der Benutzer die Option **Gelöschte Datei** wählen, um manuell zu bestätigen, dass die Datei gelöscht wurde, und Kommentare angeben.<br><br>Hier können Sie auch die erweiterten Antwortoptionen auswählen. **Beispiel: E-Mail-Freigabe aus Quarantäne anfordern**. |
| Eskalation | Aktion zum Eskalieren des Incident. Sie können den Incident eskalieren, indem Sie den Benutzer auswählen, an den er eskaliert werden soll. Sie können auch zusätzliche Informationen im Feld Kommentare eingeben. |
| Klonen Sie den Incident | Aktion zum Erstellen eines Klon-Incident, wenn der Incident-Datensatz mehrere Benutzer betrifft. Sie können die geklonten Incidents mehreren Stakeholdern zuweisen, z. B. Rechtsabteilung/IT.<br><br>Nachdem Sie einen geklonten Incident-Datensatz erstellt haben, wird unter dem übergeordneten DLP-Incident eine neue Registerkarte „ **Geklonte Incidents** “ erstellt, und alle geklonten Incidents werden in dieser Ansicht aufgelistet. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

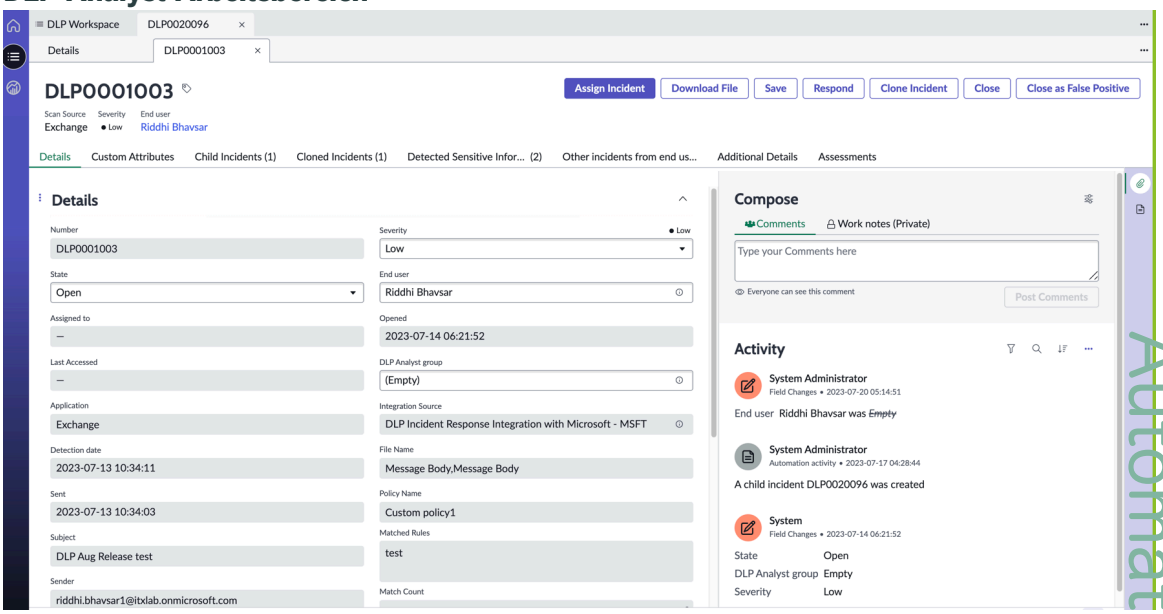
| Option | Beschreibung |
| --- | --- |
| | **Hinweis:**<br>▪ Wenn der übergeordnete DLP-Incident-Datensatz geschlossen wird, werden alle geklonten Incident-Datensätze automatisch geschlossen.<br>▪ Wenn ein DLP-Incident-Datensatz einen geklonten Incident enthält, kann dieser nicht Endbenutzern zugewiesen werden. Die übergeordneten DLP-Incident-Datensätze können nur von Benutzern mit der Rolle „Analyst“ verwaltet werden.<br>▪ Sie haben auch die Möglichkeit, den übergeordneten Status basierend auf dem Status der geklonten Incidents im Modul „Standardkonfiguration“ automatisch zu aktualisieren. Wenn beispielsweise alle geklonten Incidents in den Status „Eskaliert“ verschoben werden, wird auch der übergeordnete Incident in den Status „Eskaliert“ verschoben. |
| Schließen | Aktion zum Schließen des Incident. Sie können auch zusätzliche Kommentare hinzufügen, bevor Sie den Incident schließen. |
| Als falsch positiv schließen | Aktion, um den Incident als falsch positiv zu schließen. Sie können auch zusätzliche |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Option | Beschreibung |
| --- | --- |
| | Kommentare hinzufügen, bevor Sie den Incident schließen. |

**DLP-Analyst-Arbeitsbereich**




6. Sie können die Listenansicht auf der Homepage anzeigen, indem Sie oben links auf der Seite auf die Registerkarte **Listen** klicken.
   Die Kategorie „Listen“ besteht aus den standardmäßigen und benutzerdefinierten Listenseiten für DLP-Incidents.
   - Registerkarte „ **Listen** “: Standardlisten für DLP-Incidents. Im Folgenden sind die Standardlisten aufgeführt:
     - Alle
     - Offen
     - Meine Incidents
     - Meiner Gruppe zugewiesen
     - Eskaliert
     - Überfällig
     - Ausstehende Bewertungen
     - Anwenderaktion ausstehend
     - Geklonte Incidents
     - Archivierte Incidents
   - Registerkarte **Meine Listen**: Zeigt alle Listen an, die Sie umbenannt haben, und alle Listen, die Sie erstellt haben.

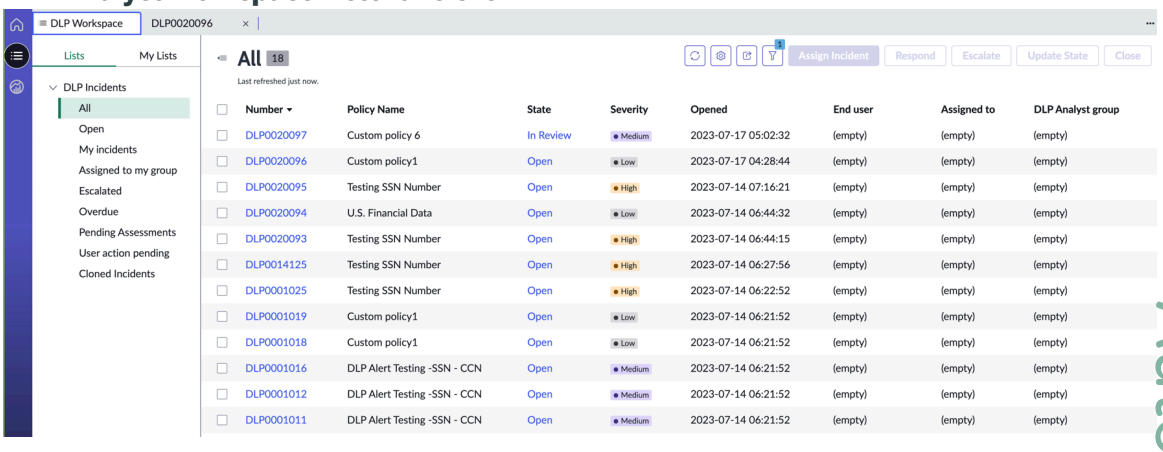
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Example

Das folgende Beispiel zeigt den DLP-Arbeitsbereich mit den Listenansichtskategorien. Die Option **Alle** Listenansicht ist ausgewählt.

**DLP Analyst Workspace Listenansicht**




## Zeigen Sie archivierte DLP-Incidents an

Verwenden Sie den DLP-Analysten-Arbeitsbereich, um die archivierten DLP-Incidents anzuzeigen

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst – DLP-Incidents bearbeiten und anzeigen.
- sn_dlir.analyst_read und sn_dlir.read – DLP-Incidents anzeigen.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Analyst-Arbeitsbereich**.
   Standardmäßig wird der Abschnitt Meine Incidents angezeigt.
2. Klicken Sie auf **Archivierte Incidents**.
   Die Liste der archivierten DLP-Incidents wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Incident** -Anzahl anzeigen, um die Anzahl der archivierten Incidents anzuzeigen.

   **Hinweis:**

   - Standardmäßig ist die Anzahl der archivierten Incidents ausgeblendet, um die Ladezeit der Liste zu verbessern. Sie müssen auf die Schaltfläche Incident-Anzahl anzeigen klicken, um die Anzahl der **Incidents** anzuzeigen. Außerdem wird eine Informationsmeldung mit der Anzahl der Incidents angezeigt.
   - Die Systemeigenschaft glide.ui.list.seismic.omit.count ist im Basissystem für die archivierten Incidents aktiviert, um die Anzahl der Incidents-Listen auszublenden.

4. Wählen Sie einen oder mehrere DLP-Incidents aus, die Sie anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der DLP-Incident zeigt den Abschnitt mit Incident-Details an.

**Hinweis:**

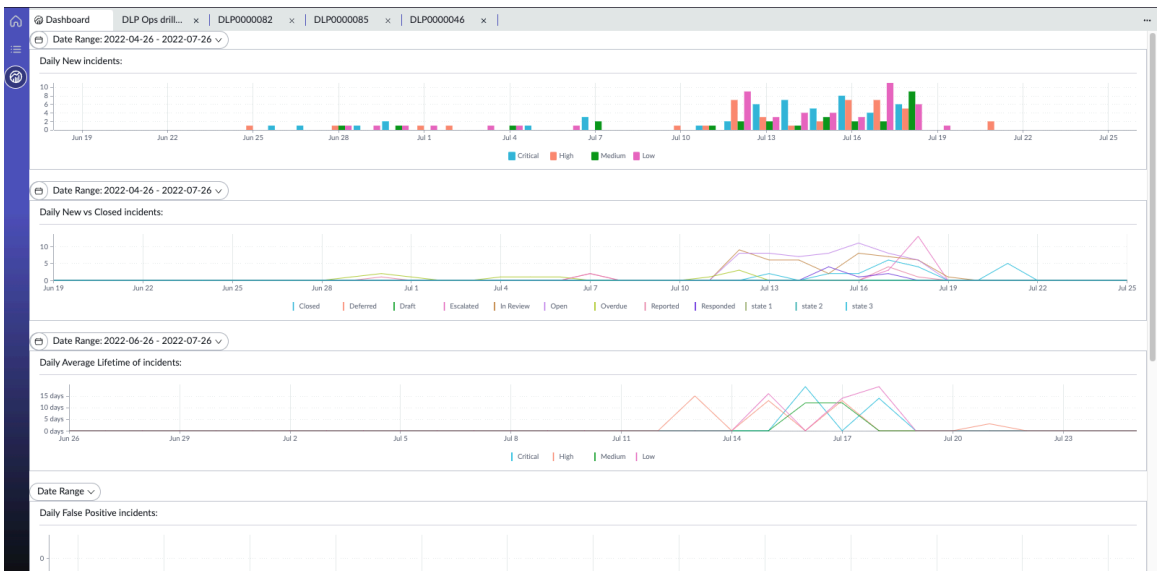
- Die Registerkarte **Andere Incidents von Endbenutzern** enthält auch die archivierten Incidents.
- **„Inhalt abgleichen** “ wird für alle archivierten Incidents unterstützt (was auch in allen Integrationen unterstützt wird), **„Datei herunterladen“** wird jedoch nur für Microsoft-Integrationen unterstützt.

## Data Loss Prevention Incident Response-Dashboard

Das Data Loss Prevention Incident Response (DLP IR) Dashboard bietet eine allgemeine Übersicht über Ihre DLP-Incidents und täglichen Incident-Trends in Ihrer Instanz in Form von grafischen Diagrammen. Mit diesen Diagrammen können Sie DLP-Incidents effektiv anzeigen, verwalten und beheben.

Das Dashboard Data Loss Prevention Incident Response bietet täglich wichtige Einblicke in Ihre DLP-Incidents. Sie können Indikatoren einrichten und regelmäßig Daten-Snapshots der Incidents erfassen, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert. Um die DLP-Incidents in verschiedenen Zeitintervallen zu analysieren, können Sie verschiedene Datumsbereiche anwenden.

**DLP-Dashboard**




### Analysieren Sie die täglichen Incident-Trends in Ihren DLP-Incidents

Greifen Sie auf das Dashboard Data Loss Prevention Incident Response (DLP IR) zu, um die täglichen Trends in Ihren DLP-Incidents zu analysieren und sie effektiv zu beheben.

#### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.analyst – DLP-Incidents bearbeiten und anzeigen.
- sn_dlir.analyst_read und sn_dlir.read – DLP-Incidents anzeigen.

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können die täglichen Trends mithilfe von Widgets im DLP-Dashboard visualisieren. Die Daten oder Statistiken für die täglichen Trends Ihrer DLP-Incidents werden aus den von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihrer Organisation definierten Indikatoreigenschaften für tägliche Incidents erfasst. Sie können wichtige Einblicke gewinnen, indem Sie verschiedene Datenbereiche anwenden, um die DLP-Incidents in verschiedenen Zeitintervallen für die folgenden Diagramme zu analysieren:

- **Tägliche neue Incidents**: Daten der gesamten DLP-Incidents, die täglich erstellt werden, unabhängig vom Status der Incidents. Die DLP-Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich Mittel, Kritisch, Hoch und Niedrig. Jeder DLP-Incident-Schweregrad wird im Diagramm durch eine bestimmte Farbe dargestellt.
- **Tägliche neue und geschlossene Incidents**: Die verschiedenen Status der DLP-Incidents und ein Vergleich zwischen den täglichen neuen Incidents und den täglichen geschlossenen Incidents. Die Kategorie „Täglich neu“ enthält alle DLP-Incidents mit den Status „Offen“, „Entwurf“, „Eskaliert“, „Wird überprüft“, „Überfällig“, „Gemeldet“, „Beantwortet“ oder „Benutzerdefiniert“ (falls vorhanden). Die Incident-Kategorie „Geschlossen“ enthält die geschlossenen DLP-Incidents. Jeder DLP-Incident-Status wird im Diagramm durch eine bestimmte Farbe dargestellt.
- **Tägliche durchschnittliche Lebensdauer von Incidents**: Die Lebensdauer eines Incident ist der Zeitraum zwischen dem Öffnen und Schließen eines bestimmten DLP-Incidents. Die tägliche durchschnittliche Lebensdauer wird nur für geschlossene DLP-Incidents berechnet.
- **Tägliche falsch positive Incidents**: Daten aller DLP-Incidents, die als tägliche falsch positive Meldungen gemeldet werden. Die täglichen falsch positiven Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich Mittel, Kritisch, Hoch und Niedrig. Jeder tägliche falsch positive Incident-Schweregrad wird durch eine bestimmte Farbe im Diagramm dargestellt.
- **Alter vs. Schweregrad der Incidents**: Datenvergleich aller DLP-Incidents, kategorisiert nach Alter und konfiguriert mit dem Schweregrad der DLP-Incidents. Die Alterskategorie enthält alle DLP-Incidents unter dem von Ihrer Organisation definierten Alter. Weitere Informationen zu Altersdiagrammen finden Sie unter Konfigurieren Sie das Altersdiagramm für Ihre DLP-Incidents. Der Schweregrad der Incidents umfasst alle DLP-Incidents in der Kategorie „Hoch“ oder „Niedrig“. Jeder Schweregrad wird im Diagramm durch eine bestimmte Farbe dargestellt.
- **Täglich eskalierte Incidents**: Daten aller täglich eskalierten DLP-Incidents. Die täglich eskalierten Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich Mittel, Kritisch, Hoch und Niedrig. Jeder täglich eskalierte Incident-Schweregrad wird im Diagramm durch eine bestimmte Farbe dargestellt.

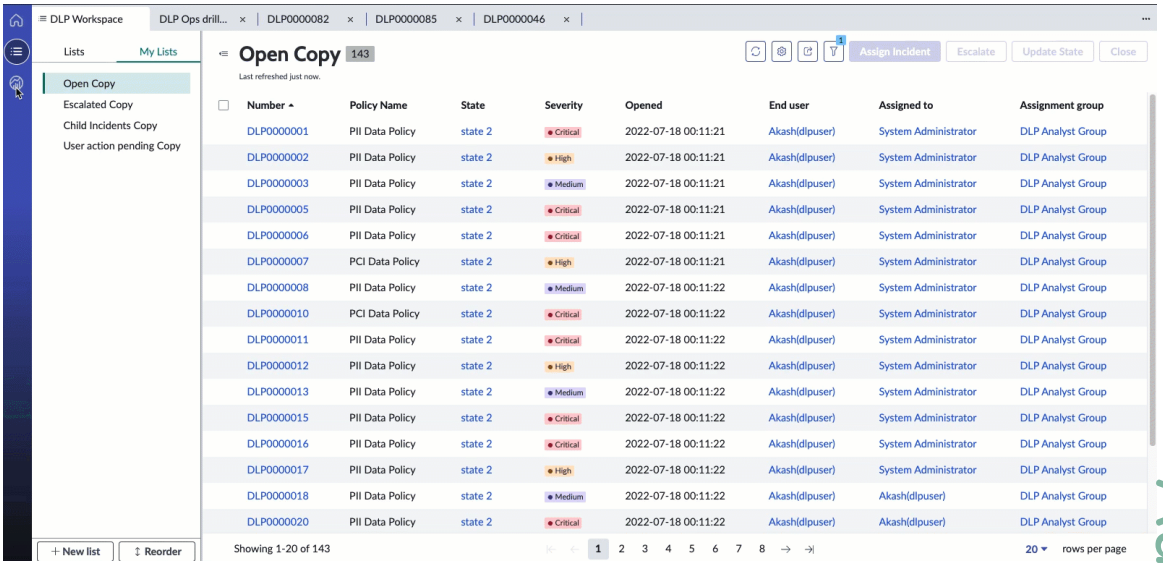
### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Dashboard**.
   Die Seite „Mein DLP-Dashboard“ wird auf einer neuen Browserregisterkarte angezeigt.
2. Wählen Sie ein Dashboard-Widget aus, für das Sie eine tägliche Trendanalyse durchführen möchten. Zum Beispiel das Diagramm „Tägliche neue Incidents“.
3. Überprüfen Sie die Dashboard-Widgets, um Trends zu erkennen.
4. Klicken Sie auf **Datumsbereich**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**DLP-Dashboard – Übersicht**




5. Wählen Sie im Kalender einen Datumsbereich aus, und klicken Sie auf **Anwenden**.

   **Example**
   Beispielsweise wird das Diagramm „Tägliche neue Incidents“ für den ausgewählten Datenbereich aktualisiert.

6. Verwenden Sie die Filter unter dem Diagramm, um Detailinformationen und eine eingehendere Analyse durchzuführen.

## Eingehende Integration für Data Loss Prevention Incident Response

Erstellen Sie einzelne oder mehrere DLP-Incidents mithilfe der Inbound REST API.

### Erstellen Sie einen einzelnen DLP-Incident

Erforderliche Rolle: sn_dlir.api_integration_user.

Um einen einzelnen DLP-Incident zu erstellen, definieren Sie die folgenden Parameter nach Bedarf:

| Feld | Beschreibung |
|---|---|
| HTTP-Methode | `POST` |
| URL | https://{instance}/api/now/import/sn_dlir_incident_import |
| Anforderungs-Header | **Akzeptieren:** `application/json` **Inhaltstyp:** `application/json` |
| Beispielnutzlast | `{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>",` |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | "data_owner_email": "<value>",<br>"destination": "<value>",<br>"dest_ip": "<value>",<br>"dest_ip_port": "<value>",<br>"detection_date": "<value>",<br>"endpoint_on_corporate_net": "<value>",<br>"files": "",<br>"file_created": "",<br>"file_created_by": "",<br>"file_location": "",<br>"file_modified_by": "",<br>"file_name": "",<br>"file_owner": "",<br>"file_permissions": "",<br>"ftp_user_name": "",<br>"last_modified": "",<br>"machine_ip": "",<br>"machine_name": "",<br>"match_count": "",<br>"policy_id": "",<br>"policy_name": "",<br>"printer_name": "",<br>"printer_type": "",<br>"print_job_name": "",<br>"recipients": "",<br>"scanned_machine": "",<br>"scan_source": "",<br>"seen_before": "",<br>"sender":"",<br>"source":"",<br>"source_file":"",<br>"source_ip":"",<br>"source_ip_port":"",<br>"subject":"",<br>"url":"",<br>"user_justification":""<br>} |
| Beispielantwort | {<br>"import_set": "ISET0010003",<br>"staging_table": "sn_dlir_incident_import",<br>"result": [<br>{<br>"transform_map": "",<br>"table": "sn_dlir_incident",<br>"display_name": "number",<br>"display_value": "DLP0001012",<br>"record_link":<br>"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",<br>"status": "inserted",<br>"sys_id": "7cda322297c2411056a43d1e6253af1f"<br>} |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | ]<br>} |

### Erstellen Sie mehrere DLP-Incidents

Erforderliche Rolle: sn_dlir.api_integration_user.

Um mehrere DLP-Incidents aus derselben Anforderung zu erstellen, definieren Sie die folgenden Parameter nach Bedarf:

| Feld | Beschreibung |
| --- | --- |
| HTTP-Methode | `POST` |
| URL | https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple |
| Anforderungs-Header | **Akzeptieren:**<br>`application/json`<br>**Inhaltstyp:**<br>`application/json` |
| Beispielnutzlast | <pre>{<br>"records": [<br>{<br>"file_name": "<value>",<br>"file_modified_by": "<value>",<br>"work_notes": "<value>",<br>"url": "<value>",<br>"scan_source": "<value>",<br>"data_owner_email": "<value>",<br>"file_created_by": "<value>",<br>"file_owner": "<value>",<br>"policy_name": "<value>"<br>},<br>{<br>"dest_ip": "<value>",<br>"dest_ip_port": "<value>",<br>"detection_date": "<value>",<br>"endpoint_on_corporate_net": "<value>",<br>"files": "<value>",<br>"file_created": "<value>",<br>"file_created_by": "<value>",<br>"file_location": "<value>",<br>"file_modified_by": "<value>",<br>"file_name": "<value>",<br>"file_owner": "<value>",<br>}<br>]<br>}</pre> |
| Beispielantwort | <pre>{<br>"import_set_id": "a38f69229734dd1056a43d1e6253af75",</pre> |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | "multi_import_set_id": "e78f69229734dd1056a43d1e6253af75" } |

**Hinweis:**
Standardmäßig ist die Transformation asynchron. Um die synchrone Transformation festzulegen, erstellen Sie einen neuen Datensatz in der Tabelle „REST – Mehrere einfügen“ [sys_rest_insert_multiple], wählen Sie als **Quelltabelle sn_dlir_incident_import aus**, und legen Sie die Transformation auf **synchron**fest.

## DLP-Integrationen

Das Data Loss Prevention Incident Response -Basissystem enthält Integrationen in Softwarepakete zur Verhinderung von Datenverlust von Drittanbietern.

Dieser Abschnitt enthält Anweisungen zum Aktivieren der Plugins und zum Konfigurieren von ServiceNow und Integrationen von Drittanbietern. Außerdem sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen enthalten, die im Basissystem enthalten sind.

### Integrationskonfigurationen

Das Basissystem enthält eine Reihe von Karten für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von Security Operations -Plugins aufweisen. Die Integrationskarten können durch Auswahl von angezeigt werden **Security Operations** > **Integrationskonfigurationen**.

Data Loss Prevention Incident Response unterstützt die folgenden Softwarepakete von Drittanbietern zur Verhinderung von Datenverlust:

### Symantec Integration für Data Loss Prevention Incident Response

Die Symantec DLP-Integration unterstützt die Erfassung von Data Loss Prevention Incident Response Incidents, die in der Bereitstellung von [ Symantec Data Loss Prevention Incident Response erstellt wurden. Nach der Erfassung können Sie die Incident Management-Funktionalitäten verwenden, um die DLP-Incidents zu beheben.

### Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

### Übersicht und wichtige Funktionen

Die Symantec DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Möglichkeit, mehrere Integrationsprofile für verschiedene Symantec API-Endpunkte zu erstellen.
- Geplante Erfassung von DLP-Incidents aus Symantec in Ihrer Instanz von [ ServiceNow.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Möglichkeit, API-Filter anzuwenden, um die Incidents abzurufen, die den Filterkriterien entsprechen, und auch den Filter für Symantec DLP-Incidents anzugeben, die importiert werden müssen.
- Ordnen Sie die DLP-Incident-Status in Ihrer Instanz ServiceNow den DLP-Incident-Status in Symanteczu.
- Aktualisieren Sie den Incident-Status in Symantec automatisch, wenn sich der Status in Ihrer Instanz von ServiceNow ändert.
- Möglichkeit zum Anpassen und Definieren der Schweregradzuordnung zwischen Symantec DLP-Incidents und ServiceNow-Incidents.

Weitere Informationen zur Integration finden Sie in der Symantec-Produktdokumentation .

### Erste Schritte mit der Symantec DLP-Integration für Data Loss Prevention

Bevor Sie die Integration verwenden können, müssen Sie sie aus dem ServiceNow® Storeherunterladen.

## Prüfliste

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihrer Symantec DLP-Integration zur Verhinderung von Datenverlust beginnen.

**Prüfliste**

| Feld | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen MID-Anwendungsrollen Now Platform, Data Loss Prevention-Anwendung und zugewiesen haben. | Die folgenden Rollen werden in der DLP-Integration von [] auf SymantecNow Platformverwendet:<br>• Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow® Store und weist den Data Loss Prevention-Administrator (sn_dlir.admin) zu.<br>• Benutzer mit der Rolle „sn_dlir.admin“ können die Integration konfigurieren und die Incident-Profile einrichten.<br>• Die Benutzer mit der Rolle „sn_dlir.analyst“ haben Leserollen in der gesamten Integration. |
| Weisen Sie die erforderlichen Symantec DLP-Benutzerrollen zu. | Überprüfen Sie die Rollen und Berechtigungen für die Symantec DLP-Integration. |
| Vergewissern Sie sich, dass Sie Symantec DLP 15.8 verwenden | Die Symantec DLP-Integration für Data Loss Prevention wird mit Version 15.8 von Symantec Data Loss Prevention getestet.<br>**Hinweis:**<br>Stellen Sie sicher, dass Sie Symantec DLP 15.8 verwenden |
| Vergewissern Sie sich, dass ServiceNow® Kernanwendungen, die zur Unterstützung der | Vergewissern Sie sich, dass die folgenden DLP-Anwendungen und allgemeinen Sicherheitsunterstützungsanwendungen aus dem |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Feld | Beschreibung |
|---|---|
| Symantec DLP-Integration erforderlich sind, installiert und aktiviert sind. | ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung.<br>• Security Support Common<br>• Data Loss Prevention Incident Response |

### Installieren und konfigurieren Sie die Symantec DLP-Integration für Data Loss Prevention

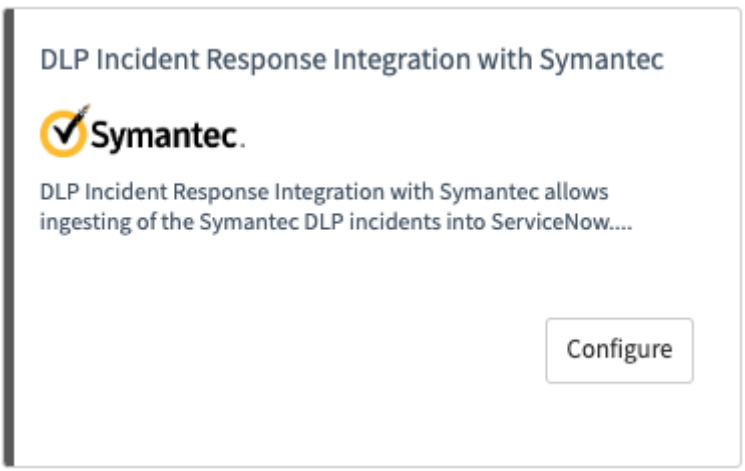
Installieren und konfigurieren Sie die Symantec DLP-Integration aus dem ServiceNow® Store in Ihrer Now Platform -Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mit den Symantec DLP-Incident-Daten.

### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

### Prozedur

1. Laden Sie die Symantec DLP-Integration aus dem ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel „DLP Incident Response Integration with Symantec“, und klicken Sie auf **Konfigurieren**.




4. Füllen Sie die Felder des Formulars aus.

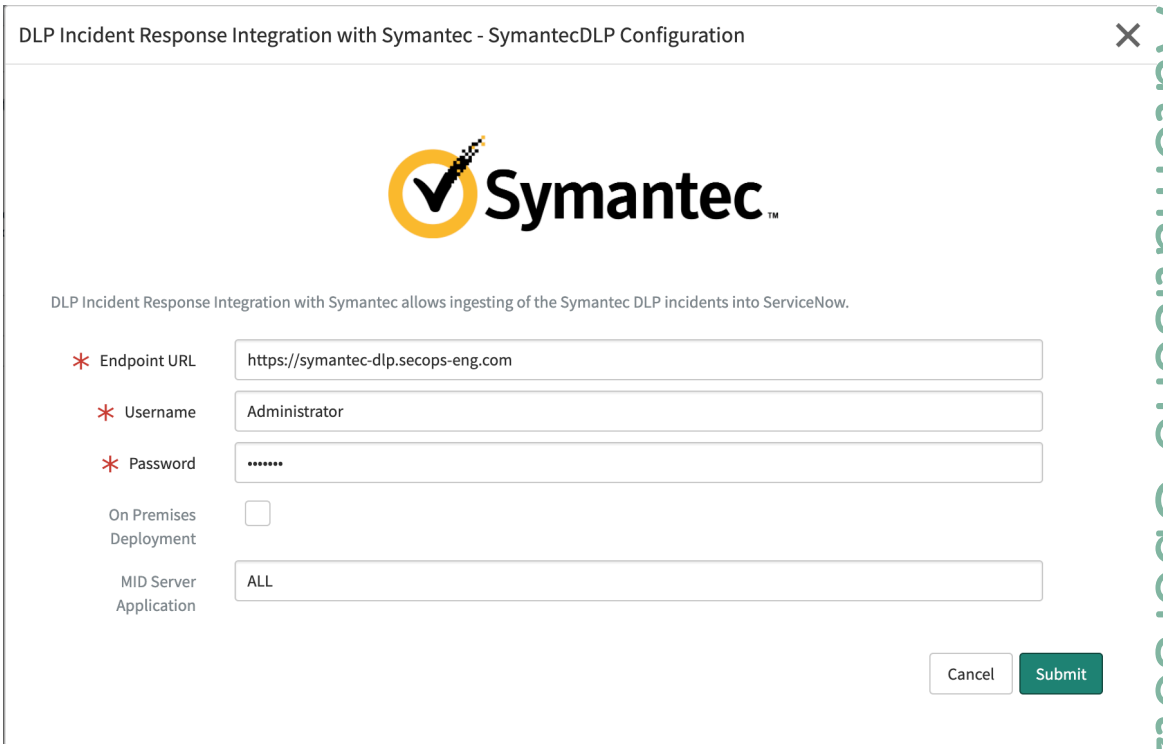
**Formular „Konfiguration der Symantec DLP-Integration“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Symantec DLP-Integrationskonfiguration. |
| Endpunkt-URL | Symantec REST-API-Endpunkt. |
| Benutzername | Symantec Kontoname. Weitere Informationen zu den erforderlichen Rollen und Berechtigungen finden Sie unter Rollen und Berechtigungen . |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Passwort | Symantec -Kontopasswort. |
| Lokale Bereitstellung | Option, die Sie auswählen können, wenn Symantec in einer lokalen Instanz bereitgestellt wird. Wenn Sie diese Option auswählen, müssen Sie den MID Server verwenden, um eine Verbindung zu Symantec herzustellen. |
| MID-Server-Anwendung | Der MID-Anwendungsname, der für die Kommunikation mit Symantecverwendet wird.<br><br>Dieses Feld ist erforderlich, wenn Sie die Option **Lokale Bereitstellung** auswählen. |




Automatische Übersetzung

5. Klicken Sie auf **Absenden**.

### Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Symantec DLP-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

## Erstellen Sie ein Profil für die Symantec DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform. Bestimmen Sie die Symantec DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

### Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie [], um die DLP-Incidents vom Endpunkt SymantecNow Platform® abzurufen. Speichern Sie diese Incidents in Ihrer Instanz ServiceNow® als DLP-Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Symantec DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt „Name“ aus.

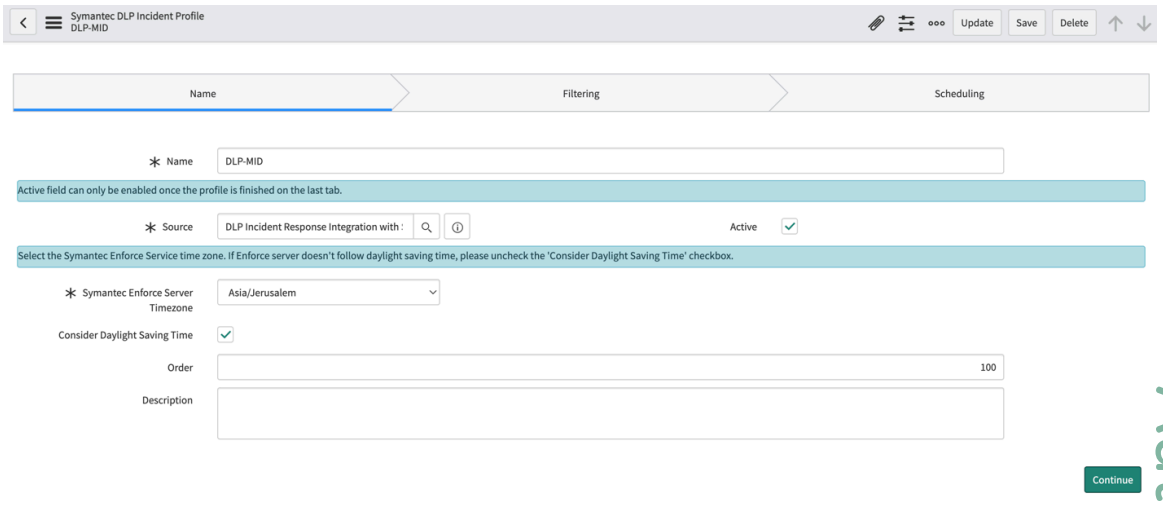
#### Erstellen Sie ein Profil

| Feld | Beschreibung |
|---|---|
| Name | Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren.<br>**Hinweis:**<br>Der Name muss für jedes Profil eindeutig sein. |
| Quelle | Symantec DLP-Instanz, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten. |
| Aktiv | Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann erst aktiviert werden, nachdem Sie im Abschnitt Zeitplanung auf Fertigstellen **geklickt** haben.<br>Wenn das Profil aktiv ist, bedeutet dies, dass Now Platform aktiv Symantec DLP-Incidents abfragt. Die entsprechenden DLP-Incidents werden in DLP erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Planungsparametern abgeglichen werden. |
| Symantec Enforce Server – Zeitzone | Wählen Sie die Zeitzone für den Symantec Enforce-Server im Profil aus, damit Incidents aufgrund von Zeitzonenproblemen nicht übersehen werden. |
| Sommerzeit berücksichtigen | Aktivieren Sie diese Checkbox, wenn der Erzwingungsserver die Sommerzeit einhält. |
| Reihenfolge | Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet.<br>Standardmäßig ist der Wert 100. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Beschreibung | Eindeutige Beschreibung für dieses Profil. |




## Nächste Maßnahme

Klicken Sie auf **Fortfahren**, um zum Abschnitt Filtern zu wechseln.

### Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden Symantec DLP-Incidents aufzuschlüsseln. Bestimmen Sie die Incidents, die als DLP-Incidents in ServiceNow® erstellt werden sollen.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Warum und wann dieser Vorgang ausgeführt wird

Durch das Filtern können Sie DLP-Incidents isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents begrenzen. Wenn zusätzliche Filterkriterien festgelegt werden, werden nur Incidents erstellt, die den Bedingungen entsprechen.

## Prozedur

1. Aktivieren Sie das Kontrollkästchen **API-basierter Filter für Incident-** Erfassung, um die API-Filter anzuwenden und die Incidents abzurufen, die den Filterkriterien entsprechen.
2. Fügen Sie die API-Filter hinzu.
   Das folgende Beispiel zeigt die API-Filter.

```
{
            "operandOne": {
               "name": "incidentStatusName"
            },
            "filterType": "string",
            "operator": "EQ",
            "operandTwoValues": [
               "incident.status.New"
            ]
         }
```

Automatische Übersetzung

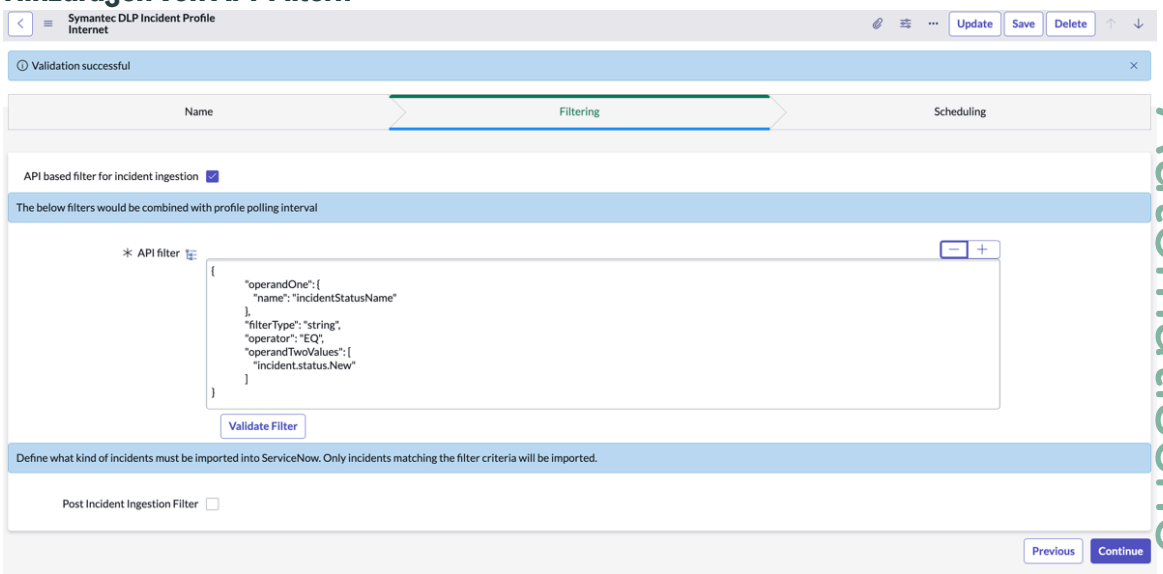
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Weitere Informationen zu den API-Filtern in der Symantec-Integration finden Sie unter Incident-Listen: Parameter – Anforderungsobjektdetails .

3. Klicken Sie auf **Filter validieren**, nachdem Sie die API-Filter angewendet haben.

**Hinweis:**
Wenn die Validierung nicht erfolgreich ist, wird eine Fehlermeldung angezeigt, die besagt, dass die Validierung fehlgeschlagen ist. Dies geschieht, wenn die Filter gemäß den Symantec-APIs nicht ordnungsgemäß eingegeben wurden.

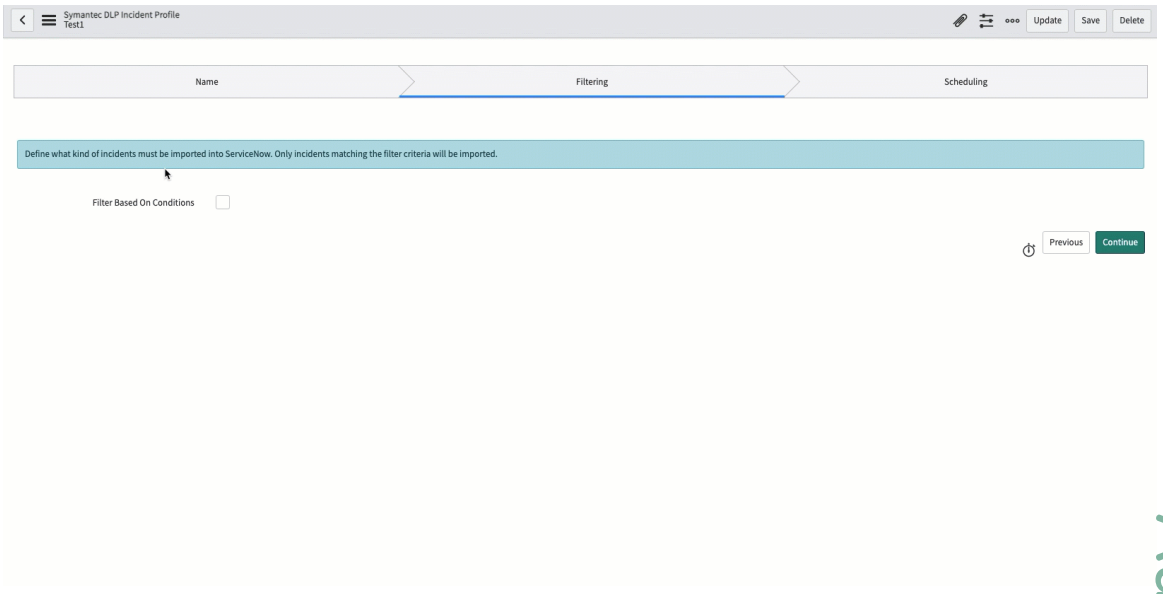
**Hinzufügen von API-Filtern**




4. Aktivieren Sie das Kontrollkästchen **Post Incident Ingestion Filter (Filter** für Nach-Incident-Erfassung), um die Kriterien zu definieren, die ein eingehender Symantec-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
Die Optionen im ersten Feld in den Filterbedingungen stimmen mit den Feldern überein, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.
5. Legen Sie im Bedingungsgenerator die Filter im Feld **Filterbedingungen** fest.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




6. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND**oder **ODER**.
   - Wenn **UND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR**ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.

### Nächste Maßnahme
Um den Zeitplan zu konfigurieren, klicken Sie auf **Fortfahren**.

## Planen Sie den Symantec DLP-Incident-Abruf

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und Symantec DLP-Incidents zu erfassen, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um festzulegen, wie und wann Sie Incidents aus Symantecabrufen .

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

### Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Zeitplanung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen **Einmaliger Abruf** so konfiguriert werden, dass es nur einmal abgerufen wird. Das Verlaufsdatum kann bis zu den letzten drei Monaten ab dem aktuellen Datum reichen.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Symantec DLP-Incident-Integration auswirken. Planen Sie bei der Zeitplanung, dass die Systemlast auf die Dringlichkeit eines Incident abgestimmt wird.

### Prozedur

1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie die Felder im Formular aus.



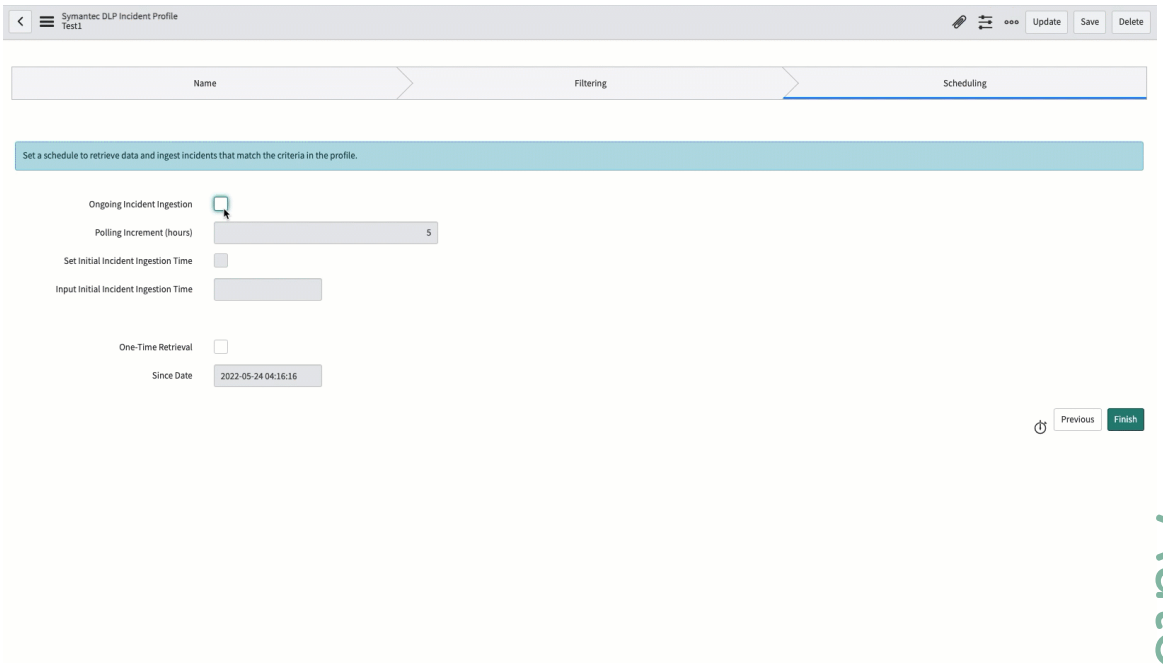
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Zeitplan für den DLP-Incident

| Feld | Beschreibung |
|---|---|
| Laufende Incident-Erfassung | Die laufende Incident-Erfassung, die die Instanz Now Platform für neue Incidents von Symantec abruft. DLP-Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung übereinstimmen. |
| Abfrageschritt (Minuten) | Die Abfragehäufigkeit, die in Minuten definiert ist. Dieses Feld wird automatisch auf 300 Minuten festgelegt. |
| Zeitpunkt der ersten Incident-Erfassung festlegen | Option zum Definieren eines Datums und einer Uhrzeit für die erste Erfassung. Nachfolgende Erfassungen basieren auf dem Abfrageintervall. |
| Zeitpunkt der ersten Incident-Erfassung eingeben | Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben. |
| Zeitpunkt der ersten Incident-Erfassung | Zeitpunkt der ersten Erfassung der Daten.<br><br>Sie können sehen, dass Werte angezeigt werden, wenn die anfängliche Incident-Erfassungszeit festgelegt wird. |
| Nächste Incident-Erfassungszeit (geschätzt) | Nächster Zeitraum für eine geschätzte Incident-Erfassung. |
| Einmaliger Abruf | Option zum Aktivieren des einmaligen Abrufens historischer Daten.<br><br>Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten aus Symantec DLP gemäß dem Datum abgerufen, das im Feld **Seit Datum** hinzugefügt wurde. |
| Seit Datum | Datum, ab dem Daten von Symantec abgerufen werden sollen<br><br>Dieses Feld kann auf höchstens drei Monate festgelegt werden. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.






3. Um die erstellte Profilkonfiguration zu speichern, klicken Sie im Popup-Fenster auf **Fertig** stellen.
4. Um das Profil zu aktivieren, öffnen Sie das erstellte Profil.
5. Aktivieren Sie die Option **Aktiv**.
6. Klicken Sie auf **Aktualisieren**.

## Ergebnisse

Nach der erfolgreichen Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der DLP-Incident-Tabelle hinzugefügt.

### Zuordnung von Symantec DLP-Incident-Status zu ServiceNow Incident-Status

Synchronisieren Sie den Status der in ServiceNow erfassten DLP-Incidents mit den DLP-Incidents von Symantec. Ordnen Sie das Feld **ServiceNow Incident-Status** dem Feld **Symantec Incident-Status** zu.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Warum und wann dieser Vorgang ausgeführt wird

Der Incident-Status wird dynamisch aus der Endpunktquelle Symantec abgerufen, die in der Zuordnung hinzugefügt wird. Sie müssen eine 1:1-Zuordnung des Incident-Status durchführen.

## Prozedur

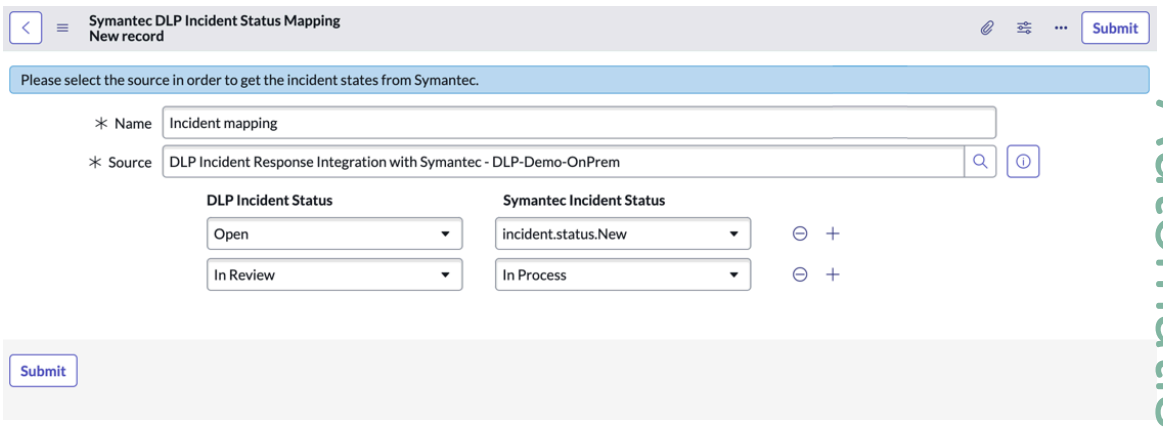
1. Navigieren zu **Symantec DLP-Integration** > **Incident-Statuszuordnung**.
2. Geben Sie einen **Namen** an, um die Zuordnung zu identifizieren.
3. Wählen Sie die **Quellintegration** aus, aus der Sie den Status abrufen möchten.
4. Ordnen Sie den **DLP-Incident-Status** dem **Symantec Incident-Status**zu.

**Hinweis:**
Es ist nicht erforderlich, alle Status zuzuordnen. Sie können nur die erforderlichen Status zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Statuszuordnung für Symantec-DLP-Incident

| Feld | Beschreibung |
|---|---|
| Name | Name des Zuordnungsdatensatzes. |
| Quelle | Die konfigurierte Symantec-Endpunktquelle, aus der Sie den Incident-Status abrufen möchten. |
| DLP-Incident-Status | Liste mit Status von DLP-Incidents. |
| Symantec-Incident-Status | Liste des Status, der aus der Quelle abgerufen wurde (Symantec-Endpunkt). |




5. Klicken Sie auf **Absenden**.

## Ergebnisse

Nach der erfolgreichen Erstellung des Datensatzes für die Zuordnungsstatus der ServiceNowServiceNow Incidents wird der Incident-Status Symantec mit dem DLP-Incident-Status [] synchronisiert.

Wenn Sie den Status eines DLP-Incident in Ihrer Instanz SymantecServiceNow ändern, wird der Status der zugeordneten DLP-Incidents auf der Quellplattform Symantec basierend auf der im Datensatz festgelegten Zuordnung geändert.

### Schweregradzuordnung zwischen Symantec DLP-Incidents und ServiceNow-Incidents

Verwenden Sie die Schweregradzuordnungsfunktion, um die Zuordnung zwischen Symantec -Incidents und Now Platform® -Incidents zu konfigurieren und zu synchronisieren.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Warum und wann dieser Vorgang ausgeführt wird

Mit der DLP-Schweregradzuordnung können Sie den Quellschweregrad dem DLP-Incident-Schweregrad zuordnen. Sie können den Quellschweregrad anpassen und definieren und ihn dem gewünschten DLP-Incident-Schweregradwert zuordnen.

## Prozedur

1. Navigieren zu **Symantec DLP-Integration** > **Incident-Schweregradzuordnung**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

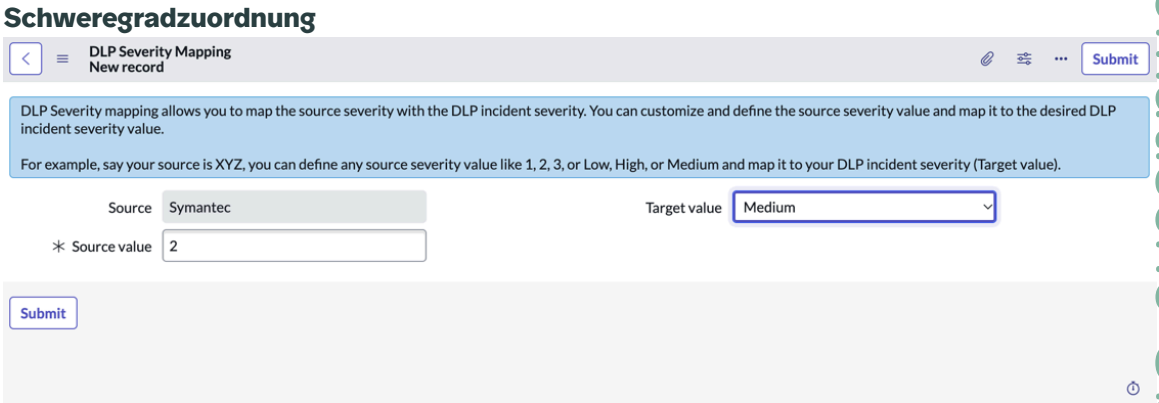
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### DLP-Schweregradzuordnung

| Feld | Beschreibung |
|---|---|
| Quelle | Die konfigurierte Symantec-Endpunktquelle, aus der Sie den Incident abrufen möchten. |
| Zielwert | Zielwert ist die DLP-Incident-Schweregrad-ID. Die verfügbaren Werte sind Kritisch, Hoch, Mittel, Niedrig und Info (wird in Symantec als Info-Schweregrad verwendet). |
| Quellwert | Quellwert ist der Schweregrad des Symantec-Incident. |

**Hinweis:**
Im Basissystem gibt es vier Schweregradzuordnungen, die an die DLP-Benutzer gesendet werden.

4. Klicken Sie auf **Absenden**.




## Konfigurieren Sie die Symantec DLP-Integrationseinstellungen

Ändern Sie die Standardsystemeigenschaften der Symantec DLP-Integration.

### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

### Prozedur

1. Navigieren zu **Symantec DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

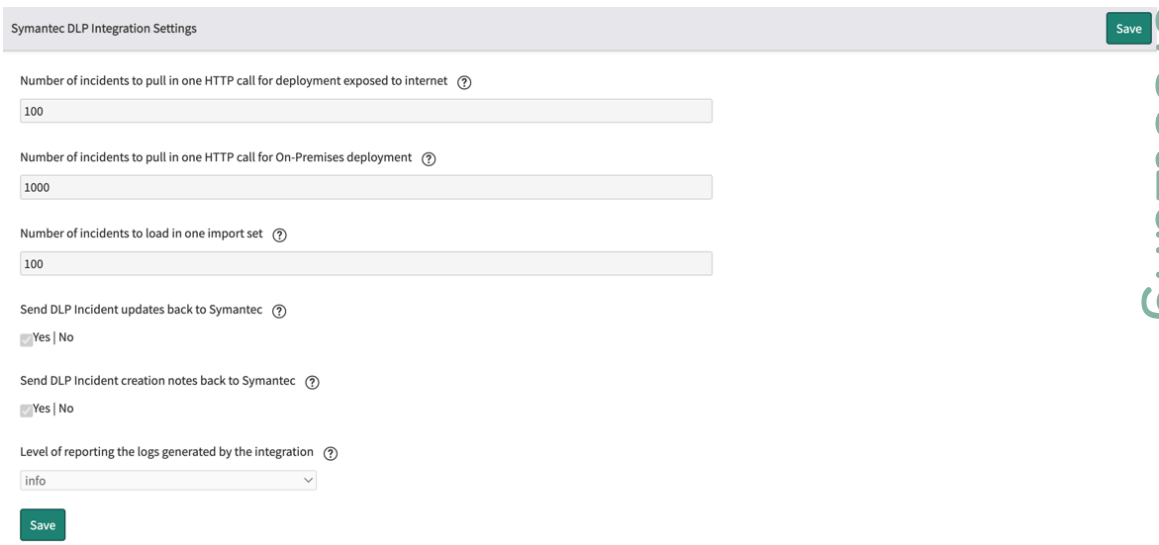
### Einstellungen

| Feld | Beschreibung |
|---|---|
| Erzwingen Sie eine Begrenzung der Anzahl der Incidents, die in einem HTTP-Aufruf für die lokale Bereitstellung sn_sym_dlp.page_size_on_prem abgerufen werden sollen | Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für die lokale Bereitstellung von Symantecabgerufen werden sollen.<br>○ Typ: Ganzzahl<br>○ Standardwert: 1000 |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| Erzwingen Sie eine Begrenzung der Anzahl der Incidents, die in einem HTTP-Aufruf für die Bereitstellung im Internet abgerufen werden sollen sn_sym_dlp.page_size_on_internet | Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für eine Symantec -Bereitstellung abgerufen werden sollen, die über das Internet verfügbar gemacht wird.<br>○ Typ: Ganzzahl<br>○ Standardwert: 100 |
| Anzahl der Incidents, die in einem Import Set sn_sym_dlp.incidents_per_attachment geladen werden sollen | Anzahl der Datensätze, die zur Verarbeitung in einer Anhangdatei gespeichert werden sollen.<br>○ Typ: Ganzzahl<br>○ Standardwert: 100 |
| Senden Sie DLP-Incident-Updates an Symantec sn_sym_dlp.incident_update zurück | Mit dieser Eigenschaft können Sie die Statussynchronisierung zwischen ServiceNow und Symantec DLP-Incidents einschränken.<br>○ Typ: Boolesch<br>○ Standardwert: **true** |
| Senden Sie DLP-Incident-Erstellungshinweise an Symantec sn_sym_dlp.incident_creation_notes | Mit dieser Eigenschaft können Sie eine Notiz an Symantec zurücksenden, sobald ein Incident in ServiceNowerstellt wird.<br>○ Typ: Boolesch<br>○ Standardwert: **true** |
| Ebene der Berichterstellung für die von der Integration sn_sym_dlp.logging.verbosity generierten Protokolle | Eigenschaft, die die Berichterstellung der von der Integration generierten Protokolle definiert. |




Automatische Übersetzung

3. Klicken Sie auf **Speichern**.

### Domänentrennung in der Symantec DLP-Integration

Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

### Support-Stufe

Support: Standard.

### Funktionsweise der Domänentrennung mit der Symantec DLP-Integration

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die DLP-Integrationsvorgänge Symantec in der entsprechenden Domäne aus.

### Integration von Data Loss Prevention Incident Response mit Proofpoint

Die Proofpoint DLP-Integration unterstützt die Erfassung von Data Loss Prevention-Incidents, die in der Data Loss Prevention-Bereitstellung von Proofpoint erstellt wurden. Nach der Erfassung können Sie die Incident Management-Funktionalitäten verwenden, um die DLP-Incidents zu beheben.

### Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

### Übersicht und wichtige Funktionen

Die Proofpoint DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellung mehrerer Profile für verschiedene Proofpoint -Endpunkte.
- Automatisierung der Erstellung von DLP-Incidents.
- Zuordnung des DLP-Incident-Statusfelds Proofpoint zum DLP-Incident-Statusfeld.
- Filtern von Proofpoint DLP-Incidents.
- Erfassung von Incidents in Ihrer Instanz ServiceNow, sobald die Incidents im DLP-Mandanten Proofpoint erstellt werden.
- Proofpoint Die DLP-Integration unterstützt sowohl Endpunkte als auch E-Mail-Typen von Incidents.
- Automatische Aktualisierungen für den DLP-Incident-Status Proofpoint und Kommentare für die DLP-Incident-Erstellung sowie für Statusänderung und -abschluss auf ServiceNow.

### Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| Proofpoint Produktdokumentations-Website | Proofpoint-Produktdokumentation |
| ServiceNow® Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erste Schritte mit der Proofpoint -Integration für Data Loss Prevention

Die Proofpoint DLP-Integration unterstützt die Erfassung von Data Loss Prevention-Incidents, die im Mandanten von Proofpoint Data Loss Prevention erstellt wurden. Nach der Erfassung werden die Incident-Management-Funktionalitäten verwendet, die die DLP-Incidents beheben.

## Prüfliste

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihrer Proofpoint DLP-Integration für Data Loss Prevention beginnen.

**Prüfliste**

| Feld | Beschreibung |
|---|---|
| Vergewissern Sie sich, dass Sie die erforderlichen Anwendungsrollen Now Platform und Data Loss Prevention Incident Response zugewiesen haben. | Die folgenden Rollen werden in der DLP-Integration von [] auf ProofpointNow Platformverwendet:<br>• Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow® Store und weist den Administrator für die Verhinderung von Datenverlust (sn_dlir.admin) zu.<br>• Benutzer mit der Rolle „sn_dlir.admin“ können die Integration konfigurieren und die Incident-Profile einrichten.<br>• Die Benutzer mit der Rolle „sn_dlir.analyst“ haben Leserollen in der gesamten Integration. |
| Weisen Sie die erforderlichen Proofpoint DLP-Benutzerrollen zu. | Überprüfen Sie die Rollen und Berechtigungen für die Proofpoint DLP-Integration. |
| Vergewissern Sie sich, dass Sie Proofpoint DLP 1.0.1 oder höher verwenden. | Die Proofpoint DLP-Integration für Data Loss Prevention wird mit Proofpoint Data Loss Prevention, Version 1.0.1 oder höher, getestet. |
| Vergewissern Sie sich, dass die zur Unterstützung der Proofpoint DLP-Integration erforderliche Endbenutzer-Kernanwendung installiert und aktiviert ist. | Vergewissern Sie sich, dass die folgenden DLP-Anwendungen und allgemeinen Anwendungen mit Sicherheitsunterstützung aus dem ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung.<br>• Security Support Common<br>• Data Loss Prevention Incident Response |

### Installieren und konfigurieren Sie die Proofpoint -Integration für Data Loss Prevention

Installieren und konfigurieren Sie die Proofpoint DLP-Integration aus dem ServiceNow® Store in Ihrer Now Platform -Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mit den Proofpoint DLP-Incident-Daten.

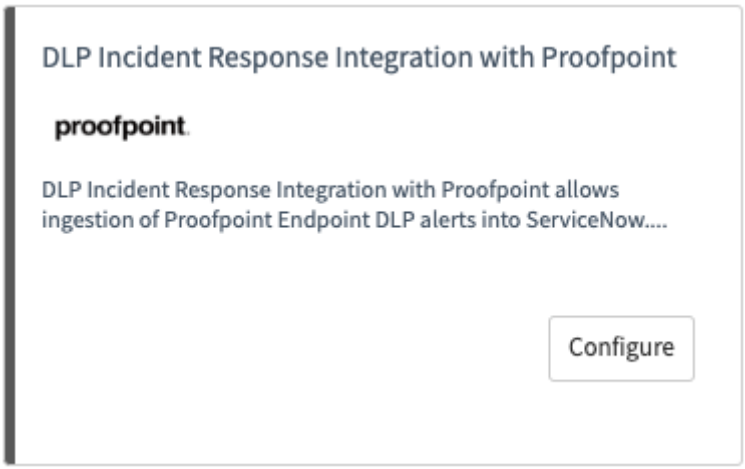
**Vorbereitungen**
Erforderliche Rolle: sn_dlir.admin



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Laden Sie die Proofpoint DLP-Integration aus dem ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Suchen Sie nach der Kachel „DLP Incident Response Integration with Proofpoint“ und klicken Sie auf **Konfigurieren**.



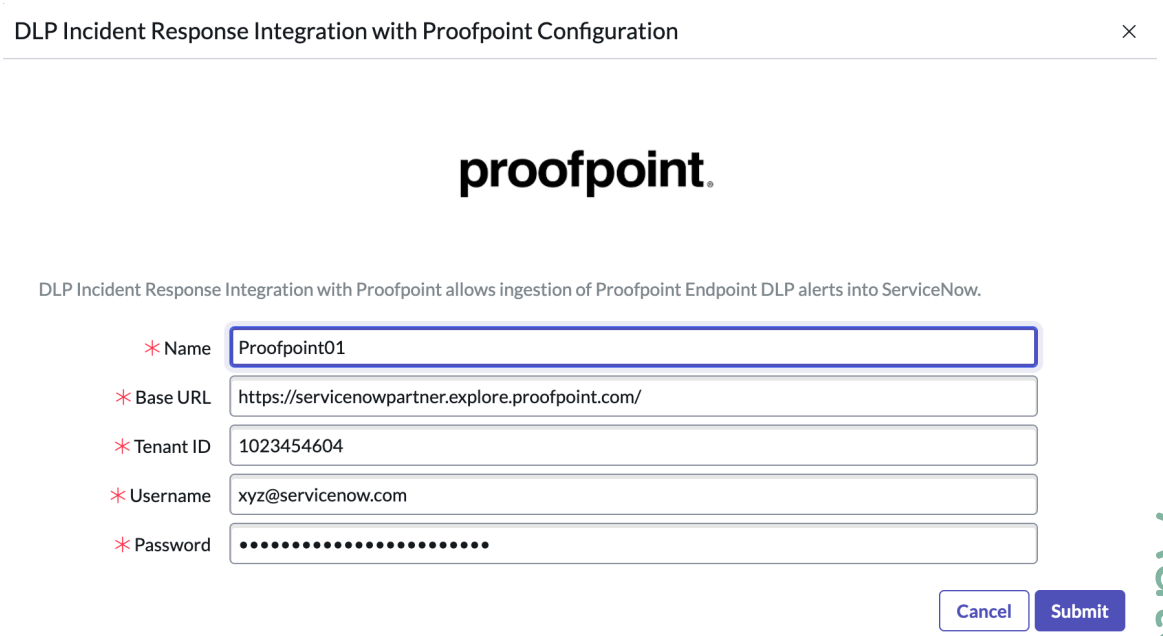

4. Füllen Sie die Felder des Formulars aus.

**Proofpoint Formular „DLP-Integrationskonfiguration“.**

| Feld | Beschreibung |
|---|---|
| Name | Name der Proofpoint DLP-Integrationskonfiguration. |
| Basis-URL | URL für Proofpoint, der als REST-Endpunkt dient |
| Mandanten-ID | ID des zu verwendenden Mandanten Proofpoint. |
| Benutzername | Benutzername, der für Ihren Benutzeraccount auf Proofpointkonfiguriert wurde. |
| Passwort | Für Ihren Benutzeraccount auf Proofpointkonfiguriertes Passwort. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




5. Klicken Sie auf **Absenden**.

## Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Proofpoint DLP-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

### Konfigurieren Sie den Webhook im DLP-Mandanten Proofpoint für Warnungsbenachrichtigungen an ServiceNow.

Konfigurieren Sie einen Webhook auf Proofpoint mit dem REST-API-Endpunkt, um die Warnungen vom DLP-Mandanten Proofpoint abzurufen. Ihre Instanz ServiceNow erstellt aus diesen Warnungen DLP-Incidents. Die Proofpoint DLP-Integration bietet einen REST API-Endpunkt für Endbenutzer zum Konfigurieren des Webhooks.

## Vorbereitungen

Erforderliche Rolle: sn_pp_dlp.api_integration_user

## Prozedur

1. Melden Sie sich bei **Proofpoint**an.
2. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Integration** > **Benachrichtigungsrichtlinien**.
3. Erstellen Sie eine Benachrichtigungsrichtlinie mit einem entsprechenden Namen.
4. Klicken Sie auf die **Benachrichtigungsrichtlinie,** und verwalten Sie die in der Benachrichtigungsrichtlinie konfigurierten Webhooks.
5. Erstellen Sie eine neue Webhook-Konfiguration, indem Sie auf **Webhooks**hinzufügen klicken.
6. Wählen Sie als Webhook-Typ **Generisch**aus.
7. Geben Sie in URL-Eingabe eine URL im Format https://ein.<Instance_Name> .service-now.com/api/sn_pp_dlp/ Proofpointalertapi/getalerts .
8. Behalten Sie die Methode als **POST**bei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Fügen Sie dem Webhook die folgenden Header hinzu:
   - Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
   - Name: Content-Type
     Value: application/json
10. Ändern Sie die anderen Werte nicht.
11. Klicken Sie auf **Speichern**.
12. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Richtlinien** > **Regeln**.
13. Wählen Sie im Abschnitt „Aktionen“ die Regeln aus, für die die Webhook-Benachrichtigung generiert werden soll.
14. Fügen Sie die neu erstellten Benachrichtigungsrichtlinien hinzu, für die ein Webhook konfiguriert ist.
15. Klicken Sie auf **Speichern**.

### Erstellen Sie ein Profil für die Proofpoint DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform. Bestimmen Sie die Proofpoint DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

#### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie Now Platform, um DLP-Warnungen von Proofpointauszufüllen. Speichern Sie die Warnungen als DLP-Incidents in Ihrer ServiceNow -Instanz.

#### Prozedur
1. Navigieren zu **Proofpoint DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt „ **Name** “ aus.

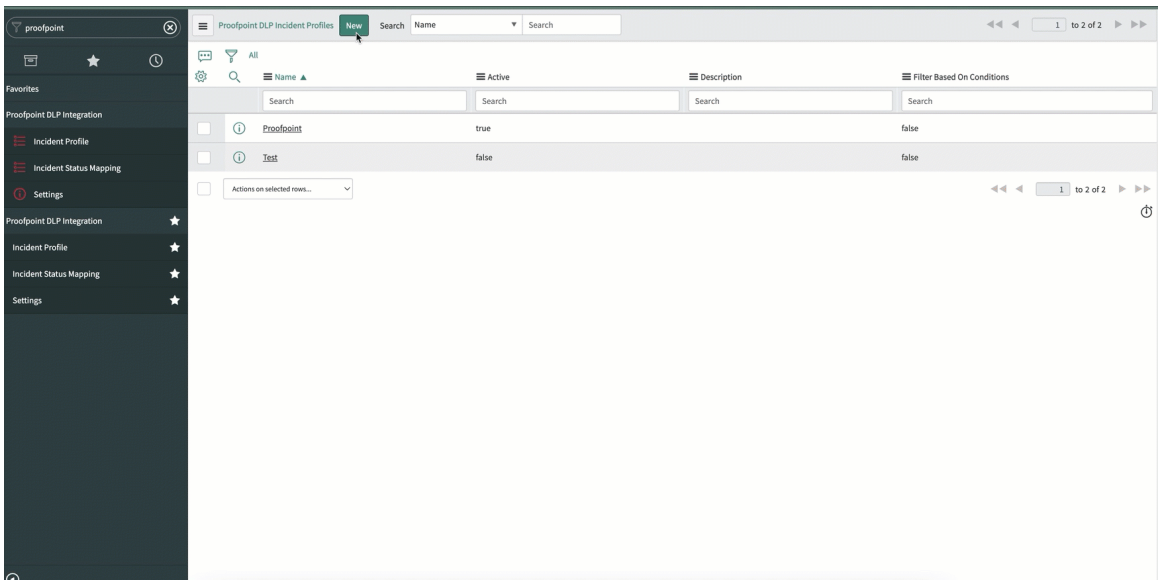
#### Erstellen Sie ein Profil für das DLP-Integrationsformular Proofpoint .

| Feld | Beschreibung |
|---|---|
| Name | Name des Profils. Anhand dieses Namens können Sie das Profil identifizieren.<br>**Hinweis:**<br>Der Name muss für jedes Profil eindeutig sein. |
| Quelle | Die Proofpoint DLP-Instanz, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten. |
| Aktiv | Option zum Aktivieren des Profils. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | Wenn das Profil aktiv ist, ist Ihre Instanz Now Platform bereit, die Incidents von Proofpointzu empfangen. |
| Beschreibung | Beschreibung, um dieses Profil von anderen Profilen zu unterscheiden. |




4. Klicken Sie auf **Fortfahren**, und wechseln Sie zum Abschnitt Filtern.

### Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden Proofpoint DLP-Incidents zu filtern. Steuern Sie, welche DLP-Incidents auf ServiceNow®erstellt werden sollen.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt werden, werden nur Incidents erstellt, die den Bedingungen entsprechen.

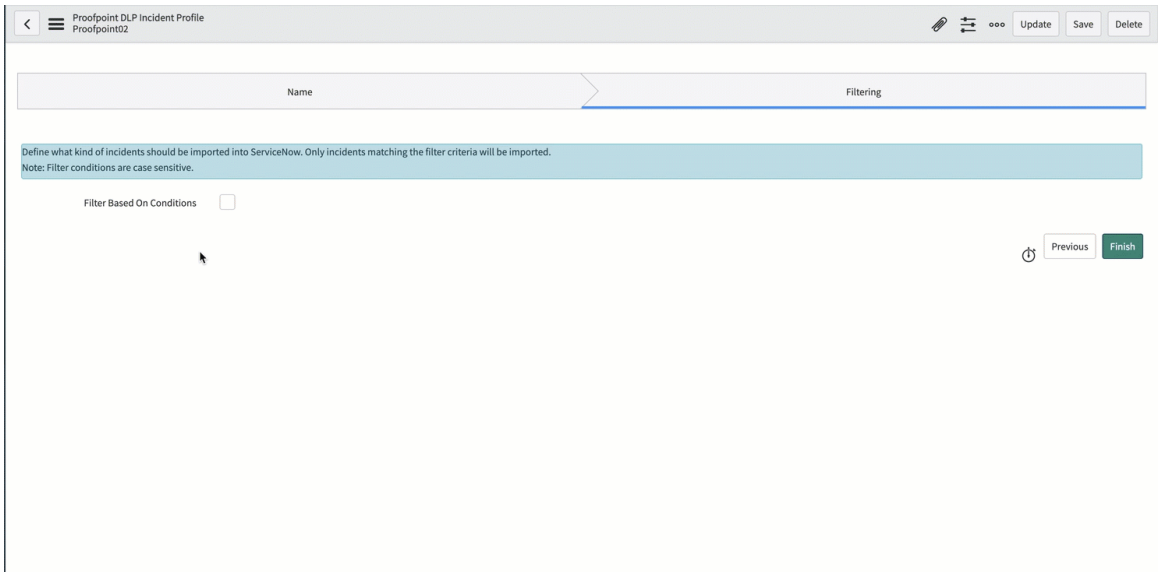
## Prozedur

1. Wählen Sie die Option **Filter basierend auf Bedingungen aus**, und definieren Sie die Kriterien, die ein eingehender Proofpoint DLP-Incident erfüllen muss, damit ein Security Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Die Optionen im ersten Feld in den **Filterbedingungen stimmen** mit den Feldern überein, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **UND**oder **ODER**klicken.
   - Wenn **UND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR**ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. Klicken Sie auf **Fertigstellen**.

### Ordnen Sie den Status von DLP-Incidents [ Proofpoint dem Incident-Status ServiceNow zu

Synchronisieren Sie den Status der in Ihrer Instanz ServiceNow erfassten DLP-Incidents und der DLP-Incidents von Proofpoint. Ordnen Sie den Incident-Status [ ServiceNow dem Incident-Status Proofpoint zu.

#### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

#### Prozedur

1. Navigieren zu **Proofpoint DLP-Integration** > **Incident** > **Incident-Statuszuordnung**.
2. Geben Sie einen **Namen** an, um die Zuordnung zu identifizieren.
3. Wählen Sie die Kachel **Quelle** (Integrationskonfiguration) aus, für die die Statuszuordnung angewendet werden soll.
4. Ordnen Sie den **ServiceNow-DLP-Incident-Status** dem **Proofpoint-Incident-Status**zu.

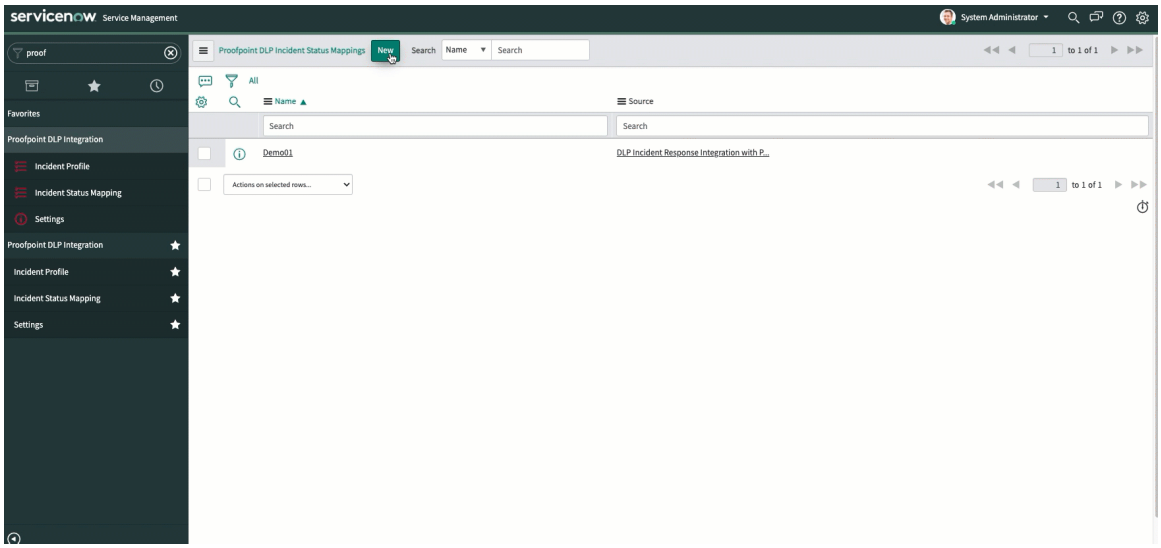
### Ordnen Sie den Status von Proofpoint-DLP-Incidents dem ServiceNow-Incident-Statusformular zu

| Feld | Beschreibung |
|---|---|
| Name | Platzhalter für den Zuordnungsdatensatz. |
| Quelle | Konfigurierte Proofpoint Endpunktquelle, aus der Sie den Incident-Status abrufen möchten. |
| ServiceNow-Incident-Status | Liste mit Status von DLP-Incidents. |
| Status des Proofpoint-Incidents | Standardmäßig zugeordnete Werte für Standardstatus, die in DLP-Incidents verfügbar sind. Für benutzerdefinierte Status lautet der |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Standardstatus Proofpoint**Neu**. Sie können den erforderlichen Status Proofpoint im Eingabefeld ändern und hinzufügen. |




5. Klicken Sie auf **Absenden**.

## Ergebnisse

Ein Datensatz für die Zuordnung wurde erfolgreich erstellt. Die Status der ServiceNow Incidents werden mit Proofpoint DLP-Incidents synchronisiert.

Wenn Sie den Status eines DLP-Incidents in Ihrer Instanz ServiceNow ändern, wird der Status des zugeordneten DLP-Incidents auf der Quellplattform ProofpointProofpoint gemäß der im Datensatz festgelegten Zuordnung geändert.

### Konfigurieren Sie Proofpoint DLP-Integrationseinstellungen

Ändern Sie die Standardsystemeigenschaften der Proofpoint DLP-Integration.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Prozedur

1. Navigieren zu **Proofpoint-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.
3. Klicken Sie auf **Speichern**.

## Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

### Domänentrennung in Proofpoint DLP-Integration

Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Support-Stufe

Support: Standard.

## Funktionsweise der Domänentrennung mit der Proofpoint DLP-Integration

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die DLP-Integrationsvorgänge Proofpoint in der entsprechenden Domäne aus.

## Integration von Data Loss Prevention Incident Response mit Netskope

Die Netskope DLP-Integration unterstützt die Erfassung von Data Loss Prevention-Incidents, die in der Data Loss Prevention-Bereitstellung von Netskope erstellt wurden. Netskope DLP hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Nach der Erfassung können Sie die Incident Management-Funktionalitäten verwenden, um die DLP-Incidents zu beheben.

## Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellung mehrerer Profile für verschiedene Netskope -Endpunkte.
- Automatisierung der Erstellung von DLP-Incidents aus Netskope DLP-Warnungen.
- Filterung von Netskope DLP-Warnungen.
- Geplante Erfassung von DLP-Incidents, die DLP-Incidents erstellen.
- Benachrichtigung per E-Mail an Anwender bei Ablauf der Anmeldeinformationen Netskope.

### Erste Schritte mit der Netskope DLP-Integration für Data Loss Prevention

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihrer Netskope DLP-Integration für Data Loss Prevention beginnen.

### Installieren und konfigurieren Sie die Netskope DLP-Integration für Data Loss Prevention

Installieren und konfigurieren Sie die Netskope DLP-Integration aus der Instanz ServiceNowServiceNow StoreNow Platform . Sie können mit der Untersuchung von DLP-Incidents mit den Netskope DLP-Incident-Daten beginnen.

#### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

#### Prozedur

1. Laden Sie die Netskope DLP-Integration aus dem ServiceNow ServiceNow Store herunter, und installieren Sie sie.
2. Navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**
3. Suchen Sie nach der Kachel DLP Incident Response Integration with Netskope, und klicken Sie auf **Konfigurieren**.
4. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Name | Name der Netskope DLP-Integrationskonfiguration. |
| Endpunkt-URL | URL für die Instanz Netskope, die als REST-Endpunkt dient. |
| Token | Token, das für REST API v2 in Ihrem Benutzerkonto unter Netskopekonfiguriert ist. |

5. Klicken Sie auf **Absenden**.

### Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Netskope DLP-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

#### Erstellen Sie ein Profil für die Netskope DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform. Bestimmen Sie die Netskope DLP-Warnungen, die zum Erstellen von DLP-Incidents geeignet sind.

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

### Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie die Plattform Now Platform, um die DLP-Incidents vom Endpunkt Netskope ] abzurufen. Speichern Sie die Incidents in Ihrer ServiceNow -Instanz als DLP-Incidents.

### Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

#### Erstellen Sie ein Profil

| Feld | Beschreibung |
|---|---|
| Name | Name des Profils. Der Name muss für jedes Profil eindeutig sein. Anhand dieses Namens können Sie das Profil identifizieren. |
| Quelle | Netskope DLP-Instanz, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten. |
| Aktiv | Indikator, der angibt, dass das Profil aktiv ist.<br>**Hinweis:**<br>Dieses Feld ist nur verfügbar, nachdem Sie im letzten Abschnitt „Zeitplanung“ auf Fertigstellen **geklickt** haben.<br>Wenn das Profil aktiv ist, fragt Ihre Instanz Now Platform aktiv Netskope DLP- |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Incidents ab. Entsprechende DLP-Incidents werden in DLIR erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Planungsparametern abgeglichen werden. |
| Reihenfolge | Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet.<br><br>Standardmäßig ist der Wert 100. |
| Beschreibung | Beschreibung, die Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden. |

4. Klicken Sie auf **Fortfahren**, und wechseln Sie zum Abschnitt Filtern.

### Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden Netskope DLP-Incidents zu filtern. Steuern Sie, welche dieser Incidents als DLP-Incidents in Ihrer ServiceNow -Instanz erstellt werden sollen.

#### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

#### Warum und wann dieser Vorgang ausgeführt wird
Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt werden, werden nur Incidents erstellt, die den Bedingungen entsprechen.

#### Prozedur

1. Wählen Sie die Option **Filter basierend auf Bedingungen aus**, und definieren Sie die Kriterien, die ein eingehender Netskope DLP-Incident erfüllen muss, damit ein Security Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Die Optionen im ersten Feld in den **Filterbedingungen** stimmen mit den Feldern überein, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.
3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **UND**oder **ODER**klicken.
   - Wenn **UND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR**ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. Klicken Sie auf **Fortfahren**, und wechseln Sie zum Abschnitt Zeitplanung.

### Planen Sie den Abruf von Netskope Data Loss Prevention-Warnungen

Legen Sie einen Zeitplan fest, um die Warnungsdaten abzurufen und Netskope DLP-Incidents zu erfassen, die den Kriterien im Profil entsprechen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

### Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Zeitplanung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen **Einmaliger Abruf** so konfiguriert werden, dass es nur einmal abgerufen wird. Das Verlaufsdatum kann bis zu drei Monate in der Vergangenheit liegen.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Netskope DLP-Incident-Integration auswirken. Planen Sie bei der Zeitplanung, dass die Systemlast auf die Dringlichkeit eines Incident abgestimmt wird.

### Prozedur
1. Konfigurieren Sie den Zeitplan, um festzulegen, wie und wann Sie Warnungen aus Netskopeabrufen.
2. Füllen Sie die Felder des Formulars aus.

**Planen Sie die Netskope DLP-Warnungen**

| Feld | Beschreibung |
|---|---|
| Laufende Incident-Erfassung | Laufende Incident-Erfassung, die Ihre Instanz Now PlatformNetskope ] für neue Incidents aus abruft. Wenn ausgelöste Warnungen gefunden werden, die den Incident-Filterkriterien entsprechen, werden DLP-Incidents erstellt. |
| Abfrageschritt (Stunden) | Abfragehäufigkeit, die in Stunden definiert ist. Dieses Feld wird automatisch auf **5**gesetzt. |
| Zeitpunkt der ersten Incident-Erfassung festlegen | Option zum Festlegen der ersten Incident-Erfassung basierend auf dem konfigurierten Datum und der Uhrzeit.<br><br>Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die erste Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall. |
| Zeitpunkt der ersten Incident-Erfassung eingeben | Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben. |
| Zeitpunkt der ersten Incident-Erfassung | Das erste Mal, wenn Daten erfasst werden.<br><br>**Hinweis:**<br>Der Wert ist nur sichtbar, wenn die Option **Anfängliche Incident-Erfassungszeit** festlegen ausgewählt ist. |
| Nächste Incident-Erfassungszeit (geschätzt) | Nächste geschätzte Incident-Erfassungszeit. |
| Einmaliger Abruf | Option zum Aktivieren des einmaligen Abrufens historischer Daten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Hinweis:** Wenn diese Option ausgewählt ist, werden Verlaufsdaten aus Netskope DLP gemäß dem Datum abgerufen, das in „ **Seit Datum**“ hinzugefügt wurde. |
| Seit Datum | Datum, ab dem Daten aus Netskopeabgerufen werden.<br>**Hinweis:** Höchstens die letzten drei Monate der Daten können aus Netskopeabgerufen werden. |

3. Klicken Sie auf **Fertigstellen**.
4. Speichern Sie im Popup-Fenster die erstellte Profilkonfiguration, indem Sie auf **Fertigstellen klicken**.
5. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Legen Sie **Aktiv** auf **true fest**.
   c. Klicken Sie auf **Aktualisieren**.

## Ergebnisse

Nach der erfolgreichen Erstellung und Aktivierung des Profils werden Warnungen regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen. Die Warnungen werden der DLP-Incident-Tabelle hinzugefügt.

### Konfigurieren Sie Netskope DLP-Integrationseinstellungen

Ändern Sie die Standardsystemeigenschaften der Netskope DLP-Integration.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

## Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

### Konfigurieren Sie Netskope DLP-Integrationseinstellungen

| Feld | Beschreibung |
|---|---|
| Erzwingen Sie eine Begrenzung der Anzahl von Incidents, die in einem HTTP-Aufruf von Netskope sn_ns_dlp.page_size abgerufen werden sollen | Maximale Zeitüberschreitung für HTTP-Aufrufe in Sekunden. Dieses Feld wird automatisch auf **30**festgelegt. |
| Ebene der Berichterstellung für die von der Integration sn_ns_dlp.logging.verbosity generierten Protokolle | Definieren Sie die Ebene der von der Integration generierten Berichtsprotokolle. Dieses Feld wird automatisch auf **„info“**gesetzt. |

3. Klicken Sie auf **Speichern**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

#### Benachrichtigungen für Benutzer beim Ablauf der Anmeldeinformationen

Das Token Netskope kann für REST-API v2 bis zu 12 Monate gültig sein. Wenn das in der Instanz [ ServiceNow verwendete Token abläuft, sendet Netskope eine E-Mail-Benachrichtigung an Benutzer mit der Rolle „DLP-Administrator“ (sn_dlir.admin).

Nachdem das Setup der Integrationskonfiguration abgeschlossen ist, stellen Sie die Rolle „DLP-Administrator“ (sn_dlir.admin) für die Benutzer bereit, die benachrichtigt werden sollen, wenn das Token abgelaufen ist.

Wenn das Token abläuft, wird die Datenerfassung für zugeordnete Profile angehalten, bis das Ticket mit einem gültigen Token aktualisiert wird.

Sie müssen ein Token erstellen oder das alte auf Netskopeerneuern und dann das Token auf der Instanz ServiceNow aktualisieren. Wenn Sie das Token verlängern, indem Sie die Ablaufzeit verlängern, erkennt die Anwendung Netskope die Verlängerung automatisch und fährt mit der Datenerfassung fort. Wenn Sie ein Token erstellen, müssen Sie das Token in der Konfiguration aktualisieren.

#### Domänentrennung in Netskope DLP-Integration

Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

## Support-Stufe

Support: Standard.

## Funktionsweise der Domänentrennung mit der Netskope DLP-Integration

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die DLP-Integrationsvorgänge Netskope in der entsprechenden Domäne aus.

## Data Loss Prevention Incident Response mit Microsoft

Data Loss Prevention Incident Response mit Microsoft bietet ein Kern-Framework zum Importieren von DLP-Incidents (Data Loss Prevention) aus mehreren Quellen, z. B. aus Microsoft Purview-Apps (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive for Business). Endpunktgeräte ermöglichen einen Fehlerkorrektur-Workflow unter Einbeziehung von Endbenutzern, Managern und DLP-Betriebsteams mit automatisierter Incident-Zuweisung und Eskalationen.

## Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erstellen Sie mehrere Profile für verschiedene Accounts.
- Automatisieren Sie die Erstellung von DLP IR Incidents.
- Ordnen Sie die Ereignisfelder Microsoft DLP IR ] den Incident-Feldern DLP IR zu.
- Filtern Sie Microsoft DLP IR Events.
- Planen Sie die Erfassung von DLP IR Events, die regelmäßig DLP IR Incidents erstellen.
- Speichern Sie den übereinstimmenden Inhalt jedes Microsoft DLP-Events im externen Cloud-Speicher.
- Löschen Sie übereinstimmende Inhalte im externen Cloud-Speicher, nachdem Sie den Incident [ DLP IR in ServiceNowgelöscht haben.
- Laden Sie Dateien für DLP IR Incidents vom Typ Exchange, OneDrive und SharePoint herunter.

## Weitere Informationen zu dieser Integration

| Dokumentbezeichner | Dokumententitel |
|---|---|
| Microsoft Produktdokumentations-Website | Microsoft-Website mit Produktdokumentation |
| ServiceNow Produktdokumentations-Website | ServiceNow-Website mit Produktdokumentation |

### Erste Schritte mit der Microsoft DLP IR -Integration zur Verhinderung von Datenverlust

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihrer Microsoft DLP IR -Integration zur Verhinderung von Datenverlust beginnen.

#### Prüfliste

| Setupaufgabe | Beschreibung |
|---|---|
| Rufen Sie die Microsoft Purview-Anmeldeinformationen ab, um die Event-Daten abzurufen, und die Anmeldeinformationen des AWS/ Azure Storage-Kontos, um den übereinstimmenden Inhalt zu speichern<br><br>Registrieren Sie eine Anwendung bei Microsoft Identity Platform | Registrieren Sie hier eine Anwendung auf der Microsoft Azure-Plattform, um die Client-ID, den geheimen Clientschlüssel und die Mandanten-ID zu erhalten. Weitere Informationen zu den für die Erstellung einer Anwendung erforderlichen Rollen finden Sie unter Voraussetzungen .<br><br>Informationen zu den API-Berechtigungen/ -Rollen, die für eine Microsoft Azure-Anwendung erforderlich sind, um sie in der ServiceNow Microsoft DLP-Integration zu konfigurieren, finden Sie in der folgenden Tabelle. |
| Berechtigungen, die für den Azure-Benutzer erforderlich sind, um Zugriff auf das Lesen/ Schreiben/Löschen von Blobs in Azure Storage zu erhalten | Der Azure-Benutzer muss die Rolle **„Beitragender zu Speicher-Blobdaten“** haben, um Blobs in Azure Storage zu lesen, zu schreiben und zu löschen. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Prüfliste (Fortsetzung)**

| Setupaufgabe | Beschreibung |
|---|---|
| Berechtigungen, die für den AWS-Benutzer erforderlich sind, um Zugriff auf das Lesen/ Schreiben/Löschen von Objekten in AWS-Speicher zu erhalten | Es sollte eine Richtlinie erstellt werden, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt in AWS S3-Speicher gewährt. |
| Weisen Sie zu und überprüfen Sie, ob Sie über die erforderlichen Rollen für Now Platform und Datenverlustverwaltung verfügen. | Die folgenden Rollen sind für die Konfiguration und Überprüfung der erwarteten Ergebnisse erforderlich:<br>• Die Administratorrolle installiert die Integration aus dem ServiceNow Store und weist die Rolle sn_dlir.admin zu.<br>• Die Rolle sn_dlir.admin führt die folgenden Aufgaben aus:<br>◦ Konfiguriert die Integration.<br>◦ Richtet die Incident-Profile ein. |
| Vergewissern Sie sich, dass die für die Unterstützung der Microsoft-Integration ServiceNow erforderlichen Kernanwendungen von DLP IR installiert und aktiviert sind, bevor Sie diese Integration konfigurieren. | Vergewissern Sie sich, dass die folgenden DLP IR -Anwendungen und allgemeinen Anwendungen mit Sicherheitsunterstützung aus dem ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren und aktivieren Sie in der Anwendung.<br>• Security Support Common<br>• Data Loss Prevention Incident Response |

### Erforderliche API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung

***Sie benötigen die folgenden API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung, um sie in der ServiceNow Microsoft DLP-Integration zu konfigurieren.***

| API | Berechtigungsnam | Typ | Beschreibun | Für welche ServiceNow-Funktionalität erforderlich? | Ist die Zustimmung des Administrators erforderlich? |
|---|---|---|---|---|---|
| Office 365 Management-API | AktivitätsFeed.ReadDLP | Anwendung | Lesen Sie DLP-Richtlinien-Ereignisse, einschließlich erkannter vertraulicher Daten. | Zum Erfassen der DLP-Ereignisse aus MSFT Purview in ServiceNow.<br>**Hinweis:** Diese Berechtigung ist erforderlich, um die MSFT-Daten in ServiceNowabzurufen. | Ja |
| Microsoft Graph-API | Dateien.Lesen.Alle | Anwendung | Lesen Sie Dateien in allen | Datei herunterladen: Zum Herunterladen des Anhangs in der | Ja |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Erforderliche API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung**
*Sie benötigen die folgenden API-Berechtigungen/-Rollen für eine Microsoft Azure-Anwendung, um sie in der* **ServiceNow** *Microsoft DLP-Integration zu konfigurieren.*

**(Fortsetzung)**

| API | Berechtigungsnam | Typ | Beschreibun | Für welche ServiceNow-Funktionalität erforderlich? | Ist die Zustimmung des Administrators erforderlich? |
|---|---|---|---|---|---|
| | | | Websitesammlungen, auf die Sie zugreifen können. | Sie ServiceNow-Instanz, die das DLP-Ereignis von OneDrive oder SharePoint verursacht hat<br>**Hinweis:** Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie nicht möchten, dass die Analysten den Anhang herunterladen, der das DLP-Ereignis verursacht hat. | |
| | Mail.Lesen | Anwendung | Lesen Sie E-Mails in allen Postfächern. | Datei herunterladen: Zum Herunterladen des E-Mail-Inhalts (Text und Anhang) in der ServiceNow-Instanz, die das DLP-Ereignis von Exchange verursacht hat.<br>**Hinweis:** Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie nicht möchten, dass die Analysten den E-Mail-Inhalt (Text, Anhang) herunterladen, der das DLP-Ereignis verursacht hat. | Ja |
| | Benutzer.Lesen | Delegiert | Melden Sie sich an, und lesen Sie das Benutzerprofil. | Dies ist die Standardberechtigung, die für alle neuen Anwendungen verfügbar ist. | Nein |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erkannte vertrauliche Informationen (optional)

Der Übereinstimmungsinhalt wird extern in Azure Blob Storage oder im Amazon S3-Bucket gespeichert und aus dem externen Speicher abgerufen, wenn der Benutzer einen Incident anzeigt.

Eine der folgenden Berechtigungen ist erforderlich, wenn die Benutzer Abgleichinhalte/ erkannte vertrauliche Informationen in der DLP Core-Anwendung anzeigen möchten:

1. Wenn Sie Microsoft Azure -Benutzer sind, müssen Sie die Rolle „Beitragender für Speicher-Blobdaten“ haben, um Blobs in Azure Storage zu lesen, zu schreiben und zu löschen.
2. Wenn Sie Amazon S3-Benutzer sind, müssen Sie eine Richtlinie erstellen, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt in Amazon S3 Storage gewährt.

### Installieren und konfigurieren Sie die Microsoft DLP-Integration

Installieren und konfigurieren Sie die DLP Incident Response-Integration mit Microsoft DLP aus ServiceNow® Store in Ihrer Instanz Now Platform. Beginnen Sie mit der Untersuchung von DLP-Incidents mit den Microsoft DLP-Ereignisdaten.

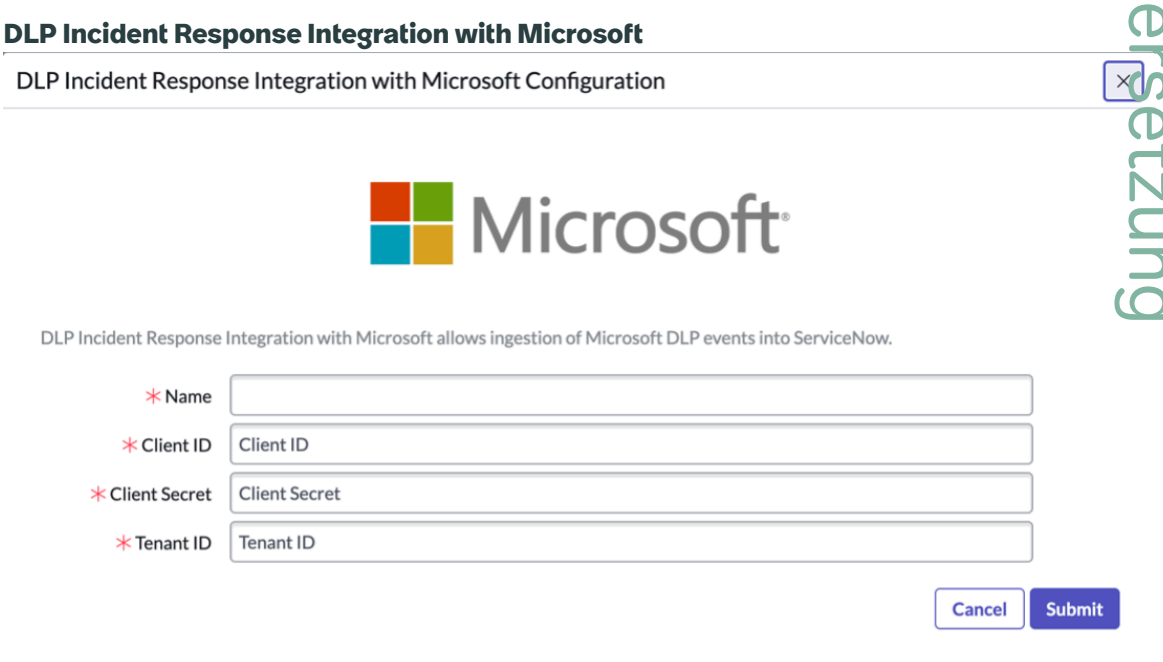
#### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

#### Prozedur

1. Laden Sie die Microsoft DLP-Integration aus dem ServiceNow® Store herunter, und installieren Sie sie.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**.
3. Konfigurieren Sie die Microsoft DLP-Integration.

   a. Suchen Sie nach der Kachel **DLP Incident Response Integration with Microsoft**, und klicken Sie auf **Konfigurieren**.




   b. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Formular „Microsoft DLP-Integrationskonfiguration“

| Feld | Beschreibung |
|---|---|
| Name | Name der Microsoft DLP-Integrationskonfiguration. |
| Client-ID | Client-ID der im Microsoft Azure-Portal erstellten App. |
| Geheimer Clientschlüssel | Geheimer Clientschlüssel der im Microsoft Azure-Portal erstellten App. |
| Mandanten-ID | Mandanten-ID des Benutzers |

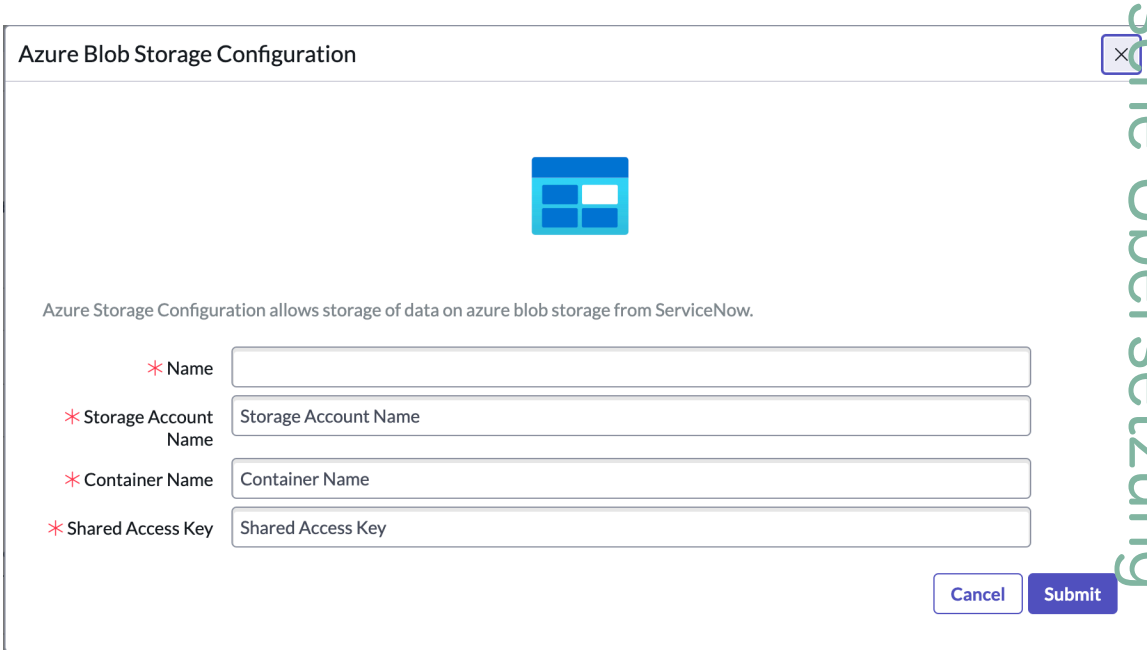
**c.** Klicken Sie auf **Absenden**.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Microsoft DLP-Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

**4.** Aktualisieren Sie die Azure Storage-Konfiguration.

**a.** Suchen Sie auf der Seite „Sicherheitsintegrationen“ nach der Kachel **Azure Storage-Konfiguration**.

**b.** Klicken Sie in der Kachel „Azure Storage-Konfiguration“ auf **Aktualisieren**.




**c.** Füllen Sie die Felder des Formulars aus.

### Formular Azure Storage-Konfiguration

| Feld | Beschreibung |
|---|---|
| Name | Name der Azure Storage-Konfiguration |
| Name des Speicher-Accounts | Name des im Azure-Portal erstellten Speicherkontos |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Containername | Containername, der im Speicherkonto im Azure-Portal erstellt wurde. |
| Freigegebener Zugriffsschlüssel | Freigegebener Zugriffsschlüssel für das Speicherkonto |

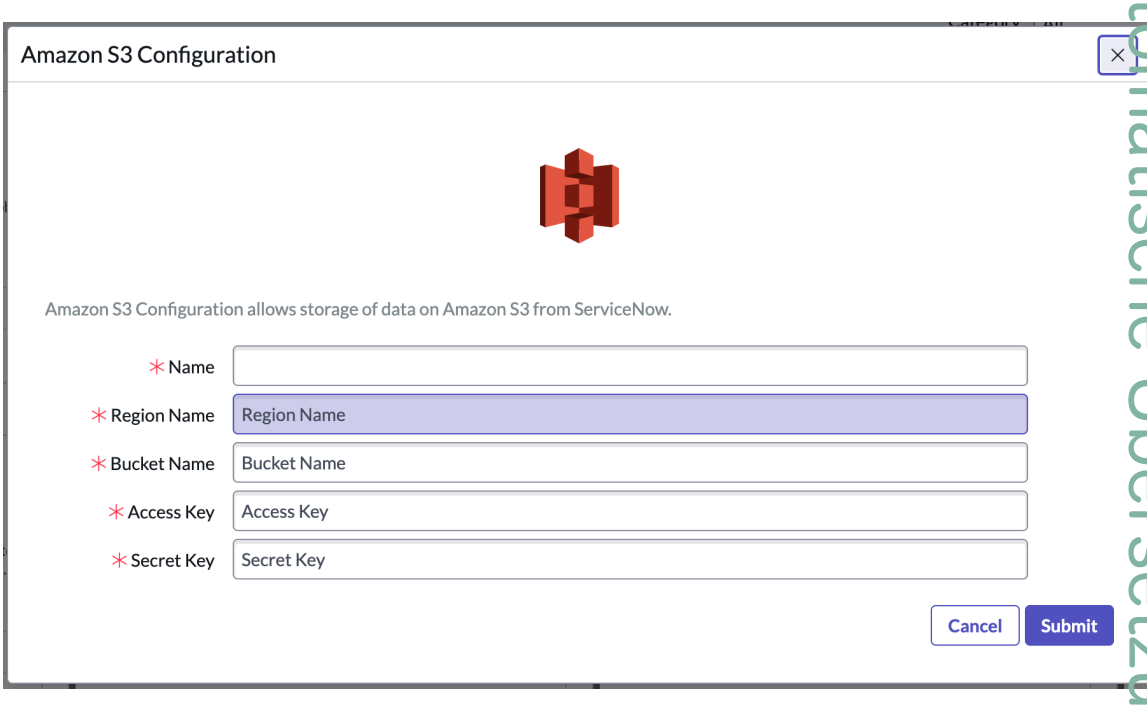
**d.** Klicken Sie auf **Absenden**.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Azure Storage-Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

**5.** Aktualisieren Sie die AWS-Speicherkonfiguration.

**a.** Suchen Sie auf der Seite „Sicherheitsintegrationen“ nach der Kachel **AWS-Speicherkonfiguration**.

**b.** Klicken Sie in der Kachel „AWS-Speicherkonfiguration“ auf **Aktualisieren**.




**c.** Füllen Sie die Felder des Formulars aus.

### Formular AWS-Speicherkonfiguration

| Feld | Beschreibung |
|---|---|
| Name | Name der AWS-Speicherkonfiguration |
| Regionsname | Regionsname des AWS-Speicherkontos. |
| Bucket-Name | Im AWS-Portal erstellter Bucket-Name. |
| Zugriffsschlüssel | Zugriffsschlüssel mit Lese-, Schreib- und Löschzugriff. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| Geheimer Schlüssel | Freigegebener Schlüssel mit Lese-, Schreib- und Löschzugriff |

**d.** Klicken Sie auf **Absenden**.

### Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die AWS S3-Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

#### Erstellen Sie ein neues Incident-Profil für die Microsoft DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrer Instanz Now Platform, um die Daten aus Microsoft Purview abzurufen und die Daten der Incident-Tabelle ServiceNow DLP IR hinzuzufügen.

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Anzeigen (schreibgeschützt)

### Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie Now Platform®, um die Events aus dem Purview von Microsoft abzurufen. Speichern Sie diese Events in der Incident-Tabelle [ DLP IR in Ihrer Instanz ServiceNow®.

### Prozedur

1. Navigieren zu **Microsoft DLP-Integration** > **Incident-Profil**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt „Name“ aus.

#### Erstellen Sie ein Profilformular

| Feld | Beschreibung |
|---|---|
| Name | Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren.<br>**Hinweis:**<br>Der Name muss für jedes Profil eindeutig sein. |
| Quelle | Die Instanz Microsoft DLP IR, die Sie für die Erfassung von Incidents konfiguriert haben. Wenn Sie mehrere Integrationskonfigurationen haben, wählen Sie den entsprechenden Integrationskonfigurationsdatensatz für die Incident-Typen aus, die Sie für das Profil erfassen möchten. |
| Aktiv | Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann nur aktiviert werden, nachdem Sie im Abschnitt Zeitplanung auf das Feld Fertigstellen **geklickt** haben.<br>Wenn das Profil aktiv ist, bedeutet dies, dass Now Platform ] basierend auf der |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | im Profil definierten Konfiguration aktiv Microsoft DLP IR Events abruft. |
| Reihenfolge | Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge wird als höchste Priorität betrachtet.<br><br>Standardmäßig ist der Wert 100. |
| Beschreibung | Eindeutige Beschreibung für das Profil. |

### Nächste Maßnahme
Um zum Abschnitt Filtern zu wechseln, klicken Sie auf **Fortfahren**.

#### Definieren Sie Filter, die auf die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden Microsoft DLP-Events zu filtern. Legen Sie fest, welche dieser Ereignisse als DLP IR Incidents in Ihrer Instanz ServiceNow erstellt werden sollen.

### Vorbereitungen
Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Anzeigen (schreibgeschützt)

### Warum und wann dieser Vorgang ausgeführt wird
Mit dieser Art der Filterung können Sie Microsoft DLP-Ereignisse isolieren, um die Anzahl der von Ihnen erstellten DLP IR Incidents zu begrenzen. Wenn die Filterkriterien festgelegt sind, werden nur Events, die den Bedingungen entsprechen, als DLP-Incidents erstellt.

### Prozedur

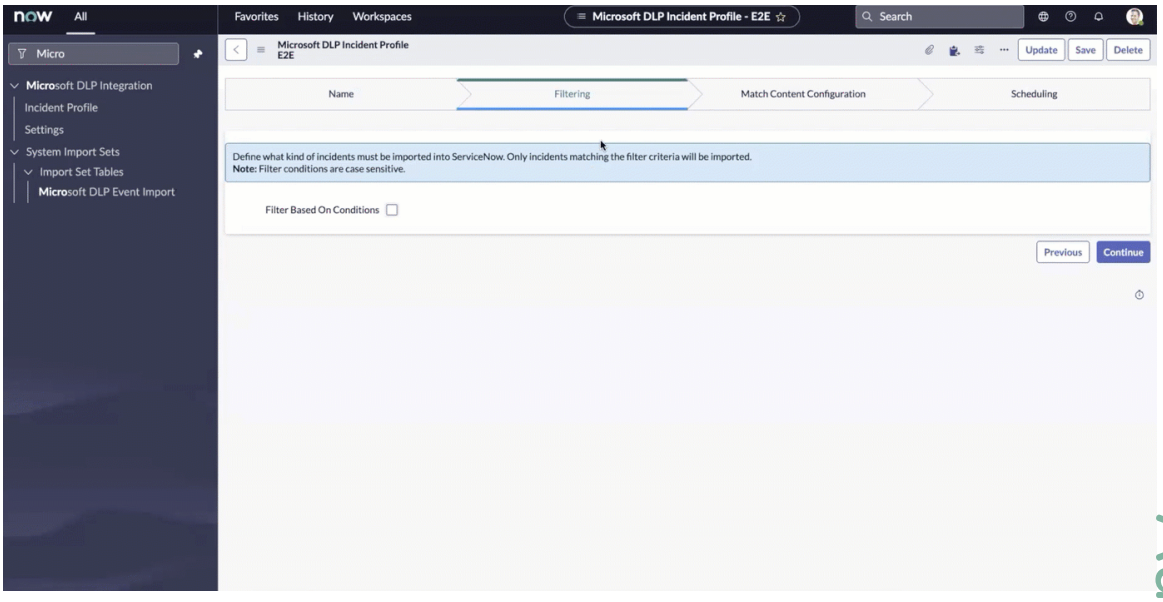
1. Wählen Sie die Option **Anhand von Bedingungen** filtern aus.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter im Feld **Filterbedingungen** fest.

   Definieren Sie die Kriterien, die ein eingehendes Microsoft DLP-Event erfüllen muss, damit ein DLP-Incident erstellt wird.

   Die Optionen im ersten Feld in den **Filterbedingungen** stimmen mit den Feldern überein, die im Microsoft DLP-Ereignis verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass die von Ihnen definierten Kriterien mit den Werten des Events übereinstimmen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf **UND**oder **ODER**klicken.
   - Wenn **UND**ausgewählt ist, müssen alle Bedingungen erfüllt sein.
   - Wenn **OR**ausgewählt ist, kann eine der beiden Bedingungen erfüllt sein.
4. Klicken Sie auf **Fortsetzen**, und wechseln Sie zum Abschnitt „Konfiguration des Inhalts abgleichen“.

### Konfigurieren Sie den Abgleichinhalt für den Incident

Geben Sie die Konfiguration an, um die vertraulichen Informationen im externen Cloud-Speicher wie Azure Storage oder AWS S3-Bucket zu speichern, um diesen Inhalt beim Zugriff auf den DLP-IR-Incident beim Laden abzurufen.

## Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Anzeigen (schreibgeschützt)

## Prozedur

1. Klicken Sie in der Fortschrittsleiste auf den Schritt **„Konfiguration des Inhalts abgleichen** “.
2. Füllen Sie die Felder des Formulars aus.

### Inhaltskonfiguration abgleichen

| Feld | Beschreibung |
|---|---|
| Abgleichsinhalt speichern | Option zum Speichern des übereinstimmenden Inhalts im Cloud-Speicher. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
| --- | --- |
| | **Wichtig:**<br>Wenn diese Option nicht ausgewählt ist, kann der Inhalt der Richtlinienübereinstimmung für DLP-Incidents im DLP-Arbeitsbereich nicht angezeigt werden. Durch Aktivieren dieser Option wird sichergestellt, dass übereinstimmende Inhalte, die in den DLP-Incidents zurückgegeben werden, im externen Cloud-Speicher (z. B. Azure, AWS) gespeichert werden. Sie können den übereinstimmenden Inhalt auch abrufen und anzeigen, wenn ein DLP-Incident im Arbeitsbereich geöffnet wird.<br><br>Weitere Informationen zur Konfiguration des externen Cloud-Speichers finden Sie unter Installieren und konfigurieren Sie die Microsoft DLP-Integration. |
| Abgleichinhalt bei Incident-Löschung löschen | Option zum Löschen des Incident-Übereinstimmungsinhalts aus dem externen Cloud-Speicher. Diese Option ist nur sichtbar, wenn das Feld **Abgleichinhalt speichern** ausgewählt ist. |
| Externe Cloud-Anmeldeinformationen | Der externe Cloud-Speicher, in dem der übereinstimmende Inhalt gespeichert wird. Sie können sich auf die für die Speicherkonfiguration hinzugefügten externen Cloud-Anmeldeinformationen beziehen. Diese Option ist nur sichtbar, wenn das Feld **Abgleichinhalt speichern** ausgewählt ist. |

3. Klicken Sie auf **Fortfahren**, und wechseln Sie zum Abschnitt Zeitplanung.

### Planen Sie den DLP IR Microsoft-Incident-Abruf

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und Microsoft DLP IR Incidents zu erfassen, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um festzulegen, wie und wann Sie Incidents aus Microsoftabrufen .

#### Vorbereitungen

Erforderliche Rolle: sn_dlir.admin (Erstellen, Bearbeiten und Löschen)

sn_dlir.analyst – Anzeigen (schreibgeschützt)

#### Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Zeitplanung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann mit dem Kontrollkästchen **Einmaliger Abruf** so konfiguriert werden, dass es nur einmal abgerufen wird. Das Verlaufsdatum kann bis zu den letzten drei Monaten ab dem aktuellen Datum reichen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die unterschiedlichen Abfrageintervalle können sich auf die Leistung der Incident-Integration von Microsoft DLP IR auswirken. Planen Sie bei der Zeitplanung, dass die Systemlast auf die Dringlichkeit eines Incident abgestimmt wird.

### Prozedur

1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie die Felder des Formulars aus.

**Zeitplan für das DLP-Incident-Formular**

| Feld | Beschreibung |
|---|---|
| Laufende Incident-Erfassung | Die laufende Incident-Erfassung, die die Instanz Now Platform für neue Incidents von Microsoft abruft. DLP IR Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung übereinstimmen. |
| Abfrageschritt (Minuten) | Die Abfragehäufigkeit von Microsoft. Dieses Feld wird automatisch auf 300 Minuten festgelegt. |
| Zeitpunkt der ersten Incident-Erfassung festlegen | Option zum Definieren eines Datums und einer Uhrzeit für die erste Erfassung. Nachfolgende Erfassungen basieren auf dem Abfrageintervall.<br>Diese Option ist nur sichtbar, wenn das Feld **Laufende Incident** -Erfassung ausgewählt ist. |
| Zeitpunkt der ersten Incident-Erfassung eingeben | Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.<br>○ Wenn der Wert festgelegt ist, beginnt das Abrufen der Daten von Microsoft ab dem hinzugefügten Datum in der Zukunft.<br>○ Dieses Feld ist nur sichtbar, wenn **Anfängliche Erfassungszeit festlegen** ausgewählt ist. |
| Zeitpunkt der ersten Incident-Erfassung | Zeitpunkt der ersten Erfassung der Daten.<br>Sie können sehen, dass Werte angezeigt werden, wenn die anfängliche Incident-Erfassungszeit festgelegt wird. |
| Nächste Incident-Erfassungszeit (geschätzt) | Nächster Zeitraum für eine geschätzte Incident-Erfassung. |
| Einmaliger Abruf | Option zum Aktivieren einmaliger Abrufe historischer Daten.<br>Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten entsprechend dem im Feld |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | **Seit Datum** hinzugefügten Datum aus Microsoft DLP IR abgerufen. |
| Seit Datum | Datum, ab dem Daten von Microsoft abgerufen werden sollen.<br><br>Dieses Feld kann auf maximal 7 Tage festgelegt werden. |

3. Speichern Sie die erstellte Profilkonfiguration, indem Sie im Popup-Fenster auf **Fertigstellen klicken**.
4. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Aktivieren Sie die Option **Aktiv**.
   c. Klicken Sie auf **Aktualisieren**.

## Ergebnisse
Nach der erfolgreichen Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der DLP-Incident-Tabelle hinzugefügt.

### Konfigurieren Sie die Microsoft DLP IR -Integrationseinstellungen

Ändern Sie die Standardsystemeigenschaften der Microsoft DLP IR -Integration.

## Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

## Prozedur
1. Navigieren zu **Microsoft-DLP-Integration** > **Einstellungen**.
2. Ändern Sie die folgenden Eigenschaften nach Bedarf.

### Microsoft DLP-Integrationseinstellungen

| Feld | Beschreibung |
|---|---|
| Maximale Zeitüberschreitung für HTTP-Aufrufe (sn_pp_dlp.maximum_http_time_out) | Maximale Zeitüberschreitung für HTTP-Aufrufe (in Sekunden).<br>○ Typ: Ganzzahl<br>○ Standardwert: 30 |
| Ebene der Berichterstellung für die von der Integration generierten Protokolle (sn_pp_dlp.logging.verbosity) | Die Ebene der von der Integration generierten Berichtsprotokolle, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren:<br>○ **Fehler**<br>○ **warnen**<br>○ **Info**<br>○ **debuggen**<br>○ **aus** |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Beschreibung |
|---|---|
| | Standardmäßig ist der Wert **info**. |
| Ziel der Berichterstellung für die von der Integration generierten Protokolle (sn_pp_dlp.logging.destination) | Das Ziel für die Protokolle, die von der Integration generiert werden. Sie können den Wert auch auf die folgenden Optionen aktualisieren:<br>○ **DB**<br>○ **Datei**<br>○ **Keine**<br>Standardmäßig lautet der Wert **db**. |

3. Klicken Sie auf **Speichern**.

## Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

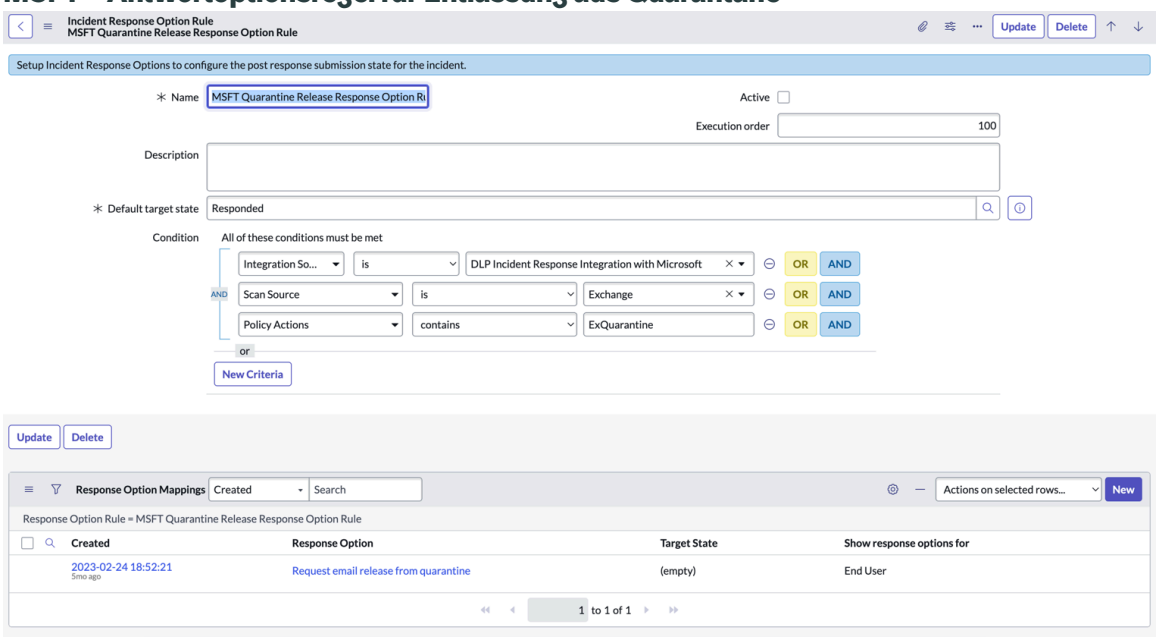
### Fordern Sie die Freigabe-E-Mail aus der Quarantäne an

Verwenden Sie diese Funktion, um die unter Quarantäne gestellte E-Mail aus dem Compliance-Portal von Microsoft Purview freizugeben.

## Vorbereitungen

Standardmäßig stellt das Basissystem die Antwortoption „E- **Mail-Freigabe aus Quarantäne** anfordern“ und **die Antwortoptionsregel „MSFT-Quarantänefreigabe“ bereit**, um die E-Mail aus der Quarantäne freizugeben. Mit diesem Standarddatensatz wird auch die Genehmigungsregel für **Quarantänefreigaben** konfiguriert, um die Genehmigungsfunktion für diese Aktion zu nutzen. Weitere Informationen finden Sie unter Richten Sie Optionsregeln für die Reaktion auf Incidents für Ihre DLP-Incidents ein, Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents und Konfigurieren Sie Genehmigungsregeln.

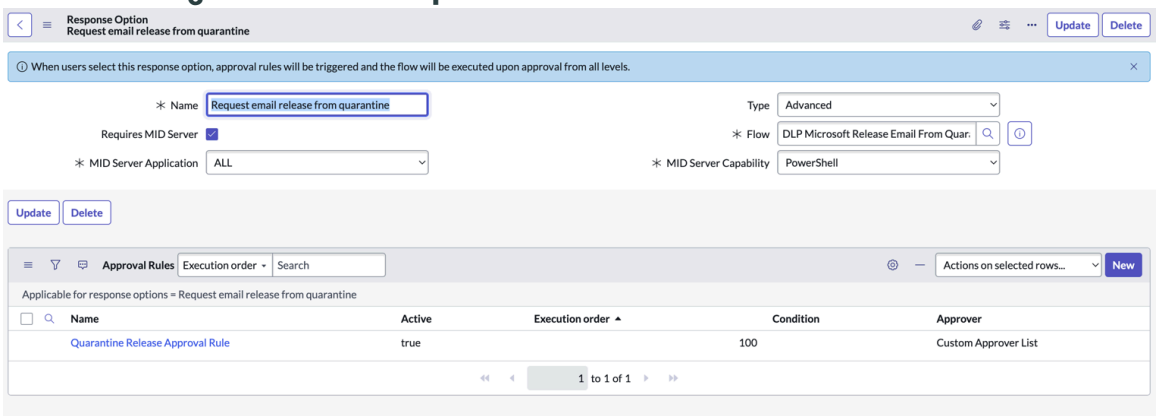
**MSFT – Antwortoptionsregel für Entlassung aus Quarantäne**




Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Standardmäßige MSFT-Antwortoption**




**Hinweis:**

Wenn Sie diese Antwortoption verwenden, stellen Sie sicher, dass der MID-Server mit PowerShell-Fähigkeit ausgeführt wird. Wenn ein MID-Server nicht ausgeführt wird und nicht über PowerShell-Fähigkeiten verfügt, kann der Endbenutzer im DLP-Benutzerarbeitsbereich die Aktion E- **Mail-Freigabe aus Quarantäne anfordern** nicht auswählen. Weitere Informationen finden Sie unter Richten Sie Optionsregeln für die Reaktion auf Incidents für Ihre DLP-Incidents ein und Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents.

- Wenn Sie einen bestimmten MID-Server aus der Liste auswählen möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Anschließend muss mindestens ein konfigurierter MID-Server in den ausgewählten MID-Anwendungen ausgeführt werden und über verfügen PowerShell-Fähigkeit.
- Damit Sie die Option Aus Quarantäne freigeben verwenden können, benötigen Sie API-Berechtigungen. Überprüfen Sie auf der Seite „API-Berechtigungen“ von Microsoft **Office 365 Exchange Online** > **Exchange.VerwaltenAlsApp** wird aufgelistet und enthält die folgenden Werte:
  - **Typ**: **Anwendung**.
  - **Administratoreinwilligung erforderlich**: **Ja**.
  - **Status**: Der aktuelle falsche Wert ist **Nicht gewährt für** <Organization> für den Eintrag **Office 365 Exchange Online** > **Exchange.ManageAsApp** und ändern Sie den Statuswert. Weitere Schritte zu den API-Berechtigungen finden Sie unter API-Berechtigungen der Anwendung zuweisen auf der Microsoft-Dokumentationswebsite.

    **Hinweis:**

    Dieser Schritt ist erforderlich, um über das Serviceprinzip eine Verbindung zu Exchange Online herzustellen.

- Sie benötigen auch die Rolle „ **Sicherheitsadministrator“** im Serviceprinzip.
  - Suchen Sie im Microsoft Azure-Portal nach **Microsoft Entra ID-Rollen und Administratoren**, fügen Sie der registrierten App (Service-Prinzip) Zuweisungen hinzu, und befolgen Sie dann das in der Microsoft-Dokumentation erläuterte Verfahren zum Zuweisen einer Rolle .
- Diese Option gilt nur für Microsoft Exchange-Incidents, bei denen in der Incident-Formularansicht die Option **Richtlinienaktion auf ExQuarantine festgelegtist**.

Erforderliche Rolle: Endbenutzer



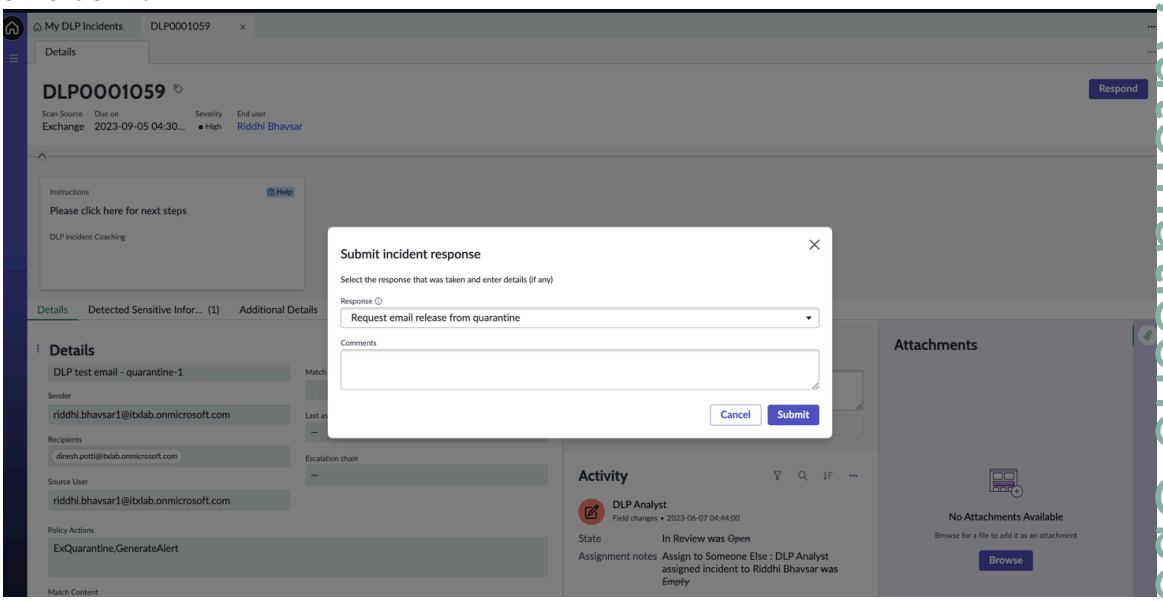
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Verfahren wird erläutert, wie diese Aktion über den DLP-Benutzerarbeitsbereich übermittelt wird.

### Prozedur

1. Navigieren zu **DLP** > **DLP-Benutzerarbeitsbereich**.
2. Öffnen Sie einen beliebigen Microsoft Exchange DLP-Incident.
   Vergewissern Sie sich, dass die Incident **-Richtlinienaktion** auf ExQuarantine festgelegt ist.
3. Klicken Sie **auf Antworten**.
4. Wählen Sie in der Dropdown-Liste Antwort die Option **Release-E-Mail aus Quarantäne anfordern aus**.

**Incident-Antwort übermitteln – Option „E-Mail-Freigabe aus Quarantäne anfordern“.**




5. Klicken Sie auf **Absenden**.

**Hinweis:**
Wenn eine Genehmigungsregel für diese Aktion konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst. Nach Erhalt aller Genehmigungen wird der Flow „E-Mail-Freigabe aus Quarantäne anfordern“ ausgelöst, und die E-Mail wird aus der Quarantäne freigegeben. Der Status des DLP-Incidents wird nach der erfolgreichen Freigabe auf „ **Aus Quarantäne freigegeben** “ aktualisiert.

## Laden Sie Dateien für DLP-Incidents vom Typ Exchange Online, OneDrive und SharePoint herunter

Laden Sie Dateien oder E-Mails herunter, die gegen die DLP-Richtlinie in Microsoft Purview verstoßen. Laden Sie diese Datei herunter, oder senden Sie sie per E-Mail aus der Incident-Ansicht DLP IR an Ihren lokalen Computer. Sie können die Dateien für DLP IR Incidents vom Typ Scanquelle Exchange Online, OneDrive und SharePoint herunterladen.

### Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin, sn_dlir.analyst
- Beliebiger gültiger Genehmiger

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Analyst-Arbeitsbereich**.
2. Öffnen Sie einen DLP-Incident-Datensatz vom Typ Scan-Quelle Exchange Online, OneDrive oder SharePoint, der aus der Microsoft-Quelle erfasst wird.
3. Klicken Sie **auf Datei herunterladen**.
   Die Datei oder E-Mail, die gegen die DLP-Richtlinie auf der Microsoft Purview-Seite verstoßen hat, wird auf den lokalen Computer des Benutzers heruntergeladen.

**Hinweis:**
Der DLP-Administrator kann den Zugriff auf die Aktion „ **Datei** herunterladen“ steuern, indem er die Einstellung **Sollte das Herunterladen der verletzten Datei des gemeldeten Incidents zulassen** auf der Seite „Erweiterte Einstellungen“ deaktivieren. Weitere Informationen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Data Loss Prevention Incident Response.

#### Domänentrennung in der Microsoft DLP-Integration

Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

### Support-Stufe

Support: Standard.

### Funktionsweise der Domänentrennung mit der Microsoft DLP-Integration

Befolgen Sie diese Schritte, um eine Domänentrennung zu erreichen:

- Erstellen Sie einen Benutzer mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie die DLP-Integrationsvorgänge Microsoft in der entsprechenden Domäne aus.

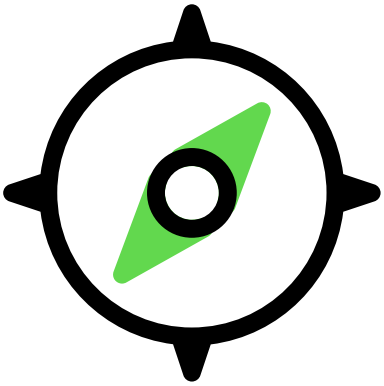
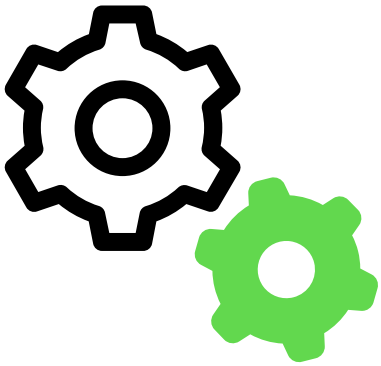
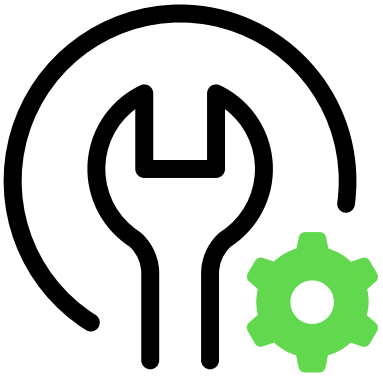
## Software-Stückliste

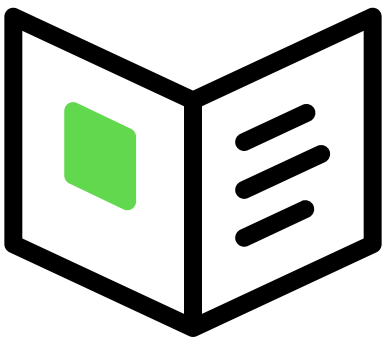
Zeigen Sie eine Liste der Open Source-Softwarekomponenten und Softwarekomponenten von Drittanbietern an, die Sie in Ihrer Anwendungsentwicklung verwenden. Erhalten Sie Einblicke in Softwarelizenzen, Versionsinformationen und die bekannten Schwachstellen in Ihren Komponenten in den Software-Stücklistendateien (SBOM), die Sie in Ihre Instanz hochladen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## Erste Schritte

| Erkunden | Konfigurieren | Verwenden |
| --- | --- | --- |
|  |  |  |
| Erfahren Sie mehr über die Konzepte und Funktionen von SBOM. | Konfigurieren Sie SBOM Anwendungen. | Erfahren Sie, wie Sie SBOM -Komponenten importieren und Daten im Arbeitsbereich anzeigen. |

| Referenz |
| --- |
|  |
| Rufen Sie Details zu SBOM Formularen, Feldern, Tabellen und Eigenschaften ab. |

Automatische Übersetzung

## Problembehandlung und Hilfe

- CycleneDX – Software-Stückliste (SBOM)
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

# Software Bill of Materials erkunden

Identifizieren Sie die in den Anwendungen Ihrer Organisation verwendeten Komponenten aus Software Bill of Materials (SBOM) Dateien, die Sie in Ihre Instanz hochladen. Machen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie sich mit allen Risiken vertraut, die mit der Verwendung von Open Source-Software verbunden sind, damit Sie Ihr potenzielles Risiko ermitteln und Schwachstellen beheben können.

### Verfügbare Versionen Software Bill of Materials .

| Release-Version | Versionsinformationen |
|---|---|
| Datenmodell für SBOM<br>v1.3, v1.1, v1.0 | Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes<br>Application Vulnerability Response release notes |
| SBOM Zentral<br>v2.1, v2.0, v1.0 | |
| SBOM Antwort<br>v3.1, v3.0, v2.0 | |

### SBOM – Anwendungsfall

Drittanbieter- und Open Source-Komponenten bieten Ihnen viele Vorteile für die schnelle Erstellung und Veröffentlichung Ihrer Softwareprojekte. In einigen Fällen sind jedoch mit der Verwendung öffentlich zugänglicher Komponenten Risiken verbunden, z. B.:

- Mangelnde Transparenz der Komponentenintegrität
- Schwachstellen in der Software
- Lizenzierungs-Compliance

Mit drei Software Bill of Materials Anwendungen können Sie einen genauen Bestand Ihrer Softwarekomponenten anzeigen:

- Datenmodell für SBOM
- SBOM Zentral
- SBOM Antwort

Sie können Ihre Software-Stücklistendateien über eine API oder manuell hochladen. Zeigen Sie die Dateien an, die Sie als Entitäten importieren, bei denen es sich um Bestände der in Ihrer Software verwendeten Komponentenbibliotheken von Drittanbietern handelt, einschließlich aller Transitabhängigkeiten. Weitere Informationen dazu, was in den Softwarebeständen in SBOMs für ZykloneDX enthalten ist, finden Sie unter ZykloneDX - Software Bill of Material (SBOM) .

### Datenmodell für SBOM

Diese Anwendung stellt die Tabellen bereit, die zum Speichern von SBOM-Daten verwendet werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

## SBOM Zentral

Laden Sie Ihre Software-Stücklistendateien im Format „CycloneDXJSON“ in Ihre Now Platform® -Instanz hoch, analysieren Sie sie und verarbeiten Sie sie. Zeigen Sie Stücklistenentitäten (BOM) und einen Bestand Ihrer Softwarekomponenten an. Eine Stücklistenentität ist die Komponente auf Stammebene in einer SBOM-Datei. Beispiel: Für eine SBOM vom Typ „CycloneDX“ wird die in den Metadaten aufgeführte Komponente als Stücklistenentität betrachtet.

## SBOM Antwort

Zeigen Sie Ihren Komponentenbestand an, und bewerten Sie Ihr Risiko im SBOM-Arbeitsbereich. Sie können feststellen, ob bekannte Schwachstellen Softwarekomponenten zugeordnet sind, und Lizenzierungs- und Versionsinformationen sowie andere Details anzeigen.

In der folgenden Tabelle finden Sie weitere Informationen zu jeder ServiceNow® SBOM-Anwendung.

### Erforderliche Anwendungen für SBOM

| Anwendung ServiceNow | Beschreibung |
|---|---|
| Datenmodell für SBOM | Diese Anwendung ist erforderlich. Sie enthält die Tabellen, ACLs und Rollen, die zum Lesen von SBOM Daten erforderlich sind. |
| SBOM **Kern** | Diese Anwendung ist erforderlich. Sie enthält die API, die zum Hochladen von SBOM Dokumenten erforderlich ist, und die Geschäftslogik, die zum Analysieren und Importieren der Daten aus diesen Dokumenten in Ihre Instanz erforderlich ist. Ab v2.1 können Sie einen Bestand Ihrer Softwarekomponenten im SBOM-Arbeitsbereich anzeigen. |
| SBOM **Antwort** | Die Anwendung Vulnerability Response ist erforderlich, wenn Sie die Anwendung SBOM Response installieren. Installieren Sie Vulnerability Response, bevor Sie SBOM Response installieren.<br><br>Zeigen Sie Ihren Komponentenbestand an, und bewerten Sie Ihr Risiko im SBOM-Arbeitsbereich. Richten Sie Regeln ein, um automatisch angreifbare Elemente in Anwendungen (AVITs) zu erstellen und mit dem Application Vulnerability Response-Workflow zu beheben.<br><br>Die Integrationen OSV.dev und Deps.dev sind in der Installation von SBOM Response enthalten. |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Erforderliche Anwendungen für SBOM (Fortsetzung)**

| Anwendung ServiceNow | Beschreibung |
|---|---|
| | • OSV.dev ist eine Open Source-API, die Vulnerability Intelligence-Informationen für eine bestimmte Version eines Pakets oder einer Bibliothek bereitstellt.<br>• Deps.dev ist eine Open Source-API, die eine Versionsliste für ein bestimmtes Paket oder eine bestimmte Bibliothek bereitstellt. |

Durch die Installation unterstützter Vulnerability Intelligence- und anderer Integrationen von Drittparteien können Sie die Anzahl der Komponenten anzeigen, die als veraltet und verworfen gelten, sowie Informationen dazu, ob Sie mit den Komponenten verbundene Schwachstellen beheben können. Die in der folgenden Tabelle aufgeführten Anwendungen ServiceNow® und Drittanbieterintegrationen werden von der Anwendung SBOM unterstützt. Diese Anwendungen stellen Ihnen erweiterte Schwachstellendaten, Schwachstelleninformationen und andere wichtige Informationen bereit, die Ihnen helfen können, die mit SBOM -Dateien verknüpften Schwachstellen anzuzeigen und zu priorisieren. Alle diese Anwendungen und Integrationen sind über den ServiceNow Storeverfügbar.

**Andere unterstützte Anwendungen für SBOM**

| Anwendung | Beschreibung |
|---|---|
| Vulnerability Response | Erforderlich, wenn Sie die Anwendung SBOM Response installieren. Die Funktionen von Application Vulnerability Response werden mit Vulnerability Response installiert. Diese Funktionen ermöglichen den Zugriff auf den Vulnerability Manager-Arbeitsbereich in der Anwendung Vulnerability Response und den Schwachstellen-Workflow, um Sie bei der Korrektur von angreifbaren Elementen in Anwendungen (AVITs) zu unterstützen. Bietet Zugriff auf die National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) und Anwendungsschwachdaten von Drittparteien. |
| Die Integration von Vulnerability Response mit geplanten NVD- und CWE-Aufgaben | Zeigen Sie erweiterte NVD-Schwachstellen- und Schweregraddaten an. Wenn Sie SBOM Response installiert haben, können Sie importierte Daten aus den NVD- und CWE-Integrationen anzeigen, um alle Schwachstellendaten zu ergänzen, die Sie in Ihren SBOM -Daten finden könnten.<br><br>Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Bibliotheken von Drittanbietern. |
| Veracode Vulnerability Integration | Importieren Sie Software-Stücklistendateien mit Veracode Vulnerability Integration. Wenn Sie diese Integration bereits installiert haben, können Sie auch |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Andere unterstützte Anwendungen für SBOM (Fortsetzung)**

| Anwendung | Beschreibung |
|---|---|
| | importierte Veracode-Daten SBOM im JSON-Format „CycloneDX“ hochladen. |

## Installieren Sie die unterstützten Anwendungen für Software Bill of Materials

Laden Sie die erforderlichen Anwendungen für die Anwendung Software Bill of Materials (SBOM) herunter, und aktivieren Sie sie, bevor Sie Dateien hochladen.

### Vorbereitungen

Erforderliche Rollen: admin für Download, Installation und Aktivierung aller Anwendungen und Rollenzuweisungen in Ihrer Instanz.

### Warum und wann dieser Vorgang ausgeführt wird

### Prozedur

1. Laden Sie die erforderlichen SBOM -Anwendungen von ServiceNow Store in Ihre ServiceNow -Instanz herunter.

   Mit diesen Anwendungen können Sie SBOM-Dateien hochladen und in Ihre Instanz importieren. Sie können Komponentendaten im SBOM-Arbeitsbereich ab Version 2.1 von SBOM Core anzeigen.

   - Datenmodell für SBOM
   - SBOM Zentral

   Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie unter:

   - Security Operations und der ServiceNow Store
   - Laden Sie zum ersten Mal eine Anwendung aus dem ServiceNow Store herunter

2. **Wahlweise:** Wenn Sie Ihre SBOM -Daten im SBOM -Arbeitsbereich anzeigen, importierte Schwachstelleninformationen von Drittanbietern anzeigen, Ihr Risiko bewerten und Schwachstellen mit den Workflows „Application Vulnerability Response“ und „Vulnerability Response“ beheben möchten, laden Sie die folgenden Anwendungen herunter:

   - Vulnerability Response und ihre Abhängigkeiten
   - Vulnerability Response Integration with NVD
   - SBOM Antwort

   Weitere Informationen zu diesen und anderen unterstützten SBOM Anwendungen finden Sie unter Software Bill of Materials erkunden.

3. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
4. Suchen Sie die heruntergeladenen Anwendungen SBOM, und wählen **Sie Installieren** aus, um sie zusammen mit ihren Abhängigkeiten zu aktivieren.

   Eine Nachricht wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde. Aktivieren Sie die Anwendungen in der folgenden Reihenfolge:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vulnerability Response und ihre Abhängigkeiten
- Vulnerability Response Integration with NVD
- Datenmodell für SBOM
- SBOM Zentral
- SBOM Antwort, einschließlich der Integrationen OSV.dev und Deps.dev

Wenn installiert, ist die Deps.dev-Integration standardmäßig aktiviert (Kontrollkästchen „Aktiv“ im Integrationsdatensatz aktiviert) und für die wöchentliche Ausführung geplant. Sie können den Zeitplan bearbeiten und die geplante Aufgabe bei Bedarf über den Integrationsdatensatz initiieren. Navigieren zu **Alle** > **Vulnerability Response** > **Integrationen** > **Deps.dev-Integration**. Die Rolle sn_vul.app_configure_integrations ist erforderlich, um den Zeitplan dieser Integration zu bearbeiten.

Die **Deps.dev** -Integration wird verwendet, um Komponenten zu identifizieren, die sich im Status „Veraltet“ und „ **Verworfen** “ befinden. Die Version einer veralteten Komponente liegt mehr als zwei Hauptversionen hinter der neuesten Version und zwei Jahre hinter der neuesten Version zurück. Eine verworfene Komponente wurde mehr als zwei Jahre lang nicht aktualisiert. Die Schwellenwerte für zwei Jahre und zwei Versionen können mit Systemeigenschaften bearbeitet werden. Um diese Parameter zu bearbeiten, navigieren Sie zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** und suchen Sie die folgenden Datensätze:

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Die Schwellenwerte für „Verworfen“ und „Veraltet“ werden in Monaten angegeben. Der Schwellenwert für die Version ist numerisch.

Falls installiert, ist die OSV.dev-Integration standardmäßig aktiviert (Kontrollkästchen „Aktiv“ im Integrationsdatensatz aktiviert). Sie müssen sie jedoch bei Bedarf über den Integrationsdatensatz initiieren. Navigieren zu **Alle** > **Vulnerability Response** > **Integrationen** > **OSV.dev-Integration – Umfassend**. Die Rolle sn_vul.app_configure_integrations ist erforderlich, um den Zeitplan dieser Integration zu bearbeiten.

**Hinweis:**
Sie können den Integrationsparameter `batchSize` von OSV.dev unter Open Source Vulnerabilities Integration (Integration von Open Source-Schwachstellen) konfigurieren. Der Standardwert beträgt 75 PURLs pro API-Aufruf.

5. **Wahlweise:** Aktivieren Sie Integrationen, indem Sie zu navigieren **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** , und wählen **Sie Installieren aus**.

   (Optional) Weitere Informationen zu diesen Integrationen und den von ihnen bereitgestellten Funktionen finden Sie unter Software Bill of Materials erkunden.

   - Vulnerability Response Integration with Veracode. Weitere Informationen finden Sie unter ServiceNow Vulnerability Response Integration with Veracodeinstallieren.
   - Integration von Vulnerability Response mit NVD, die erforderlich ist, wenn Sie die erweiterten Daten für Schwachstellen anzeigen möchten, die mit hochgeladenen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten verbunden sind. Weitere Informationen finden Sie unter Grundlegendes zu den NVD-Integrationen.

- CWE Comprehensive 2000-Integration. Weitere Informationen zum Aktivieren dieser geplanten Aufgabe finden Sie unter Konfigurieren Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen, und führen Sie sie aus.
- Snyk Vulnerability Insights-Integration. Weitere Informationen finden Sie in der Snyk-Dokumentation .

Eine Nachricht wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

6. Weisen Sie Benutzern die folgenden Rollen zu.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
7. **Wahlweise:** Weisen Sie Benutzer der App-Sec-Manager-Gruppe zu, wenn Sie angreifbare Anwendungselemente für Schwachstellen in Ihren importierten SBOM -Daten erstellen.

   (Optional) Benutzer, die der App-Sec-Manager-Gruppe zugewiesen sind, priorisieren und verwalten angreifbare Anwendungselemente. Benutzer in dieser Gruppe erben viele der Rollen, die zum Lesen und Bearbeiten von Datensätzen und zum Konfigurieren der von der Anwendung Application Vulnerability Response unterstützten Anwendungen und ihren Nachbesserungs-Workflows erforderlich sind.

### Nächste Maßnahme

Laden Sie Ihre SBOM -Dateien hoch. Weitere Informationen finden Sie unter Laden Sie Software Bill of Materials Dateien manuell hoch und Software Bill of Materials Dateien mit einer REST-API werden hochgeladen.

## Verwenden des Software-Arbeitsbereichs „Stückliste“.

Mit den SBOM-Anwendungen können Sie Dateien hochladen und Details für Entitäten und Komponentenbestände im Arbeitsbereich Software Bill of Materials (SBOM) anzeigen.

Mit den Anwendungen SBOM können Sie die folgenden Aufgaben ausführen:

1. Laden Sie Dateien mit einer API oder manuell hoch.

   Weitere Informationen finden Sie unter Software Bill of Materials Dateien mit einer REST-API werden hochgeladen und Laden Sie Software Bill of Materials Dateien manuell hoch.

2. Überprüfen Sie die hochgeladenen Stücklistenkomponenten im Arbeitsbereich. Wie Sie Komponenten überprüfen, hängt von den installierten Anwendungen ab.

   Weitere Informationen finden Sie unter Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials.

3. Bewerten Sie Ihr Risiko, und erstellen Sie angreifbare Anwendungselemente für Komponenten, denen Schwachstellen zugeordnet sind.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Identifizieren Sie, ob bekannte Schwachstellen Softwarekomponenten zugeordnet sind.
- Überprüfen Sie erweiterte Vulnerability Intelligence-Details wie Versionsinformationen, Verfügbarkeit von korrigierten Versionen und Lizenzierungsinformationen, um angreifbare Elemente zu beheben.

Weitere Informationen finden Sie unter Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials und Erstellen von Regeln für angreifbare Anwendungselemente im Software Bill of Materials -Arbeitsbereich.

### Software Bill of Materials Dateien mit einer REST-API werden hochgeladen

Überprüfen Sie die folgenden Informationen, bevor Sie Software Bill of Materials -Dateien mit einer API hochladen.

## REST-API

Um Daten mit einer API hochzuladen, verwenden Sie den folgenden geskripteten REST-Endpunkt. Die Rolle sn_sbom_core.sbom_ingest ist erforderlich.

<host_name*/api/sbom/core/upload*.

**Hinweis:**
<host_name>ist Ihr Instanzname ServiceNow .

Nachdem SBOM erfolgreich verarbeitet wurde, hängt es von den verwendeten Anwendungen ab, wo Sie die hochgeladenen Datensätze anzeigen.

- Wenn Sie SBOM Response verwenden, wird der Datensatz der Stücklistenentität in der Liste SBOM „ Ingestion Status“ (Erfassungsstatus) im Modul „BOM-Warteschlange“ im Arbeitsbereich SBOM angezeigt.
- Wenn Sie SBOM Core verwenden, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**.

## Verwenden der REST-API

Sie können nur SBOM Dateien im JSON-Format „CycloneDX“ hochladen.

Wenn der aufrufende Benutzer erfolgreich authentifiziert wurde und die Rolle sn_sbom_core.sbom_ingest in Ihrer Instanz ServiceNow hat, können Sie von außerhalb Ihrer Instanz auf die API zugreifen, um die Daten SBOM hochzuladen.

SBOM -Inhalt kann entweder als Text der HTTP-Anforderung oder über eine Befehlszeilenanforderung mit einer SBOM -Datendatei an die API gesendet werden. Beispielsweise können Sie das Befehlszeilentool *curl* verwenden, sofern Ihre Benutzer über einen eigenen Prozess zum Verwalten der Dateien verfügen.

Darüber hinaus können Sie die sys_id des Produktmodells und die Geschäftsanwendung in Ihre Abfrageparameter aufnehmen. Die Stücklistenentität wird diesen Parametern zugeordnet, wenn Sie sie einbeziehen. Die folgenden Parameter werden unterstützt:

- produktModellId
- Geschäftsanwendungs-ID

Jeder API-Aufruf wird in die Warteschlange gestellt, und eine sys_id des Datensatzes in der Warteschlange wird als API-Antwort zurückgegeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Über die REST-API werden die Daten SBOM an Ihre Instanz Now Platform ] gesendet.

Nachdem die Daten hochgeladen wurden, werden sie analysiert. Bevor Daten analysiert werden, werden die folgenden Anforderungen überprüft:

- Bei eingehenden Daten wird überprüft, ob es sich um gültige JSON-Daten handelt.
- Das Stücklistenformat wird unterstützt. Für diese Integration wird nur das Format „CycloneDX“ unterstützt.
- Die Mindestanzahl von Feldern ist verfügbar, damit Daten analysiert werden können.

Nachdem diese Prüfungen verifiziert wurden, erfolgt ein Eintrag in der Tabelle „Stückliste“ [sn_sbom_doc] mit eingehenden SBOM Daten als Anhang.

Die Geschäftsregel *`Process BOM file`* wird automatisch als Ergebnis der Datensatzeinfügung und Datenanalyse ausgelöst.

**Hinweis:**
Diese Geschäftsregel wird während der Installation von SBOM Core standardmäßig aktiviert.

Alle in einem SBOM aufgeführten Komponenten haben einen definierten Typ.

- Komponenten, für die SBOM Dateien hochgeladen wurden, werden als Stücklistenentitäten betrachtet.
- Komponenten, die als type=library aufgeführt sind, werden als Komponenten von Drittparteien betrachtet.

**Zugehörige Informationen**

Upload-Status für Software Bill of Materials Dateien wird angezeigt

Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

### Laden Sie Software Bill of Materials Dateien manuell hoch

Laden Sie Software Bill of Materials (SBOM) Dateien manuell hoch.

#### Vorbereitungen

Sie können nur SBOM Dateien im JSON-Format „CycloneDX“ hochladen.

Erforderliche Rolle: sn_sbom_core.sbom_ingest

#### Prozedur

1. Laden Sie die Dateien manuell hoch.

   Die Methode, die Sie zum Hochladen Ihrer Dateien verwenden, hängt davon ab, ob Sie die Anwendungen SBOM Core oder SBOM Response installiert haben.

2. **Wahlweise:** Laden Sie SBOM-Dateien hoch, die von Veracode Vulnerability Integrationimportiert wurden.

   **Hinweis:**
   Sie können Veracode-Dateien im JSON-Format nur dann hochladen, wenn Sie die Veracode -Integration mit Application Vulnerability Responseinstalliert und aktiviert haben. Weitere Informationen finden Sie unter Veracode Vulnerability Integration.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Ergebnisse

Nachdem SBOM erfolgreich verarbeitet wurde, hängt es von den verwendeten Anwendungen ab, wo Sie den Upload-Status anzeigen.

- Wenn Sie SBOM Response verwenden, wird der Datensatz der Stücklistenentität in der Liste SBOM „ Ingestion Status“ (Erfassungsstatus) im Modul „BOM-Warteschlange“ im Arbeitsbereich SBOM angezeigt.
- Wenn Sie SBOM Core verwenden, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**.

#### Zugehörige Informationen

Software Bill of Materials Dateien mit einer REST-API werden hochgeladen

## Anzeigen von Berichten und Dashboards im Arbeitsbereich Software Bill of Materials

Schwachstellenanalysten zeigen hochgeladene Software-Stücklistendateien in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen im Arbeitsbereich Software Bill of Materials (SBOM) an.

### Anforderungen zum Anzeigen von Daten

### SBOM-Core

Ab Version 2.1 der Anwendung SBOM Core können Sie Stücklistenentitäten und eine Liste der Komponenten anzeigen, die Sie auf der Startseite (Zielseite) und im Modul „Komponenten“ im SBOM-Arbeitsbereich hochgeladen haben. Navigieren Sie vor v2.1 zu **SBOM-Core** > **Stücklisten-Erfassungsstatus** , um die Komponenten anzuzeigen.

### SBOM-Antwort

Die Anwendung „SBOM Response“ bietet Datenvisualisierungen mit detaillierten Informationen zu Stücklistenentitäten, Entitäten mit Schwachstellen und aktiven angreifbaren Anwendungselementen auf der Startseite (Zielseite) im SBOM-Arbeitsbereich. Der Arbeitsbereich mit SBOM Response umfasst die folgenden Module:

- Homepage: Datenvisualisierungen und erweiterte Schwachstellendetails.
- Komponenten: Versions- und Korrekturinformationen für Komponenten.
- Erstellungsregeln für AVIT (angreifbares Anwendungselement): Bedingungen für die Erstellung von angreifbaren Elementen in Anwendungen (AVITs).
- Stücklisten-Warteschlange: Status und Verlauf des Dateiuploads.
- Liste: AVIT-Datensätze für angreifbare Komponenten und Bibliotheken (NVD, CWE und Anwendungsschwachstellen).

Die folgenden Themen enthalten weitere Informationen dazu, wie Sie Details zu Ihren Komponenten im Software Bill of Materials -Arbeitsbereich finden.

- Überprüfen der Homepage im Software Bill of Materials -Arbeitsbereich
- Überprüfen des Komponentenmoduls im Software Bill of Materials -Arbeitsbereich
- Upload-Status für Software Bill of Materials Dateien wird angezeigt
- Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Überprüfen der Homepage im Software Bill of Materials -Arbeitsbereich

Für hochgeladene Daten wird ein Rollup zu den Visualisierungen auf der Zielseite (Homepage) im Arbeitsbereich Software Bill of Materials (SBOM) durchgeführt. Daten werden geändert, nachdem Sie Dateien hochgeladen haben, damit Schwachstellenanalysten Trends anzeigen und aktuelle Informationen zu Ihren Komponenten überprüfen können.

## Anzeigen der -Homepage

Erforderliche Rollen:

- Ab Version 2.1 von SBOM Core – sn_sbom_resp.sbom_analyst
- Vor v2.1 von SBOM Core – sn_sbom_resp.admin

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich**. Standardmäßig wird die Zielseite (Homepage) von angezeigt.

   Was Sie im Modul sehen können, hängt von den installierten Anwendungen ab.

| Installierte Anwendung | Beschreibung |
|---|---|
| Wenn Sie SBOM Core ab v2.1 installiert haben | , eine Liste von Stücklistenentitäten. Die Liste enthält den Namen, den Klassifizierer (Anwendung, Container, Bibliothek usw.) und die Komponentenanzahl für jede Entität. Eine Stücklistenentität verweist auf die Komponente auf Stammebene in einer SBOM-Datei, für die ein Dokument SBOM generiert und hochgeladen wurde.<br><br>Navigieren Sie vor v2.1 zu **SBOM Core** > **Stücklisten-Erfassungsstatus**, um die Liste der Stücklistenentitäten anzuzeigen. |
| Wenn Sie SBOM Response installiert haben, werden | die folgenden Datenvisualisierungen angezeigt.<br>○ Alle Stücklistenentitäten: Eine Aufgliederung der Stücklistenentitäten nach Typ: Anwendung, Container, Bibliothek und Sonstige. Eine Stücklistenentität verweist auf die Komponente auf Stammebene in einer SBOM-Datei, für die ein Dokument SBOM generiert und hochgeladen wurde.<br>○ Stücklistenentitäten mit Schwachstellen: Entitäten, bei denen eine Schwachstelle einer Komponente zugeordnet ist, von der sie abhängig sind. Wenn eine Entitätsabhängigkeit eine **kritische** Schwachstelle aufweist, wird der Schweregrad der Entität als kritisch betrachtet.<br>○ Aktive AVIs: Der Trend für die Anzahl der täglich erstellten angreifbaren Elemente (AVIs). |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Installierte Anwendung | Beschreibung |
|---|---|
| | Die Datenvisualisierungen zeigen Daten für die letzten 30 Tage an. Der 30-Tage-Bereich kann nicht bearbeitet werden. Diese Daten sind verfügbar, nachdem Sie die Erstellungsregeln für angreifbare Anwendungselemente überprüft und eingerichtet haben. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente im Software Bill of Materials -Arbeitsbereich. |

2. Wählen Sie eine Datenvisualisierungskarte aus, um die Liste der Datensätze anzuzeigen.
3. Wählen Sie die Registerkarte **Homepage** aus, um zur Zielseite zurückzukehren.
4. Wählen Sie einen Datensatz unter der Liste der **Stücklistenentitäten** aus.

   Der Name und die Version der Entität werden oben im Datensatz angezeigt, z. B. SNC-SECOPS-SIR2.0.

5. Wählen Sie die Registerkarten im Entitätsdatensatz aus, um die Daten zu überprüfen.
   a. Wenn nicht ausgewählt, wählen Sie die Registerkarte **Übersicht**.

      Überprüfen Sie die Daten. Wenn ein Feld in diesem Datensatz nicht ausgefüllt wird, waren die Daten nicht in den von Ihnen hochgeladenen SBOM Dateien enthalten.

| Name | Beschreibung |
|---|---|
| Name | Entitätsname. |
| Klassifizierungsentitätstyp | , z. B. eine Anwendung, Komponente oder Bibliothek. |
| Version | Versionsnummer der Entität. |
| Lieferant | : Produkt, von dem die Entität geliefert wurde. |
| Produktmodell | Wenn kein Produktmodell vorhanden ist oder Sie zum Zeitpunkt des Uploads von SBOM über die API keines hinzufügen, wird eines erstellt. Der Name der Entität wird für den Produktmodelldatensatz verwendet, z. B. SNC-SECOPS-SIR2.0. |

   b. Wählen Sie die Registerkarte **Abhängig von aus**.

      Alle Abhängigkeiten dieser Entität werden zusammen mit Klassifizierern aufgelistet, z. B. Bibliothek. Die Versionsnummer, Lizenzenund andere Informationen werden angezeigt.

      Durch Auswahl eines Links in dieser Liste wird ein Datensatz geöffnet. Die zugehörige Registerkarte wird unter den Registerkarten „Startseite“ und „Entitätsdatensatz“ angezeigt. Der Datensatz, den Sie öffnen, kann die folgenden zugehörigen Listen enthalten, die Sie überprüfen können: Übersicht, Hashes, Stücklistenentitäten, Schwachstellen und angreifbare Elemente in Anwendungen (AVITs).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der zugehörigen Liste „Stücklistenentitäten“ werden alle Entitäten angezeigt, in denen dieses angezeigte Element verwendet wird.

**c.** Wählen Sie die Registerkarte **Schwachstellen** aus, um die Schwachstellen anzuzeigen, die einer Abhängigkeit dieser Entität zugeordnet sind.

Weitere Informationen zu den für eine Entität angezeigten Schwachstellen finden Sie unter Upload-Status für Software Bill of Materials Dateien wird angezeigt.

**d.** Wählen Sie die Registerkarte **AVIs** aus, um zu sehen, ob angreifbare Anwendungselemente für diese Entität vorhanden sind.

### Überprüfen des Komponentenmoduls im Software Bill of Materials -Arbeitsbereich

Das Komponentenmodul im Arbeitsbereich Software Bill of Materials (SBOM) zeigt aktuelle Informationen zu angreifbaren, veralteten, verworfenen und risikoreichen Kombinationen für die Komponenten an, die Sie importieren.

## Komponentenmodul anzeigen

Erforderliche Rollen:

- Ab Version 2.1 von SBOM Core – sn_sbom_resp.sbom_analyst
- Vor v2.1 von SBOM Core – sn_sbom_resp.admin

Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Komponenten**.

Was Sie im Modul sehen können, hängt von den installierten Anwendungen ab.

| Installierte Anwendung | Beschreibung |
|---|---|
| Wenn Sie SBOM Core installiert haben | Ab v2.1 eine Bestandsliste aller hochgeladenen Komponenten, die die folgenden Informationen enthält:<br>• Name<br>• Beschreibung<br>• Version<br>• Anzahl der Stücklistenentitäten |
| Wenn Sie SBOM Response installiert haben | Wählen Sie ab Version 3.1 von SBOM Response ein Diagramm oder eine Zahl im Diagramm aus, um eine Liste der zugehörigen Datensätze anzuzeigen.<br>**Alle Komponenten**<br>Die Liste der **veralteten** und **verworfenen** Komponenten sowie der Komponenten mit mindestens einer Schwachstelle in der Gesamtanzahl der Komponenten. Diese Anzahlen können Ihnen helfen, Komponenten zu identifizieren, die Ihre Aufmerksamkeit erfordern. Diese Teilmengen von Komponenten |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Installierte Anwendung | Beschreibung |
| --- | --- |
| | stimmen möglicherweise nicht mit Ihrer Gesamtkomponentenanzahl überein, da möglicherweise nicht alle Ihre Komponenten in diese Kategorien passen.<br>• Die Version einer veralteten Komponente liegt mehr als zwei Hauptversionen hinter der neuesten Version und zwei Jahre hinter der neuesten Version zurück.<br>• Eine verworfene Komponente wurde mehr als zwei Jahre lang nicht aktualisiert.<br>• Angreifbare Komponenten sind Komponenten, die Schwachstellen mit dem Schweregrad „ **Hoch“** oder höher aufweisen.<br>**Kombinationen mit hohem Risiko**<br>Komponenten mit hohem Risiko erfordern möglicherweise sofortige Aufmerksamkeit. Die **Deps.dev** -Integration, die bei der Installation der Anwendung SBOM Response installiert wird, stellt die **Paketinformationen** für Komponenten im Status „Veraltet“ und „Verworfen“ bereit. Wenn die Snyk Vulnerability Insights-Integration installiert ist, können Sie die Korrekturinformationen für eine Schwachstelle in einer Komponente anzeigen. Beachten Sie, dass Korrekturen möglicherweise nicht für alle Komponenten verfügbar sind.<br>Importierte Kombinationen mit hohem Risiko bestehen aus veralteten und verworfenen Komponenten mit mindestens einer schwerwiegenden Schwachstelle (**Kritisch** oder **Hoch**), die Sie durch Updates, Ersatz oder eine andere Art von Reparatur beheben können. Der Status **Vollständig reparierbar** bedeutet, dass für eine Komponente eine |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Installierte Anwendung | Beschreibung |
| --- | --- |
| | Version verfügbar ist, die das Problem beheben kann. Der Prozentsatz der Gesamtzahl der Komponenten mit hohem Risiko, die über reparierbare Versionen verfügen, wird notiert.<br>**Angreifbare Komponenten mit Behebbarkeit**<br>Summen und Aufgliederungen der Komponenten mit **kritischen**, **hohen**, **mittleren**und **niedrigen** Schwachstellen und ob einige oder alle ihrer Schwachstellen behoben werden können. Wenn eine Komponente mehr als eine Schwachstelle aufweist, hat die kritischste Schwachstelle Vorrang.<br>Der Korrekturstatus:<br>• Vollständig – Es gibt Korrekturversionen für alle Schwachstellen, die der aktuellen Version der Komponente zugeordnet sind.<br>• Teilweise – Es gibt eine Korrekturversion für mindestens eine, aber nicht alle der Schwachstellen, die der aktuellen Version der Komponente zugeordnet sind.<br>**Komponenten nach Lizenz**<br>Summen und Aufgliederungen von Komponenten nach Lizenzen.<br>In der Komponentenliste unter den Diagrammen können Sie Name, Beschreibung, Version und Anzahl der Entitäten anzeigen. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben. Die Spalten Allgemeine Schwachstellen und Gefährdung (**CVE**) und **Reparierbarkeit** werden ebenfalls angezeigt. |

## Bewerten Sie Ihr Risiko mit Vulnerability Intelligence

Weitere Informationen zum Überprüfen von Vulnerability Intelligence-Daten im Arbeitsbereich finden Sie unter Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Erstellen von Regeln für angreifbare Anwendungselemente im Software Bill of Materials -Arbeitsbereich

Bevor Sie angreifbare Anwendungselemente (AVITs) im Arbeitsbereich „Software-Stückliste“ (SBOM) anzeigen können, müssen Sie die Bedingungen einrichten, unter denen AVITs erstellt werden.

## AVITs im SBOM -Arbeitsbereich

Wenn Sie die Anwendung „SBOM Response“ installiert und aktiviert haben, werden AVITs für SBOM Dateien erstellt, wenn eine der importierten Daten den Bedingungen Ihrer vorhandenen AVIT-Erstellungsregeln entspricht.

Die Anwendungen SBOM Response und Vulnerability Response sind erforderlich, um Regeln für die automatische Erstellung von angreifbaren Elementen in Anwendungen (AVITs) und deren Korrektur mit dem Application Vulnerability Response-Workflow einzurichten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Sie müssen AVIT-Erstellungsregeln im SBOM -Arbeitsbereich hinzufügen, bevor Sie AVITs für die Schwachstellen erstellen können, die in Ihren erfassten SBOM -Daten gefunden wurden. Mit AVITs können Sie die Integrität der Drittanbieterkomponenten in Ihren Anwendungen bewerten. Eine AVIT wird in Ihrer Instanz erstellt, wenn eine Anwendung mit einer Komponente abgeglichen wird, der eine Schwachstelle zugeordnet ist.

Im Arbeitsbereich SBOM können Sie nur SBOM-AVITs anzeigen. Sie können jedoch SBOM-AVITs zusammen mit anderen Arten von angreifbaren Elementen im Arbeitsbereich von Vulnerability Manager in Vulnerability Response anzeigen. Sie können alle AVITs anzeigen, die im SBOM-Arbeitsbereich im Listenmodul erstellt wurden. Das Listenmodul enthält auch alle NVD- und CWE-Einträge und Anwendungsschwachstellen.

Wenn Sie die Snyk Vulnerability Integration haben oder die OSV.dev-Integration ausgeführt haben und Korrekturinformationen verfügbar sind, werden sie in einer zugehörigen Liste im AVIT-Datensatz angezeigt.

Sie können AVITs auch basierend auf Empfehlungen aus bekannten Schwachstellenlisten wie der National Vulnerability Database (NVD) zur Korrektur zuweisen. Eine regelmäßige Aufgabe wird ausgelöst, und wenn die Bedingungen Ihrer Erstellungsregeln mit den erfassten Daten übereinstimmen, werden AVITs erstellt.

Sie können AVITs nachverfolgen und beheben, indem Sie benutzerdefinierte Regeln einrichten.

Informationen zum Erstellen einer Regel finden Sie unter Erstellen Sie im Software Bill of Materials -Arbeitsbereich eine Regel für angreifbare Anwendungselemente.

## SBOM AVITs in Vulnerability Manager Workspace in Vulnerability Response

Sie können alle SBOM AVITs anzeigen, die im Arbeitsbereich SBOM in Vulnerability Manager Workspace erstellt wurden, wenn Sie Zugriff darauf haben.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Hinweis:**
Um nur SBOM AVITs aus der Liste der angreifbaren Anwendungselemente in Vulnerability Manager Workspace anzuzeigen und nicht alle AVITs, legen Sie die Bedingung **[Quelle] [ist] [SBOM] UND [Scan-Typ] [ist] [SBOM-SCA]** für die angreifbare Anwendung fest Tabelle „Elemente“ [sn_vul_app_vulnerable_item]. Um die Tabelle anzuzeigen, navigieren Sie in Ihrer Instanz zu **Alle**, und geben **Sie sn_vul_app_vulnerable_item.list** in den Filternavigator ein.

Weitere Informationen zu Vulnerability Manager Workspace, zum Anzeigen von Überwachungsthemen, zu Anwendungskorrekturmaßnahmen und Regeln für Anwendungskorrekturaufgaben für AVITs, die über die Anwendung Vulnerability Response in der Vulnerability Manager Workspacekonfiguriert werden, finden Sie unter Verwenden Sie Überwachungsthemen in Vulnerability Manager Workspace.

Korrekturaufgaben (AVULs) werden aus AVITs erstellt und basierend auf Ihren Zuweisungsregeln automatisch Gruppen zur Korrektur zugewiesen. Weitere Informationen zum Erstellen dieser Regeln finden Sie unter den folgenden Themen:

- Erstellen oder bearbeiten Sie Vulnerability Response Zuweisungsregeln
- Erstellen oder bearbeiten Sie Vulnerability Response Regeln für Korrekturaufgabenund Erstellen Sie im Arbeitsbereich von Vulnerability Manager eine Korrekturmaßnahme.

### Upload-Status für Software Bill of Materials Dateien wird angezeigt

Überprüfen Sie den Upload-Status für die Software-Stücklistendateien (SBOM), die Sie im Modul „Stücklisten-Warteschlange“ im Arbeitsbereich Software Bill of Materials (SBOM) hochgeladen haben. Verfolgen Sie die Dateien, die Sie erfolgreich hochgeladen haben, Ihren Upload-Verlauf und Fehler nach.

Erforderliche Rolle:

- Ab Version 2.1 von SBOM Core – sn_sbom_resp.sbom_analyst
- Vor v2.1 von SBOM Core – sn_sbom_resp.admin

1. Zeigen Sie Ihren Upload-Status an.

   Die Methode, mit der Sie Ihren Upload-Status anzeigen, hängt von den installierten Anwendungen ab.

   Die Statusinformationen in der Stücklistentabelle [sn_sbom_doc_list] und im Stücklisten-Warteschlangenmodul enthalten beide Stücklistenformate, den Erfassungsstatus und die Stücklisten-Generierungszeit. Die Statusspalte für die Stücklistenerfassung enthält die folgenden Status:

   - In der Warteschlange – SBOM Daten wurden hochgeladen.
   - Wird verarbeitet – Die Komponentendaten werden als Teil des Imports verarbeitet.
   - Verarbeitet – Datenerfassung wurde erfolgreich abgeschlossen.
   - Fehler: Während der Verarbeitung ist ein Fehler aufgetreten.

   Zusätzlich zum Status Ihrer hochgeladenen Dateien können Sie Listen der von Ihnen erfassten Komponenten anzeigen, indem Sie einen Stücklisten-Entitätsdatensatz auswählen.

2. Greifen Sie auf weitere Informationen zu Fehlern und Upload-Status zu, indem Sie das Zahnradsymbol und das ⚙ auswählen und Felder wie **Fehlerkategorie** und **Fehlerdetail**hinzufügen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

### Eine Software Bill of Materials -Entität wird auf Schwachstellen überprüft

Bestimmen Sie, ob den Komponenten in einer hochgeladenen Datei Software Bill of Materials (SBOM) Schwachstellen zugeordnet sind.

Die folgenden Anwendungen müssen installiert und aktiviert sein, bevor Sie die Schwachstellen und erweiterten Schwachstellendaten anzeigen können:

- SBOM Antwort
- Integration von Vulnerability Response mit NVD- und CWE-Jobs
- Vulnerability Response

Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle:

- Ab Version 2.1 von SBOM Core – sn_sbom_resp.sbom_analyst
- Vor v2.1 von SBOM Core – sn_sbom_resp.admin

1. Navigieren zu **Alle** > **SBOM-Arbeitsbereich** > **Komponenten**.
2. Vor Version 3.1 von SBOM Response können Sie Schwachstelleninformationen entweder über eine Visualisierung oder einen Komponentendatensatz anzeigen.

### Bewerten Sie Ihr Risiko mit Vulnerability Intelligence

Ab Version 3.1 von SBOM Response können Sie mit SBOM Response weitere erweiterte Schwachstellendaten für Komponentendatensätze anzeigen. Die unter Unterstützte Anwendungen beschriebenen geplanten Aufgaben SBOM Response, Vulnerability Response, National Vulnerability Database (NVD) Integration und Common Weakness Enumeration (CWE) müssen installiert und aktiviert sein.

1. Wählen Sie das Diagramm **Alle Komponenten** aus, um die Liste der zugehörigen Datensätze anzuzeigen.
2. Wählen Sie einen Link in der Spalte **Name** aus, um einen Datensatz zu öffnen.

   Die Status, **Veraltet**, **Verworfen**und **Angreifbar** werden unter dem Komponentennamen angezeigt. Eine Komponente kann eine beliebige Kombination dieser Status haben. Wenn kein Status angezeigt wird, ist die Komponente nicht veraltet, aufgegeben oder angreifbar.

   Überprüfen Sie die aktuelle Version und die letzte veröffentlichte Version. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben, und ihre Position in der Liste kann Ihnen Einblicke geben, warum eine Komponente **Veraltet**, **Verworfen**und **Angreifbar**ist. Beispielsweise verwenden Sie möglicherweise eine ältere Version einer Komponente.

3. Wählen Sie im Datensatz die zugehörigen Registerkarten **Übersicht**, **Hashes**, **Stücklistenentitäten**, **Schwachstellen**und **AVIs** aus.
   - Übersicht: Eine Zusammenfassung der Komponentendetails.
   - Stücklistenentitäten: Eine Liste der Entitäten, die dieser Komponente zugeordnet sind.
   - Hashes: Wenn importiert, werden Hashes angezeigt.
   - Schwachstellen: Informationen zu bekannten Schwachstellen, die dieser Komponente zugeordnet sind. Wenn diese Liste leer ist, sind keine Schwachstellen bekannt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Liste ausgefüllt ist, wählen Sie die Registerkarte aus, um Schwachstellen-IDs, Zusammenfassungen und andere Schwachstelleninformationen für Common Vulnerabilities and Exposures (CVE) und Common Weakness Enumeration (CWE)-Daten anzuzeigen, die mit diesem Datensatz verknüpft sind. CVEs werden nach Schweregrad aufgeschlüsselt, CWEs werden danach aufgeschlüsselt, wie wahrscheinlich die Komponente ausgenutzt werden kann. Sie können die erweiterten Schwachstellendatensätze in den Anwendungen Vulnerability Response oder Application Vulnerability Response anzeigen, indem Sie auf den Link der Schwachstellen-ID klicken.

- AVIs (AVITs): Angreifbare Anwendungselemente, die dieser Komponente zugeordnet sind, wenn Sie AVIT-Erstellungsregeln erstellt haben, die die Komponente einer bekannten Schwachstelle zuordnen. Die Anwendung Application Vulnerability Response (AVR) verknüpft eine Schwachstelle mit einer Anwendung, um einen AVI-Datensatz zu erstellen. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente im Software Bill of Materials -Arbeitsbereich.

## Mit den Anwendungen Software Bill of Materials installierte Komponenten

Bei der Aktivierung der Software Bill of Materials -Anwendungen werden verschiedene Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und geplante Aufgaben.

### Installierte Rollen

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| SBOM schreiben [sn_sbom_dm.app_write], SBOM erstellen [sn_sbom_dm.app_create], SBOM lesen [sbom_dm.app_read] | Diese Rollen werden mit der Anwendung „Data Model for SBOM “ installiert.<br><br>Sie ermöglichen das Lesen, Erstellen und Bearbeiten von Datensätzen in Tabellen SBOM. | Keine |
| SBOM ] Core-Erfassungen [sn_sbom_core.sbom_ingest] und SBOM Core-Administrator [sn_sbom_core.admin] | Diese Rollen werden mit der Anwendung SBOM Core installiert.<br><br>Mit der Rolle „sn_sbom_core.sbom_ingest“ können Sie SBOMs manuell und über die REST-API hochladen. Mit der Rolle „sn_sbom_core.admin“ können Sie Daten erstellen, lesen, bearbeiten und SBOMs hochladen.<br><br>Mit dieser Rolle haben Sie auch Zugriff auf die SBOM Core-Module in Ihrer Instanz. Sie erbt die Rollen | • sn_sbom_dm.app_write<br>• sn_sbom_dm.app_create<br>• sn_ sbom_dm.app_read |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Rollentitel [Name] | Beschreibung | Enthält Rollen |
|---|---|---|
| | von der Anwendung Data Model for SBOM. | |
| SBOM-Analyst<br><br>[sn_sbom_resp.sbom_analyst] | Diese Rolle wird mit der Anwendung SBOM Response installiert.<br><br>Sie erbt die Rolle sn_sbom_core.admin und ermöglicht Ihnen den Zugriff auf den Arbeitsbereich SBOM. | • sn_sbom_core.admin<br>• sn_sbom_dm.app_write<br>• sn_sbom_dm.app_create<br>• sn_ sbom_dm.app_read<br>• sn_sbom_resp.manage_avi_rule<br>• Tabelle sn_sbom_config_rule |

## Mit den -Anwendungen SBOM installierte Tabellen

Die in der folgenden Tabelle aufgeführten Tabellen werden mit der Anwendung Data model for SBOM installiert.

### Datenmodell für SBOM -Tabellen

| Tabelle | Beschreibung |
|---|---|
| SBOM Dokument<br><br>[sn_sbom_doc] | Enthält die von Ihnen hochgeladenen Stücklistenentitäten |
| SBOM Komponente<br><br>[sn_sbom_component] | Enthält importierte SBOM Komponenten, Klassifizierer und Versionen, die in der übergeordneten Komponente enthalten sind. |
| SBOM Komponentenbeziehung<br><br>[sn_sbom_comp_relationship] | Enthält Komponenten und ihre Abhängigkeiten. |
| SBOM m2m-Stücklistenkomponente<br><br>[sn_sbom_m2m_bom_comp] | Enthält die Stücklistenkomponentenzuordnungen |
| SBOM-Lizenz<br><br>[sn_sbom_license] | Enthält die Open Source-Lizenz-IDs, die für -Komponenten verwendet werden |
| SBOM Lieferant<br><br>[sn_sbom_supplier] | Enthält die Organisation, die die Komponente bereitgestellt hat, z. B. Hersteller, Händler oder Repacker. |
| SBOM Komponenten-ID | Enthält die Komponentenbezeichner. |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**Datenmodell für SBOM -Tabellen (Fortsetzung)**

| Tabelle | Beschreibung |
|---|---|
| [sn_sbom_comp_id] | |
| SBOM Komponenteneigenschaften [sn_sbom_comp_property] | Enthält die Name-Wert-Eigenschaften der Komponente. |
| SBOM Hash [sn_sbom_hash] | Enthält Komponenten-Hashing-Algorithmen. |
| SBOM Kontakt [sn_sbom_contact] | Enthält Kontaktinformationen für den Lieferanten. |
| SBOM externe Referenzen [sn_sbom_comp_external_ref] | Enthält Komponenten, Komponententypen und externe URLs, die Systeme, Sites und Informationen dokumentieren, die relevant sein könnten, aber nicht in SBOMenthalten sind. |
| SBOM Paketgruppe [sn_sbom_pkg_group] | Enthält die Paketgruppeninformationen für jede Komponente. Mehrere Versionen von Bibliotheken können in Anwendungen verwendet werden. Versionen derselben Komponenten werden gruppiert und dieser Tabelle hinzugefügt, um zu vermeiden, dass dieselben Daten mehrmals abgerufen werden. |

Die in der folgenden Tabelle aufgeführten Tabellen werden mit der Anwendung SBOM Response installiert

**SBOM Antworttabellen**

| Tabelle | Beschreibung |
|---|---|
| SBOM Konfiguration der Erstellungsregel [sn_sbom_config_rule] | Enthält AVIT-Erstellungsregeln, die im Arbeitsbereich SBOM verwendet werden. |
| SBOM m2m-Komponentenschwachstellen [sn_sbom_m2m_comp_vuln] | Enthält die Komponenten und zugehörigen Schwachstellen |
| Informationen zur Korrektur von Komponentenschwachstelle [sn_sbom_comp_vuln_fix_info] | Enthält die Korrekturversionen für jede Schwachstelle einer Drittpartei, die einer Version der Komponente zugeordnet ist. |
| Komponentenberichtseinblicke [sn_sbom_comp_report_insight] | Enthält Einblicke in veraltete, verworfene und Reparierbarkeitsdaten für -Komponenten |



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

**SBOM Antworttabellen (Fortsetzung)**

| Tabelle | Beschreibung |
|---|---|
| Deps-Integrationsimporte<br><br>[sn_sbom_deps_integration_import] | Enthält importierte Versionslisteninformationen für ein bestimmtes Paket oder eine bestimmte Bibliothek. |
| OSV-Integrationsimporte<br><br>[sn_sbom_osv_integration_import] | Enthält Vulnerability Intelligence-Informationen für eine bestimmte Version eines Pakets oder einer Bibliothek. |
| Komponentenversionslisten<br><br>[sn_sbom_st_version_list] | Enthält Versionsinformationen und Veröffentlichungsdaten für Komponenten. |

## Geplante Aufgaben

| Auftrag | Beschreibung |
|---|---|
| Berechnet die Reparierbarkeit und Schwachstelle von Komponenten | Berechnet Informationen darüber, wie Komponenten mit Schwachstellen repariert werden können und wie wahrscheinlich es ist, dass Komponenten repariert werden können. |
| OSV-Integration – Neue Komponenten | Ruft alle öffentlich bekannten Schwachstellen ab, die Paketen (Bibliotheken) zugeordnet sind, die nach der letzten Integrationsausführung importiert wurden. |
| OSV Integration Comprehensive | Ruft alle öffentlich bekannten Schwachstellen ab, die allen importierten Paketen zugeordnet sind. |
| Deps.dev-Integration | Ruft alle öffentlich bekannten Versionen für Pakete ab, die mit verwendet werden, um Komponenten im Status „ **Veraltet“** und „ **Verworfen** “ zu identifizieren. |
| Aktualisieren Sie „vuln_based_criticality“ für Stücklistenkomponenten | Aktualisiert die Relevanz für Komponenten mit Schwachstellen. |

### Erstellen Sie im Software Bill of Materials -Arbeitsbereich eine Regel für angreifbare Anwendungselemente

Richten Sie die Bedingungen ein, unter denen angreifbare Elemente in Anwendungen (AVITs) automatisch im Modul „AVI-Erstellungsregeln“ im Arbeitsbereich Software Bill of Materials (SBOM) erstellt werden.

#### Vorbereitungen

Die Anwendung SBOM Response ist erforderlich, wenn Sie angreifbare Anwendungselemente erstellen möchten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle: sn_sbom_resp.manage_avi_rule.

#### Prozedur

1. Navigieren zu **SBOM-Arbeitsbereich** > **AVI-Erstellungsregeln**.
2. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.


Automatische Übersetzung

**3.** Füllen Sie die Felder aus.

| Feld | Beschreibung |
|---|---|
| Name | Name der Regel. |
| Aktiv | Gibt an, ob die Erstellungsregel aktiviert ist. |
| Ausführungsbefehl | Reihenfolge, in der die Regeln ausgewertet werden. Die Regel mit dem niedrigsten numerischen Wert wird zuerst ausgeführt.<br><br>Sie können beispielsweise Regeln mit höherer Priorität für Elemente erstellen, die eine spezielle Behandlung erfordern, oder für Elemente, bei denen das Risiko kritisch ist, sodass sie zuerst ausgeführt werden. Erstellen Sie als Nächstes allgemeine Regeln für Elemente, die keine spezielle Behandlung erfordern. Erstellen Sie abschließend eine Standardregel, um alle Komponenten zu erfassen, die Schwachstellen aufweisen. |
| Beschreibung | Beschreibung der Regel, damit Sie sie von anderen Regeln unterscheiden können. |
| Regeln | Erstellen Sie die Bedingungen, unter denen angreifbare Elemente in Anwendungen (AVIs) erstellt werden.<br><br>Sie können beispielsweise **[Schwachstelle > Schweregrad][ist][1-Kritisch]** auswählen, um AVITs für Komponenten zu erstellen, die Schwachstellen aufweisen, die ein hohes Risiko darstellen und schwerwiegende Auswirkungen auf Sie haben könnten.<br><br>Beachten Sie, dass Sie weitere Bedingungen hinzufügen können. |

**4.** Wählen Sie **Speichern**.
Ihre Erstellungsregel wird nach dem nächsten Upload automatisch ausgeführt und erstellt AVIs für Komponenten, die Ihren Bedingungen entsprechen. Sie können die Regel auch bei Bedarf über das Modul „AVI-Erstellungsregeln“ ausführen, indem Sie **Jetzt**ausführen auswählen.

### Ergebnisse

Nachdem sie erstellt wurden, können Sie überprüfen, ob eine AVIT speziell für SBOM Daten erstellt wurde, indem Sie die Werte in den Feldern **Quelle** und **Scan-Typ** in einem AVI-Datensatz überprüfen.

| Feld | Wert |
|---|---|
| Quelle | SBOM |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

| Feld | Wert |
| --- | --- |
| Überprüfungstyp | SBOM-SCA |

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.